



Intellitactics Brief: FISMA Updates

December 2009

Consensus Audit Guidelines for Federal Agencies

Securing the nation against cyber attacks is a top priority. The Federal Information Security Management Act in drafting the [US ICE Act of 2009 \(the new FISMA\)](#) calls on federal agencies to "monitor, detect, analyze, protect, report and respond against known vulnerabilities, attacks and exploitations". Because federal agencies don't have unlimited money, the CIOs and CISOs agreed that jointly establishing a prioritized baseline of information security measures and controls that can be monitored by automated mechanisms would improve effectiveness while controlling the cost of compliance. Also, the legislation prescribes that "offense must inform defense" meaning that "knowledge of actual attacks that have compromised systems provides the essential foundation on which to construct effective defenses."

The [Consensus Audit Guidelines](#), the prioritized baseline of information security measures and controls, offer a rational way to meet requirements by establishing a baseline of measures and controls that can be continuously monitored through automated mechanisms. Potentially, this could mean that interconnected agencies, managing to the prioritized set of controls, would potentially increase security effectiveness across their agencies and across the federal government.

Following is the list of twenty controls:

Twenty Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Additional Critical Controls (not directly supported by automated measurement & validation):

16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

Intellitactics Security Manager

SANS Institute was able to validate that Intellitactics Security Manager, a SIEM solution, enabled at least three of the controls directly and consolidates the results of multiple security products for centralized security operations. This brief focuses on Controls 6 and 8. See [SANS' complete list of vendor products](#) enabling the Twenty Controls.

The following describes Controls 6 and 8 with the SANS content that includes How attackers exploit the lack of this control. Then SANS suggests Quick Wins (QW) you can get from implementing the controls. How Intellitactics SIEM solutions provide automation is provided in blue.

Critical Control 6: Maintenance, Monitoring, & Analysis of Audit Logs

How do attackers exploit the lack of this control?

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems were compromised, without protected and complete logging records, the victim is blind to the details of the attack and to the subsequent actions taken by the attackers. **Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.** Sometimes logging records are the only evidence of a successful attack. Many organizations **keep audit records for compliance purposes but attackers rely on the fact that such organizations rarely look at the audit logs so they do not know that their systems have been compromised.** Because of **poor or non-existent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.**

This is the most fundamental uses of Intellitactics SIEM solutions, Security Manager and Intellitactics SAFE (appliance), automating the collection and review of audit logs. The logging is done continuously and the raw logs and parsed logs or events are not only stored as prescribed but are easily accessible. The SIEM solution automatically correlates events looking for logs that indicate suspicious or out of scope behavior. The advantage of an automated SIEM over manual log review is that the SIEM generates an alert or notification, so the security administrator can quickly begin investigation, further searching of logs or visual analysis of an evolving attack involving a specific source or target. Intellitactics SIEM solutions enable consistent logging and automated examination of log files to uncover control violations or attacks in progress.

How can this control be implemented, automated, and its effectiveness measured?

QW: Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression (CEE) initiative. If systems cannot generate logs in a standardized format, deploy log normalization tools to convert logs into a standardized format.

Intellitactics SIEM solutions are infused with the intelligence to accurately collect the logs that are required for each device type of data source being monitored. The SIEM solutions are aware of what logs are required for reports, both operational and compliance, correlation, advanced correlation, analytics and incident investigation. The collection of logs can also be customized for each device or data source during a service engagement; support for devices or data sources, not currently supported by Intellitactics is also available.

QW: Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals.

Intellitactics SIEM solutions are designed to store and archive logs without using additional storage devices. Both SAFE and ISM can also connect to SANS devices as this is the preferred method for storage and archival.

QW: System administrators and security personnel should devise profiles of common events from given systems, so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

The advantage of Intellitactics SIEM solutions over simple logging tools is that a large percentage of this type of tuning is provided automatically by ISM and SAFE. The administrators use an interface to adapt the system to agency or regulatory policy. There are dozens of packaged correlations that reduce false positives.

