ESG Lab Validation

McAfee Enterprise Security Manager

Intelligent, Actionable, and Integrated Security Information and Event Management (SIEM)

By Tony Palmer, Senior IT Validation Analyst; and Alex Arcilla, IT Validation Analyst

May 2018

This ESG Lab Report was commissioned by McAfee and is distributed under license from ESG.

Contents

Introduction 3
Background 3
The Solution: McAfee Enterprise Security Manager 4
ESG Lab Validation 5
Actionable Threat Intelligence 5
ESG Lab Testing 5
Advanced Analytics 8
ESG Lab Testing 8
Incident Response 10
ESG Lab Testing 10
The Bigger Truth 12

ESG Validation Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

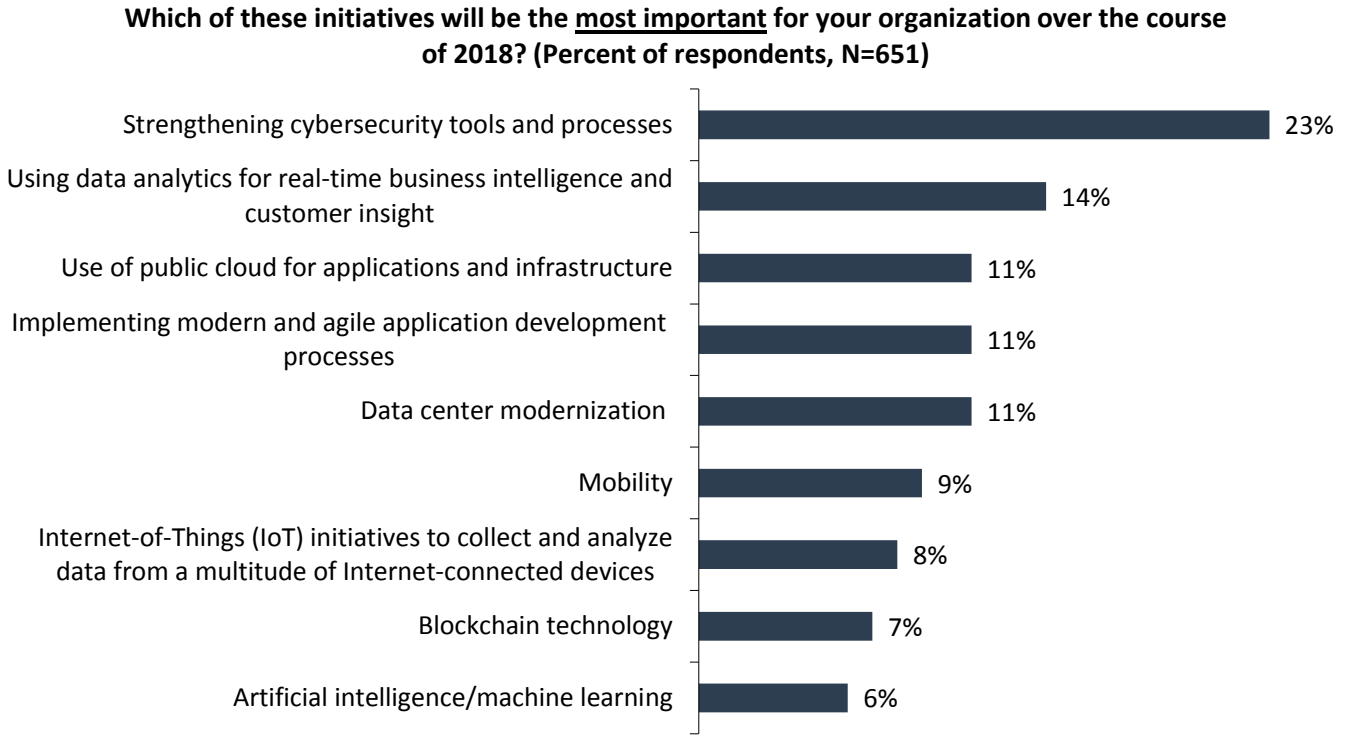
Introduction

This ESG Lab Validation report documents hands-on testing of the McAfee next-generation SIEM solution. ESG Lab focused on the McAfee Enterprise Security Manager (ESM), the core product of McAfee's end-to-end solution for addressing comprehensive threat detection and remediation. Testing was designed to explore how the solution accurately detects advanced threats using a layered approach, the speed and effectiveness of responding to an attack, and the operational efficiencies of this integrated solution.

Background

ESG recently asked 651 IT professionals and managers to identify their most important IT initiatives for 2018. We found that 23% seek to strengthen cybersecurity tools and processes, making it the most-often cited response by a wide margin, as shown in Figure 1.[1]

Figure 1. Top IT Initiatives for 2018



Source: Enterprise Strategy Group

IT has long understood the data security threats to their organizations, such as unauthorized access, viruses, malware, data collection, and exfiltration of sensitive information. The current security model focuses heavily on perimeter security and point solutions, traditionally preventing unauthorized access by attempting to stop it at the gates with firewalls.

