RSA ADVANCED SECURITY OPERATIONS CENTER SOLUTION

Visibility. Analysis. Action

AT A GLANCE

- Incident detection with complete visibility.
- Deep investigations and prioritized incident triage.
- Endpoint threat detection and analysis.
- IR, breach response, and SOC program management.
- Cyber defense consulting and Incident Response services.
- SOC training from security practitioners

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime.

With over 30 years of industry expertise, RSA believes that our portfolio of products, services, and intelligence is better able to address today's security challenges than any other company in the industry.

SECURITY HAS BECOME MORE DIFFICULT

Security teams need to evolve to stay in front of attackers and the latest threats, but in recent years this has become much more difficult. Attackers continue to advance and use sophisticated techniques to infiltrate organizations. Attackers spend significant resources performing reconnaissance to learn about organizations and develop techniques specifically designed to bypass the security tools being used. The result is that:

- **Security teams are missing attacks that significantly impact their organization.** This leads to theft of sensitive information, as well as to the disruption of business operations. The attackers are often persistent and very focused, which means that detection is an ongoing challenge as attackers modify and evolve their attack and obfuscation techniques. Traditional security controls struggle with the unique, targeted threats that can cause the most damage to organizations.
- **Security teams don't have the size or expertise to keep up with attacks.** Security operations teams struggle to function with the speed and efficiency needed to accurately prioritize incidents, investigate and determine how to take action. Investigations are slow, often taking hours, days, and even weeks, and rarely provide the detail needed to really understand what is happening. This allows attackers to maintain a tactical advantage. Due to staff shortages, security teams often pursue only the most obvious incidents, while incidents that "fly under the radar" get ignored or deprioritized.
- **Current installed monitoring solutions are failing to meet business needs.** Many security teams have invested a large amount of time and money in monitoring solutions such as SIEMs with the expectation that they would provide them with the visibility to identify and prioritize attacks and protect their organization. Most security teams that have experienced breaches were using a SIEM tool, only to have found the solution lacking. Since these solutions are primarily log-centric, and logs only contain a fraction of the information needed to distinguish attacks or malicious activity, they only deliver a fraction of the capability needed in the detection or investigation of an incident. Faced with this reality, organizations need either to replace their existing monitoring solution, augment what they have with additional visibility, investigation, and workflow capabilities, or risk being unable to adequately protect their business.

USE CASES

RSA's flexible, integrated, yet modular architecture lets organizations choose the full solution or augment existing tools. The RSA solution allows organization to address multiple use cases at once or choose to the use case they want to focus on. Common use cases include:

- Enhance or replace an existing SIEM's capabilities with better visibility, analysis and workflow.
- Evolve from a log-centric view with network packet capture to enable deep network forensics and detection.
- Augment traditional AV with advanced endpoint malware detection.

To integrate with other tools in the SOC, users can create their own custom security solutions by using Security Analytics' open API. This enables other tools to integrate with the Security Analytics platform and extends the value of their existing investments.

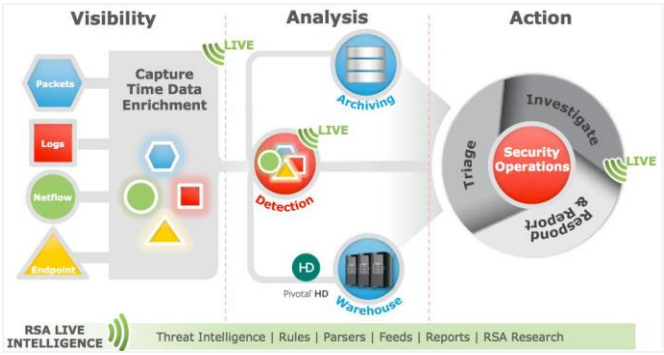
KEY BENEFITS

- 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 your existing security team to get the upper hand on attackers
- Evolve existing SIEMs and monitoring toolset with better visibility and workflow.

VISIBILITY, ANALYSIS AND ACTION

The RSA Advanced SOC Solution achieves these goals by providing Security Operations teams with tools and services that give them the ability to:

- **Gain complete visibility to identify and investigate attacks.** The RSA Advanced SOC Solution lets security teams eliminate blind spots with visibility across logs, networks, and endpoints. At the time of collection, every network, packet session and log event is inspected for threat indicators. Additionally, RSA helps manage the process of gathering business and IT data, which can provide valuable context in determining the most relevant information.
- **Detect and analyze even the most advanced attacks before they can impact the business.** RSA Advanced SOC Solution enables security teams to discover attacks missed by traditional SIEMs and signature-based tools by correlating network packets, NetFlow, logs, and endpoint information, and identify malware missed by conventional AV. The RSA solution also provides out–of-the-box reporting, intelligence and rules to let security teams start finding incidents immediately without weeks of configuration.
- **Take targeted action on the most important incidents.** The RSA Advanced SOC Solution provides security analysts with the tools to instantly pivot from incidents into deep endpoint and network packet detail to perform incident forensics and understand the true nature and scope of the issue. Also, with prioritized investigations and analyst workflows, the RSA Advanced SOC Solution maximizes your team's potential by implementing RSA's best practice-based security operations management tools and training.



RSA ADVANCED SECURITY OPERATIONS CENTER (SOC) SOLUTION COMPONENTS:

RSA Security Analytics is a security monitoring solution that helps security analysts discover, investigate, and remediate advanced threats that are often missed by other security tools. RSA Security Analytics combines full network session reconstruction, centralized log and NetFlow collection, endpoint integration and external threat intelligence to help security teams to be more effective and efficient in protecting their organizations' digital assets.

RSA ECAT (Enterprise Compromise Assessment Tool) is an endpoint threat detection solution that detects malware and other threats, highlights suspicious activity for investigation and instantly determines the scope of a compromise to help security teams stop advanced threats faster. RSA ECAT monitors endpoints, both clients and servers, and alerts on suspicious activity in real time, and leverages unique scanning techniques that provide the deep endpoint visibility and anomaly detection security teams need to detect and respond to threats.

RSA Security Operations Management (SecOps) enables enterprises to orchestrate people, processes, and technology to effectively respond to security incidents. Architected and designed by benchmarking world-class security operations centers, the solution is SOC process and persona focused. SecOps enables organizations to manage the overall incident response, breach response, and SOC program so that it is aligned to business risk.

RSA Advanced Cyber Defense (ACD) Practice is a set of professional services that helps organizations improve their security maturity and posture, and prepare for and respond to security incidents and to evolve with the threat environment. These services also help organizations develop strategies and tactics for building and improving their security operations programs, with a specific focus on the design and optimization of security operation centers (SOCs) or incident response teams as well as the effective use of threat intelligence.

RSA Advanced Cyber Defense Training & Certification is a set of education courses that provides a comprehensive learning path for security analysts. The training focuses on teaching proven methodologies for operating and managing a CIRC/SOC and includes hands-on labs designed around real-world use cases often requiring effective teamwork. The courses, delivered by highly experienced RSA security practitioners, include criteria built for incident analysts, incident handlers and forensic analysts, as well as training for malware and threat analysts.