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.

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 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

McAfee
Enterprise Security Manager (ESM)

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.