However, experience tells us that no single system can be 100% successful in preventing all compromises. This is especially true in today's always on, always connected world, where unsuspecting users are being targeted by social engineering and sophisticated, well-financed cybercriminals who relentlessly attack with advanced persistent threats that look to invade and exploit any security vulnerability. What is needed is a holistic approach that can leverage multiple interconnected

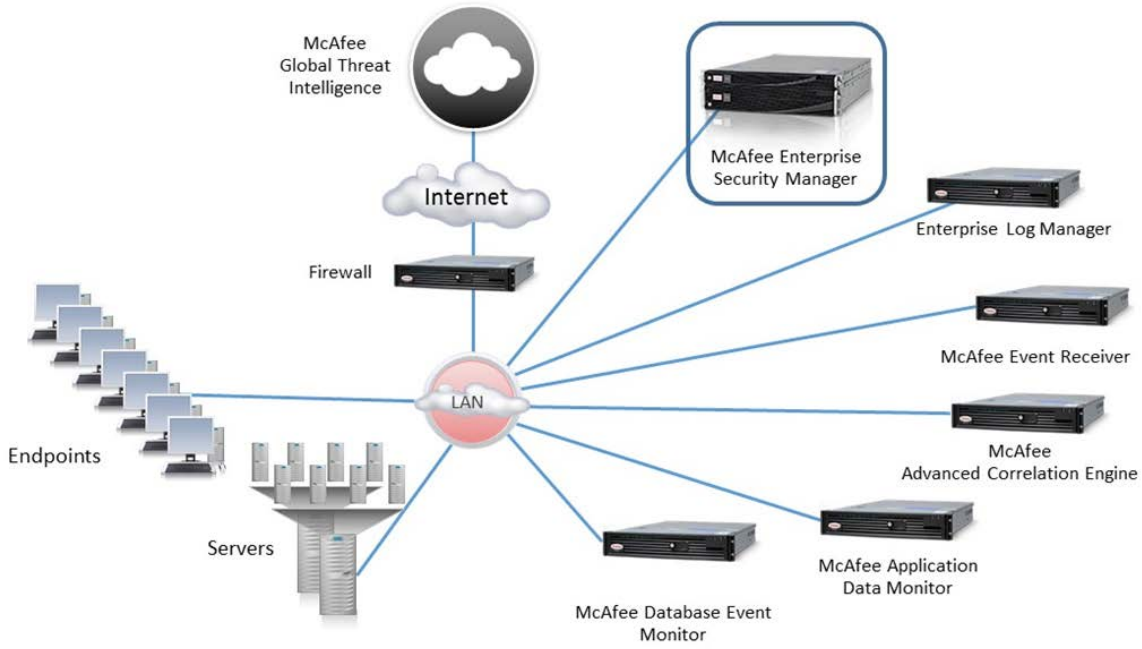
[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

security solutions as a single security ecosystem, providing security analysts the actionable intelligence they need to secure the modern IT environment.

The Solution: McAfee Enterprise Security Manager

The McAfee Enterprise Security Manager (ESM) is a SIEM solution that brings event, threat, and risk data together to provide advanced security intelligence, rapid incident response, seamless log management, and an extensible compliance framework.

Figure 2. McAfee Enterprise Security Manager



Source: Enterprise Strategy Group

Key benefits of the McAfee ESM include:

- Advanced threat intelligence—The McAfee ESM detects variations from normal network, user, or application activity that could indicate a threat is imminent and that data or infrastructure is at risk. In real time, ESM calculates baseline activity for all collected information, provides prioritized alerts of potential threats before they occur, and analyzes data for patterns that may indicate a larger threat. It also leverages contextual information, such as vulnerability scans and identity and authentication management systems and enriches each event with that context for a better understanding of how security events can impact security and business risk. In addition, ESM supports network- and host-based solutions from multiple vendors of advanced threat technologies to receive indicators of compromise (IOC). Utilizing the IOC data, ESM can provide alerts for new events corresponding to the IOC details. McAfee ESM also features BackTrace, which automatically provides details of historical events corresponding to IOC data, designed to provide faster, more accurate incident response.

- The availability of critical facts in minutes—The McAfee ESM database appliance is engineered to collect, process, and correlate billions of log events at the speed enterprises require, and retain them for multiple years with other data streams. McAfee ESM can store billions of events and flows, keeping all information available for immediate ad hoc queries, forensics, rules validation, and compliance.

- A solution built for high data volume processing—McAfee ESM mines large data volumes to find critical security information, which is a key SIEM requirement. McAfee ESM is built to leverage these large volumes of security data and goes far beyond pattern matching to provide long-term historical IOCs and actionable threat intelligence.

- Simplified compliance—McAfee ESM enables centralized and automated compliance monitoring and reporting. Integration with the Unified Compliance Framework (UCF) enables a "collect once, comply with many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum.

- The ability to connect the IT infrastructure—McAfee ESM offers active integrations with hundreds of Security Innovation Alliance (McAfee SIA) Partners' security solutions as well as direct integrations with McAfee ePolicy Orchestrator (McAfee ePO) for policy-based endpoint management; McAfee Advanced Threat Defense (McAfee ATD) to search, correlate, and act on McAfee ATD-sourced IOCs; McAfee Network Security Manager (McAfee NSM) for intrusion prevention; and McAfee Vulnerability Manager (MVM) for vulnerability scanning. With these integrations, McAfee ESM is designed to automate many first response actions, helping organizations respond to attacks more quickly and efficiently.

McAfee ESM is integrated with McAfee Threat Intelligence Exchange to provide organizations with detailed, closed-loop workflows from discovery to containment. Based on endpoint monitoring, McAfee Threat Intelligence Exchange aggregates low prevalence attacks, leveraging global, third-party, and local threat intelligence, and sharing this information with other security devices. McAfee Global Threat Intelligence (McAfee GTI) integration with McAfee ESM includes data from McAfee Labs with more than 100 million global threat sensors, offering a constantly updated feed of known malicious IP addresses, and includes threat lookup from the dashboard and categorization of IP addresses for policy and security monitoring.

ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of McAfee ESM, the central component of the McAfee SIEM solution, remotely and at a McAfee facility in Santa Clara, California. Testing was designed to assess the ability of McAfee ESM to provide next-generation SIEM functionality, including log management, continuous monitoring, threat detection and remediation, and advanced correlation and analytics.

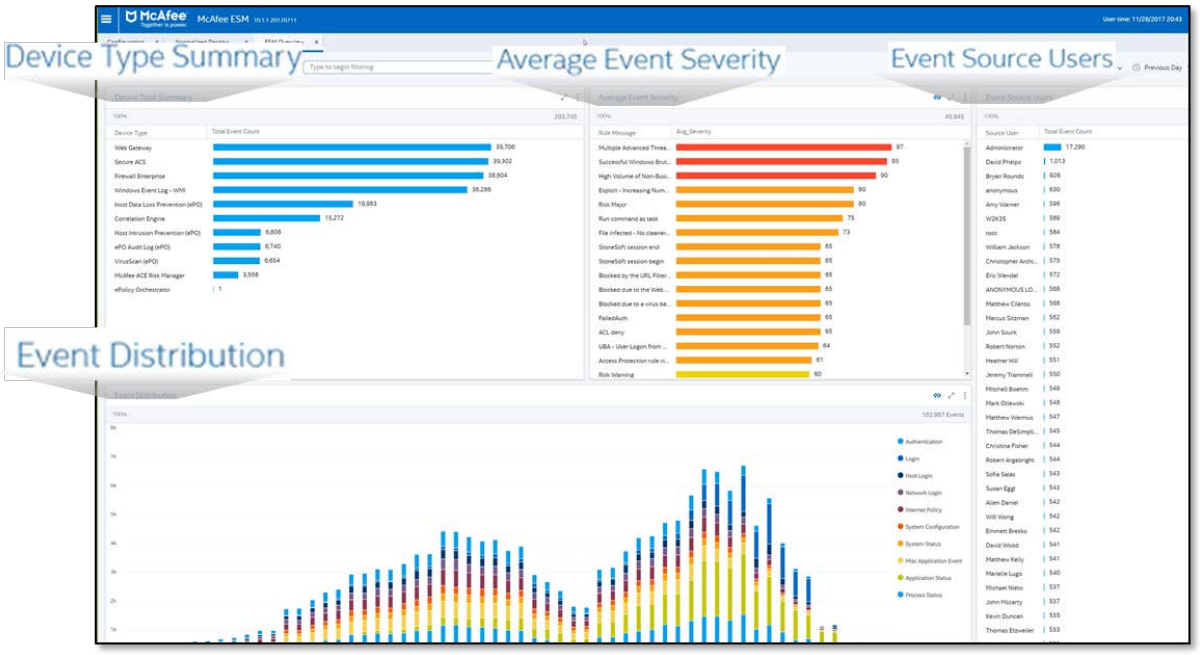
Actionable Threat Intelligence

McAfee ESM collects data from more than 400 external sources—perimeter devices, identity management, endpoints, and premium and open source threat intelligence feeds—to provide security operations teams with a better understanding of both their overall security posture and individual threats. Data is collected, analyzed, and correlated with context, prioritized, and imbued with actionable information accessible via a tabbed user interface along with right-click menu functionality.

ESG Lab Testing

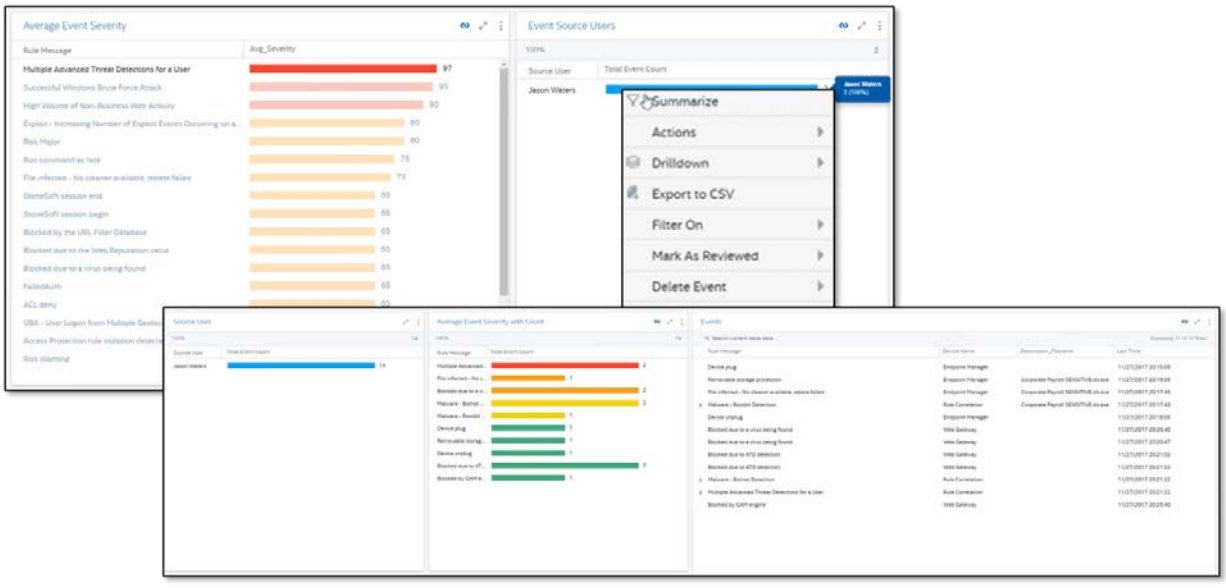
ESG Lab began with the McAfee ESM *Overview* tab shown in Figure 3, which revealed a comprehensive view of nearly 200 million daily events and 135 billion total events collected from hundreds of data sources. Figure 3 shows the default view including summaries of events based on device type (e.g., gateway, firewall), average severity of occurred events, event counts per user in the organization, and event distribution over time.

