CHANGING THE SECURITY MONITORING STATUS QUO
Solving SIEM problems with RSA Security Analytics

RSA Security Analytics is a new way of looking at SIEM
Brings together traditional SIEM, Network Security Monitoring, Big Data Management & Analytics
Next generation unified platform for:
• Security monitoring
• Incident investigations
• Compliance reporting

TRADITIONAL SIEMS ARE SHOWING THEIR AGE
Security Information and Event Management (SIEM) tools have been a staple tool of security analysts and Security Operations Centers for over ten years. They have been essential in satisfying log related compliance requirements, correlating and prioritizing alerts, and making diverse and distributed system logs centrally available to security analysts to speed up incident investigations. Security teams generally have had considerable success implementing SIEMs to gain visibility where they previously had none, and to automate the previously highly manual process of generating compliance reports.

However, traditional SIEMs have limitations, and many security teams have become frustrated when they try to get more value, particularly security value, from their current SIEM solutions. There are multiple reasons for this:

• Today’s threats are much more multifaceted and more dynamic and stealthy than in the past. Much more advanced tools and techniques are now needed to detect and investigate them
• The most dangerous attacks, almost by definition, have never been seen before – that means exclusively looking for “known bad” sequences of events won't work.
• The status quo approach of collecting more and more logs from more and more sources won't help in detecting and responding to advanced threats. Logs are inherently limited in the level of security visibility that they provide.

SIEM tools need Innovation
To remain relevant to security analysts, SIEM tools need to be able to detect today’s threats. This means being able to detect and investigate the most effective current attack techniques, including:

• Lateral movement of threats across an organization’s network. Today’s threats often use general user workstations to gain a foothold in the organization rather than doing so on heavily monitored, critical systems which would create log events. Attackers use these workstations to gain information about more privileged users and systems, such as IT administrators or highly privileged employees. Since SIEMs are not focused on monitoring these non-critical systems, they are ineffective against threats that use this approach.
• Covert characteristics of attack tactics, techniques & procedures. Modern threats often make themselves difficult to detect by masquerading as innocent traffic – like standard web traffic - or by hiding zero-day malware payloads in common files like pdfs or jogs. These techniques are generally not recorded in systems logs or in NetFlow and therefore will easily evade current SIEM solutions which depend on those data sources.

• Exfiltration or sabotage of critical data. In the event of an attack, to respond appropriately security analysts must be able to determine the impact of the attack, and be able to see exactly the information that the attacker stole.

Today’s IT environments are much more complex than they were just a few years ago. They are larger, more diverse and continually use new technologies to build and deploy applications. Security monitoring tools need to be able to scale to cope with the today’s data realities, namely:

• The volume and variety of data that need to be captured has increased exponentially. Although logs are still highly useful for an effective compliance and security monitoring program, it is no longer sufficient to rely solely on log information to understand what is going on in the environment. In addition to capturing logs we also need much more detailed information and context about the users or systems that are being monitored.

• Navigating larger and vastly more diverse datasets requires purpose built security analytic tools to provide fast, accurate and unified support of security detection and investigations, including alert prioritization and response, report generation, incident investigation, and malware analysis.

In a breach situation, the time taken to respond is critical. Executives and IT personnel alike need answers to very specific questions to determine the right course of action. They need fast, accurate and detailed information – and today’s SIEMs often fall short – since analysts often cannot get the response times they need out of these systems.

RSA SECURITY ANALYTICS PROVIDES A DIFFERENT APPROACH

RSA Security Analytics is the security solution that enables comprehensive security monitoring, incident detection and investigation, long term archiving and analytics, Big Data analytics, malware analytics, and compliance reporting via a unified, browser-based interface. It enables security analysts to be more effective and efficient in their job of protecting the organization’s digital assets and IT systems. RSA Security Analytics provides:

• A single platform for capturing and analyzing large amounts of log data alongside full network sessions and other data

• Up-to-the-minute threat intelligence, including rules, views, parsers, reports and watchlists, automatically distributed to customer installations

• Capture time data enrichment providing efficient indexing, storage, search-ability, and indications of compromise

• Big Data architecture for archiving and analysis of long term security data, delivering high performance and scalability.
Compliance reporting through its data management infrastructure incorporating both data parsing and full text search.

