Many organizations today are using security event management tools to gather, correlate and report on security data within their environments. Although some are still using traditional log management tools, the need for more effective event intelligence and deeper analysis of activity within the environment is driving more interest in, and use of, security information and event management (SIEM) platforms. In 2012, the SANS 8th Annual Log Management Survey revealed that the majority of responding organizations are leveraging security event data for the following:¹

- Detecting and tracking suspicious behavior
- Supporting forensic analysis and correlation
- Achieving/proving compliance with regulatory requirements

These are essentially the same use cases year after year, with a continued emphasis on saving time and making security operations as efficient as possible. Unfortunately these goals are complicated by an ever-increasing volume of event data and the growing sophistication of attacks. For example, respondents to the SANS log management survey indicated that one of their biggest challenges was the identification of key events from background activity—in other words, finding the needles in the haystack. They perceived detection of advanced threats as being difficult, including the day-to-day use cases for SIEM tools, such as tracking suspicious behavior, supporting forensics analysis or preventing incidents.

Given the nature of today's attacks, this use of SIEM is merely scratching the surface. Security teams need tools that can help them identify events quickly, distill large volumes of event data into simple timeframes for rapid analysis, and incorporate more types of data than ever before. An increasing number of organizations are looking to develop and incorporate new sources of threat intelligence, with the hope of getting ahead of threats. To do this, new and different data from a variety of different sources is needed, and advanced analysis capabilities to normalize and correlate this data with security information will be useful, as well. On top of this, analysts need tools they can implement with ease in a reasonable time period, while quickly extracting meaningful information from event stores.

To this end, we had the opportunity to review McAfee's Enterprise Security Manager (ESM) 9.2 with a focus on fundamental SIEM features and capabilities to meet this new business demand for security and threat intelligence. Overall, the tools were easy to use. Key features such as the ability to integrate related McAfee products, including Vulnerability Manager, Network Security Platform, ePolicy Orchestrator (ePO) and Global Threat Intelligence (GTI) were tested. Overall, the product performed in a means that was intuitive and easy on the security admin or manager. These and other details are covered in this paper.

¹ [www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf](http://www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf)
The ESM Interface

Naturally enough, we began the review by exploring the ESM interface, which within minutes, felt almost infinitely customizable. Although this review did not include physical setup, we did configure features within the interface as part of our evaluation.

Users can shape the interface into views that contain numerous different displays of information, and creating these and switching among them was incredibly simple. This is a vitally important feature for enterprise security teams: Focusing and simplifying the UI of a complex investigative tool such as a SIEM system can save hundreds of operations hours each year, and makes for much easier installation and tuning. ESM offers one of the most user-friendly interfaces we have seen from a SIEM system to date, offering immediate benefits to IT teams with minimal time spent setting it up.

The ESM interface is composed of several distinct panes:

- **Event Summary**: Displays major malicious events detected
- **Source IPs**: Displays source IP addresses noted in events
- **Total Events**: Displays a simple metric for keeping up with overall event counts in the environment
- **Event Distribution**: Charts event counts as a graph over time
- **Destination Geolocation**: Displays the location of events in a specified period

Figure 1 shows a typical dashboard view of these panes.

![Figure 1. The ESM Dashboard](image-url)
In the uppermost right corner of the center pane is a drop-down menu for specifying the time range viewed, with built-in ranges from the last minute to several years (shown in Figure 1 immediately above the “Total Events” gauge, with the “Current Month” selected). Custom ranges can be set easily as well. On the left side of the display, users can create or select different “displays,” enabling them to customize their system navigation. Many users might opt for a display of the entire aggregated set of data within the ESM platform—for others, circumstances may dictate the display of only a single device type or source for drill down and deeper analysis.

