



Intellitactics Security Manager v5.7

Report List

Table of Contents

Controls.....	6
Access Control.....	6
Account Management.....	6
Least Privilege.....	7
Monitor Login Activity.....	7
Network Access Control.....	8
Remote Access Control.....	8
Session Control.....	9
Use of Non-Repudiation.....	9
Wireless Access Control.....	9
Business Continuity.....	9
Alternate Communications, Systems and Storage.....	9
Software and Data Backup.....	10
Certification - Accreditation - Compliance.....	10
Continuous Monitoring of Controls.....	10
Communications and System Protection.....	11
Acceptable Use of Systems and Services.....	11
Mobile Code Protection.....	11
Use of Cryptography.....	12
Voice over IP Security.....	12
Incident Response Management.....	12
Incident Handling.....	12
Incident Reporting.....	12
Operations Management.....	13
Asset Management.....	13
Capacity Management.....	13
Monitoring Audit Logs.....	14
Monitoring Configuration Activity.....	14
Monitoring System Faults.....	14
Monitoring Use of Privileges.....	15
Physical and Environmental Security.....	15
Physical Access Control.....	15
Risk Assessment.....	15
Assessment of Risk.....	15
Vulnerability Assessment.....	16
System Acquisition - Development - Maintenance.....	17
Use of System Maintenance Tools.....	17
System and Data Integrity.....	17
Data Integrity Monitoring.....	17
Electronic Messaging Security.....	18
Intrusion Detection and Protection.....	18
Malicious Code Protection.....	18

Compliance	19
FISMA Reports	19
Access Control	19
Audit and Accountability	22
Certification, Accreditation, and Security Assessments.....	22
Configuration Management.....	23
Contingency Planning.....	25
Identification and Authentication	25
Incident Response	25
Maintenance	26
Risk Assessment	26
System and Communications Protection	27
System and Information Integrity.....	29
GLB Reports.....	32
Access Control.....	32
Business Continuity	35
Certification - Accreditation - Compliance	36
Communications and System Protection	37
Incident Response Management.....	38
Operations Management.....	39
Physical and Environmental Security.....	41
Risk Assessment	41
System Acquisition - Development - Maintenance	43
System and Data Integrity.....	43
HIPAA Reports	45
Access Control.....	45
Business Continuity	48
Certification - Accreditation - Compliance	49
Communications and System Protection	50
Incident Response Management.....	51
Operations Management.....	52
Physical and Environmental Security.....	54
Risk Assessment	54
System Acquisition - Development - Maintenance	56
System and Data Integrity.....	56
PCI Reports	58
1. Install and Maintain a Firewall Configuration	58
2. Secure Default Configuration	58
3. Protect Stored Cardholder Data.....	59
4. Encrypt Sensitive Data	59
5. Anti-Virus Measures.....	60
6. Develop and Maintain Secure Systems	60
7. Restrict Access to Cardholder Data	61
8. User Authentication	62
9. Physical Security	63
10. Monitor Network Access	64

11. Test Security Systems and Processes.....	65
12. Maintain a Security Policy	66
Sarbanes-Oxley Reports.....	67
Access Control.....	68
Business Continuity	71
Certification - Accreditation - Compliance	72
Communications and System Protection.....	72
Incident Response Management.....	73
Operations Management.....	74
Physical and Environmental Security.....	77
Risk Assessment	77
System Acquisition - Development - Maintenance	78
System and Data Integrity.....	79
Event Management.....	80
Event Search.....	81
Event Summaries	81
AAA Reports	82
AV Reports	83
Application Reports	85
DB Reports	86
Firewall Reports.....	87
Host IDS Reports	89
IPS Reports.....	90
Network IDS Reports	91
OS Reports.....	92
Account Management.....	94
Proxy Reports.....	94
Router Reports.....	95
Switch Reports	96
Web Service Reports.....	98
Alert Management	99
By Device Type.....	99
Incident Management.....	101
Operations Activity and Status.....	101
Security Environment.....	102
Assets and Zones	102
Vulnerabilities	102
Intellitactics Security Manager.....	103
Administration	103
User Activity	104
Health Monitoring	104
System Statistics	104

Log Management 104
Event Management 105

Controls

Reports supporting specific security controls.

Access Control

Metacontrols which serve to limit and monitor the activities of users.

Account Management

The organization manages all aspects of user account management including additions, deletions, modifications, lockouts, suspensions, activations and privilege changes.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.
Windows Account Creations Template ID: report_impl_xml-164	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes Template ID: report_impl_xml-165	This report shows the deletion of Windows accounts, audited by Windows event 630,

	sorted from the most recent to the oldest.
Windows Account Disables Template ID: report_impl_xml-166	This report shows the disabling of Windows accounts, audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables Template ID: report_impl_xml-167	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to the oldest.
Windows Account Unlocked Template ID: report_impl_xml-170	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most recent to the oldest.

Least Privilege

The organization should ensure that users are provided with the most minimal set of privileges required to carry out their designated duties in order to minimize the risk to organizational assets and business objectives. This mechanism shall include periodic reviews of privilege to identify users with excess privileges.

Group Changes Template ID: report_impl_xml-8	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
Security Manager Group Management Template ID: report_impl_xml-188	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.

Monitor Login Activity

The organization should monitor all login activities to critical systems to ensure that data confidentiality and data integrity policies are followed.

Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Windows Account Lockouts Template ID: report_impl_xml-168	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.

Windows Failed Logins Template ID: report_impl_xml-169	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.
---	---

Network Access Control

Access to assets and their connected assets should be restricted to only those assets and accounts with a need to access network services and network protocols in order to further a business process or goal.

Top Firewall Denied Sources Template ID: intellitactics-top_fw_denied_sources	This report shows the most frequently blocked source addresses.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.

Remote Access Control

Organizations should have an authorization and approval process in place to control the granting of remote access to ensure that only the privileges required for carrying out assigned tasks and are provided via remote access. Additionally All remote access should be regularly monitored to ensure conformity with remote access policies.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
VPN Account Login Summary Template ID: intellitactics-vpn_account_login_summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity Template ID: report_impl_xml-17	This report shows denied attempts to log into VPN services.
VPN Login Activity Template ID: report_impl_xml-69	This report shows VPN login activity of a given user for a specified time period.

Session Control

Information processing systems should be configured to automatically require re-authentication after a configurable period of time or inactivity.

Session Expiry for Privileged Account Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Use of Non-Repudiation

The organization should employ non-repudiation methods for critical systems in order to irrevocably assign responsibility for system actions to a given individual or account.

Non-Repudiation Exception Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Wireless Access Control

The use of wireless technologies used to connect to information processing systems should be monitored closely to account for the additional risks as compared to other access control technical methods. Strong methods of authentication including physical access control, encryption, and multiple factor authentication.

Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.
WiFi Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.

Business Continuity

Metacontrols which ensure that business continues in the face of unplanned events.

Alternate Communications, Systems and Storage

The organization should provide alternate or redundant communications, systems and storage for information systems that are deemed vital to its continuity. These systems should be identified as part of a business continuity risk assessment.

Assets Unavailable Template ID: report_impl_xml-24	This report shows all events for a specified time period, where an asset has been shut down, restarted,
---	---

	or has encountered an error condition that has caused it to become unavailable.
Failover/HA Events Template ID: report_impl_xml-22	This report shows all events related to failover and high availability activities, including errors and other activities reported by devices, for a specified time period. This expands the scope of entries returned above the 'All Failover/HA Occurrences' report. These events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.
Failover/HA Occurrences Template ID: report_impl_xml-23	This report shows all failover and high availability events noted by Security Manager for a specified time period. Such events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.

Software and Data Backup

Organizations must maintain recent and complete backup copies of software and data required for business continuity. These back-ups will be periodically validated to ensure they can be used to restore information processing systems to a current (data) and working (software) state.

Backup Service Activity Template ID: report_impl_xml-25	This report shows all activity related to backup services for a specified time period.
Security Manager SDW Backup Template ID: report_impl_xml-191	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.

Certification - Accreditation - Compliance

Metacontrols ensuring compliance with regulations and fulfillment of the requirements of relevant certifications and accreditations.

Continuous Monitoring of Controls

Organizations must continuously monitor controls to ensure adequate control coverage and acceptable control performance.

Registered Control Alerts	This report shows the registered control alerts for a
---------------------------	---

Template ID: report_impl_xml-184	specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.
Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.

Communications and System Protection

Metacontrols ensuring the protection of communication channels and the systems that use them.

Acceptable Use of Systems and Services

Organizations should have clear policies procedures regarding acceptable usage of systems & services. Monitoring should be performed to ensure that violations are detected and remediated.

Abuse by Account Template ID: report_impl_xml-27	This report shows all abuse-related events against the entered account for a specified time period.
Abuse by Asset Template ID: report_impl_xml-26	This report shows all abuse-related events for an entered source asset IP address over a specified time period. If a source asset IP address is not entered, results are grouped by the source asset IP address, regardless of whether or not it is a registered asset.
Top Web Referrals with Suspicious Responses Template ID: intellitactics-top_web_referrals_with_suspicious_responses	This report lists the URLs of pages referring to pages which, when requested, produce unusual HTTP response codes (307, 400, 401, 402, 405, 406, 408, 409, 410 through 419 and all 500 series).

Mobile Code Protection

Organizations should create and enforce a policy on the proper use of mobile code in their information systems and networks.

Blocked Active Content to Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
--	---

Use of Cryptography

The organization should employ cryptographic techniques to aid in lowering risks to information processing systems and assets of disclosure and alteration.

VPN Errors Template ID: intellitactics-vpn_errors	This report shows all VPN errors reported for a specified time period.
--	--

Voice over IP Security

Organizations should control the use of VOIP technology to ensure that availability of communications infrastructure is not impacted and to ensure that communications to and from the organization are always visible.

VOIP Service Activity Template ID: report_impl_xml-29	This report shows all activity related to VOIP services for a specified time period.
--	--

Incident Response Management

Metacontrols ensuring that incidents are resolved in a thorough, timely and cost effective manner.

Incident Handling

The organization should follow preestablished policies and procedures to prepare for, detect, analyze, contain, eliminate and recover from security incidents.

All Incidents Template ID: report_impl_xml-74	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Status Template ID: report_impl_xml-75	This report shows all incidents at each status for a specified time period.
Incidents by Close Date Template ID: report_impl_xml-77	This report shows the incidents closed for a specified time period.
Incidents by Create Date Template ID: report_impl_xml-76	This report shows the incidents created for a specified time period.
Open Incidents Template ID: report_impl_xml-73	This report shows all open incidents sorted from oldest to most recent for a specified time period.

Incident Reporting

The organization should ensure that all necessary stakeholders are informed of incidents and that incidents are escalated as required by their risks. Escalation and notification processes should be well defined and automated whenever possible.

Incident Summary by Closing User Template ID: report_impl_xml-80	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: report_impl_xml-79	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: report_impl_xml-78	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

Operations Management

Metacontrols which ensure that the organization's operations are carried out in a secure fashion.

Asset Management

Organizations should classify information system assets by defining security categories that are based on established risk levels. This security categorization should be based on a risk assessment that takes into account the asset's value and the costs associated with the potential loss to the organization should controls fail to protect the asset.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

Capacity Management

Resource allocation and usage should be monitored, reviewed and adjusted with a view to forecasted future capacity requirements. Systems should be optimized for efficiency and increased capacity.

Average Count of Events per Day Template ID: report_impl_xml-162	This report shows the average number of events per day over a given period of time.
Average Count of Managed Events per Day Template ID: report_impl_xml-162-event	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.

Count of Events by Day Template ID: report_impl_xml-161	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.
Count of Managed Events by Day Template ID: report_impl_xml-161-event	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

Monitoring Audit Logs

Organizations should continuously monitor all audit logs to ensure that both information systems and the privileges provided to users on those systems are consistent with normal business usage.