**RSA Security Analytics addresses common SIEM use cases better than traditional SIEM tools**

Security Analytics satisfies common SIEM security oriented use cases, by collecting and analyzing log and network packet information. These use cases include the following:

<table>
<thead>
<tr>
<th>Use case</th>
<th>RSA Security Analytics Alert/Report example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized privileged access</td>
<td>Administrative commands (e.g. su, useradd) from a username not in a list of administrators</td>
</tr>
<tr>
<td></td>
<td>Unusual commands being executed on a critical system</td>
</tr>
<tr>
<td>Unusual protocol use</td>
<td>Unexpected protocol hitting a firewall/gateway</td>
</tr>
<tr>
<td></td>
<td>Large file transfers across a gateway</td>
</tr>
<tr>
<td>Virus outbreak</td>
<td>High # of alerts from the organization’s AV systems</td>
</tr>
<tr>
<td>Trojan Backdoor use</td>
<td>Specific event classes from an IDS</td>
</tr>
<tr>
<td>Abnormal system access</td>
<td>High # of failed logons from a given IP address</td>
</tr>
<tr>
<td></td>
<td>Access from an unexpected geography</td>
</tr>
<tr>
<td>Unauthorized account administration</td>
<td>Account enable from list of locked accounts</td>
</tr>
<tr>
<td>Access policies</td>
<td>Access from an unauthorized location</td>
</tr>
</tbody>
</table>

When detecting threats or policy violations, RSA Security Analytics can generate notifications, provide interactive alerts, and provide context as part of a scheduled alert. Security analysts can personalize how they want to consume specific types of information based upon its security and business impact.

In addition to detecting threats or policy violations, RSA Security Analytics also provides a wide range of out-of-the-box compliance reports, aligned to common regulations across several legal jurisdictions.
<table>
<thead>
<tr>
<th>Geography</th>
<th>Compliance Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>ISO27002, Basel II, PCI</td>
</tr>
<tr>
<td>US</td>
<td>SOX, HIPAA, FISMA, FERPA, FFIEC, GLBA, NISPOM, NERC, SSAE 16</td>
</tr>
<tr>
<td>Canada</td>
<td>Bill 198</td>
</tr>
<tr>
<td>UK</td>
<td>GPG13</td>
</tr>
</tbody>
</table>

SECURITY ANALYTICS TAKES NEW APPROACH TO SOLVING SIEM USE CASES

There are several common SIEM use cases where Security Analytics takes a different, more effective approach to detecting threats.

Example: Account takeover

Account takeover commonly occurs when an attacker uses brute force or other means to take over a legitimate account and thus be able to execute the attack using a legitimate user’s account. This gives the attacker a useful platform to launch the next stage of the attack.

The traditional SIEM approach to detecting account takeover is to create an alert for very obvious signs of account compromise - like creating a correlated alert for several failed logons followed by a successful logon. The problem with this approach is that it creates a large amount of noise – as legitimate users often have problems remembering and typing their password. Also, a determined attacker can easily evade detection by adopting a “low and slow” approach - spreading out access attempts over a long period of time.

RSA Security Analytics takes a different approach to detecting this attack by flagging log or network sessions with common signs of attack activity. For example:

- High # of failed logons originating from a particular IP address
- Host or user accessing critical assets
- Common bot protocols being used
- Nonstandard user tools being used (i.e. not IE, Outlook, Chrome, Mozilla, Safari etc)
- Unexpected source geography

A single instance of or a combination of these indicators is a much better way to detect account takeover than trying to use a rules based approach. Some of these indicators require full network session collection and reconstruction, but others can be detected through more effective log analysis alone.
**Example: Known attack pattern**

Security teams often use SIEMs (via correlation rules) to look for specific attack patterns that they or peer organizations have experienced before. They often create correlated alerts for specific sequences – e.g. a series of failed logons, followed by a successful logon, followed by a connection to a database, followed by a connection to a specific geography.

