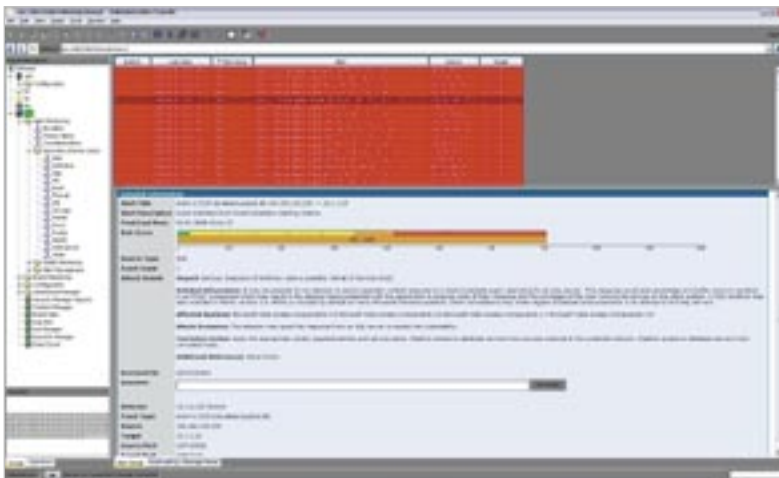


Intellitactics⁺ Intellitactics Security Manager

ISM Alert Extensions

Generic security alerts generated by many security event management products are simple notifications generated from a rule or automatically occur when patterns of security events are discovered. Intellitactics Security Manager (ISM) provides Alerts that do more than notify. Intellitactics Security Manager (ISM) offers the most capable and extensible security information and event management solution. ISM automates all the functionality of log management, event management and alerting and features an interface for understanding and investigating security events and alerts. Alerts in the ISM hierarchy are correlated events that include detail and context that combined accelerate incident response and reduce the overall financial impact of security incidents.

ISM rapidly and automatically transforms logs from anything located anywhere into a fewer number of events. Events are transformed into actionable alerts that streamline the ability to isolate and respond to security incidents. ISM Alerts are more than notifications and are unique because they provide another layer of abstraction based on analysis and correlation of security events. With one click on an ISM Alert the analyst sees all the detail related to the Alert. Alerts can be enriched by extending the alert attributes.



Intellitactics Security Manager (ISM) offers the most capable and extensible security information and event management solution. ISM automates log and event management and features an interface, the Alert UI, for understanding and investigating security events and control violations. Alerts in the ISM hierarchy are correlated events that include the detail required to accelerate incident response and reduce risk.

ALERT EXTENSIONS

In addition to displaying various default alert details in the UI, ISM provides a capability for Alert Extensions. Using Alert Extensions, ISM links to external systems to pull in extra information about the Alert based on its attributes.

This functionality is especially useful in monitoring and analyzing signature-based products like SNORT, Sourcefire and ISSReal Secure. For example, SNORT publishes their signature knowledgebase online, which is shared with Sourcefire. ISM links to this knowledgebase eliminating the need for the analyst to access another console. This may shave minutes from an investigation; improving productivity and preventing a successful external attack. The same functionality is available for ISS Real Secure.

Another example of an Alert Extension provides the facility for integrating with incident records of an external ticketing system, like Archer. The Alert Extension appears as a new section in ISM's Alert Detail where it automatically displays relevant Archer incident record information, eliminating the need to find and review the record in yet another separate interface or console. The analyst can also add the SNORT payload data to Alert Detail using the Alert Extension.

The Alert Extension makes it possible to present additional information about a highlighted ISM alert to the user inside the Alert Details UI. Because this information is provided automatically, and presented alongside other Alert details, also provided by ISM, the operator/analyst has all the information needed to make a decision as well as recommended corrective action. The alert detail is appended to alerts sent to incident management solutions, like Archer or Remedy, to accelerate incident response.

ONE PLACE, ONE CLICK

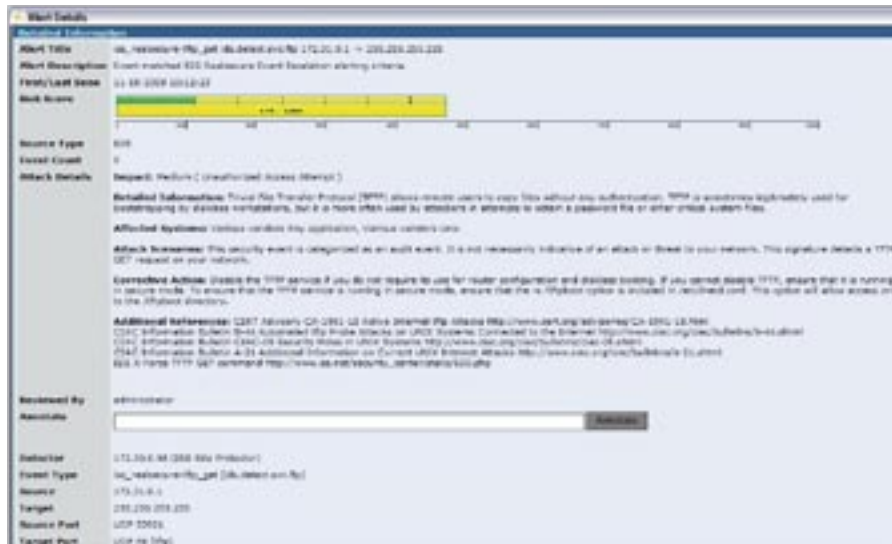
Without Alert Extension, the operator/analyst would have to first open a Sourcefire console, then identify the type of alert and manually navigate to the Knowledgebase to get the event ID explanation. When every second counts, this requires too many steps and takes too much time.

BENEFITS of ALERT EXTENSIONS

The benefit of Alert Extensions is increased effectiveness and efficiency. Alert Extensions save the analyst time by replacing time consuming look ups on multiple consoles with consolidated, relevant information in one place. Alert Extension capably deals with all the values of an Alert including multiple sources and targets. This feature increases productivity resulting in fewer security incidents and more efficient investigation of incidents that accelerate response.



The screenshot above depicts a Sourcefire generated ISM Alert. When the analyst clicks on the Alert, ISM automatically goes out to web based SNORT knowledge base and pulls the information associated with the Snort event_id in the alert.



This is another example of ISM's Alert Extensions. The ISS Real Secure generated ISM Alert is depicted in the ISM Alert Details UI.

Committed to Your Success

Intellitactics features a low total cost of ownership. Primarily agentless data collection reduces the burden on the infrastructure. The unique Security Data Warehouse, which combines an embedded, self-managing relational database requiring no DBA and compressed stores of raw logs, is easy on the storage budget. The product architecture grows with you as you add more data sources or evolve your risk policies. Intellitactics features 'security know-how' in packaged reports, metrics and correlations. The Customer Center, located at www.intellitactics.com, features instant access to new reports and metrics, and automates support functions for faster response to all inquiries.

Intellitactics
Enterprise Security Management

intellitactics.com

1800 Alexander Bell Drive
Reston, Virginia 20191
703 620 3800 | 877 746 7658