RSA SECURITY ANALYTICS

Overview

AT A GLANCE

- RSA Security Analytics is the lynchpin of the RSA Advanced SOC Solution
- Augment existing SIEMs with complete visibility and rapid investigations through network forensics
- Focus on the most critical tasks with complete end-to-end incident management in minutes, not hours
- Achieve baseline SIEM requirements, such as compliance, and go way beyond with a tool built for security first and foremost

SECURITY IS EVOLVING

Security teams constantly need to adapt to stay in front of attackers and the latest threats, but over the past few years this has become much more difficult. Attackers continue to advance and use sophisticated and highly targeted techniques to infiltrate organizations. They spend significant resources performing reconnaissance to learn about organizations and develop techniques specifically to bypass the security system that in use. The result is that:

- Security teams are missing attacks that significantly impact their organization.
- Security teams don't have the size or expertise to keep up with attacks.
- Current installed monitoring tools such as SIEM solutions are failing to meet the organization's needs.

Flexible, modular approach

Most security teams seldom have the budget, bandwidth or desire to "rip and replace" their existing security tools that are providing some value. As security organizations evolve their need to improve their ability to detect and respond to security incidents, the modular architecture of RSA Security Analytics allows them to solve specific problems and integrate with their existing environment and then expand or evolve.

RSA Security Analytics provides the security team a flexible, modular approach to meet several use cases:

Complete visibility and rapid investigations through network forensics. RSA Security Analytics enables security teams to focus on the most important incidents, and rapidly investigate them using network data from full network packet capture and NetFlow, as well as endpoint data and logs. This lets security teams understand the true nature, scope, and impact of an incident allowing them to take targeted action.

Analytic capabilities way beyond SIEM and its log-centric approach.

RSA Security Analytics gives security teams the ability to collect and use endpoint and network data, in addition to logs, to spot incidents that logs alone can't. RSA Security Analytics also provides out–of-the-box reporting, intelligence and rules to let security teams start finding incidents immediately without weeks of configuration and customization.

Keep current with compliance mandates with built-in compliance templates. RSA Security Analytics has over 90 report templates covering dozens of major regulatory requirements like SOX, HIPAA & PCI, eliminating the tedium from generating compliance reports.

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 get the upper hand on attackers
- Evolve existing SIEMs and monitoring toolset with better visibility and workflow

GAIN COMPLETE VISIBILITY – FROM THE ENDPOINT TO THE CLOUD

RSA Security Analytics provides a single monitoring platform to gain the visibility organizations need, combining logs (both from cloud environments and on premise), network (both packets and NetFlow) and endpoint visibility to see what is happening across the enterprise. This makes it easier to view the environment in totality, rather than in piecemeal, making the analyst more efficient with a much greater chance of detecting attacks. Since all these capabilities are in a single tool, there is also less deployment risk due to incompatibility and cross-product integration.

Capture time data enrichment

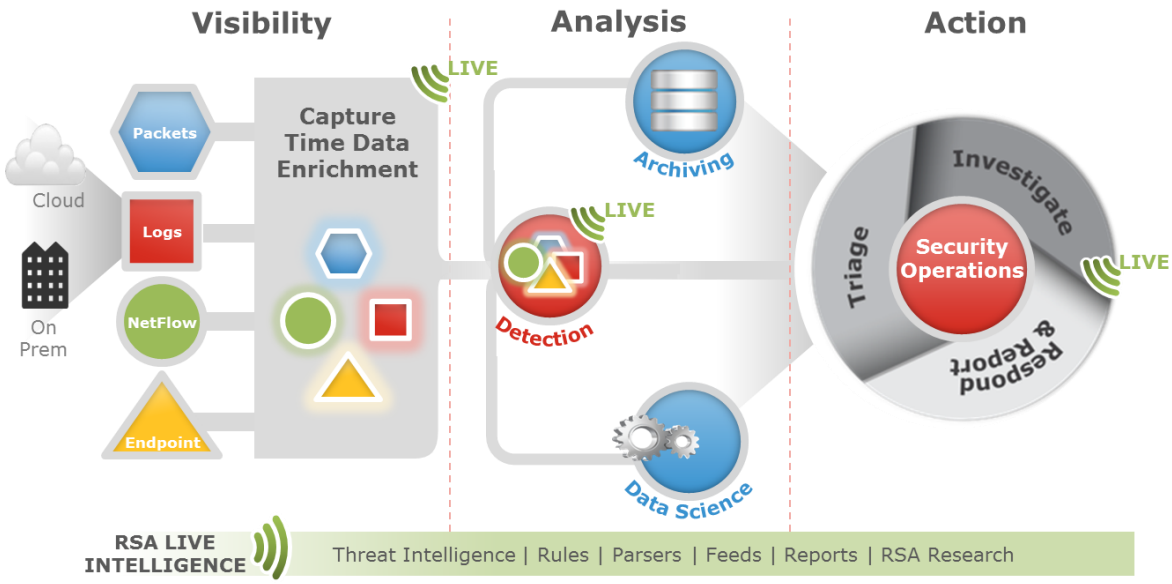
RSA Security Analytics inspects and performs deep capture time data enrichment making it much faster and more valuable for analysis in the midst of an investigation. This includes tagging threat indicators as well as interesting characteristics about the log or network session that could be useful as part of an alert, report or investigation. With more security clues available, an analyst can quickly detect, triage, and investigate issues.