Acquired Devices Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Unparsed Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.
Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.

Monitoring Configuration Activity

Organizations should continuously monitor all configuration changes to information processing systems. This process includes verifying that users are authorized to make changes to an asset and the changes made are consistent with established policies and practices for that asset.

Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

Monitoring System Faults

System errors and faults should be monitored to identify assets that require intervention to maintain acceptable integrity and availability.

Critical Asset Error Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Hosts with Errors Summary Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

Monitoring Use of Privileges

The organizations should monitor the activities of administrative users and the use of administrative privileges and utilities to ensure usage consistent with business policies and business needs.

SU/SUDO Use Template ID: report_impl_xml-45	This report shows all use of SU and SUDO tools for a specified time period.
--	---

Physical and Environmental Security

Metacontrols which ensure that the physical information technology environment is secure.

Physical Access Control

Organization should protect all means of gaining physical entry to it's facilities adequately by employing detective and preventive measures such keypad locks, electronic card readers, guards and cameras.

Physical Access Denied Template ID: report_impl_xml-46	This report shows all denied attempts to access secured areas/rooms for a specified time period.
---	--

Risk Assessment

Metacontrols which ensure that the organization measures risks to make informed security decisions.

Assessment of Risk

Organizations must periodically employ risk assessment mechanisms that take into account factors such as: threats, vulnerabilities, assets, operational risk and business

priorities. This ensures that all decisions regarding policies, controls and incidents are made with a full understanding of the potential cost or benefit to the organization.

High Risk Alerts Template ID: report_impl_xml-47	This report shows high risk alerts for a specified time period.
High Risk Alerts Involving Accounts Template ID: report_impl_xml-49	This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a specified time period.
High Risk Alerts on Critical Assets Template ID: report_impl_xml-48	This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater than or equal to the entered value for a specified time period.

Vulnerability Assessment

The organization should maintain continuous awareness of newly discovered technical vulnerabilities that affect its information systems and rapidly assess and mitigate the risks as appropriate.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1

	to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
<p>Most Vulnerable Zones</p> <p>Template ID: report_impl_xml-55</p>	<p>This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.</p>

System Acquisition - Development - Maintenance

Metacontrols ensuring that systems are acquired, developed and maintained to meet defined requirements and do so in a secure way.

Use of System Maintenance Tools

Organizations should monitor the tools and utilities used for system maintenance to ensure they are not used to circumvent privileges levels and restrictions.

<p>New Executable Loaded on Critical Asset Alerts</p> <p>Template ID: intellitactics-alerts_by_registration_id</p>	<p>This report shows alerts of the given type for a specified time period.</p>
--	--

System and Data Integrity

Metacontrols to ensure that system and information changes are made in a planned, controlled and audited manner.

Data Integrity Monitoring

The organization should monitor information systems for changes to system software, applications & application data to detect unauthorized or irregular changes to data that could put the organization at risk with its customers, employees and partners.

<p>Database Schema Changes</p> <p>Template ID: report_impl_xml-56</p>	<p>This report shows all events where a database schema change has occurred, for a specified time period. Compare these results to organizational change requests to identify unauthorized changes. This report is also useful when troubleshooting database driven application errors.</p>
<p>Monitored File Changes on Critical Asset Alerts</p>	<p>This report shows alerts of the given type for a specified time period.</p>

Template ID: [intellitactics-alerts_by_registration_id](#)

Electronic Messaging Security

The organization should monitor the security of all electronic messaging platforms to ensure the confidentiality, integrity and availability of all messages originating from or destined to the organization and its stakeholders.

Authentication to Email Failures Template ID: report_impl_xml-58	This report shows events where an account has failed to authenticate to electronic messaging services (Email only).
Blocked Electronic Messages Template ID: report_impl_xml-59	This report shows events that specify that an electronic message was not delivered. The reasons for message delivery failure will be indicated in the result set and will be attributed to one of the following conditions: 1. A firewall blocked the message from delivery due to a policy employed on the firewall. 2. Antivirus software interfered with message delivery. 3. A message was redirected to another delivery point (such as spam). 4. A message was partially modified by content filters (such as spam and antivirus prior to being delivered).

Intrusion Detection and Protection

The organization should employ technologies and procedures monitor and protect all information systems from unwanted or unauthorized access attempts.

IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

Malicious Code Protection

The organization should take adequate measures to protect it's IT infrastructure against malicious code such as viruses, worms and trojans by employing protective technologies on its networks and information systems.

Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as the 'Types/Host' column.
Top Malware Types Template ID: intellitactics-top_malware_types	This report shows the most frequently observed malware types.

Compliance

Compliance Reports

FISMA Reports

Reports supporting compliance with the Federal Information Security Management Act (FISMA) and the NIST Special Publication 800-53.

Access Control

AC-2 - Account Management

Reports supporting NIST 800-53 control number AC-2.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period.

	This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.
Windows Account Creations Template ID: report_impl_xml-164	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes Template ID: report_impl_xml-165	This report shows the deletion of Windows accounts, audited by Windows event 630, sorted from the most recent to the oldest.
Windows Account Disables Template ID: report_impl_xml-166	This report shows the disabling of Windows accounts, audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables Template ID: report_impl_xml-167	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to the oldest.
Windows Account Unlocked Template ID: report_impl_xml-170	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most recent to the oldest.

AC-6 - Least Privilege

Reports supporting NIST 800-53 control number AC-6.

Group Changes Template ID: report_impl_xml-8	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
Security Manager Group Management Template ID: report_impl_xml-188	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.

AC-7 - Unsuccessful Login Attempts

Reports supporting NIST 800-53 control number AC-7.

Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
--	--

Windows Account Lockouts Template ID: report_impl_xml-168	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.
Windows Failed Logins Template ID: report_impl_xml-169	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.

AC-12 - Session Termination

Reports supporting NIST 800-53 control number AC-12.

Session Expiry for Privileged Account Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

AC-13 - Supervision and Review

Reports supporting NIST 800-53 control number AC-13.

Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.
Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.

AC-17 - Remote Access

Reports supporting NIST 800-53 control number AC-17.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
VPN Account Login Summary Template ID: intellitactics-vpn_account_login_summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity Template ID: report_impl_xml-17	This report shows denied attempts to log into VPN services.
VPN Login Activity	This report shows VPN login activity of a given user for a

Template ID: report_impl_xml-69	specified time period.
---------------------------------	------------------------

AC-18 - Wireless Access Restrictions

Reports supporting NIST 800-53 control number AC-18.

Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.
WIFI Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.

Audit and Accountability

AU-10 - Non-Repudiation

Reports supporting NIST 800-53 control number AU-10.

Non-Repudiation Exception Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Certification, Accreditation, and Security Assessments

CA-2 - Security Assessments

Reports supporting NIST 800-53 control number CA-2.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.
Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.

CA-3 - Information System Connections

Reports supporting NIST 800-53 control number CA-3.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Firewall Denied Sources Template ID: intellitactics-top_fw_denied_sources	This report shows the most frequently blocked source addresses.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.

CA-7 - Continuous Monitoring

Reports supporting NIST 800-53 control number CA-7.

Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.
Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.

Configuration Management

CM-2 - Baseline Configuration

Reports supporting NIST 800-53 control number CM-2.

Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

CM-4 - Monitoring Configuration Changes

Reports supporting NIST 800-53 control number CM-4.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

CM-6 - Configuration Settings

Reports supporting NIST 800-53 control number CM-6.

Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

CM-7 - Least Functionality

Reports supporting NIST 800-53 control number CM-7.

Abuse by Account Template ID: report_impl_xml-27	This report shows all abuse-related events against the entered account for a specified time period.
Abuse by Asset Template ID: report_impl_xml-26	This report shows all abuse-related events for an entered source asset IP address over a specified time period. If a source asset IP address is not entered, results are grouped by the source asset IP address, regardless of whether or not

	it is a registered asset.
Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
New Executable Loaded on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

Contingency Planning

CP-9 - Information System Backup

Reports supporting NIST 800-53 control number CP-9.

Backup Service Activity Template ID: report_impl_xml-25	This report shows all activity related to backup services for a specified time period.
Security Manager SDW Backup Template ID: report_impl_xml-191	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.

Identification and Authentication

IA-7 - Cryptographic Module Authentication

Reports supporting NIST 800-53 control number IA-7.

VPN Errors Template ID: intellitactics-vpn_errors	This report shows all VPN errors reported for a specified time period.
--	--

Incident Response

IR-4 - Incident Handling

Reports supporting NIST 800-53 control number IR-4.

All Incidents Template ID: report_impl_xml-74	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Status Template ID: report_impl_xml-75	This report shows all incidents at each status for a specified time period.
Incidents by Close Date Template ID: report_impl_xml-77	This report shows the incidents closed for a specified time period.
Incidents by Create Date	This report shows the incidents created for a specified time

Template ID: report_impl_xml-76	period.
Open Incidents Template ID: report_impl_xml-73	This report shows all open incidents sorted from oldest to most recent for a specified time period.

IR-6 - Incident Reporting

Reports supporting NIST 800-53 control number IR-6.

Incident Summary by Closing User Template ID: report_impl_xml-80	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: report_impl_xml-79	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: report_impl_xml-78	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

Maintenance

MA-3 - Maintenance Tools

Reports supporting NIST 800-53 control number MA-3.

New Executable Loaded on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
SU/SUDO Use Template ID: report_impl_xml-45	This report shows all use of SU and SUDO tools for a specified time period.

Risk Assessment

RA-3 - Risk Assessment

Reports supporting NIST 800-53 control number RA-3.

High Risk Alerts Template ID: report_impl_xml-47	This report shows high risk alerts for a specified time period.
High Risk Alerts Involving Accounts Template ID: report_impl_xml-49	This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a specified time period.
High Risk Alerts on Critical Assets Template ID: report_impl_xml-48	This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater

	than or equal to the entered value for a specified time period.
--	---

RA-5 - Vulnerability Scanning

Reports supporting NIST 800-53 control number RA-5.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones Template ID: report_impl_xml-55	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

System and Communications Protection

SC-6 - Resource Priority

Reports supporting NIST 800-53 control number SC-6.

Average Count of Events per Day Template ID: report_impl_xml-162	This report shows the average number of events per day over a given period of time.
Average Count of Managed Events per Day Template ID: report_impl_xml-162-event	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.
Count of Events by Day Template ID: report_impl_xml-161	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.
Count of Managed Events by Day Template ID: report_impl_xml-161-event	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

SC-7 - Boundary Protection

Reports supporting NIST 800-53 control number SC-7.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Firewall Denied Sources Template ID: intellitactics-top_fw_denied_sources	This report shows the most frequently blocked source addresses.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.

Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.

SC-13 - Use of Validated Cryptography

Reports supporting NIST 800-53 control number SC-13.

VPN Errors Template ID: intellitactics-vpn_errors	This report shows all VPN errors reported for a specified time period.
--	--

SC-15 - Collaborative Computing

Reports supporting NIST 800-53 control number SC-15.

VOIP Service Activity Template ID: report_impl_xml-29	This report shows all activity related to VOIP services for a specified time period.
--	--

SC-19 - Voice Over Internet Protocol

Reports supporting NIST 800-53 control number SC-19.

VOIP Service Activity Template ID: report_impl_xml-29	This report shows all activity related to VOIP services for a specified time period.
--	--

System and Information Integrity

SI-3 - Malicious Code Protection

Reports supporting NIST 800-53 control number SI-3.

Blocked Active Content to Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Hosts with Most Malware Types Template ID: intellitactics-	This report shows which hosts are exposed to the widest variety of malware types.

hosts_with_most_malware_types	
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as the 'Types/Host' column.
Top Malware Types Template ID: intellitactics-top_malware_types	This report shows the most frequently observed malware types.

SI-4 - Intrusion Detection Tools and Techniques

Reports supporting NIST 800-53 control number SI-4.

IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

SI-7 - Software and Information Integrity

Reports supporting NIST 800-53 control number SI-7.