QW: All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely.

Intellitactics SIEM solutions offer both the performance and capacity for handling these data sources without impact to the analytic or reporting capabilities of the SIEM.

QW: Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions.

This capability is used by most of the SIEM users.

QW: Security personnel and/or system administrators should run bi-weekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.

This task is routinely set up in the reporting function of the SIEM solution. Likewise, immediate notification or alerting on anomalies can also be accommodated.

Vis/Attrib: Each agency network should include at least two synchronized time sources, from which all servers and network equipment retrieve time information on a regular basis, so that timestamps in logs are consistent.

Accommodated by Intellitactics.

Vis/Attrib: Network boundary devices, including firewalls, network-based IPSs, and inbound and outbound proxies should be configured to log verbosely all traffic (both allowed and blocked) arriving at the device.

Accommodated by Intellitactics.

Vis/Attrib: For all servers, organizations should ensure logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.

Accommodated by Intellitactics.

QW: Config/Hygiene: Organizations should periodically test the audit analysis process by creating controlled, benign events in logs and monitoring devices and measuring the amount of time that passes before the events are discovered and action is taken. Ensure that a trusted person is in place to coordinate activities between the incident response team and the personnel conducting such tests.

This test for the health and maintenance of the SIEM is included with the solutions.

NOTE: Advanced: Organizations should **deploy a Security Event/Information Management (SEIM) system tool for log aggregation and consolidation from multiple machines and for log correlation and analysis.** Deploy and monitor standard government scripts for analysis of the logs, as well as using customized local scripts. Furthermore, event logs should be correlated with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. And, secondly, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a known-vulnerable target.

This feature is used by almost all users of the Intellitactics SIEM solutions. Because this capability is largely automated and the intelligence for this type of correlation is included with the SIEM, this advanced capability can be deployed by any size organization regardless of the maturity or size of the security team.

Associated NIST SP 800-53 Rev 3 Priority 1 Controls:

AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)

Procedures and tools for implementing this control: Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such **logging should be activated, with logs sent to centralized logging servers.** Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for **verbose logging, storing all the information available for logging** should a follow up investigation be required.

Intellitactics Security Manager (ISM) and Intellitactics SAFE, a fully capable SIEM appliance, collects logs from any number and types of devices and data sources: network, OS, databases, applications and other data sources to collect vulnerability data, asset, identity, endpoint etc.

Furthermore, **operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges.** To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled as part of Critical Control 1, to ensure that each managed item actively connected to the network is periodically generating logs.

Intellitactics collects access control logs and provides context to leading role management and identity management solutions like SUN's Identity and Role Manager Solutions with packaged integration which was jointly developed with SUN.

Analytical programs for reviewing logs can be useful, but the capabilities employed to analyze audit logs is quite wide-ranging, including just a cursory examination by a human. **Actual correlation tools can make audit logs far more useful for subsequent manual inspection by people.** Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

Intellitactics enable the skilled information security personnel and administrators to be more productive – less time spent looking for anomalies leaving more time for resolution and remediation. Intellitactics SIEM assesses correlated events or higher level Intellitactics Alerts and puts all the detail of the Alert, events and logs at the fingertips of the professional accelerating investigation, improving understanding and enabling response.

Critical Control 8: Controlled Use of Administrative Privileges

How do attackers exploit the lack of this control?

According to some Blue Team personnel as well as investigators of large-scale Personally Identifiable Information (PII) breaches, the **misuse of administrator privileges** is the **number one method for attackers to spread inside a target enterprise**. Two very common attacker techniques take advantage of uncontrolled administrative privileges:

In the first, a workstation user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious web site, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges. One of the most common of these attacks involves the domain administration privileges in large Windows environments, giving the attacker significant control over large numbers of machines and access to the data they contain.

How can this control be implemented, automated, and its effectiveness measured?

QW: Organizations should inventory all administrative passwords and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive and that his/her administrative password has at least 12 semi-random characters, consistent with the Federal Desktop Core Configuration (FDCC) standard.

