RSA ADVANCED SECURITY OPERATIONS CENTER SOLUTION

Pervasive Visibility, Rapid Detection, Effective Response

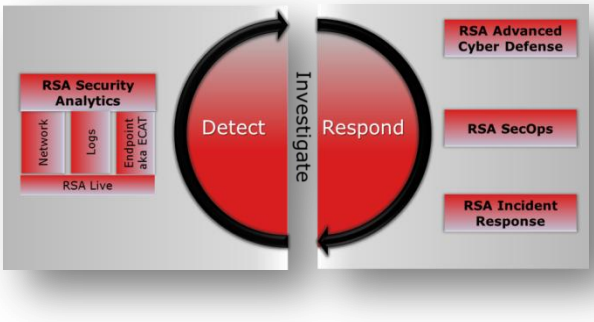
OVERVIEW

One can hardly pick up a newspaper or turn on the news without hearing about the latest security breaches. The Verizon 2015 Data Breach Investigations Report, as well as many other reports, highlights the fact that attackers are regularly outpacing the defenders. In fact, in the Verizon report, the attackers generally took days or less to compromise an organization and the defenders generally took much longer to discover those same attacks. The bottom line is that the attackers are generally winning.

Why are attackers so successful? There are several reasons: Attackers are becoming more sophisticated and targeted, they have larger attack surfaces to exploit and organizations' existing security controls are failing.

Against this backdrop, organizations need to take their security incident detection, investigation and response capabilities or their Security Operations Centers (SOCs) to the next level. There are three areas of focus to most effectively improve these capabilities: people, process and technology.

The RSA Advanced SOC Solution provides the foundation with pervasive visibility, enabling improved detection, investigation and response to security incidents.



The RSA Advanced SOC solution consists of individual technologies and services solutions that are integrated to provide a more comprehensive solution.

- **RSA Security Analytics** provides security visibility into your infrastructure from on-premise to public cloud services by ingesting in real-time logs, network packets and NetFlow data and analyzing this data using event stream analysis and behavior analysis models to detect and recognize threats before the adversary can cause damage.
- **RSA Enterprise Compromise Assessment Tool (ECAT)** provides visibility into your endpoints at the user and kernel level to flag anomalous activity, provide machine/endpoint suspect scores and block/quarantine the process.
- **RSA Security Operations Management (SecOps)** provides a solution to help better prioritize, investigate and respond to security incidents by automating and orchestrating your people, process and technology in a repeatable way.
- **RSA Advanced Cyber Defense Practice** provides services to assess and develop your SOC strategy, readiness and resilience.
- **RSA Incident Response (IR) Practice** provides services to help organizations detect and investigate incidents and breaches in order to identify root causes and develop containment and remediation plans.

No matter where your organization is with respect to your security operations capabilities, you can leverage the RSA Advanced SOC Solution and take your organization to the next level to better detect, investigate and respond to security incidents.

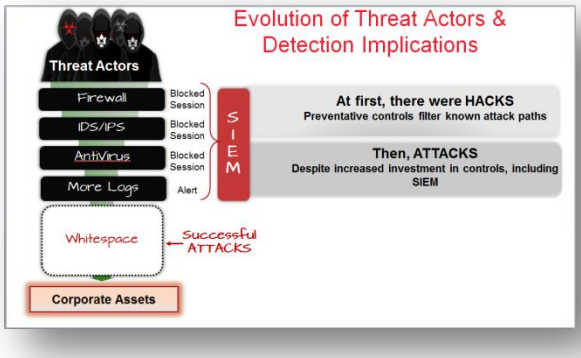
CURRENT SITUATION

Threat actors are persistent and are leveraging open source methodologies to gain access and compromise organizations. It is simple and there is tremendous return on investment for attackers to collaborate and use previously engineered exploits. The open source methodologies are being used by cyber criminals, nation states and hacktivists for financial gains and to gain access to intellectual property (IP) or personally identified information (PII).

Tools, Techniques and Procedures (TTPs) are the ways the attackers work to target, exploit and compromise an organization. In recent years, attacker TTPs have become more sophisticated, mimicking normal user and enterprise behavior, and undetectable by preventative,

perimeter-based security controls. For example, phishing attacks typically use covert channels to deliver malware to victims, making it difficult to spot delivery of a malicious payload.

Organizations are at a crossroads right now, having invested in perimeter-based, preventative controls and log-centric Security Incident and Event Management (SIEM) systems. Attackers are getting past the preventative controls and are going undetected by the SIEM by using valid user credentials, trusted access paths and new exploits that look like normal user behavior. Traditional perimeter-based security and SIEMs are not detecting the sophisticated attacker TTPs. As show in the diagram below, there is a "white space" where attackers are successful with their attack campaigns.