Figure 3. McAfee ESM Dashboard - Overview



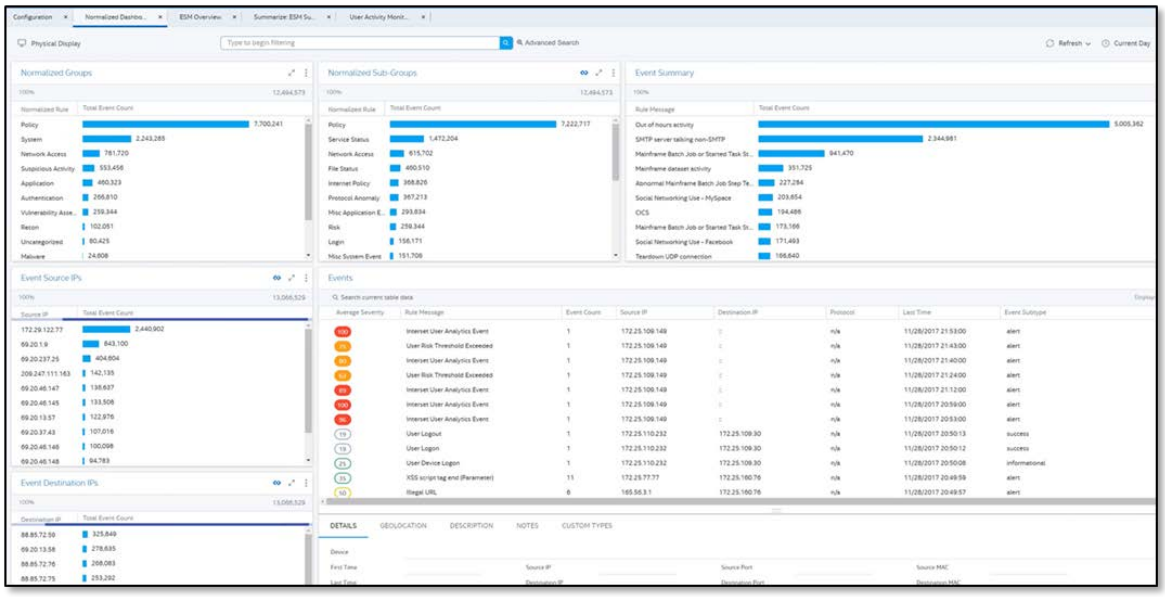
ESG Lab right-clicked on the first event under the *Average Event Severity* list to see the users that are associated with the event "Multiple Advanced Threats for a User." When we clicked on the red bar, we uncovered that "Jason Waters" was the User. We then performed a real-time drilldown of events related only to Jason Waters by right-clicking on the bar next to his name and chose ***Summarize***. After choosing a preconfigured view via another menu, we saw a Summary, as shown in Figure 4. ESG Lab noted that a security analyst can gain a comprehensive overview of events that require immediate attention for an entire organization or an individual and prioritize any investigation.

Figure 4. Real-Time Drilldown of Events Associated with 'Jason Waters'



As seen in Figure 5, McAfee ESM displayed data in normalized groups that can provide real-time context and identify anomalous events. ESM normalized all events as part of the parsing process, assigning unified categories to individual events that represent similar types of activities.