Database Schema Changes Template ID: report_impl_xml-56	This report shows all events where a database schema change has occurred, for a specified time period. Compare these results to organizational change requests to identify unauthorized changes. This report is also useful when troubleshooting database driven application errors.
Monitored File Changes on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

SI-8 - Spam and Spyware Protection

Reports supporting NIST 800-53 control number SI-8.

Authentication to Email Failures Template ID: report_impl_xml-58	This report shows events where an account has failed to authenticate to electronic messaging services (Email only).
Blocked Active Content to Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Blocked Electronic Messages Template ID: report_impl_xml-59	This report shows events that specify that an electronic message was not delivered. The reasons for message delivery failure will be indicated in the result set and will be attributed to one of the following conditions: 1. A firewall blocked the message from delivery due to a policy employed on the firewall. 2. Antivirus software interfered with message delivery. 3. A message was redirected to another delivery point (such as spam). 4. A message was partially modified by content filters (such as spam and antivirus prior to being delivered).
Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as the 'Types/Host' column.
Top Malware Types Template ID: intellitactics-top_malware_types	This report shows the most frequently observed malware types.

SI-11 - Error Handling

Reports supporting NIST 800-53 control number SI-11.

Critical Asset Error Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Hosts with Errors Summary	This report shows hosts reporting errors within a specified

Template ID: intellitactics-hosts_with_errors_summary	time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

GLB Reports

Reports supporting compliance with the Gramm-Leach-Bliley Act (GLB).

Access Control

Metacontrols which serve to limit and monitor the activities of users.

Account Management

The organization manages all aspects of user account management including additions, deletions, modifications, lockouts, suspensions, activations and privilege changes.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.
Windows Account Creations Template ID: report_impl_xml-164	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes Template ID: report_impl_xml-165	This report shows the deletion of Windows accounts, audited by Windows event 630, sorted from the most recent to the oldest.
Windows Account Disables	This report shows the disabling of Windows accounts,

Template ID: report_impl_xml-166	audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables Template ID: report_impl_xml-167	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to the oldest.
Windows Account Unlocked Template ID: report_impl_xml-170	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most recent to the oldest.

Least Privilege

The organization should ensure that users are provided with the most minimal set of privileges required to carry out their designated duties in order to minimize the risk to organizational assets and business objectives. This mechanism shall include periodic reviews of privilege to identify users with excess privileges.

Group Changes Template ID: report_impl_xml-8	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
Security Manager Group Management Template ID: report_impl_xml-188	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.

Monitor Login Activity

The organization should monitor all login activities to critical systems to ensure that data confidentiality and data integrity policies are followed.

Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Windows Account Lockouts Template ID: report_impl_xml-168	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.
Windows Failed Logins Template ID: report_impl_xml-169	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.

Network Access Control

Access to assets and their connected assets should be restricted to only those assets and accounts with a need to access network services and network protocols in order to further a business process or goal.

Top Firewall Denied Sources Template ID: intellitactics-top_fw_denied_sources	This report shows the most frequently blocked source addresses.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.

Remote Access Control

Organizations should have an authorization and approval process in place to control the granting of remote access to ensure that only the privileges required for carrying out assigned tasks and are provided via remote access. Additionally All remote access should be regularly monitored to ensure conformity with remote access policies.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
VPN Account Login Summary Template ID: intellitactics-vpn_account_login_summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity Template ID: report_impl_xml-17	This report shows denied attempts to log into VPN services.
VPN Login Activity Template ID: report_impl_xml-69	This report shows VPN login activity of a given user for a specified time period.

Session Control

Information processing systems should be configured to automatically require re-authentication after a configurable period of time or inactivity.

Session Expiry for Privileged Account Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Use of Non-Repudiation

The organization should employ non-repudiation methods for critical systems in order to irrevocably assign responsibility for system actions to a given individual or account.

Non-Repudiation Exception Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Wireless Access Control

The use of wireless technologies used to connect to information processing systems should be monitored closely to account for the additional risks as compared to other access control technical methods. Strong methods of authentication including physical access control, encryption, and multiple factor authentication.

Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.
WIFI Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.

Business Continuity

Metacontrols which ensure that business continues in the face of unplanned events.

Alternate Communications, Systems and Storage

The organization should provide alternate or redundant communications, systems and storage for information systems that are deemed vital to its continuity. These systems should be identified as part of a business continuity risk assessment.

Assets Unavailable Template ID: report_impl_xml-24	This report shows all events for a specified time period, where an asset has been shut down, restarted, or has encountered an error condition that has caused it to become unavailable.
Failover/HA Events Template ID: report_impl_xml-22	This report shows all events related to failover and high availability activities, including errors and other activities reported by devices, for a specified time period. This expands the scope of entries returned above the 'All

	Failover/HA Occurrences' report. These events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.
Failover/HA Occurrences Template ID: report_impl_xml-23	This report shows all failover and high availability events noted by Security Manager for a specified time period. Such events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.

Software and Data Backup

Organizations must maintain recent and complete backup copies of software and data required for business continuity. These back-ups will be periodically validated to ensure they can be used to restore information processing systems to a current (data) and working (software) state.

Backup Service Activity Template ID: report_impl_xml-25	This report shows all activity related to backup services for a specified time period.
Security Manager SDW Backup Template ID: report_impl_xml-191	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.

Certification - Accreditation - Compliance

Metacontrols ensuring compliance with regulations and fulfillment of the requirements of relevant certifications and accreditations.

Continuous Monitoring of Controls

Organizations must continuously monitor controls to ensure adequate control coverage and acceptable control performance.

Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.
Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.

Communications and System Protection

Metacontrols ensuring the protection of communication channels and the systems that use them.

Acceptable Use of Systems and Services

Organizations should have clear policies procedures regarding acceptable usage of systems & services. Monitoring should be performed to ensure that violations are detected and remediated.

Abuse by Account Template ID: report_impl_xml-27	This report shows all abuse-related events against the entered account for a specified time period.
Abuse by Asset Template ID: report_impl_xml-26	This report shows all abuse-related events for an entered source asset IP address over a specified time period. If a source asset IP address is not entered, results are grouped by the source asset IP address, regardless of whether or not it is a registered asset.
Top Web Referrals with Suspicious Responses Template ID: intellitactics-top_web_referrals_with_suspicious_responses	This report lists the URLs of pages referring to pages which, when requested, produce unusual HTTP response codes (307, 400, 401, 402, 405, 406, 408, 409, 410 through 419 and all 500 series).

Mobile Code Protection

Organizations should create and enforce a policy on the proper use of mobile code in their information systems and networks.

Blocked Active Content to Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
--	---

Use of Cryptography

The organization should employ cryptographic techniques to aid in lowering risks to information processing systems and assets of disclosure and alteration.

VPN Errors Template ID: intellitactics-vpn_errors	This report shows all VPN errors reported for a specified time period.
--	--

Voice over IP Security

Organizations should control the use of VOIP technology to ensure that availability of communications infrastructure is not impacted and to ensure that communications to and from the organization are always visible.

VOIP Service Activity Template ID: report_impl_xml-29	This report shows all activity related to VOIP services for a specified time period.
--	--

Incident Response Management

Metacontrols ensuring that incidents are resolved in a thorough, timely and cost effective manner.

Incident Handling

The organization should follow preestablished policies and procedures to prepare for, detect, analyze, contain, eliminate and recover from security incidents.

All Incidents Template ID: report_impl_xml-74	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Status Template ID: report_impl_xml-75	This report shows all incidents at each status for a specified time period.
Incidents by Close Date Template ID: report_impl_xml-77	This report shows the incidents closed for a specified time period.
Incidents by Create Date Template ID: report_impl_xml-76	This report shows the incidents created for a specified time period.
Open Incidents Template ID: report_impl_xml-73	This report shows all open incidents sorted from oldest to most recent for a specified time period.

Incident Reporting

The organization should ensure that all necessary stakeholders are informed of incidents and that incidents are escalated as required by their risks. Escalation and notification processes should be well defined and automated whenever possible.

Incident Summary by Closing User Template ID: report_impl_xml-80	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: report_impl_xml-79	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: report_impl_xml-78	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

Operations Management

Metacontrols which ensure that the organization's operations are carried out in a secure fashion.

Asset Management

Organizations should classify information system assets by defining security categories that are based on established risk levels. This security categorization should be based on a risk assessment that takes into account the asset's value and the costs associated with the potential loss to the organization should controls fail to protect the asset.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

Capacity Management

Resource allocation and usage should be monitored, reviewed and adjusted with a view to forecasted future capacity requirements. Systems should be optimized for efficiency and increased capacity.

Average Count of Events per Day Template ID: report_impl_xml-162	This report shows the average number of events per day over a given period of time.
Average Count of Managed Events per Day Template ID: report_impl_xml-162-event	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.
Count of Events by Day Template ID: report_impl_xml-161	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.
Count of Managed Events by Day Template ID: report_impl_xml-161-event	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

Monitoring Audit Logs

Organizations should continuously monitor all audit logs to ensure that both information systems and the privileges provided to users on those systems are consistent with normal business usage.

Acquired Devices Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Unparsed Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.
Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.

Monitoring Configuration Activity

Organizations should continuously monitor all configuration changes to information processing systems. This process includes verifying that users are authorized to make changes to an asset and the changes made are consistent with established policies and practices for that asset.

Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

Monitoring System Faults

System errors and faults should be monitored to identify assets that require intervention to maintain acceptable integrity and availability.

Critical Asset Error Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Hosts with Errors Summary Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that

	has been met or exceeded for a specified time period.
--	---

Monitoring Use of Privileges

The organizations should monitor the activities of administrative users and the use of administrative privileges and utilities to ensure usage consistent with business policies and business needs.

SU/SUDO Use Template ID: report_impl_xml-45	This report shows all use of SU and SUDO tools for a specified time period.
--	---

Physical and Environmental Security

Metacontrols which ensure that the physical information technology environment is secure.

Physical Access Control

Organization should protect all means of gaining physical entry to it's facilities adequately by employing detective and preventive measures such keypad locks, electronic card readers, guards and cameras.

Physical Access Denied Template ID: report_impl_xml-46	This report shows all denied attempts to access secured areas/rooms for a specified time period.
---	--

Risk Assessment

Metacontrols which ensure that the organization measures risks to make informed security decisions.

Assessment of Risk

Organizations must periodically employ risk assessment mechanisms that take into account factors such as: threats, vulnerabilities, assets, operational risk and business priorities. This ensures that all decisions regarding policies, controls and incidents are made with a full understanding of the potential cost or benefit to the organization.

High Risk Alerts Template ID: report_impl_xml-47	This report shows high risk alerts for a specified time period.
High Risk Alerts Involving Accounts Template ID: report_impl_xml-49	This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a specified time period.
High Risk Alerts on Critical Assets Template ID: report_impl_xml-48	This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater

than or equal to the entered value for a specified time period.

Vulnerability Assessment

The organization should maintain continuous awareness of newly discovered technical vulnerabilities that affect its information systems and rapidly assess and mitigate the risks as appropriate.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones Template ID: report_impl_xml-55	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

System Acquisition - Development - Maintenance

Metacontrols ensuring that systems are acquired, developed and maintained to meet defined requirements and do so in a secure way.

Use of System Maintenance Tools

Organizations should monitor the tools and utilities used for system maintenance to ensure they are not used to circumvent privileges levels and restrictions.

New Executable Loaded on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

System and Data Integrity

Metacontrols to ensure that system and information changes are made in a planned, controlled and audited manner.

Data Integrity Monitoring

The organization should monitor information systems for changes to system software, applications & application data to detect unauthorized or irregular changes to data that could put the organization at risk with its customers, employees and partners.