Integrate threat intelligence via RSA Live

To get more value out of threat intelligence RSA Security Analytics automatically delivers intelligence to customers via RSA Live, enabling them to detect the latest threats immediately. RSA Live converts threat intelligence it into hundreds of parsers and correlation rules as well as intelligence feeds. The intelligence is then fused with customer data within RSA Security Analytics. This means that users are able to take advantage of what others have already found and know what to look for. They can then apply the latest threat intelligence in real-time to incoming or to historical data.

Scale Linearly

The unique architecture allows organizations to scale linearly and still collect and analyze large amounts of data. The federated infrastructure allows organizations to scale, while still maintaining the ability to analyze and query seamlessly across the system at top speeds.



RSA Security Analytics Architecture

DETECT AND ANALYZE THE MOST ADVANCED ATTACKS BEFORE THEY MAKE IMPACT

Correlation across multiple data sources

RSA Security Analytics uses all the data it collects to detect issues, not just logs. It discovers attacks as they're happening by correlating logs, packets, NetFlow and endpoint data together in a single platform – giving a much wider set of threat indicators to look for. This means that RSA Security Analytics can detect and investigate attacks in real-time that other systems can't – like detecting a PDF containing an executable, followed by encrypted traffic to a blacklisted country.

Big Data and data science

Analysts have 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 collected. RSA Security Analytics uses data science techniques to analyze these large data sets over extended periods of time to spot issues like "beaconing hosts" or activity with suspicious Web domains. This gives analysts more tools to "hunt" for attacks without having to rely as heavily on in-house data science expertise.

TAKE TARGETED ACTION ON THE MOST IMPORTANT INCIDENTS

Investigate down to finest details

RSA Security Analytics' gives analysts the ability to investigate incidents rapidly down to the most granular detail to understand exactly what is happening and what to do about it. Analysts can ask any question of their data and get detailed contextual answers back. Investigations are faster, more efficient and more effective than ever before,, which reduces incident response time and decreases the attacker's free time in the environment.

Prioritized and unified analyst workflow

Prioritized analyst workflow, provided by the native incident management capability, gives analysts the ability to focus on their most critical tasks and complete end-to-end incident management in minutes, not hours. This gives teams the ability to do more with same amount of people by spending their time on the incidents that have the biggest risk to their organization and completing them as fast as possible. It also provides a single tool to perform actions currently within a disparate set of interfaces.

Integrate SOC best practices

Customers who leverage RSA Security Analytics can connect with the rest of RSA's other SOC enabling tools and services. This includes RSA Security Operations Management for broader SOC orchestration & management, and professional services such as the RSA Advanced Cyber Defense (ACD) consulting and education services (training) to give organizations the process and tools they need to operate with an incredible level of precision. This means that SOC teams can leverage best practices to get the most out of their people and process, and not just throw more technology at the problem. It also gives SOC managers the ability to get more value out of the tools they have already purchased by using them to the best of their ability

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 www.emc.com/rsa.

RSA