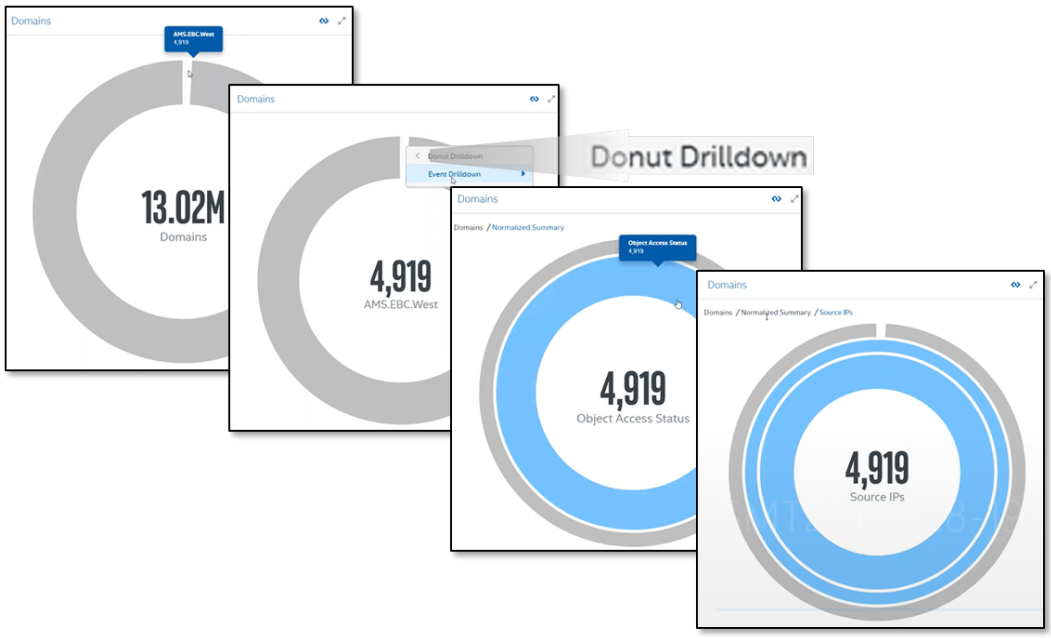
Figure 5. ESM Normalized Dashboard



ESG Lab then viewed how the ESM allows an analyst to drill down into event category details, as shown in Figure 6. We navigated to the *Domain* card and saw that 13.02M domains were noted in events gathered by the ESM. We clicked on the white sliver of the donut to uncover additional details and found that 4,919 domains were related to a region called "AMS_EBC_West." We then right-clicked on that donut to drill down to reveal a Normalized Summary of 4,919 events related to "Object Access Status." We drilled down into the donut one more time to reveal that 4,919 Source IPs are to be considered when investigating the 4,919 events in the chosen region. We noted that an analyst can perform a maximum of three drilldowns.

ESG Lab saw that an analyst can investigate specific events without navigating to other screens, maintaining context via the donut drilldowns. We viewed this as an efficient way for an analyst to acquire intelligence about events without navigating to multiple screens.

Figure 6. 'Donut' Chart Drilldown



Why This Matters

ESG asked cybersecurity professionals to name the biggest cybersecurity challenges facing their organizations. Four of the top five most-cited challenges were related to managing the security infrastructure.[2] From staffing shortages to manual processes and managing the complexity of disconnected point tools, these challenges represent necessary security activities that are both time consuming and demanding of attention to detail, distracting IT from other pressing issues.

McAfee ESM collects the torrent of data from the multitude of systems and security platforms in an organization's environment, then adds real-time context, analytics, and alerts for a more complete understanding of threats than can be afforded with any standalone system. The intuitive and responsive dashboard made it easy for ESG Lab to drill down quickly from hundreds of millions of events to specific, targeted events with just a few mouse clicks, within a few seconds. McAfee ESM enabled rapid, efficient analysis and identification of related incidents.

ESG Lab validated that McAfee ESM captures, indexes, and analyzes real-world network security information consisting of hundreds of millions of daily events from hundreds of diverse devices and systems, and provides clear, concise, real-time actionable intelligence.

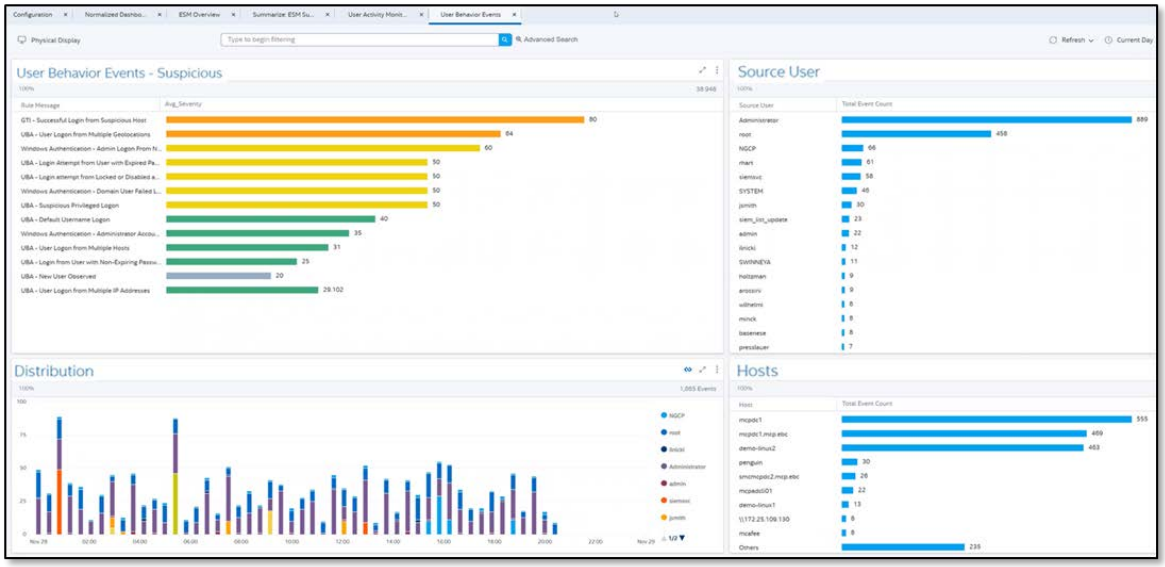
Advanced Analytics

McAfee Enterprise Security Manager provides advanced real-time and user behavior analytics for early threat detection. ESG Lab examined the performance of the system along with depth of correlation and behavior/end-user profiling.

ESG Lab Testing

First ESG Lab examined the *User Behavior Events* tab, as shown in Figure 7. This specific view detailed suspicious activity based on analysis of user behaviors and associated severity, rank order of users according to suspicious events, distribution of user events occurring over time, and rank order of events by host. ESM generated these counts based on correlated events and watchlist behaviors. Other user behavior views were available, such as behavior according to geolocation.