In the center, we started with the view of the SIEM’s event analysis. To create a new view/dashboard element, we clicked the appropriate button from the left pane, then dragged and dropped different elements (for example, graphs, tables, and source and destination graphs and lists) onto the page. Then we selected the types of queries (system details, traffic types and so on) that will feed these elements. Finally, we placed the elements where desired. Figure 2 shows an example of this process, in which we created a new view that includes a pie chart of OS deployments.

![View Editing Toolbar](image)

**Figure 2. Customizing the ESM Interface**

On the right-hand side of the interface, the user can create a number of flexible filters to look for and select only specific data from the view. The number and types of filters are extensive, with options for filtering on traffic, device attributes, protocols, specific services and other characteristics.
Finally, the upper-right corner of the ESM interface displays up to nine small “Quick Launch” icons that direct users to important product features, as shown in Figure 3.

![Figure 3. Typical Set of Quick Launch Icons](image)

These provide access to the following functions and capabilities (in order, left to right):

- **System Properties.** This contains information about the system, its hardware platform, application and OS licenses and other basic details.

- **Asset Manager.** The Asset Manager polls devices discovered on the network for their configuration details. It can group discovered assets into zones for risk classification and identification, and is useful in configuring network discovery tasks.

- **Reports.** You can set ESM to generate reports on the fly or according to a schedule. The reports can be custom or standard reports provided through ESM.

- **Alarms.** These can send a variety of alerts, which can be aggregated into a simple view, to analysts. For example, an analyst could have an alarm triggered by a specific threshold of traffic, or certain types of rules that were triggered, and ESM could send an e-mail notifying the team.

- **Watchlists.** These can monitor for specific objects or identified systems, users, traffic, protocols, ports, addresses and more. When the targeted object is spotted, a rule will then notify an assigned analyst.

- **Case Management.** In this feature, you can create and track event “cases.” This is a simple incident tracking system that functions in a manner similar to basic ticketing applications.

- **Enterprise Log Manager (ELM) Search.** This feature queries specific log events if ESM is connected to McAfee’s Enterprise Log Manager.

Not seen in Figure 3 are the remaining Quick Launch icons:

- **Policy Editor.** The platform’s rule engine operates in a variety of categories, ranging from intrusion prevention system (IPS) signatures to firewall rules, database monitoring, and others.

- **Correlation.** This icon accesses the correlation engine, which combines policy rules and custom parameters to create complex filtering and alerting definitions that only trigger alerts when several conditions are met, such as IPS rules and specific source addresses appearing together.
Rapid Event Analysis

Given the amount of data many security teams are collecting today and the complexity of current threat scenarios, it is vital that the security teams be able to rapidly pinpoint events of interest and view granular details of events and network traffic. In breach and attack scenarios where seconds count, security teams will appreciate ESM’s ability to find what they’re looking for quickly.

We tested a variety of scenarios, using different dashboard views that were populated with security events and correlated data, to see how quickly we could find useful information for security analysis. Ultimately, the easiest way to get started was to find the specific information pane in the dashboard that we were interested in, highlight a data range or specific event type, and quickly “zoom” into this data for more in-depth searching and analysis. For example, by clicking a specific event type (for example, “Malware sent from internal source”) in the Event Summary pane, we could immediately update other panes, such as Source IPs and Event Distribution, with this event type. This type of self-learning and updating is important because threats and attack methodologies continue to advance.

Having loaded the various panes with specific event data we wanted to capture, we then drilled into the data by highlighting a cross-section of the visible data, continuing this process until we reached an appropriate level of detail and granularity. For example, we selected successively smaller date ranges for events in the Event Distribution pane until we had several thousand malware events within a several minute period on a single day. Highlighting any one of these events then updates the Source IP pane with the event’s source IP address, as shown in Figure 4.