Database Schema Changes Template ID: report_impl_xml-56	This report shows all events where a database schema change has occurred, for a specified time period. Compare these results to organizational change requests to identify unauthorized changes. This report is also useful when troubleshooting database driven application errors.
Monitored File Changes on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

Electronic Messaging Security

The organization should monitor the security of all electronic messaging platforms to ensure the confidentiality, integrity and availability of all messages originating from or destined to the organization and its stakeholders.

Authentication to Email Failures Template ID: report_impl_xml-58	This report shows events where an account has failed to authenticate to electronic messaging services (Email only).
Blocked Electronic Messages	This report shows events that specify that an electronic

Template ID: report_impl_xml-59	message was not delivered. The reasons for message delivery failure will be indicated in the result set and will be attributed to one of the following conditions: 1. A firewall blocked the message from delivery due to a policy employed on the firewall. 2. Antivirus software interfered with message delivery. 3. A message was redirected to another delivery point (such as spam). 4. A message was partially modified by content filters (such as spam and antivirus prior to being delivered).
---------------------------------	--

Intrusion Detection and Protection

The organization should employ technologies and procedures monitor and protect all information systems from unwanted or unauthorized access attempts.

IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

Malicious Code Protection

The organization should take adequate measures to protect it's IT infrastructure against malicious code such as viruses, worms and trojans by employing protective technologies on its networks and information systems.

Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as

	the 'Types/Host' column.
Top Malware Types Template ID: intellitactics-top_malware_types	This report shows the most frequently observed malware types.

HIPAA Reports

Reports supporting compliance with the Health Insurance Portability and Accountability Act (HIPAA).

Access Control

Metacontrols which serve to limit and monitor the activities of users.

Account Management

The organization manages all aspects of user account management including additions, deletions, modifications, lockouts, suspensions, activations and privilege changes.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.
Windows Account Creations Template ID: report_impl_xml-164	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes Template ID: report_impl_xml-165	This report shows the deletion of Windows accounts, audited by Windows event 630, sorted from the most recent to the oldest.
Windows Account Disables	This report shows the disabling of Windows accounts,

Template ID: report_impl_xml-166	audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables Template ID: report_impl_xml-167	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to the oldest.
Windows Account Unlocked Template ID: report_impl_xml-170	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most recent to the oldest.

Least Privilege

The organization should ensure that users are provided with the most minimal set of privileges required to carry out their designated duties in order to minimize the risk to organizational assets and business objectives. This mechanism shall include periodic reviews of privilege to identify users with excess privileges.

Group Changes Template ID: report_impl_xml-8	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
Security Manager Group Management Template ID: report_impl_xml-188	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.

Monitor Login Activity

The organization should monitor all login activities to critical systems to ensure that data confidentiality and data integrity policies are followed.

Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Windows Account Lockouts Template ID: report_impl_xml-168	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.
Windows Failed Logins Template ID: report_impl_xml-169	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.

Network Access Control

Access to assets and their connected assets should be restricted to only those assets and accounts with a need to access network services and network protocols in order to further a business process or goal.

Top Firewall Denied Sources Template ID: intellitactics-top_fw_denied_sources	This report shows the most frequently blocked source addresses.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.

Remote Access Control

Organizations should have an authorization and approval process in place to control the granting of remote access to ensure that only the privileges required for carrying out assigned tasks and are provided via remote access. Additionally All remote access should be regularly monitored to ensure conformity with remote access policies.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
VPN Account Login Summary Template ID: intellitactics-vpn_account_login_summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity Template ID: report_impl_xml-17	This report shows denied attempts to log into VPN services.
VPN Login Activity Template ID: report_impl_xml-69	This report shows VPN login activity of a given user for a specified time period.

Session Control

Information processing systems should be configured to automatically require re-authentication after a configurable period of time or inactivity.

Session Expiry for Privileged Account Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Use of Non-Repudiation

The organization should employ non-repudiation methods for critical systems in order to irrevocably assign responsibility for system actions to a given individual or account.

Non-Repudiation Exception Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Wireless Access Control

The use of wireless technologies used to connect to information processing systems should be monitored closely to account for the additional risks as compared to other access control technical methods. Strong methods of authentication including physical access control, encryption, and multiple factor authentication.

Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.
WIFI Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.

Business Continuity

Metacontrols which ensure that business continues in the face of unplanned events.

Alternate Communications, Systems and Storage

The organization should provide alternate or redundant communications, systems and storage for information systems that are deemed vital to its continuity. These systems should be identified as part of a business continuity risk assessment.

Assets Unavailable Template ID: report_impl_xml-24	This report shows all events for a specified time period, where an asset has been shut down, restarted, or has encountered an error condition that has caused it to become unavailable.
Failover/HA Events Template ID: report_impl_xml-22	This report shows all events related to failover and high availability activities, including errors and other activities reported by devices, for a specified time period. This expands the scope of entries returned above the 'All

	Failover/HA Occurrences' report. These events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.
Failover/HA Occurrences Template ID: report_impl_xml-23	This report shows all failover and high availability events noted by Security Manager for a specified time period. Such events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.

Software and Data Backup

Organizations must maintain recent and complete backup copies of software and data required for business continuity. These back-ups will be periodically validated to ensure they can be used to restore information processing systems to a current (data) and working (software) state.

Backup Service Activity Template ID: report_impl_xml-25	This report shows all activity related to backup services for a specified time period.
Security Manager SDW Backup Template ID: report_impl_xml-191	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.

Certification - Accreditation - Compliance

Metacontrols ensuring compliance with regulations and fulfillment of the requirements of relevant certifications and accreditations.

Continuous Monitoring of Controls

Organizations must continuously monitor controls to ensure adequate control coverage and acceptable control performance.

Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.
Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.

Communications and System Protection

Metacontrols ensuring the protection of communication channels and the systems that use them.

Acceptable Use of Systems and Services

Organizations should have clear policies procedures regarding acceptable usage of systems & services. Monitoring should be performed to ensure that violations are detected and remediated.

Abuse by Account Template ID: report_impl_xml-27	This report shows all abuse-related events against the entered account for a specified time period.
Abuse by Asset Template ID: report_impl_xml-26	This report shows all abuse-related events for an entered source asset IP address over a specified time period. If a source asset IP address is not entered, results are grouped by the source asset IP address, regardless of whether or not it is a registered asset.
Top Web Referrals with Suspicious Responses Template ID: intellitactics-top_web_referrals_with_suspicious_responses	This report lists the URLs of pages referring to pages which, when requested, produce unusual HTTP response codes (307, 400, 401, 402, 405, 406, 408, 409, 410 through 419 and all 500 series).

Mobile Code Protection

Organizations should create and enforce a policy on the proper use of mobile code in their information systems and networks.

Blocked Active Content to Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
--	---

Use of Cryptography

The organization should employ cryptographic techniques to aid in lowering risks to information processing systems and assets of disclosure and alteration.

VPN Errors Template ID: intellitactics-vpn_errors	This report shows all VPN errors reported for a specified time period.
--	--

Voice over IP Security

Organizations should control the use of VOIP technology to ensure that availability of communications infrastructure is not impacted and to ensure that communications to and from the organization are always visible.

VOIP Service Activity Template ID: report_impl_xml-29	This report shows all activity related to VOIP services for a specified time period.
--	--

Incident Response Management

Metacontrols ensuring that incidents are resolved in a thorough, timely and cost effective manner.

Incident Handling

The organization should follow preestablished policies and procedures to prepare for, detect, analyze, contain, eliminate and recover from security incidents.

All Incidents Template ID: report_impl_xml-74	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Status Template ID: report_impl_xml-75	This report shows all incidents at each status for a specified time period.
Incidents by Close Date Template ID: report_impl_xml-77	This report shows the incidents closed for a specified time period.
Incidents by Create Date Template ID: report_impl_xml-76	This report shows the incidents created for a specified time period.
Open Incidents Template ID: report_impl_xml-73	This report shows all open incidents sorted from oldest to most recent for a specified time period.

Incident Reporting

The organization should ensure that all necessary stakeholders are informed of incidents and that incidents are escalated as required by their risks. Escalation and notification processes should be well defined and automated whenever possible.

Incident Summary by Closing User Template ID: report_impl_xml-80	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: report_impl_xml-79	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: report_impl_xml-78	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

Operations Management

Metacontrols which ensure that the organization's operations are carried out in a secure fashion.

Asset Management

Organizations should classify information system assets by defining security categories that are based on established risk levels. This security categorization should be based on a risk assessment that takes into account the asset's value and the costs associated with the potential loss to the organization should controls fail to protect the asset.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

Capacity Management

Resource allocation and usage should be monitored, reviewed and adjusted with a view to forecasted future capacity requirements. Systems should be optimized for efficiency and increased capacity.

Average Count of Events per Day Template ID: report_impl_xml-162	This report shows the average number of events per day over a given period of time.
Average Count of Managed Events per Day Template ID: report_impl_xml-162-event	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.
Count of Events by Day Template ID: report_impl_xml-161	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.
Count of Managed Events by Day Template ID: report_impl_xml-161-event	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

Monitoring Audit Logs

Organizations should continuously monitor all audit logs to ensure that both information systems and the privileges provided to users on those systems are consistent with normal business usage.

Acquired Devices Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Unparsed Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.
Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.

Monitoring Configuration Activity

Organizations should continuously monitor all configuration changes to information processing systems. This process includes verifying that users are authorized to make changes to an asset and the changes made are consistent with established policies and practices for that asset.

Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

Monitoring System Faults

System errors and faults should be monitored to identify assets that require intervention to maintain acceptable integrity and availability.

Critical Asset Error Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Hosts with Errors Summary Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that

	has been met or exceeded for a specified time period.
--	---

Monitoring Use of Privileges

The organizations should monitor the activities of administrative users and the use of administrative privileges and utilities to ensure usage consistent with business policies and business needs.

SU/SUDO Use Template ID: report_impl_xml-45	This report shows all use of SU and SUDO tools for a specified time period.
--	---

Physical and Environmental Security

Metacontrols which ensure that the physical information technology environment is secure.

Physical Access Control

Organization should protect all means of gaining physical entry to it's facilities adequately by employing detective and preventive measures such keypad locks, electronic card readers, guards and cameras.

Physical Access Denied Template ID: report_impl_xml-46	This report shows all denied attempts to access secured areas/rooms for a specified time period.
---	--

Risk Assessment

Metacontrols which ensure that the organization measures risks to make informed security decisions.

Assessment of Risk

Organizations must periodically employ risk assessment mechanisms that take into account factors such as: threats, vulnerabilities, assets, operational risk and business priorities. This ensures that all decisions regarding policies, controls and incidents are made with a full understanding of the potential cost or benefit to the organization.

High Risk Alerts Template ID: report_impl_xml-47	This report shows high risk alerts for a specified time period.
High Risk Alerts Involving Accounts Template ID: report_impl_xml-49	This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a specified time period.
High Risk Alerts on Critical Assets Template ID: report_impl_xml-48	This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater

than or equal to the entered value for a specified time period.

Vulnerability Assessment

The organization should maintain continuous awareness of newly discovered technical vulnerabilities that affect its information systems and rapidly assess and mitigate the risks as appropriate.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones Template ID: report_impl_xml-55	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

System Acquisition - Development - Maintenance

Metacontrols ensuring that systems are acquired, developed and maintained to meet defined requirements and do so in a secure way.

Use of System Maintenance Tools

Organizations should monitor the tools and utilities used for system maintenance to ensure they are not used to circumvent privileges levels and restrictions.

New Executable Loaded on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

System and Data Integrity

Metacontrols to ensure that system and information changes are made in a planned, controlled and audited manner.

Data Integrity Monitoring

The organization should monitor information systems for changes to system software, applications & application data to detect unauthorized or irregular changes to data that could put the organization at risk with its customers, employees and partners.

Database Schema Changes Template ID: report_impl_xml-56	This report shows all events where a database schema change has occurred, for a specified time period. Compare these results to organizational change requests to identify unauthorized changes. This report is also useful when troubleshooting database driven application errors.
Monitored File Changes on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

Electronic Messaging Security

The organization should monitor the security of all electronic messaging platforms to ensure the confidentiality, integrity and availability of all messages originating from or destined to the organization and its stakeholders.