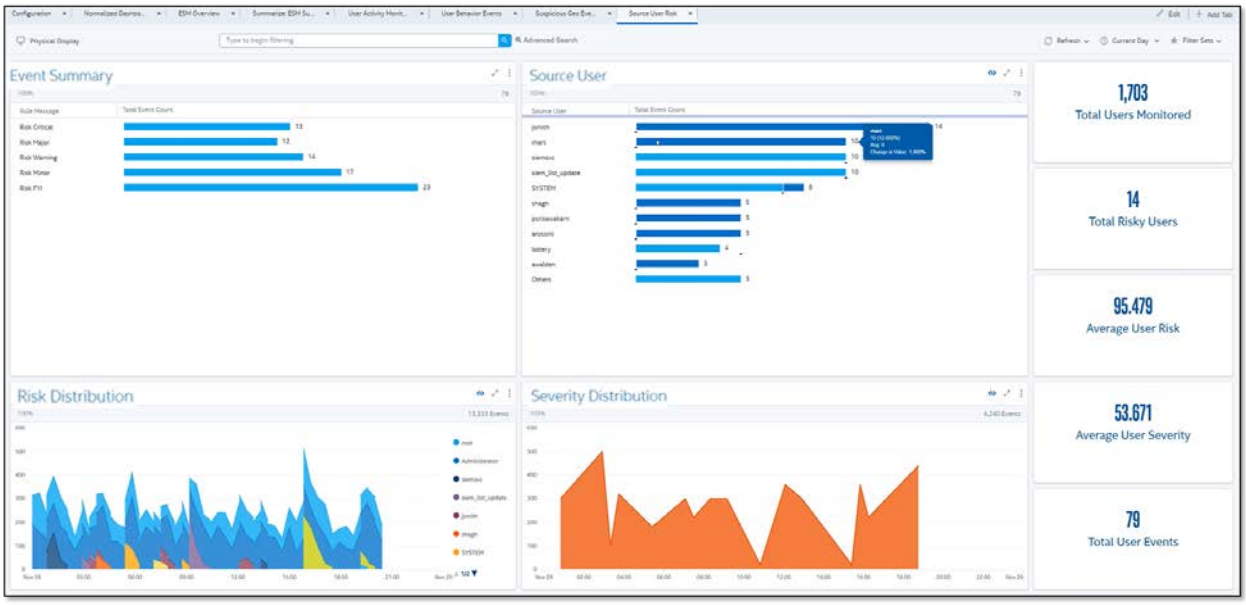
Figure 7. User Behavior Events View



[2] Source: ESG Research Report, *ESG/ISSA Research Report: The Life and Times of Cybersecurity Professionals*, November 2017.

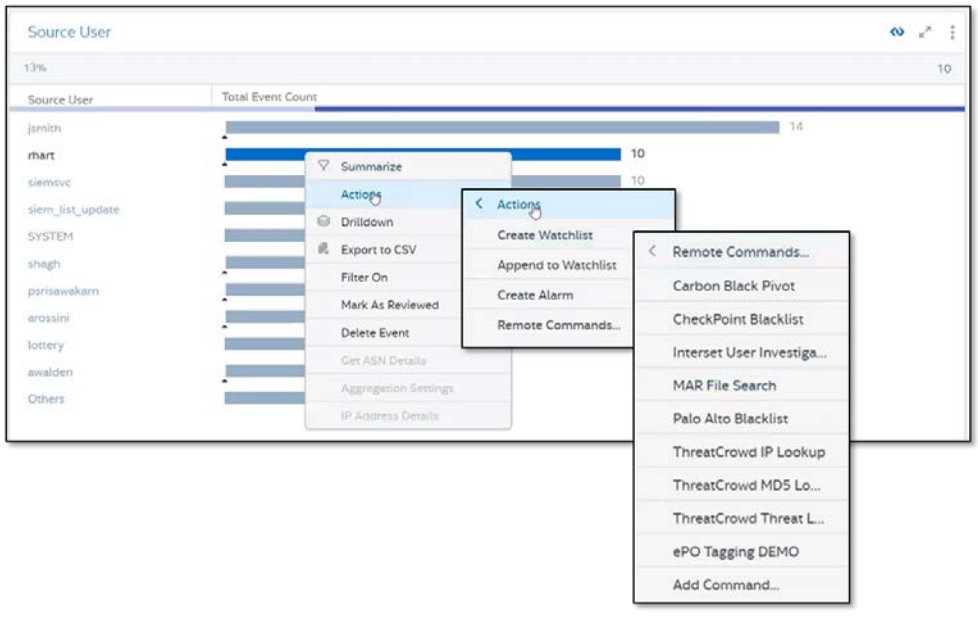
We then examined the *Source User Risk* view, a tab displayed in Figure 8. This view showed users displaying the riskiest behavior based on an internal risk allocation correlation engine. This machine learning engine determined user behavior based on patterns and standard deviation from those patterns. According to this view, we saw that an analyst can see immediately that, of the 1,703 monitored users, 14 of them are generating the riskiest behavior, with average scores of 95.479 in user risk and 53.671 in user severity. Thus, the view can inform the analyst of those users requiring the most attention in terms of investigation and remediation.

Figure 8. Source User Risk View Generated by Machine Learning Engine



ESG Lab then observed how an analyst can take immediate action to mitigate the risky behavior of a single user. Figure 9 shows how the analyst can right-click on one user, *rhart*, and choose ***Actions*** from the drop-down menu. We saw that an analyst can choose from various actions to mitigate any further risk from *rhart*, such as adding the user activity to a blacklist or performing an IP Lookup via Threatcrowd, an open source threat intelligence feed.

Figure 9. Taking Immediate Action against User's Risky Activities via Source User Risk View



Why This Matters

Comprehensive data collection and accuracy of the analysis are key capabilities to effectively provide advanced analytics. This is much more challenging than simply collecting and processing millions of events and alerts. Finding patterns, relationships, context, and insight depends on the breadth and accuracy of data capture as well as a sophisticated analytical engine to help filter out the noise and false positives so security organizations can focus on what is important.