![Figure 4. Rapid Drill-Down into Events](image-url)
As for speed and efficiency, we managed to get to this level of fine-grained detail in only a few seconds, which was impressive—and absolutely critical in the case of an event in progress. We also explored a variety of different dashboard panes and views, some of which are available in the product in its default configuration. The views we used included the following:

- **Application Activity.** This view shows specific applications and services communicating in the environment, ranging from SSH to Kerberos and QuickTime. We were able to quickly discern the top traffic related to these services, in terms of hosts, source and destination users and IP addresses, and total events and severity of the events detected. Figure 5 shows this dashboard.
• **Incidents.** This dashboard showed us the correlated events over a given period, with source and destination IP addresses, events and event distribution over time, severity, and network flows between source and destination. This enabled us to explore the Flow Source and Destination Graph pane, which instructs the analyst to drag a source or destination to the center of the pane to display and highlight its connections. Figure 6 depicts this graph, after some simple tuning and investigation.

• **Flow—Packets by Destination and Source.** This is another useful gauge of network flows that can be correlated against our last example. A quick display of source and destination IPs appeared, with the number of flows by packet count displayed. This data is useful for tracking the event to specific IPs to gauge where the event originated from as well as its attempts to spread.

We then explored the drill-down options for these views. First, we expanded the destination IP addresses to show a separate view of source ports alongside it, as shown in Figure 7.
Rapid Event Analysis (CONTINUED)

This enabled us to start analyzing traffic and determining what applications might be communicating most frequently. This is a good means for baselining normal traffic as well as detecting abnormal flows.

Then, we drilled into the distribution of noted vulnerabilities by asset from the same pane, which enabled us to look at data fed to the ESM platform by McAfee’s Vulnerability Manager product. This is critical for organizations needing to distinguish real events from noise and to make critical improvements so that such events cannot occur again.

In summary, with one set of actions in a single pane, we started with source and destination flows by packet, expanded packets by destination to include source ports, and then looked at noted vulnerabilities for these destination systems as well, all in the space of several minutes. We found the speed of analysis and the quality of data presentation to be excellent.
Next, we turned our focus to the policy and correlation rule engine within ESM, which can be one of the most complex aspects of a SIEM system. Security teams need a relatively simple interface, coupled with a flexible and powerful rule engine. Most security teams spend a fair amount of time creating and tuning rules, so this process needs to be as easy to use as possible.

Creating Rules

After opening the policy editor, analysts can first evaluate or create new variables. These variables are useful for defining network details and other data for use within rules and help clarify the purpose of the rules and simplify their creation. For example, a basic variable called HOME_NET (a McAfee default variable) can be configured to represent an internal IP address range (for example, 10.0.0.0/24) and then called from within rules as needed.

Analysts can create many different rule types in several major categories. The first rule category is “IPS.” This type focuses on intrusion detection and prevention capabilities, and enables native access to—and easy inclusion of—McAfee IDS or IPS platforms within ESM. IPS preprocessor rules are anomaly detection and packet inspection rules for McAfee Nitro IDS/IPS and include fragmented packet analysis and reconstruction, port scan analyzers, HTTP traffic normalization and more.

Rules in the “Firewall” category cover basic packet analysis and traffic control; source and destination ports and IP addresses can be monitored and blocked, alerts can be sent, and other actions initiated. In addition, analysts can use these rules to generate a blacklist of addresses and/or ports automatically, consolidate the blacklists into a unified view and take further steps.

Figure 8 depicts firewall rule creation.

Figure 8. Creating Firewall Rules
Deep Packet Inspection rules enable more advanced IPS rule customization and application through the use of rule attributes and options.

Another main rules category is the set of “Receiver” rules. These rules pertain to the McAfee Event Receiver, which can accept numerous event types, including firewalls, routers, flow data, IDS/IPS, among others. Instantiating this class of rules is simple, enabling the user to define specific actions to be taken when the Event Receiver detects specific data types. For example, “Advanced Syslog Parser” rules can include regular expression pattern matching and perform specific actions on only the identified portions of logs sent to the Event Receiver by numerous platforms. “Data Source” rules are automatically created as Event Receiver notifications come in, and “Windows Event” rules activate McAfee-defined events that can trigger responses or packet data capture for Windows events that the Event Receiver sees.