Authentication to Email Failures Template ID: report_impl_xml-58	This report shows events where an account has failed to authenticate to electronic messaging services (Email only).
Blocked Electronic Messages	This report shows events that specify that an electronic

Template ID: report_impl_xml-59	message was not delivered. The reasons for message delivery failure will be indicated in the result set and will be attributed to one of the following conditions: 1. A firewall blocked the message from delivery due to a policy employed on the firewall. 2. Antivirus software interfered with message delivery. 3. A message was redirected to another delivery point (such as spam). 4. A message was partially modified by content filters (such as spam and antivirus prior to being delivered).
---------------------------------	--

Intrusion Detection and Protection

The organization should employ technologies and procedures monitor and protect all information systems from unwanted or unauthorized access attempts.

IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

Malicious Code Protection

The organization should take adequate measures to protect it's IT infrastructure against malicious code such as viruses, worms and trojans by employing protective technologies on its networks and information systems.

Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as

	the 'Types/Host' column.
Top Malware Types Template ID: intellitactics-top_malware_types	This report shows the most frequently observed malware types.

PCI Reports

Reports supporting compliance with the Payment Card Industry Data Security Standard (PCI).

1. Install and Maintain a Firewall Configuration

Reports supporting PCI Data Security Standard section 1.

1. Manage Firewall Configuration

Reports supporting PCI Data Security Standard section 1.1.

1. Manage Network Configuration Change

Reports supporting PCI Data Security Standard section 1.1.1.

Firewall Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Router Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.

2. Secure Default Configuration

Reports supporting PCI Data Security Standard section 2.

2. Develop Configuration Standards

Reports supporting PCI Data Security Standard section 2.2.

3. Apply Least Privilege Configuration

Reports supporting PCI Data Security Standard section 2.2.3.

Group Changes Template ID: report_impl_xml-8	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
---	--

Security Manager Group Management Template ID: report_impl_xml-188	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.
---	---

4. Remove Unnecessary Tools, Components

Reports supporting PCI Data Security Standard section 2.2.4.

New Executable Loaded on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

3. Protect Stored Cardholder Data

Reports supporting PCI Data Security Standard section 3.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Database Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Database Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Unauthorized Attempt to Access Sensitive Data Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

4. Encrypt Sensitive Data

Reports supporting PCI Data Security Standard section 4.

1. Encrypt Transmission of Cardholder Data

Reports supporting PCI Data Security Standard section 4.1.

1. Don't Rely Exclusively on WEP for Wi-Fi

Reports supporting PCI Data Security Standard section 4.1.1.

WIFI Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.
--	--

5. Anti-Virus Measures

Reports supporting PCI Data Security Standard section 5.

1. Deploy Anti-Virus Mechanisms

Reports supporting PCI Data Security Standard section 5.1.

AntiVirus Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
---	--

2. Keep Anti-Virus Current, Running, Auditing

Reports supporting PCI Data Security Standard section 5.2.

AntiVirus Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
AntiVirus Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
AntiVirus Review Template ID: intellitactics-spl-av_review	This report is to be used by AntiVirus administrators/analysts to periodically review AntiVirus activity and drive response tasks.
Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Top AntiVirus Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

6. Develop and Maintain Secure Systems

Reports supporting PCI Data Security Standard section 6.

2. Manage Vulnerabilities

Reports supporting PCI Data Security Standard section 6.2.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History	This report shows the vulnerability scan history of a given

<p>Template ID: report_impl_xml-233</p>	asset.
<p>Assets with Type of Vulnerability Template ID: report_impl_xml-53</p>	This report shows assets with the specified vulnerability and operational risk.
<p>Most Common Vulnerabilities Template ID: report_impl_xml-50</p>	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
<p>Most Severe Vulnerabilities Template ID: report_impl_xml-54</p>	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
<p>Most Vulnerable Assets Template ID: report_impl_xml-71</p>	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
<p>Most Vulnerable Zones Template ID: report_impl_xml-55</p>	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

7. Restrict Access to Cardholder Data

Reports supporting PCI Data Security Standard section 7.

<p>Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id</p>	This report shows alerts of the given type for a specified time period.
<p>Top Database Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication</p>	This report shows the most frequently observed accounts that fail to authenticate.
<p>Top Database Successfully Authenticated</p>	This report shows the most frequently observed accounts

Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	that authenticate successfully.
Unauthorized Attempt to Access Sensitive Data Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

8. User Authentication

Reports supporting PCI Data Security Standard section 8.

4. Encrypt Passwords for Transmission, Storage

Reports supporting PCI Data Security Standard section 8.4.

Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

5. Authentication, User Management

Reports supporting PCI Data Security Standard section 8.5.

1. Control Account Management

Reports supporting PCI Data Security Standard section 8.5.1.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management	This report shows Security Manager user creation and

Template ID: report_impl_xml-187	deletion events for a specified time period.
----------------------------------	--

13. Limit Repeated Access Attempts

Reports supporting PCI Data Security Standard section 8.5.13.

Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
--	---

15. Inactive Login Session Control

Reports supporting PCI Data Security Standard section 8.5.15.

Session Expiry for Privileged Account Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

16. Authenticate Access to Cardholder Data

Reports supporting PCI Data Security Standard section 8.5.16.

Top Database Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Database Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.

9. Physical Security

Reports supporting PCI Data Security Standard section 9.

1. Limit and Monitor Physical Access

Reports supporting PCI Data Security Standard section 9.1.

3. Restrict Access to Wireless Devices

Reports supporting PCI Data Security Standard section 9.1.3.

WIFI Denied Auth Activity	This report shows denied attempts to authenticate for
---------------------------	---

Template ID: report_impl_xml-21	access to WIFI services.
---------------------------------	--------------------------

10. Monitor Network Access

Reports supporting PCI Data Security Standard section 10.

2. Automated Audit

Reports supporting PCI Data Security Standard section 10.2.

Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Top Firewall Denied Sources Template ID: intellitactics-top_fw_denied_sources	This report shows the most frequently blocked source addresses.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.

VPN Account Login Summary Template ID: intellitactics- vpn_account_login_summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity Template ID: report_impl_xml-17	This report shows denied attempts to log into VPN services.
VPN Login Activity Template ID: report_impl_xml-69	This report shows VPN login activity of a given user for a specified time period.
WIFI Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.
Windows Account Lockouts Template ID: report_impl_xml-168	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.
Windows Failed Logins Template ID: report_impl_xml-169	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.

6. Frequent Review of Audit Data

Reports supporting PCI Data Security Standard section 10.6.

Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
--	---

11. Test Security Systems and Processes

Reports supporting PCI Data Security Standard section 11.

2. Run Vulnerability Assessments

Reports supporting PCI Data Security Standard section 11.2.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each

	vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones Template ID: report_impl_xml-55	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

4. Use Intrusion Detection Technology

Reports supporting PCI Data Security Standard section 11.4.

Host IDS Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Intrusion Prevention System Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Network IDS Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.

12. Maintain a Security Policy

Reports supporting PCI Data Security Standard section 12.

5. Assign Responsibilities

Reports supporting PCI Data Security Standard section 12.5.

2. Monitor Security

Reports supporting PCI Data Security Standard section 12.5.2.

Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.
--	--

3. Establish Incident Management Capability

Reports supporting PCI Data Security Standard section 12.5.3.

Incident Summary by Closing User Template ID: report_impl_xml-80	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: report_impl_xml-79	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: report_impl_xml-78	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

4. Administer User Accounts

Reports supporting PCI Data Security Standard section 12.5.4.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.

Sarbanes-Oxley Reports

Reports measuring the application of Metacontrols as they apply to the Sarbanes-Oxley Act.

Access Control

Metacontrols which serve to limit and monitor the activities of users.

Account Management

The organization manages all aspects of user account management including additions, deletions, modifications, lockouts, suspensions, activations and privilege changes.

Account Additions Template ID: report_impl_xml-1	This report shows all accounts added to assets noted by Security Manager over a specified time period.
Account Deletions Template ID: report_impl_xml-2	This report shows all accounts deleted from assets noted by Security Manager over a specified time period.
Account Disables Template ID: report_impl_xml-6	This report shows all accounts disabled by administrators within a specified time period. Note this does not return instances of failed logins due to an account being disabled.
Account Lockouts Template ID: report_impl_xml-5	This report shows all account lockouts due to failed logins noted by Security Manager for a specified time period. This report does not include instances of failed logins due to an account being locked out.
Group Additions Template ID: report_impl_xml-3	This report shows all groups created within a specified time period.
Security Manager Account Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Account Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.
Windows Account Creations Template ID: report_impl_xml-164	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes Template ID: report_impl_xml-165	This report shows the deletion of Windows accounts, audited by Windows event 630, sorted from the most recent to the oldest.
Windows Account Disables Template ID: report_impl_xml-166	This report shows the disabling of Windows accounts, audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables Template ID: report_impl_xml-167	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to the oldest.
Windows Account Unlocked Template ID: report_impl_xml-170	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most

recent to the oldest.

Least Privilege

The organization should ensure that users are provided with the most minimal set of privileges required to carry out their designated duties in order to minimize the risk to organizational assets and business objectives. This mechanism shall include periodic reviews of privilege to identify users with excess privileges.

Group Changes Template ID: report_impl_xml-8	This report shows all changes to groups noted by Security Manager for a specified time period. This will capture all add, change, or delete activities grouped by the changed group.
Security Manager Group Management Template ID: report_impl_xml-188	This report shows Security Manager user ID and group membership subscription or removal events for a specified time period.

Monitor Login Activity

The organization should monitor all login activities to critical systems to ensure that data confidentiality and data integrity policies are followed.

Insecure Login Activity Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Windows Account Lockouts Template ID: report_impl_xml-168	This report shows the locking of Windows accounts triggered by failed logins, audited by Windows event 644, sorted from the most recent to the oldest.
Windows Failed Logins Template ID: report_impl_xml-169	This report shows failed attempts to authenticate or be authorized for access to services. Normally, the user is attempting to gain access to the Reporting Host.

Network Access Control

Access to assets and their connected assets should be restricted to only those assets and accounts with a need to access network services and network protocols in order to further a business process or goal.

Top Firewall Denied Sources	This report shows the most frequently blocked source
-----------------------------	--

Template ID: intellitactics-top_fw_denied_sources	addresses.
Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.

Remote Access Control

Organizations should have an authorization and approval process in place to control the granting of remote access to ensure that only the privileges required for carrying out assigned tasks and are provided via remote access. Additionally All remote access should be regularly monitored to ensure conformity with remote access policies.

Critical Asset Accessed Remotely Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
VPN Account Login Summary Template ID: intellitactics-vpn_account_login_summary	This report shows accounts successfully and unsuccessfully attempting to log into VPN services.
VPN Denied Login Activity Template ID: report_impl_xml-17	This report shows denied attempts to log into VPN services.
VPN Login Activity Template ID: report_impl_xml-69	This report shows VPN login activity of a given user for a specified time period.

Session Control

Information processing systems should be configured to automatically require re-authentication after a configurable period of time or inactivity.

Session Expiry for Privileged Account Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Use of Non-Repudiation

The organization should employ non-repudiation methods for critical systems in order to irrevocably assign responsibility for system actions to a given individual or account.

Non-Repudiation Exception Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

Wireless Access Control

The use of wireless technologies used to connect to information processing systems should be monitored closely to account for the additional risks as compared to other access control technical methods. Strong methods of authentication including physical access control, encryption, and multiple factor authentication.

Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.
WiFi Denied Auth Activity Template ID: report_impl_xml-21	This report shows denied attempts to authenticate for access to WIFI services.

Business Continuity

Metacontrols which ensure that business continues in the face of unplanned events.

Alternate Communications, Systems and Storage

The organization should provide alternate or redundant communications, systems and storage for information systems that are deemed vital to its continuity. These systems should be identified as part of a business continuity risk assessment.