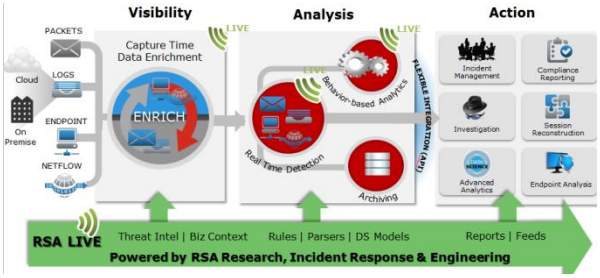
RSA SECURITY ANALYTICS

The first step in detecting and recognizing sophisticated attacks is to have complete, pervasive visibility with real-time behavior analytics. Visibility needs to be across:

- Data Sources – Full Packet Capture, NetFlow and Logs
- Threat Vectors – Endpoint, Network and Cloud

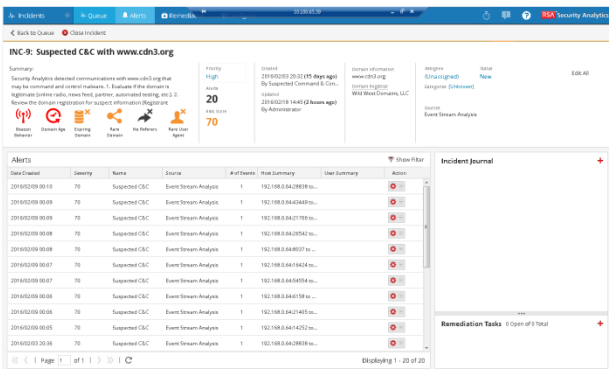
RSA Security Analytics provides pervasive visibility across data sources and threat vectors, enriching the raw data with security context at time of capture and making it valuable for security analysts during detection and investigation of security incidents. Enrichment content is provided by RSA Live. RSA Live is the platform which delivers threat intelligence, business context and out-of-the-box content for parsing data sources, defining alert rules and reporting. Customers can get quick time to value by leveraging what others have already found with RSA Live.

Event Stream Analysis (ESA) is the analytics engine for RSA Security Analytics. It correlates across data sources to detect and recognize sophisticated attacks before the attacker achieves their objective. By providing behavior analytics models, ESA is able to rapidly spot and understand attack behaviors without advanced knowledge of the attack or reliance on signatures, rules, or analyst tuning. For example, ESA can recognize sophisticated threat actors utilizing Command and Control (C2) well in advance of exfiltration of data by detecting anomalies in behavior of domains.



RSA Security Analytics is a comprehensive solution that is purpose built for detecting and investigating security incidents. Once an attack is discovered in a customer environment, RSA Security Analytics can be leveraged to reconstruct sessions, enhance investigations with context from RSA ECAT and other sources to put an effective remediation plan in place. RSA Security Analytics goes above and beyond a traditional SIEM solution. While a SIEM solution is focused on fast ingest and correlation of logs, RSA Security Analytics provides pervasive visibility and analytics across multiple data sources and threat vectors to detect sophisticated attacks. Traditional SIEM vendors are focused on use cases as compliance or IT operations, while RSA Security Analytics is focused on detecting and investigating advanced security threats.

RSA Security Analytics automates threat detection with its foundational capabilities.



For example, a series of attacker actions and a combination of anomalous activities by users and entities could be leading indicators of C2 communications which will require further investigation and counterstrike to stop the attacker.

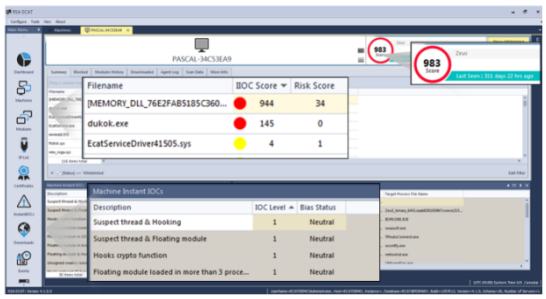
By having access to the right data, profiling attacker TTPs and detecting anomalies utilizing behavior analytics, RSA Security Analytics automates threat detection.

RSA ECAT

Endpoints such as Windows and Mac devices – servers and laptop/desktops – are threat vectors that attackers exploit by installing malware, gaining privileged access and exfiltrating sensitive data. It is imperative that organizations have visibility into the endpoints to detect threats that go undetected by traditional signature based solutions.

RSA ECAT provides endpoint visibility into attacker exploits and is fully integrated with RSA Security Analytics. When RSA ECAT detects suspicious activity or anomalous endpoint behavior, alerts/events and critical endpoint data is sent to RSA Security Analytics for correlation and visibility into endpoints. Conversely, during security incident investigations, analysts can contextually pivot back and forth between RSA Security Analytics and RSA ECAT to reduce the amount of time spent on forensic analysis.