McAfee ESM's extremely rapid correlation of such custom events enables quick and decisive identification of important events for investigation and remediation. In ESG Lab's opinion, McAfee ESM provides the real-time and historical security analytics—with correlated context—needed for organizations to confidently detect and resolve threats.

Incident Response

ESG Lab then examined how McAfee ESM provides fast response to incidents and events, paying special attention to tools, including alarm prioritization and review, cyberthreat feeds, and IOC investigations.

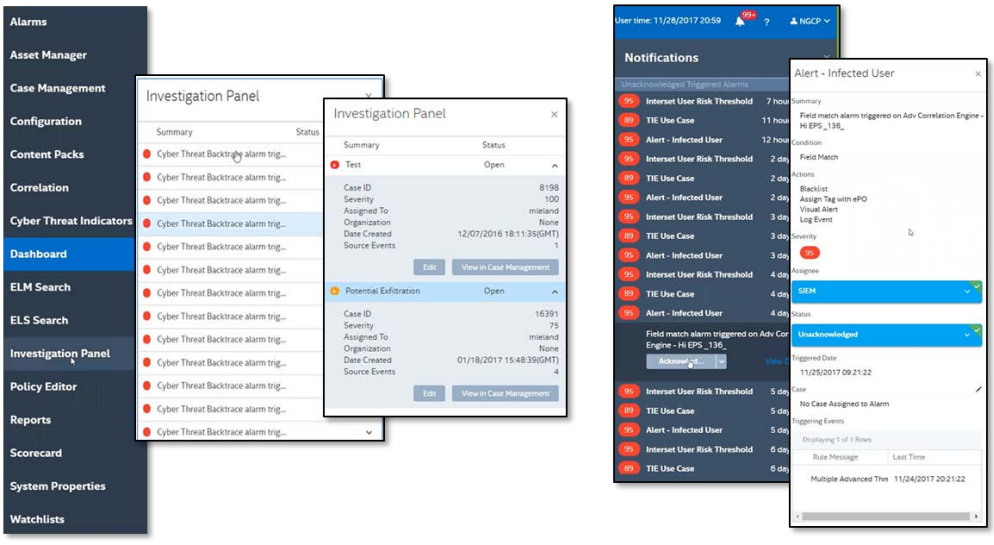
ESG Lab Testing

ESG Lab looked at McAfee ESM's ability to quickly identify alarms and manage outstanding cases for current issues. We clicked on the bell in the upper right-hand corner of the screen to view all alarms, rank-ordered by severity. The list specified triggered alarms that have yet to be acknowledged by the analyst, along with the time elapsed since ESM triggered that alarm. We then chose one alarm to view more details, specifically determining whether a user has acknowledged its presence, as well as events resulting in the trigger.

ESG Lab then observed how the ESM can help an analyst manage outstanding cases. We brought up the main menu on the left-hand side of the screen and chose Investigation Panel. The panel listed the outstanding open investigations and their statuses. We clicked on two individual cases to reveal their details, including the severity level, status, and creation date. We also saw that an analyst can click on the *View in Case Management* button to show more detail.

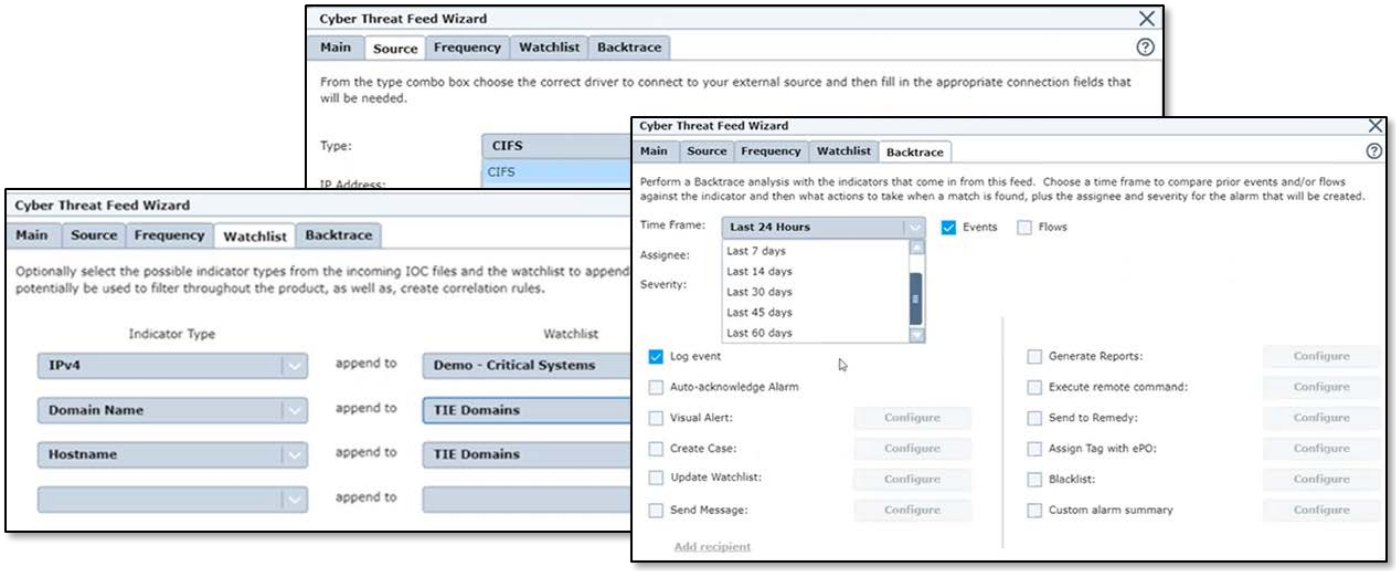
Figure 10 shows the windows that an analyst can use to manage alarms and investigations. Using these panels, ESG Lab noted that an analyst can easily find out about alarms and determine actions to remediate them quickly. As for outstanding investigations, an analyst can view this list and track those that require immediate attention (e.g., assigned open cases).