Assets Unavailable Template ID: report_impl_xml-24	This report shows all events for a specified time period, where an asset has been shut down, restarted, or has encountered an error condition that has caused it to become unavailable.
Failover/HA Events Template ID: report_impl_xml-22	This report shows all events related to failover and high availability activities, including errors and other activities reported by devices, for a specified time period. This expands the scope of entries returned above the 'All Failover/HA Occurrences' report. These events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.
Failover/HA Occurrences Template ID: report_impl_xml-23	This report shows all failover and high availability events noted by Security Manager for a specified time period.

	Such events indicate error conditions or the testing of Disaster Recovery Procedures. Results should be compared to Change Management systems for tracking purposes and cross-validation of organizational control compliance.
--	--

Software and Data Backup

Organizations must maintain recent and complete backup copies of software and data required for business continuity. These back-ups will be periodically validated to ensure they can be used to restore information processing systems to a current (data) and working (software) state.

Backup Service Activity Template ID: report_impl_xml-25	This report shows all activity related to backup services for a specified time period.
Security Manager SDW Backup Template ID: report_impl_xml-191	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.

Certification - Accreditation - Compliance

Metacontrols ensuring compliance with regulations and fulfillment of the requirements of relevant certifications and accreditations.

Continuous Monitoring of Controls

Organizations must continuously monitor controls to ensure adequate control coverage and acceptable control performance.

Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Registered Control Reports Template ID: report_impl_xml-183	This report shows the registered control reports.
Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.

Communications and System Protection

Metacontrols ensuring the protection of communication channels and the systems that use them.

Acceptable Use of Systems and Services

Organizations should have clear policies procedures regarding acceptable usage of systems & services. Monitoring should be performed to ensure that violations are detected and remediated.

Abuse by Account Template ID: report_impl_xml-27	This report shows all abuse-related events against the entered account for a specified time period.
Abuse by Asset Template ID: report_impl_xml-26	This report shows all abuse-related events for an entered source asset IP address over a specified time period. If a source asset IP address is not entered, results are grouped by the source asset IP address, regardless of whether or not it is a registered asset.
Top Web Referrals with Suspicious Responses Template ID: intellitactics-top_web_referrals_with_suspicious_responses	This report lists the URLs of pages referring to pages which, when requested, produce unusual HTTP response codes (307, 400, 401, 402, 405, 406, 408, 409, 410 through 419 and all 500 series).

Mobile Code Protection

Organizations should create and enforce a policy on the proper use of mobile code in their information systems and networks.

Blocked Active Content to Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
--	---

Use of Cryptography

The organization should employ cryptographic techniques to aid in lowering risks to information processing systems and assets of disclosure and alteration.

VPN Errors Template ID: intellitactics-vpn_errors	This report shows all VPN errors reported for a specified time period.
--	--

Voice over IP Security

Organizations should control the use of VOIP technology to ensure that availability of communications infrastructure is not impacted and to ensure that communications to and from the organization are always visible.

VOIP Service Activity Template ID: report_impl_xml-29	This report shows all activity related to VOIP services for a specified time period.
--	--

Incident Response Management

Metacontrols ensuring that incidents are resolved in a thorough, timely and cost effective manner.

Incident Handling

The organization should follow preestablished policies and procedures to prepare for, detect, analyze, contain, eliminate and recover from security incidents.

All Incidents Template ID: report_impl_xml-74	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Status Template ID: report_impl_xml-75	This report shows all incidents at each status for a specified time period.
Incidents by Close Date Template ID: report_impl_xml-77	This report shows the incidents closed for a specified time period.
Incidents by Create Date Template ID: report_impl_xml-76	This report shows the incidents created for a specified time period.
Open Incidents Template ID: report_impl_xml-73	This report shows all open incidents sorted from oldest to most recent for a specified time period.

Incident Reporting

The organization should ensure that all necessary stakeholders are informed of incidents and that incidents are escalated as required by their risks. Escalation and notification processes should be well defined and automated whenever possible.

Incident Summary by Closing User Template ID: report_impl_xml-80	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: report_impl_xml-79	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: report_impl_xml-78	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.

Operations Management

Metacontrols which ensure that the organization's operations are carried out in a secure fashion.

Asset Management

Organizations should classify information system assets by defining security categories that are based on established risk levels. This security categorization should be based on a

risk assessment that takes into account the asset's value and the costs associated with the potential loss to the organization should controls fail to protect the asset.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

Capacity Management

Resource allocation and usage should be monitored, reviewed and adjusted with a view to forecasted future capacity requirements. Systems should be optimized for efficiency and increased capacity.

Average Count of Events per Day Template ID: report_impl_xml-162	This report shows the average number of events per day over a given period of time.
Average Count of Managed Events per Day Template ID: report_impl_xml-162-event	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.
Count of Events by Day Template ID: report_impl_xml-161	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.
Count of Managed Events by Day Template ID: report_impl_xml-161-event	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

Monitoring Audit Logs

Organizations should continuously monitor all audit logs to ensure that both information systems and the privileges provided to users on those systems are consistent with normal business usage.

Acquired Devices Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
---	--

Unparsed Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.
Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.

Monitoring Configuration Activity

Organizations should continuously monitor all configuration changes to information processing systems. This process includes verifying that users are authorized to make changes to an asset and the changes made are consistent with established policies and practices for that asset.

Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Security Manager Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.

Monitoring System Faults

System errors and faults should be monitored to identify assets that require intervention to maintain acceptable integrity and availability.

Critical Asset Error Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Hosts with Errors Summary Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Resource Allocation Errors Template ID: report_impl_xml-70	This report shows assets with a resource allocation problem, or assets with a resource allocation threshold that has been met or exceeded for a specified time period.

Monitoring Use of Privileges

The organizations should monitor the activities of administrative users and the use of administrative privileges and utilities to ensure usage consistent with business policies and business needs.

SU/SUDO Use	This report shows all use of SU and SUDO tools for a
-------------	--

Template ID: report_impl_xml-45

specified time period.

Physical and Environmental Security

Metacontrols which ensure that the physical information technology environment is secure.

Physical Access Control

Organization should protect all means of gaining physical entry to its facilities adequately by employing detective and preventive measures such as keypad locks, electronic card readers, guards and cameras.

Physical Access Denied

Template ID: report_impl_xml-46

This report shows all denied attempts to access secured areas/rooms for a specified time period.

Risk Assessment

Metacontrols which ensure that the organization measures risks to make informed security decisions.

Assessment of Risk

Organizations must periodically employ risk assessment mechanisms that take into account factors such as: threats, vulnerabilities, assets, operational risk and business priorities. This ensures that all decisions regarding policies, controls and incidents are made with a full understanding of the potential cost or benefit to the organization.

High Risk Alerts

Template ID: report_impl_xml-47

This report shows high risk alerts for a specified time period.

High Risk Alerts Involving Accounts

Template ID: report_impl_xml-49

This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a specified time period.

High Risk Alerts on Critical Assets

Template ID: report_impl_xml-48

This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater than or equal to the entered value for a specified time period.

Vulnerability Assessment

The organization should maintain continuous awareness of newly discovered technical vulnerabilities that affect its information systems and rapidly assess and mitigate the risks as appropriate.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones Template ID: report_impl_xml-55	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

System Acquisition - Development - Maintenance

Metacontrols ensuring that systems are acquired, developed and maintained to meet defined requirements and do so in a secure way.

Use of System Maintenance Tools

Organizations should monitor the tools and utilities used for system maintenance to ensure they are not used to circumvent privileges levels and restrictions.

New Executable Loaded on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.
---	---

System and Data Integrity

Metacontrols to ensure that system and information changes are made in a planned, controlled and audited manner.

Data Integrity Monitoring

The organization should monitor information systems for changes to system software, applications & application data to detect unauthorized or irregular changes to data that could put the organization at risk with its customers, employees and partners.

Database Schema Changes Template ID: report_impl_xml-56	This report shows all events where a database schema change has occurred, for a specified time period. Compare these results to organizational change requests to identify unauthorized changes. This report is also useful when troubleshooting database driven application errors.
Monitored File Changes on Critical Asset Alerts Template ID: intellitactics-alerts_by_registration_id	This report shows alerts of the given type for a specified time period.

Electronic Messaging Security

The organization should monitor the security of all electronic messaging platforms to ensure the confidentiality, integrity and availability of all messages originating from or destined to the organization and its stakeholders.

Authentication to Email Failures Template ID: report_impl_xml-58	This report shows events where an account has failed to authenticate to electronic messaging services (Email only).
Blocked Electronic Messages Template ID: report_impl_xml-59	This report shows events that specify that an electronic message was not delivered. The reasons for message delivery failure will be indicated in the result set and will be attributed to one of the following conditions: 1. A firewall blocked the message from delivery due to a policy employed on the firewall. 2. Antivirus software interfered with message delivery. 3. A message was redirected to another delivery point (such as spam). 4. A message was partially modified by content filters (such as spam and antivirus prior to being delivered).

Intrusion Detection and Protection

The organization should employ technologies and procedures monitor and protect all information systems from unwanted or unauthorized access attempts.

IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

Malicious Code Protection

The organization should take adequate measures to protect it's IT infrastructure against malicious code such as viruses, worms and trojans by employing protective technologies on its networks and information systems.

Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as the 'Types/Host' column.
Top Malware Types Template ID: intellitactics-top_malware_types	This report shows the most frequently observed malware types.

Event Management

Reports organized by the devices to which they apply and related event management activities.

Acquired Devices Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
---	--

Event Search

Account Activity Template ID: report_impl_xml-7	This report shows events involving the given account within the specified time period.
Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Event ID Activity Template ID: report_impl_xml-200	This report shows records for the entered Event ID for a specified time period.
Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Events by Event ID Template ID: intellitactics-sp1-event_id_list	This report lists events with selected event IDs within the specified time period.
Host Activity as Source or Target Template ID: report_impl_xml-196	This report shows events involving the given host as a source or a target within the specified time period.
Malware Search Template ID: report_impl_xml-64	This report shows events for the entered Malware ID for a specified time period.

Event Summaries

Event Type Summary Template ID: intellitactics-sp1-event_id_summary-count	This report summarizes occurrence of event ID values within the specified time period.
Hosts with Errors Summary Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.

Top Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Top Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Unparsed Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.
Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.

AAA Reports

Reports relating to authentication, authorization, and accounting systems.

AAA Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
AAA Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
AAA Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
AAA Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
AAA Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.

Top AAA Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top AAA Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top AAA Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top AAA Hosts Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top AAA Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top AAA Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top AAA Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top AAA Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Top AAA Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top AAA Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top AAA Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top AAA Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top AAA Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed AAA Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

AV Reports

Reports relating to Anti-Virus systems.

AntiVirus Alerts Template ID: intellitactics-	This report shows alerts of the given source type for a specified time period.
--	--

alerts_by_source_type	
AntiVirus Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
AntiVirus Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
AntiVirus Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
AntiVirus Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
AntiVirus Review Template ID: intellitactics-spl-av_review	This report is to be used by AntiVirus administrators/analysts to periodically review AntiVirus activity and drive response tasks.
Hosts with Most Malware Types Template ID: intellitactics-hosts_with_most_malware_types	This report shows which hosts are exposed to the widest variety of malware types.
Malware Types per Zone Template ID: intellitactics-malware_types_per_zone	This report shows the malware types affecting each zone. If the record limit is reached, records describing the malware types that affect the greatest number of hosts are returned.
Most Malware Infested Zones Template ID: intellitactics-most_malware_infested_zones	This report shows zones most affected by malware. Zones 'most infested' are those in which hosts are exposed to the greatest variety of malware; this is reflected in the report as the 'Types/Host' column.
Top AntiVirus Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top AntiVirus Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top AntiVirus Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top AntiVirus Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top AntiVirus Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top AntiVirus Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Top Malware Types Template ID: intellitactics-	This report shows the most frequently observed malware types.

top_malware_types	
Unparsed AntiVirus Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

Application Reports

Reports related to general application event logging.