RSA ECAT is a purpose built solution to identify endpoints that are at high risk of being compromised. The risk score of an endpoint is determined by a combination of machine and process behaviors on the endpoint. Risk score is calculated using data and analysis from threat intelligence feeds, behavior of network, process and file anomalies against indicators of compromise, destination IP information and others.

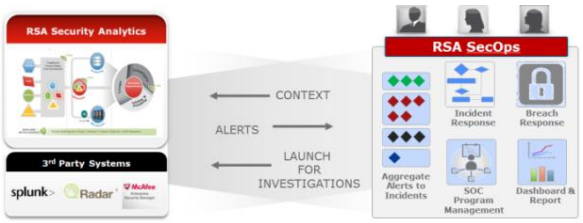


If an endpoint is flagged as having a high risk score, it is suspicious and potentially could be compromised by an attacker and will require further investigation by the security analyst.

RSA SECOPS

A Security Operations Center (SOC) is comprised of people, process and technology. The orchestration of people, process and technology increases the effectiveness of the overall SOC program. Investing in technology and considering how the three aspects of the SOC work together is an effective strategy. Orchestration and framework can increase the return on investment and maximize the value of resources in a SOC implementation.

RSA Security Operations Management (SecOps) provides the orchestration and framework for the SOC. It integrates with RSA Security Analytics, RSA ECAT and other third party security monitoring systems, aggregating events/alerts/incidents and managing the overall incident response workflow.



The workflow and capturing of incident information is aligned with industry best standards such as NIST, US-CERT, SANS and VERIS. RSA SecOps caters to the multiple personas within the SOC from the analysts, incident coordinators, SOC manager and CISO providing a view on the overall effectiveness of the SOC program. By leveraging the Incident Response, Breach Response and SOC Program Management capabilities of RSA SecOps, an organization can guarantee that the overall security incident response functionality is being managed as an effective, predictable and consistent process.

RSA ADVANCED CYBER DEFENSE PRACTICE

The RSA Advanced Cyber Defense 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 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 SOCs or incident response teams as well as the effective use of threat intelligence.

RSA INCIDENT RESPONSE

The RSA Incident Response Practice is a team of experts focused on helping customers investigate, respond and recover from a security incident or a breach. The team consists of an experienced, world-class staff of incident response practitioners leveraging battle-tested processes and specialized technology that can limit the damage when a security incident is escalated to a breach.

RSA IR services can be leveraged multiple ways from detection and response to retainer.

INDUSTRY VIEWPOINTS

Recently, industry pundits and analysts have published research and articles aligning with the RSA Advanced SOC Platform strategy. These articles and research highlight the capabilities required to implement an effective security incident detection, investigation and response program.

These articles and research mention the following:

- The Network World Incident Response "Fab Five" article – Required capabilities for an incident detection response program are:
    1. Network Forensics
    2. Host Forensics
    3. Threat Intelligence
    4. User, Behavior Monitoring
    5. Process Automation
- Forrester: Security Analytics is the Cornerstone Of Modern Detection and Response – Recommendations for Incident Response:
    1. Must have security analytics platform
    2. Must have comprehensive view of the network
    3. Must be able to detect data exfiltration
    4. Must be able to detect the unknown
    5. Must have dedicated FTEs for incident response functionality
- The Gartner Technology Overview for MSSP Advanced Threat Detection Defense (April 2015) states:
    1. Must perform traffic analysis and forensics
    2. Need visibility to endpoint behavior and endpoint forensics

RSA ADVANTAGE

RSA Advanced SOC is a comprehensive set of solutions and services that improve the overall organizational effectiveness of the security incident detection, investigation and response process.

From a solution perspective, RSA Security Analytics, RSA ECAT and RSA SecOps are fully integrated and can also integrate with third party security monitoring systems to provide comprehensive visibility, detect behavioral anomalies from endpoint to cloud and investigate and reconstruct attacker TTPs.

From a service perspective, RSA Advanced Cyber Defense services can proactively help an organization assess the gaps in their security operations program and make recommendations to close the gaps from a people, process and technology perspective. RSA IR services can be leveraged when additional help is needed to investigate and respond to security incidents.

RSA is one of few vendors that has the expertise and breadth of solutions and services to take an organization's incident response program to the next level.

The RSA Advanced SOC solution will provide immediate benefits to your organization if you are dealing with the

following concerns:

- How well prepared do you believe your organization is for an attack and can you investigate in a timely manner?
- How do you identify which assets are being compromised and what type of data is involved?
- What is your strategy for effective incident response and are you able to prove effectiveness to the C-levels?
- Are you sufficiently skilled and staffed to detect and respond to sophisticated attacks?