RSA SECURITY ANALYTICS

What SIEM Was Meant To Be

AT A GLANCE

- RSA Security Analytics is the lynchpin of the RSA Advanced SOC Solution
- Incident detection, investigation and response capabilities that far exceed log-centric approaches
- Achieve baseline SIEM requirements, such as compliance, and go way beyond with a tool built for security first and foremost
- Combine logs with network and endpoint data for complete visibility and better workflow

DATA SHEET

SIEM NEEDS TO EVOLVE

SIEM products have been around since the mid-1990's and have historically been a key element of a security team's monitoring function. The intent of SIEM though has been to provide:

- A single interface to gather and store security – primarily log - data. Manually searching and analyzing logs and security event data across multiple sources can be a tedious process.
- A processing engine that analyzes and prioritizes incidents across various sources. Security tools and other infrastructure components create a vast number of log entries and alerts. SIEM systems are meant to be able to isolate the signal from the noise and prioritize those issues that are the most pressing.
- The cornerstone of the incident detection and response function. Analysts need a place to manage their queues to provide a workbench for triage, investigation and reporting. Security analysts need to be able to manage rules and reports that they need to run. Managers need to know what the major open issues are and how well their teams are performing. SIEM systems are meant to be this workbench for security teams.

Most SIEM solutions have struggled to provide the scale, detective, investigative and analytic capability and workflow to deliver against the above needs. Thus many security teams have made huge investments into SIEM systems, but they aren't able to spot today's attacks, and are far too slow in the event of an incident to provide useful, timely information to the investigative team.

RSA Security Analytics helps to solve these problems by allowing you to:

- Gain complete **visibility** to identify and investigate attacks
- Detect and **analyze** even the most advanced of attacks before they can impact the business
- Take targeted **action** on the most important incidents

BETTER VISIBILITY, ANALYSIS AND WORKFLOW

Use RSA's flexible, modular approach allows you to deploy the solution incrementally to solve your own particular problem, whether that be complementing your existing SIEM, or replacing it altogether. RSA Security Analytics provides you with:

The only solution that has visibility across logs (both cloud and on premise), network packet, NetFlow and endpoint data in single infrastructure.

This broad view gives analysts the ability to see everything happening in their environment, not just what was logged.   RSA Security Analytics also offers

KEY BENEFITS

- Detect and analyze even the most advanced of attacks before they can impact the business
- Investigate, prioritize, and remediate incidents with unprecedented precision and speed.
- Unleash the potential of the existing security team to gain the upper hand on attackers

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at

flexible storage options to keep this wide variety of data, including basic archiving to store long term compliance data at low cost.

Correlation across log, network, and endpoint data to detect issues other SIEMs miss.

RSA Security Analytics incorporates a unique correlation engine, Event Stream Analysis, which not only looks for potentially malicious issues across logs and NetFlow, but also correlates data across full network packets and endpoints, where much of today's advanced threats tend to more readily manifest themselves. Another threat detection capability is the ability to harness the power of Big Data and data science techniques to spot attacks that would have otherwise gone unnoticed. Attacks can hide in a sea of data due to the difficulty of having to process and deeply analyze the data collectedThis means instead of just looking for obvious threats like password guessing attacks as you do with a SIEM, you're able to spot subtler threats like suspicious files being downloaded, or internal hosts "beaconing" out to a "Command and Control" site.

Out-of-the-box reporting, intelligence feeds and rules to start finding incidents immediately.

Packaged rules, parsers and data models are automatically updated and distributed to RSA Security Analytics, meaning analysts have a robust set of content that is constantly being refreshed. This includes over 400 log and network parsers and over 275 correlation rules as well as over 90 report templates covering dozens major regulatory requirements like SOX, HIPAA & PCI, eliminating the tedium from generating compliance reports.

Intuitive tools for incident triage, rapid investigation and compliance reporting.

RSA Security Analytics provides a workbench to triage alerts and incidents, plus an award-winning interface designed specifically for security investigations. In addition, since Security Analytics has access to endpoint and packet data as well as NetFlow and log data, analysts have the ability to rapidly investigate down to the most granular detail to understand exactly what is happening and what to do about it.

The only platform for managing your Security Operations program from end-to-end.

RSA Security Analytics has built in incident triage capabilities and a wide array of dashboards for analysts and managers alike to get instant feedback on specific issues or the overall state of their Security Operations environment. In addition, Security Analytics is part of a larger solution, including RSA Security Operations (SecOps) Management, which lets security teams manage their SOC processes from end to end. This lets customers efficiently define and manage incident response procedures, model what to do in the event of a breach, as well as manage day-to-day events like shift handover. This module also enables you to interoperate with the wider RSA Archer GRC platform, which allows organizations to manage and streamline IT and Enterprise Policy, Risk and Compliance programs. For further enhancement RSA offers Advanced Cyber Defense professional services and training that helps organizations improve their security maturity, and prepare for and respond to security incidents and to evolve with the

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.