Application Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Application Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Application Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Application Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Application Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top Application Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Application Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Application Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Application Hosts Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Application Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Application Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Application Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Application Successfully Authenticated Accounts	This report shows the most frequently observed accounts that authenticate successfully.

Template ID: intellitactics-top_successfully_authenticated_accounts	
Top Application Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Application Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Application Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top Application Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top Application Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Application Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

DB Reports

Reports related to database systems.

Database Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Database Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Database Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Database Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Database Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top Database Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top Database Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.

Top Database Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Database Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Database Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Database Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Database Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Database Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Top Database Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top Database Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Database Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

Firewall Reports

Reports related to firewalls.

Firewall Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Firewall Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Firewall Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Firewall Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Firewall Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.

<p>Top Firewall Accounts Failing Authentication</p> <p>Template ID: intellitactics-top_accounts_failing_authentication</p>	<p>This report shows the most frequently observed accounts that fail to authenticate.</p>
<p>Top Firewall Denied Sources</p> <p>Template ID: intellitactics-top_fw_denied_sources</p>	<p>This report shows the most frequently blocked source addresses.</p>
<p>Top Firewall Detector Zones</p> <p>Template ID: intellitactics-top_detector_zones</p>	<p>This report shows the most frequently observed detector address zones.</p>
<p>Top Firewall Detectors</p> <p>Template ID: intellitactics-top_detectors</p>	<p>This report shows the most frequently observed detector addresses.</p>
<p>Top Firewall Event Types</p> <p>Template ID: intellitactics-top_event_types</p>	<p>This report shows the most frequently occurring event types.</p>
<p>Top Firewall Hosts with Errors</p> <p>Template ID: intellitactics-hosts_with_errors_summary</p>	<p>This report shows hosts reporting errors within a specified time period.</p>
<p>Top Firewall Source Ports</p> <p>Template ID: intellitactics-top_source_ports</p>	<p>This report shows the most frequently observed source ports.</p>
<p>Top Firewall Source Zones</p> <p>Template ID: intellitactics-top_source_zones</p>	<p>This report shows the most frequently observed source address zones.</p>
<p>Top Firewall Sources</p> <p>Template ID: intellitactics-top_sources</p>	<p>This report shows the most frequently observed source addresses.</p>
<p>Top Firewall Successfully Authenticated Accounts</p> <p>Template ID: intellitactics-top_successfully_authenticated_accounts</p>	<p>This report shows the most frequently observed accounts that authenticate successfully.</p>
<p>Top Firewall Target Ports</p> <p>Template ID: intellitactics-top_target_ports</p>	<p>This report shows the most frequently observed target ports.</p>
<p>Top Firewall Target Zones</p> <p>Template ID: intellitactics-top_target_zones</p>	<p>This report shows the most frequently observed target address zones.</p>
<p>Top Firewall Targets</p> <p>Template ID: intellitactics-top_targets</p>	<p>This report shows the most frequently observed target addresses.</p>
<p>Top Firewall Taxonomy Types</p> <p>Template ID: intellitactics-top_taxonomy_types</p>	<p>This report shows the most frequently occurring event taxonomy types.</p>
<p>Top Firewall Untaxonomized Events</p> <p>Template ID: intellitactics-untaxonomized_events</p>	<p>This report shows Event ID values without taxonomy types from events within the specified time period.</p>
<p>Unparsed Firewall Event Summary</p> <p>Template ID: intellitactics-unparsed_event_summary</p>	<p>This report shows devices for which some events could not be parsed.</p>
<p>VPN Account Login Summary</p> <p>Template ID: intellitactics-</p>	<p>This report shows accounts successfully and unsuccessfully attempting to log into VPN services.</p>

Host IDS Reports

Reports related to host based intrusion detection systems.

Host IDS Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Host IDS Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Host IDS Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Host IDS Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Top Host IDS Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Host IDS Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Host IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Host IDS Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Host IDS Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Host IDS Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Host IDS Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Host IDS Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Host IDS Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Host IDS Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top Host IDS Taxonomy Types	This report shows the most frequently occurring event

Template ID: intellitactics-top_taxonomy_types	taxonomy types.
Top Host IDS Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Host IDS Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

IPS Reports

Reports related to intrusion prevention systems.

IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Intrusion Prevention System Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Intrusion Prevention System Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Intrusion Prevention System Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Intrusion Prevention System Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top Blocked IPS Signatures Template ID: intellitactics-top_blocked_ips_signatures	This report shows the most frequently blocked IPS signatures.
Top Intrusion Prevention System Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Intrusion Prevention System Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Intrusion Prevention System Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Intrusion Prevention System Hosts with Errors	This report shows hosts reporting errors within a specified time period.

<p>Template ID: intellitactics-hosts_with_errors_summary</p>	
<p>Top Intrusion Prevention System Source Ports</p> <p>Template ID: intellitactics-top_source_ports</p>	<p>This report shows the most frequently observed source ports.</p>
<p>Top Intrusion Prevention System Source Zones</p> <p>Template ID: intellitactics-top_source_zones</p>	<p>This report shows the most frequently observed source address zones.</p>
<p>Top Intrusion Prevention System Sources</p> <p>Template ID: intellitactics-top_sources</p>	<p>This report shows the most frequently observed source addresses.</p>
<p>Top Intrusion Prevention System Target Ports</p> <p>Template ID: intellitactics-top_target_ports</p>	<p>This report shows the most frequently observed target ports.</p>
<p>Top Intrusion Prevention System Target Zones</p> <p>Template ID: intellitactics-top_target_zones</p>	<p>This report shows the most frequently observed target address zones.</p>
<p>Top Intrusion Prevention System Targets</p> <p>Template ID: intellitactics-top_targets</p>	<p>This report shows the most frequently observed target addresses.</p>
<p>Top Intrusion Prevention System Taxonomy Types</p> <p>Template ID: intellitactics-top_taxonomy_types</p>	<p>This report shows the most frequently occurring event taxonomy types.</p>
<p>Top Intrusion Prevention System Untaxonomized Events</p> <p>Template ID: intellitactics-untaxonomized_events</p>	<p>This report shows Event ID values without taxonomy types from events within the specified time period.</p>
<p>Unparsed Intrusion Prevention System Event Summary</p> <p>Template ID: intellitactics-unparsed_event_summary</p>	<p>This report shows devices for which some events could not be parsed.</p>

Network IDS Reports

Reports related to network intrusion detection systems.

<p>IDS/IPS Alerts</p> <p>Template ID: intellitactics-alerts_by_source_type</p>	<p>This report shows alerts of the given source type for a specified time period.</p>
<p>Network IDS Configuration Activity</p> <p>Template ID: intellitactics-configuration_activity</p>	<p>This report shows all configuration changes reported for a specified time period.</p>
<p>Network IDS Devices Acquired</p> <p>Template ID: intellitactics-acquired_devices_with_chart</p>	<p>This report shows hosts from which ISM acquired events within the specified time period.</p>

Network IDS Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Network IDS Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top Network IDS Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Network IDS Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Network IDS Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Network IDS Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Network IDS Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Network IDS Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Network IDS Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Network IDS Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Network IDS Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Network IDS Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top Network IDS Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top Network IDS Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unauthorized WiFi WAP Summary Template ID: intellitactics-unauthorized_wifi_wap_summary	This report shows unauthorized WiFi access points.
Unparsed Network IDS Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

OS Reports

Reports related to operating system event logging.

OS Log Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
OS Log Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
OS Log Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
OS Log Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
OS Log Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top OS Log Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.
Top OS Log Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top OS Log Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top OS Log Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top OS Log Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top OS Log Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top OS Log Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top OS Log Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Top OS Log Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top OS Log Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed OS Log Event Summary Template ID: intellitactics-	This report shows devices for which some events could not be parsed.

unparsed_event_summary

Account Management

Reports showing operating system account management activity.

Windows Account Creations Template ID: report_impl_xml-164	This report shows the creation of Windows accounts, audited by Windows event 624, from the most recent to the oldest.
Windows Account Deletes Template ID: report_impl_xml-165	This report shows the deletion of Windows accounts, audited by Windows event 630, sorted from the most recent to the oldest.
Windows Account Disables Template ID: report_impl_xml-166	This report shows the disabling of Windows accounts, audited by Windows event 629, sorted from the most recent to the oldest.
Windows Account Enables Template ID: report_impl_xml-167	This report shows changes to Windows accounts, audited by Windows event 626. Results are sorted from the most recent to the oldest.
Windows Account Unlocked Template ID: report_impl_xml-170	This report shows the unlocking of Windows accounts, audited by Windows event 671, sorted from the most recent to the oldest.

Proxy Reports

Reports related to proxies.

Proxy Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Proxy Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Proxy Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Proxy Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Proxy Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top Proxy Accounts Failing Authentication Template ID: intellitactics-top_accounts_failing_authentication	This report shows the most frequently observed accounts that fail to authenticate.

Top Proxy Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Proxy Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Proxy Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Proxy Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Proxy Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Proxy Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Proxy Successfully Authenticated Accounts Template ID: intellitactics-top_successfully_authenticated_accounts	This report shows the most frequently observed accounts that authenticate successfully.
Top Proxy Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Proxy Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Proxy Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top Proxy Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top Proxy Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Proxy Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

Router Reports

Reports related to routers.

Router Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Router Configuration Activity Template ID: intellitactics-	This report shows all configuration changes reported for a specified time period.

configuration_activity	
Router Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Router Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Router Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.
Top Router Detector Zones Template ID: intellitactics-top_detector_zones	This report shows the most frequently observed detector address zones.
Top Router Detectors Template ID: intellitactics-top_detectors	This report shows the most frequently observed detector addresses.
Top Router Event Types Template ID: intellitactics-top_event_types	This report shows the most frequently occurring event types.
Top Router Hosts with Errors Template ID: intellitactics-hosts_with_errors_summary	This report shows hosts reporting errors within a specified time period.
Top Router Source Ports Template ID: intellitactics-top_source_ports	This report shows the most frequently observed source ports.
Top Router Source Zones Template ID: intellitactics-top_source_zones	This report shows the most frequently observed source address zones.
Top Router Sources Template ID: intellitactics-top_sources	This report shows the most frequently observed source addresses.
Top Router Target Ports Template ID: intellitactics-top_target_ports	This report shows the most frequently observed target ports.
Top Router Target Zones Template ID: intellitactics-top_target_zones	This report shows the most frequently observed target address zones.
Top Router Targets Template ID: intellitactics-top_targets	This report shows the most frequently observed target addresses.
Top Router Taxonomy Types Template ID: intellitactics-top_taxonomy_types	This report shows the most frequently occurring event taxonomy types.
Top Router Untaxonomized Events Template ID: intellitactics-untaxonomized_events	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Router Event Summary Template ID: intellitactics-unparsed_event_summary	This report shows devices for which some events could not be parsed.

Switch Reports

Reports related to switches.

Switch Alerts Template ID: <code>intellitactics-alerts_by_source_type</code>	This report shows alerts of the given source type for a specified time period.
Switch Configuration Activity Template ID: <code>intellitactics-configuration_activity</code>	This report shows all configuration changes reported for a specified time period.
Switch Devices Acquired Template ID: <code>intellitactics-acquired_devices_with_chart</code>	This report shows hosts from which ISM acquired events within the specified time period.
Switch Errors Template ID: <code>intellitactics-errors</code>	This report shows all errors reported for a specified time period.
Switch Events by Detector Template ID: <code>intellitactics-events_by_detector</code>	This report shows all events reported by the selected detector for a specified time period.
Top Switch Detector Zones Template ID: <code>intellitactics-top_detector_zones</code>	This report shows the most frequently observed detector address zones.
Top Switch Detectors Template ID: <code>intellitactics-top_detectors</code>	This report shows the most frequently observed detector addresses.
Top Switch Event Types Template ID: <code>intellitactics-top_event_types</code>	This report shows the most frequently occurring event types.
Top Switch Hosts with Errors Template ID: <code>intellitactics-hosts_with_errors_summary</code>	This report shows hosts reporting errors within a specified time period.
Top Switch Source Zones Template ID: <code>intellitactics-top_source_zones</code>	This report shows the most frequently observed source address zones.
Top Switch Sources Template ID: <code>intellitactics-top_sources</code>	This report shows the most frequently observed source addresses.
Top Switch Target Ports Template ID: <code>intellitactics-top_target_ports</code>	This report shows the most frequently observed target ports.
Top Switch Target Zones Template ID: <code>intellitactics-top_target_zones</code>	This report shows the most frequently observed target address zones.
Top Switch Targets Template ID: <code>intellitactics-top_targets</code>	This report shows the most frequently observed target addresses.
Top Switch Taxonomy Types Template ID: <code>intellitactics-top_taxonomy_types</code>	This report shows the most frequently occurring event taxonomy types.
Top Switch Untaxonomized Events Template ID: <code>intellitactics-untaxonomized_events</code>	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Switch Event Summary Template ID: <code>intellitactics-</code>	This report shows devices for which some events could not be parsed.