Figure 10. Alarm Management and Investigations Panel



ESG Lab then examined how an analyst can use Cyber Threat Feeds to capture IOCs to help the ESM watch out for potential attacks. In Figure 11, we proceeded to add rules that will filter IOCs. Using the *Cyber Threat Feed Wizard*, we first chose the *Source* tab from which the ESM will extract IOC artifacts. Potential sources include file uploads, third-party feeds via API and via sandbox (ATD). We then chose the *Watchlist* tab to add artifacts that can be associated with an IOC (e.g., IP address, Domain Name). We added each artifact to an existing watchlist via a drop-down menu. We then clicked on the Backtrace button to compare historic events for identifying long-term threat behavior patterns. The analyst can use past events to reveal patterns as the ESM processes IOCs, enabling faster threat identification and remediation.

Figure 11. Tracking IOCs via Cyber Threat Feeds



Why This Matters

Before, during, or after a breach, even organizations with sophisticated security environments often cannot answer the most basic questions about an incident: Who did this? How did it happen? Was a vulnerability exploited? What systems were affected? Did existing security systems miss it, and why? Did the attackers access and extract data? If so, what data? Are they still on the network? How can we be sure? The ramifications to any business are huge and the stakes are very high. Executives, the boards of directors, and shareholders will be demanding concrete answers to these fundamental questions.

McAfee ESM, integrated with detection- and prevention-based security solutions, enables an effective, in-depth defense strategy. It is designed not to replace solutions already at work, but to enhance them, providing continuous monitoring, the context they lack, and the evidence they can't provide independently, and enabling organizations to respond effectively and quickly to security incidents, threats, and breaches.

McAfee ESM demonstrated the capability to deliver context-aware visibility and situational awareness, along with the ability to drill down to specific events. This enables a security organization to discover, investigate, and manage responses to events from a single interface, which provides the tools needed to address incidents completely, taking swift, focused, confident action. By shortening the time from detection to protection, organizations can shave valuable time off their detection processes, giving them the opportunity and ability to stop threats before they become full-blown breaches.

The Bigger Truth

Everywhere you look in the IT infrastructure, there are security breaches. They can occur in smartphones, tablets, Windows desktops, databases, and application servers, and they affect large well-known companies with sophisticated IT infrastructures as well as nations. ESG research reveals that organizations that experience security incidents are impacted in multiple ways.[3] Lost productivity, extended exposure due to the time/personnel needed for remediation, and disruption of business processes, applications, and systems can be devastating to operations, company reputations, and bank accounts; and the costs may include not just resuming operations and addressing security gaps, but legal liability and regulatory fines that can be onerous burdens. This may be why strengthening cybersecurity is the most-cited (44% of respondents) business initiative driving IT spending in 2018, according to ESG research.[4]

ESG research also revealed that, when considering security analytics and operations, organizations' primary objectives include improving the ability to detect, contain, and remediate threats (34%); improving the ability to discover, prioritize, and remediate vulnerabilities (29%); improving the operationalization of intelligence (29%); and adding more intelligent analytics tools to ease staff burdens (27%).[5] Businesses need the tools to filter and analyze this torrent of data in order to identify what is really important among the millions of events and alerts.

Why are organizations monitoring, collecting, processing, and analyzing increasingly large quantities of event and incident data? Because advanced threats and sophisticated malware are circumventing existing security controls, compromising hosts, and inflicting tremendous damage. In the real world, 100% prevention is impossible with any single point solution and the numbers of devices to manage and data feeds to monitor is overwhelming. The reality is that, in practice, breaches are inevitable, as attackers only have to be successful once. Continuous monitoring of the whole environment and vigilance with security analytics solutions like next-generation SIEM can provide organizations with the visibility needed to mitigate the prevalence of attacks and prevent the spread of breaches.

McAfee ESM was designed to store, enrich, and analyze massive amounts of contextual data (hundreds of millions of data points) in near real time. Effective incident response requires delivering fast response to both simple and complex queries, with real-time and historical operations for optimizing threat investigations and forensics. ESG Lab found the McAfee ESM management console easy to use to gain insight into the overall health of the security ecosystem as well as the security of the entire network. Real-time correlation and analytics, as well as the efficient, intuitive, and easily customizable ESM dashboards, enabled ESG Lab to isolate specific incidents with specific criteria and appropriate context. The ESM interface enabled comprehensive management of security data—and more importantly, security intelligence—from a single console.

McAfee ESM leverages contextual information—vulnerability scans and identity and authentication management systems, for example—and enriches each event with context for a better understanding of how security events impact real business operations. This intelligence enables organizations to align the right data with the right people to take real-time action and make smarter decisions.

Integrating perimeter defenses and SIEM and providing a multi-layered "defense in depth" approach are no longer just nice to have; they are a necessity. McAfee ESM provides the critical functions of continuous monitoring, advanced analytics, actionable intelligence, and incident response, with high performance and intuitive ease of use. Based on our testing, ESG Lab believes that this type of end-to-end solution can effectively protect organizations against today's increasingly dangerous threats.

[3] Source: ESG Research Report, *ESG/ISSA Research Report: The Life and Times of Cybersecurity Professionals*, November 2017.
[4] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[5] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188