QW: Before deploying any new devices in a networked environment, organizations should change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to a difficult-to-guess value.

QW: Organizations should configure all administrative-level accounts to require regular password changes on a 30-, 60-, or 90-day interval.

This activity can be monitored by Intellitactics; additionally, physical security badge swipes or biometrics can be correlated with password use to determine if the owner is physically on premise for example.

QW: Organizations should ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis as is done for traditional user and administrator passwords.

QW: Passwords for all systems should be stored in a hashed or encrypted format. Furthermore, files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super-user privileges.

QW: Organizations should ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.

QW: Through policy and user awareness, organizations should require that administrators establish unique, different passwords for their administrator accounts and their non-administrative accounts. On systems with unsalted passwords, such as Windows machines, this approach can be verified in a password audit by comparing the password hashes of each account used by a single person.

QW: Organizations should configure operating systems so that passwords cannot be reused within a certain time frame, such as six months.

This task can be automated using the Intellitactics SIEM solution. Users trying to reuse passwords are immediately identified and alerts or notifications can be sent to the user and their manager notifying them of the policy violation.

Vis/Attrib: Organizations should implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior (e.g. system reconfigurations during night shift).

Accommodated by the Intellitactics SIEM

QW Vis/Attrib: Organizations should configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators group

Accommodated by the Intellitactics SIEM

QW Config/Hygiene: All administrative access, including domain administrative access, should utilize two-factor authentication.

QW Config/Hygiene: Remote access directly to a machine should be blocked for administrator-level accounts. Instead, administrators should be required to access a system remotely using a fully logged and non-administrative account. Then, once logged in to the machine without admin privileges, the administrator should then transition to administrative privileges using tools such as sudo on Linux/UNIX, run-as on Windows, and other similar facilities for other types of systems.

QW Config/Hygiene: Organizations should conduct targeted spear-phishing tests against both administrative personnel and non-administrative users to measure the quality of their defense against social engineering.

QW Advanced: Organizations should segregate administrator accounts based on defined roles within the organization. For example, "Workstation admin" accounts should only be allowed administrative access of workstations, laptops, etc.

Associated NIST SP 800-53 Rev 3 Priority 1 Controls: AC-6 (2, 5), AC-17 (3), AC-19, AU-22(4)

Procedures and tools for implementing this control: Built-in operating system features can extract lists of accounts with super user privileges, both locally on individual systems and on overall domain controllers. To verify that users with high privileged accounts do not use such accounts for day-to-day web surfing and e-mail reading, security personnel could periodically gather a list of running processes in an attempt to determine whether any browsers or e-mail readers are running with high privileges. Such information gathering can be scripted, with short shell scripts searching for a dozen or more different browsers, e-mail readers, and document editing programs running with high privileges on machines. Some legitimate system administration activity may require the execution of such programs over the short term, but long-term or frequent use of such programs with administrative privileges could indicate that an administrator is not adhering to this control.

Intellitactics SIEM: Lists of accounts with super user privileges are a data source for the Intellitactics Security Manager and Intellitactics SAFE. This data is regularly correlated with other data/logs to enable management of privileged users. Many of the manual tasks suggested here can be automated using the Intellitactics SIEM. By automating the tasks, they can be monitored, reported and anomalies or deviations to policy can generate alerts or notifications to users and/or their managers.

Additionally, to prevent administrators from accessing the web using their administrator accounts, administrative accounts can be configured to use a web proxy of 127.0.0.1 in some operating systems that allow user-level configuration of web proxy settings. Furthermore, in some environments, administrator accounts do not require the ability to receive e-mail. These accounts can be created without an e-mail box on the system. To enforce the requirement for password length of 12 or more characters, built-in operating system features for minimum password length can be configured, which prevent users from choosing short passwords. To enforce password complexity (requiring passwords to be a string of pseudo-random characters), built-in operating system settings or third-party password complexity enforcement tools can be applied.