Web Service Reports

Reports related to web services.

Top Web Accounts Failing Authentication Template ID: <code>intellitactics-top_accounts_failing_authentication</code>	This report shows the most frequently observed accounts that fail to authenticate.
Top Web Detector Zones Template ID: <code>intellitactics-top_detector_zones</code>	This report shows the most frequently observed detector address zones.
Top Web Detectors Template ID: <code>intellitactics-top_detectors</code>	This report shows the most frequently observed detector addresses.
Top Web Event Types Template ID: <code>intellitactics-top_event_types</code>	This report shows the most frequently occurring event types.
Top Web Hosts with Errors Template ID: <code>intellitactics-hosts_with_errors_summary</code>	This report shows hosts reporting errors within a specified time period.
Top Web Referrals with Suspicious Responses Template ID: <code>intellitactics-top_web_referrals_with_suspicious_responses</code>	This report lists the URLs of pages referring to pages which, when requested, produce unusual HTTP response codes (307, 400, 401, 402, 405, 406, 408, 409, 410 through 419 and all 500 series).
Top Web Source Zones Template ID: <code>intellitactics-top_source_zones</code>	This report shows the most frequently observed source address zones.
Top Web Sources Template ID: <code>intellitactics-top_sources</code>	This report shows the most frequently observed source addresses.
Top Web Successfully Authenticated Accounts Template ID: <code>intellitactics-top_successfully_authenticated_accounts</code>	This report shows the most frequently observed accounts that authenticate successfully.
Top Web Target Ports Template ID: <code>intellitactics-top_target_ports</code>	This report shows the most frequently observed target ports.
Top Web Target Zones Template ID: <code>intellitactics-top_target_zones</code>	This report shows the most frequently observed target address zones.
Top Web Targets Template ID: <code>intellitactics-top_targets</code>	This report shows the most frequently observed target addresses.
Top Web Taxonomy Types Template ID: <code>intellitactics-top_taxonomy_types</code>	This report shows the most frequently occurring event taxonomy types.
Top Web Untaxonomized Events Template ID: <code>intellitactics-untaxonomized_events</code>	This report shows Event ID values without taxonomy types from events within the specified time period.
Unparsed Web Event Summary Template ID: <code>intellitactics-</code>	This report shows devices for which some events could not be parsed.

unparsed_event_summary	
Web Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Web Configuration Activity Template ID: intellitactics-configuration_activity	This report shows all configuration changes reported for a specified time period.
Web Devices Acquired Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Web Errors Template ID: intellitactics-errors	This report shows all errors reported for a specified time period.
Web Events by Detector Template ID: intellitactics-events_by_detector	This report shows all events reported by the selected detector for a specified time period.

Alert Management

Reports supporting alert management.

Alerts by Source Type Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Alerts by Type Template ID: intellitactics-alerts_by_type	This report shows alerts of the given type for a specified time period.
High Risk Alerts Template ID: report_impl_xml-47	This report shows high risk alerts for a specified time period.
High Risk Alerts Involving Accounts Template ID: report_impl_xml-49	This report shows high risk alerts involving user accounts with a risk threshold greater than or equal to the entered value for a specified time period.
High Risk Alerts on Critical Assets Template ID: report_impl_xml-48	This report shows high risk alerts involving critical assets (as source, target or generator of alert) where the host operational risk threshold and risk threshold are greater than or equal to the entered value for a specified time period.
Registered Control Alerts Template ID: report_impl_xml-184	This report shows the registered control alerts for a specified time period.
Top Alert Types Template ID: intellitactics-top_alert_types	This report shows the most frequently occurring alert types.
Top Alert Types by Event Count Template ID: intellitactics-top_alert_types_by_event_count	This report shows the alert types with the most frequently occurring events.

By Device Type

Alerts by source device.

AAA Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
AntiVirus Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Application Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Database Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Email Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Firewall Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
IDS/IPS Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
ISM Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
OS Log Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Other Class Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Packet Analyzer Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Proxy Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Router Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.
Switch Alerts Template ID: intellitactics-alerts_by_source_type	This report shows alerts of the given source type for a specified time period.

Web Alerts Template ID: <code>intellitactics-alerts_by_source_type</code>	This report shows alerts of the given source type for a specified time period.
--	--

Incident Management

Reports supporting the management of incidents.

All Incidents Template ID: <code>report_impl_xml-74</code>	This report shows all incidents opened within the specified time period, regardless of status, starting with the most recently opened incidents.
Incident Summary by Closing User Template ID: <code>report_impl_xml-80</code>	This report shows closed incidents, grouped by the closing user, for a specified time period.
Incident Summary by Creator Template ID: <code>report_impl_xml-79</code>	This report shows incidents entered by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Owner Template ID: <code>report_impl_xml-78</code>	This report shows incidents owned by each user for a specified time period. Time range is applied to creation timestamp.
Incident Summary by Status Template ID: <code>report_impl_xml-75</code>	This report shows all incidents at each status for a specified time period.
Incidents by Close Date Template ID: <code>report_impl_xml-77</code>	This report shows the incidents closed for a specified time period.
Incidents by Create Date Template ID: <code>report_impl_xml-76</code>	This report shows the incidents created for a specified time period.
Open Incidents Template ID: <code>report_impl_xml-73</code>	This report shows all open incidents sorted from oldest to most recent for a specified time period.

Operations Activity and Status

Reports describing operations over a defined time period.

Account Management Review Template ID: <code>intellitactics-spl-act_mgmt</code>	This report summarizes account management over the specified time period.
AntiVirus Operations Activity Template ID: <code>intellitactics-op_status-av</code>	This report describes the operation of AntiVirus measures over the selected time period.
AntiVirus Review Template ID: <code>intellitactics-spl-av_review</code>	This report is to be used by AntiVirus administrators/analysts to periodically review AntiVirus activity and drive response tasks.
Security Management Operations Activity Template ID: <code>intellitactics-op_status-sec_mgmt</code>	This report describes security management operations over the selected time period.

Security Environment

Reports describing the security environment - i.e. assets, users, privileges, vulnerabilities, etc.

Assets and Zones

Reports describing known assets and zones.

Asset Additions Template ID: report_impl_xml-33	This report shows all assets added as environmental information for a specified time period.
Assets by Current Owner Template ID: report_impl_xml-30	This report shows a list of assets by current owner for a specified time period.
Assets by High Compliance Risk Template ID: report_impl_xml-32	This report shows all assets with a compliance risk equal to or higher than a user specified value. The compliance risk is a value from 1 to 5, with 5 being the highest.
Assets by High Operational Risk Template ID: report_impl_xml-31	This report shows all assets with an operational risk rating equal to or higher than a user provided value. The operational risk is a value from 1 to 5, with 5 being the highest.

Vulnerabilities

Reports supporting the management of vulnerabilities in the security environment.

Asset Vulnerabilities Template ID: report_impl_xml-81	This report shows the most recent vulnerability scan results for a given host for a specified time period.
Asset Vulnerability History Template ID: report_impl_xml-233	This report shows the vulnerability scan history of a given asset.
Assets with Type of Vulnerability Template ID: report_impl_xml-53	This report shows assets with the specified vulnerability and operational risk.
Most Common Vulnerabilities Template ID: report_impl_xml-50	This report shows the most commonly detected vulnerabilities, the severity of the vulnerabilities, the number of hosts affected, and the operational risks for the most recent scans for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each type, and provides an overall measure of risk for each type. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Severe Vulnerabilities Template ID: report_impl_xml-54	This report shows the individual vulnerabilities of greatest risk, vulnerabilities details and affected hosts for a specified time period. The risk of each vulnerability (from

	1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Assets Template ID: report_impl_xml-71	This report shows the assets and the vulnerabilities affecting them in a given zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities of each asset and provides an overall measure of risk for each. Each vulnerability's risk (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.
Most Vulnerable Zones Template ID: report_impl_xml-55	This report shows the most vulnerable zones and statistics describing the nature of the vulnerabilities detected within each zone for a specified time period. The Risk Sum column is the sum of all risk values for all vulnerabilities in each zone and provides an overall measure of risk for each zone. The risk of each vulnerability (from 1 to 1000) is calculated by scaling its priority by the operational risk of the vulnerable host.

Intellitactics Security Manager

Reports describing the use and operation of ISM.

All SM Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
All SM Activity by Type Template ID: report_impl_xml-181	This report shows all Security Manager activity grouped by event type for a specified time period.
All SM Activity by User Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.
Security Management Operations Activity Template ID: intellitactics-op_status-sec_mgmt	This report describes security management operations over the selected time period.

Administration

Reports describing the administration of ISM.

SM Correlation Configuration Management Template ID: report_impl_xml-192	This report shows Security Manager correlation configuration changes, such as event escalation or event correlation, for a specified time period.
SM DA Management Template ID: report_impl_xml-190	This report shows Security Manager new data acquisition setup, or existing data acquisition changes for a specified time period.
SM Group Management	This report shows Security Manager user ID and group

Template ID: report_impl_xml-188	membership subscription or removal events for a specified time period.
SM User Management Template ID: report_impl_xml-187	This report shows Security Manager user creation and deletion events for a specified time period.

User Activity

Reports describing the activity of the users of ISM.

Report Requests Template ID: report_impl_xml-82	This report shows all Reporting System reports requested by an account for a specified time period.
SM User Access and Authorization Template ID: report_impl_xml-186	This report shows successful and failed authorization activity and password changes for a specified time period.
Security Manager Activity Template ID: report_impl_xml-179	This report shows all Security Manager activity for a specified time period.
Security Manager Activity by Account Template ID: report_impl_xml-180	This report shows all Security Manager activity by user account for a specified time period.
Security Manager Activity by Type Template ID: report_impl_xml-181	This report shows all Security Manager activity grouped by event type for a specified time period.

Health Monitoring

Reports which assist in the monitoring of ISM availability and capacity.

SM SDW Backup Template ID: report_impl_xml-191	This report shows all Security Manager Security Data Warehouse (SDW) database backups for a specified time period.
SM System Startup Template ID: report_impl_xml-189	This report shows Security Manager user initiated or system initiated system startup for a specified time period.

System Statistics

Reports which describe the ISM environment.

Log Management

Reports describing the processing and storage of log data by ISM.

Average Count of Events per Day Template ID: report_impl_xml-162	This report shows the average number of events per day over a given period of time.
Count of Events by Day Template ID: report_impl_xml-161	This report shows the average count of events collected and processed per day by Intellitactics systems for a specified time period.

Event Management

Reports describing the processing of security event data made accessible for reporting and correlation by ISM.

Acquired Devices Template ID: intellitactics-acquired_devices_with_chart	This report shows hosts from which ISM acquired events within the specified time period.
Average Count of Managed Events per Day Template ID: report_impl_xml-162-event	This report shows the average number of events fully processed and made available for reporting and correlation per day over a given period of time.
Count of Managed Events by Day Template ID: report_impl_xml-161-event	This report shows the count of events fully processed and made available for reporting and correlation per day by Intellitactics systems for a specified time period.