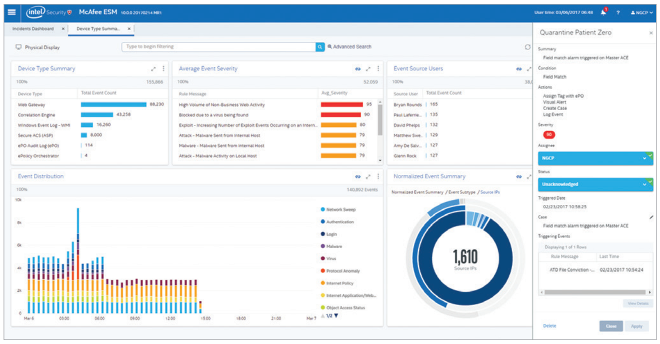
SC MEDIA ★★★★★



McAfee ESM 10.0.0 20170214 MR1

User time: 03/06/2017 06:48

Incidents Dashboard | Device Type Summa...

Physical Display | Type to begin filtering | Advanced Search

Device Type Summary (100% — 155,866)

Device Type	Total Event Count
Web Gateway	88,230
Correlation Engine	43,258
Windows Event Log - WMI	16,260
Secure ACS (ASP)	8,000
ePO Audit Log (ePO)	114
ePolicy Orchestrator	4

Average Event Severity (100% — 52,059)

Rule Message	Avg_Severity
High Volume of Non-Business Web Activity	95
Blocked due to a virus being found	90
Exploit - Increasing Number of Exploit Events Occurring on an Intern...	80
Attack - Malware Sent from Internal Host	79
Malware - Malware Sent from Internal Host	79
Attack - Malware Activity on Local Host	79

Event Source Users (100% — 38,0)

Source User	Total Event Count
Bryan Rounds	165
Paul Laferrie...	135
David Phelps	132
Matthew Swe...	129
Amy De Salv...	127
Glenn Rock	127

Quarantine Patient Zero

Summary: Field match alarm triggered on Master ACE

Condition: Field Match

Actions: Assign Tag with ePO, Visual Alert, Create Case, Log Event

Severity: 90

Assignee: NGCP

Status: Unacknowledged

Triggered Date: 02/23/2017 10:58:25

Case: Field match alarm triggered on Master ACE

Triggering Events: Displaying 1 of 1 Rows

Rule Message	Last Time
ATD File Conviction -...	02/23/2017 10:54:24

McAfee

Enterprise Security Manager (ESM)

This is another of our SC Lab Approved tools that we have been using over the past several years. For this review, we upgraded to v10 which has quite a few major improvements. The most obvious is the HTML 5 user interface. The ESM always has been a superb analyst tool, but with every new release it becomes more of a SOC tool without sacrificing the depth required by serious analysts.

SC MEDIA LAB APPROVED

In addition to the UI, the newest release uses ElasticSearch which speeds searches across large datasets significantly. The ESM always has been noted for the large number of devices, applications and operating environments from which it can take data, and this new release is no exception. However, it also interfaces directly with such McAfee applications as ePolicy Orchestrator, Advanced Threat Defense (malware), Network Security Manager (intrusion prevention), Threat Intelligence Exchange (share security data) and Active Response (search endpoint telemetry in real-time to provide targeted threat remediation). Obviously, if you are a McAfee shop, this needs to be in your kit.

The ESM uses what it calls "Receivers" as data collectors and you can distribute Receivers throughout your enterprise as needed. Log management is done by the Enterprise Log Manager (ELM). Usually these pieces are part of full deployment but they also can be deployed as a single "all-in-one" configuration as we have here in the SC Labs. That can be deployed as a virtual machine or a physical server. Log data is input by push (syslog, for example), pull (as with WMI logs) or an agent on the monitored device. Setup of monitored devices is straightforward.

In the System Properties menu, you'll also find such expected submenus as System Information, Network Settings and the like, plus new ones, such as Cyber Threat Feeds. This is unquestionably a next-generation tool, complete with advanced algorithms, big data handling and external threat feed correlation along with several nice features to make all of the other things work well, e.g., ElasticSearch.

In our deployment of the ESM in our virtual environment, we've found that it is much more efficient than earlier versions. The new UI moves things along quite smartly.

Overall, we continue to like working with this product. It really is an analyst's dream tool, but it takes a bit of learning to get the most out of it. That said, over the past decade, it has made giant strides from the lab to the SOC and we would recommend this unhesitatingly as a general purpose SIEM in the SOC. It has every feature that we can think of that might be needed for a serious SOC analyst. The little extra time spent to learn how to make it really get the best results will pay huge dividends over the long haul.

– Peter Stephenson, technology editor

DETAILS

Vendor McAfee

Product Enterprise Security Manager (ESM)

Website mcafee.com

Price $39,995 (comparable hardware pricing is $47,994).

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths This remains the top SIEM available. It is feature rich, very flexible and capable of being the "tip of the spear."

Weaknesses None.

Verdict Since this already is SC Lab Approved, we can't give it a higher rating. We like this well enough that we are extending its SC Lab Approved designation for another year. It continues to be our key analysis tool.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054 USA
www.mcafee.com
1-888-847-8766