The problem with this approach is that any slight variation of the attack will “fool” the SIEM. The rule outlined above is too rigid given today’s targeted attacks. Also, in a traditional SIEM any rule can only rely on indicators found in logs, whereas many indicators leave no log footprint. Finally, using a SIEM to look at the universe of possible attack vectors and variations will easily overwhelm the SIEM with data and calculations, and thus stop it from functioning normally.

RSA Security Analytics approach takes a new approach to threat detection which not only provides the speed and smarts to be effective, but it also has the ability to detect unknown attacks as opposed to only known attacks and attack methods. The RSA Security Analytics approach allows analysts to detect more insightful indicators, such as the ability to:

- Flag the log or session with known attack indicators - e.g. high # of failed logons, use of nonstandard protocols, unexpected use of scripting languages, unexpected source or destination IP addresses
- Scope the traffic from IP addresses or users that are also communicating with critical assets
- Replay entire sessions to give comprehensive investigative context

**Example: Beaconing host**

The term “beaconing” is used to describe the regular communication of a host with a Command and Control (C2) host on the Internet. Most beaconing happens on a regular schedule – say every three hours - and is easy to spot visually when you isolate the traffic between the two hosts, either through firewall or router logs, or through monitoring at an egress point.

Traditional SIEMs are generally only be able rely on a list of known C2 hosts, but could not detect beaconing to an unknown C2 host. This is important since C2 sites come and go frequently.

RSA Security Analytics uses the flexibility and processing power of the Security Analytics Warehouse to discover beaconing by identifying all hosts that:

- Communicate with the same host out on the Internet more than 6 times in a 24 hour period, AND
- The interval between consecutive communications has a low standard deviation i.e. happens on a regular cadence rather than in a more random, human behavior
RSA SECURITY ANALYTICS ARCHITECTURE

RSA Security Analytics is a distributed and modular system that enables highly flexible deployment architectures that scales with the needs of the organization.

Key components of the architecture include:

- **DECODER** - Captures, parses, and reconstructs, all network traffic from Layers 2-7 or log and event data from hundreds of devices.
- **CONCENTRATOR** - Indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting.
- **ANALYTIC SERVER/BROKER** - Hosts the web server for reporting, investigation, administration, and other aspects of the analyst's interface. Bridges the multiple real-time data stores held in the various decoder/concentrator pairs throughout the infrastructure. Also enables reporting on data held in the Warehouse and in archived storage.
- **EVENT STREAM ANALYSIS ENGINE** - Processes large volumes of disparate event data and brings meaning through correlation to the events flowing through your enterprise.
- **ARCHIVER** - Indexes and compresses log data and sends to archiving storage. The archiving storage is then optimized for long term data retention through compression, forensic analysis, and compliance reporting.
- **WAREHOUSE** - Hadoop based distributed computing system which collects, manages, and enables advanced analytics and reporting on longer term sets of various security data. The Warehouse can be made up of 3 or more nodes depending on the organization’s analytic, and resiliency requirements.
- **CAPACITY** - RSA Security Analytics has a modular-capacity architecture, enabled with direct-attached capacity (DACs) or storage area networks (SANs), that adapt to the organization’s short-term investigation and longer-term analytic and data-retention needs.
RSA SECURITY ANALYTICS BREAKS SIEM STAGNATION

SIEMs and log management tools can be very useful by providing a centralized view into disparate log sources and by streamlining the compliance reporting process. However, they commonly fall far short in their detection of modern threats and determining exactly what happened and what its impact is on the organization.

To adapt to the changing threat landscape and the evolving requirements of security teams, SIEM tools need to change radically. Through its high powered analytic interface, scalable infrastructure, ability to collect and analyze both log and full network session data, combined with up-to-the-minute threat intelligence, RSA Security Analytics provides the next generation security system to detect and investigate threats.