Other rule categories include “Application Data Monitor (ADM)” rules, which enable more complex and deeper analysis of application behavior profiles and traffic, and “Database Event Monitor (DEM)” rules, which can monitor database transactions for a variety of events.

We experimented with a range of rule types within ESM. Most of these were very intuitive to work with, although the number of options available is exhaustive. Many have drag-and-drop interfaces, allowing the use of simple Boolean statements, and all have a graphic interface with form fields that enable the selection of particular conditions.

McAfee has also simplified the integration and use of normalization, a key element in rule-based correlation. McAfee maintains a list of normalization rules that brings together similar rules from different vendors and products under one ID within ESM. Analysts can then use the rules in different dashboard views, filters and event summaries.
Correlating Event and Activity Data

Correlation was our next area to review. The ESM appliance that we evaluated had a number of correlation rules built in, and we generated several new ones as part of our test cases. With any SIEM product, the correlation capability and rule set tend to be critical aspects of success or failure in event monitoring and response. We found McAfee's default correlation engine to be intuitive and easy to use. As with its policy rules, analysts can easily create ESM's correlation rules through a graphic interface into which they can drag and drop data and analysis operators. For example, Figure 9 shows a simple correlation rule identifying a buffer overflow attack and subsequently looking for a connection to a backdoor that may have been opened.

![Figure 9. Buffer Overflow and Backdoor Correlation Rule](image)

Analysts can combine any number of rules and filters in various ways to create new correlation rules quickly and easily. Figure 10 shows another example, detecting a successful exploit or malware event, followed by a DNS probe.
For shops needing centralized, more in-depth correlation, McAfee offers, as a separate appliance, the Advanced Correlation Engine (ACE). ACE augments the existing correlation capabilities of ESM by adding risk scoring of correlation rules and events and performing real-time or historical correlation. Analysts can configure multiple “correlation managers” that enable ACE’s rule-less correlation engine to identify what is important to the business—a specific service or application, user or group, or profile of activity.
Knowing what’s taking place inside the network perimeter is only the beginning of what McAfee ESM can do when it comes to providing threat intelligence and early warning. A number of services and other functions easily fit into an ESM deployment, giving analysts and higher-ups a view of what’s on the other side of the hill, as well as what’s “inside the wire.”

**Global Threat Intelligence**

One of the most interesting new features within ESM 9.2 that we explored was the inclusion of data from McAfee’s Global Threat Intelligence (GTI) service, which centralizes and correlates threat and attack data from around the world and incorporates McAfee’s own security research and analysis. This feature enables the delivery of reputation-based, relevant intelligence to numerous McAfee security platforms in a manner that facilitates real-time event correlation and threat identification.

In the ESM product SANS reviewed, GTI was automatically imported in several places. First, GTI creates automatic watchlists from globally noted malicious and suspicious IP addresses, which can be integrated into filters, rules and dashboard views to quickly see what GTI is now reporting. Figure 11 shows a sample dashboard display of GTI sources and events.

![Figure 11. GTI Sources and Events](image)

Other built-in GTI dashboards include an overall summary, a threat summary and specific charts for threat sources and destinations. These dashboards can provide interesting and relevant data about what is happening to other organizations. This information can be vital to security teams who need additional, timely threat intelligence that can help them determine whether events are widespread and affecting others in general or if the organization appears to be a specific target.
Promoting Situational Awareness (CONTINUED)

**Reporting**

We examined a variety of ESM reports, from high-level executive reports to more detailed ones focusing on event and correlation data. For example, one report contained only host-based events related to user account-sharing activity so analysts could provide PCI compliance reports for this control to auditors. Analysts can customize the reports easily, again using drag-and-drop design, and store them locally, send them to a defined remote location or e-mail them to users and/or groups.

**Situational Awareness**

Even with all of the robust features we explored in ESM 9.2, one aspect of McAfee’s toolset stood out—the integration and cross-platform correlation features to gain visibility and situational awareness. McAfee is beginning to consolidate many of its products into a single central monitoring architecture, enabling enterprises to correlate and manage data from a vast range of sources from one interface.

An especially rewarding integration combines ESM with McAfee’s management platform, ePolicy Orchestrator (ePO), which many organizations already use to centrally configure and control diverse security platforms, ranging from DLP to host-based IPS and whitelisting agents. Network security devices such as McAfee’s network IPS are managed by their Network Security Platform (NSP), which integrates into ESM much like ePO does. The focus of both products’ integration with ESM is on quarantine commands that can help to quickly isolate sources of malicious events and contain their ill effects.

Thanks to the ability to natively integrate and communicate with existing ePO deployments, ESM can now work with a huge amount of security data and configuration information that ePO and NSP already know about. As a result of this integration, ESM can be used to identify threats and then instruct ePO to clarify or even remediate issues in a short time frame.

A combined solution that enables analysts to not only identify events, but also fix problems, is a powerful one. Although our evaluation did not extend to this degree of platform integration, we were able to see and work with ePO data fed into the system. For example, Figure 12 shows a dashboard summary of event information from an ePO platform.
Promoting Situational Awareness (CONTINUED)

Figure 12. ePO Dashboard and Event Integration with ESM

Between the advanced and thorough, yet easy-to-use reporting features and the advanced integration of information from monitored systems combined with threat intelligence from a wide range of sources, ESM gives security analysts some foreknowledge of what attacks they could have to fend off, how urgently they have to prepare for them, and where the vulnerabilities are most acute.
Conclusion

With today’s rapidly evolving threat landscape, the need to more quickly analyze an increasing amount of security event data over an expanding timeframe is evident. Security teams need the ability to assess and correlate data easily, track events for investigations, and report on security controls within the environment. McAfee Enterprise Security Manager 9.2 offers enterprises a relatively easy-to-use SIEM system that can perform broad and deep event analysis as well as provide a quick assessment.

The speed of the system’s interface and its flexible dashboard views enabled us to view a broad range of security events within a relatively short period of time, and the policy and correlation rules were both easy and flexible to create and manage. Reporting was simple yet thorough, and ESM provided a variety of prebuilt reports that address common requirements. Creating new reports was easy, and the intuitive drag-and-drop design engine allowed for easy customization. In addition to the foundational SIEM capabilities that ESM offered, the inclusion of threat intelligence feeds from systems around the world as well as McAfee security research teams, lent the platform a new degree of credibility in identifying and correlating security events.

Many organizations don’t have a strong set of controls in threat intelligence today, and McAfee’s GTI service offers enterprises a way to bring a much broader security analysis perspective to bear within their own environments. For organizations currently using McAfee’s ePO, IDS/IPS, Vulnerability Manager, database monitoring and related products, ESM’s new integration capabilities are making it easier than ever to create a unified security architecture with best-of-breed components that work well together. With the inclusion of ePO integration in ESM, McAfee now also offers the ability to remediate issues directly from within ESM, a significant enhancement of the product. A similar integration with McAfee Vulnerability Manager can enable ESM to trigger vulnerability scans, and the integration with Network Security Platform (NSP) enables the automation of quarantine actions when correlation rules are triggered by malicious event sources or suspicious traffic.

ESM will prove to be a capable SIEM platform for enterprises of all types—one that offers distinct advantages in the areas of flexibility and ease-of-use, as well as speed and integration.
About the Author

Dave Shackleford is the founder and principal consultant with Voodoo Security, a SANS analyst, instructor and course author, and a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert, and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft and CTO for the Center for Internet Security. Dave is the author of the Sybex book “Virtualization Security.” Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

SANS would like to thank its sponsor:

McAfee®
An Intel Company