Automate Threat Detection and Incident Response: SANS Review of RSA NetWitness Platform

In a recent SANS survey, approximately 35 percent of respondents said their greatest impediment is a skills gap in their IT environments. With that in mind, we reviewed RSA NetWitness Platform, a solution that aims to bridge the human skills gap via machine learning and analytics. This review focuses on RSA NetWitness Platform and examines different views, from responding to an incident to performing an investigation and drilling down to see an activity in real time.
Introduction

In the latest SANS Security Analytics survey, approximately 35 percent of respondents said their greatest impediment is a skills gap in their IT environments, and approximately 26 percent said they do not understand the normal behavior of their environment.1 When you consider that your business will continue to grow and information will continue to proliferate, the need to have machines automate analysis of events from disparate sources becomes an imperative. With these facts in mind, we reviewed RSA NetWitness Platform, a solution that aims to bridge the human skills gap via machine learning and analytics.

Rather than relying only on the capabilities of a security analyst, the RSA NetWitness Platform differs from conventional SIEMs by leveraging machine learning and analytics and prioritizing alerts. It provides visibility into an organization’s infrastructure with an on-premises, hybrid and cloud service product that ingests real-time logs, network packets, NetFlow data and endpoint data; it then analyzes the data. When combined with RSA NetWitness Endpoint, the RSA NetWitness Platform provides additional visibility at the user and kernel levels and offers insights on deviations and anomalies from the endpoint and user behavior baselines. With RSA NetWitness Platform, security analysts can investigate incidents and drill down to reconstruct them using data extracted from files or web pages.

---

This review will focus on RSA NetWitness Platform, including both the RSA NetWitness Logs & Network solutions, and examine different views, from responding to an incident to performing an investigation and drilling down to see an activity in real time.

**Evolved Threats Require an Evolved SIEM**

The threat landscape continues to evolve, with attackers learning increasingly more sophisticated ways to circumvent the security controls that organizations are currently deploying to detect malicious behavior. RSA attempts to tackle this problem by leveraging machine learning, analytics, and deeper and broader sets of data sources.

RSA NetWitness Platform provides visibility across an organization’s infrastructure by ingesting real-time logs, network packets, endpoint data and NetFlow data. Because this vast amount of data is nearly impossible for security analysts to tackle, RSA NetWitness Platform applies analytics and machine learning, user behavior analysis and threat intelligence to correlate the metadata and send alerts of suspicious activities to the security analysts so they can detect and investigate the extent of these threats. In addition, RSA NetWitness Platform gives security analysts visibility into all critical endpoint activity and any changes in user baselines. The Endpoint agent is compatible with Microsoft Windows, macOS and Linux systems.

RSA NetWitness Platform comes configured with rule sets and prepackaged reports that security analysts can modify according to their IT environment. Additionally, the platform comes with a set of advanced correlation rules that is applied on the session level for the defined activities over a specific period of time, and when the conditions are met, an alert is sent to the security analysts and the RSA NetWitness Incident Management. Moreover, another feature in the RSA NetWitness Platform is behavior analytics, which leverages machine learning to detect activities that differ from the baseline. RSA also offers threat intelligence feeds, RSA Live and RSA Live Connect (a community-driven threat intelligence module), which are integrated within the RSA NetWitness Platform. This data enrichment gives more insight and context to security analysts—aiding prioritization for tier 1 and 2 security analysts and investigation efforts for tier 3 and forensics security analysts.

**Architecture of RSA NetWitness Platform**

In this section we will cover the architecture of the RSA NetWitness Platform and explain its functionality.

**RSA NetWitness Server**

The RSA NetWitness Server hosts the web user interface, where all data is collected by different RSA NetWitness Platform components. The server also hosts a number of services, including a reporting engine, management module, investigation module, a broker and malware analysis.

The RSA NetWitness Server also lets users access RSA Live and the administration module.
Log Collector

The Log Collector service collects logs from different event sources in an organization’s environment and forwards them to other RSA NetWitness Platform components. Raw logs are collected, enriched and stored as metadata for use in investigations and reports.

There are two types of collectors:

- **Local Collector.** This service collects logs from different log sources such as Windows and Open Database Connectivity (ODBC). The service runs on a log decoder host and forwards all collected logs to the Log Decoder service.

- **Remote Collector.** Also known as Virtual Log Collector (VLC), this service receives logs and then sends all collected events to a Local Collector. Remote Collectors are optional and usually deployed to collect logs from a remote location. In addition, Remote Collectors compress and encrypt the logs before sending them to a Local Collector.

Decoder (Log/Packet)

RSA NetWitness Platform collects two types of data:

- **Log data.** Log data in the form of syslog, ODBC, Windows events and flat files can be collected with the Log Decoder.

- **Packet data.** This data is comprised of network packets that are collected using the Packet Decoder through the network tap or scan port.

Both types of decoders can ingest raw transactional data that is enriched and aggregated to other RSA NetWitness Platform components.

With the decoder, security analysts can control the type of traffic captured by using various feeds, rules and parsers that allow the creation of custom and metadata content.

Concentrator

Unlike decoders, which capture data, concentrators aggregate the data captured by decoders. Any data that can be indexed on the decoder is filtered by its respective concentrator. Concentrators can be queried directly within the investigation module.

Broker

Brokers are similar to concentrators in that they aggregate data; however, they are not used in every RSA NetWitness Platform deployment. Brokers aggregate from the concentrators and maintain an index for all the metadata on the concentrators and decoders down the stack.

Brokers can be physical appliances or service based. Each RSA NetWitness Server has a broker service that can be leveraged in small deployments.

In large deployments, multiple brokers are often used to cover various geographical regions, allowing the user to select a single broker to gain visibility into specific regions of the environment. In these large environments, brokers have the capability to aggregate from other brokers, which allows a single point of visibility for the security analysts.
Event Stream Analysis

The Event Stream Analysis (ESA) aggregates data collected from the concentrator and then correlates and prioritizes multiple event types. According to RSA, ESA leverages advanced event processing language to filter, aggregate, join and recognize patterns and to correlate data on the event streams collected from different sources.

As an example, ESA has the capability to configure and alert on a use case with a sequence of multiple failed login attempts followed by a successful logon and then followed by the creation of a new admin account, all within a short period of time and across all data sources (logs, network and endpoint). These events on their own might be insignificant, but correlating them could indicate suspicious activity on the network that requires further investigation.

Archiver

The RSA NetWitness Archiver is used for indexing and compressing long-term log data and then sending it to archival storage. The archival storage is optimized to store the data for long-term data retention and compliance reporting.

RSA Live

RSA Live is a platform and service that RSA uses to share content such as feeds, logs and packet parsers, rules, reports and threat intelligence with RSA NetWitness Platform customers. Unfortunately, we were unable to validate RSA Live because we only had access to a demonstration lab.

RSA Live Connect

RSA Live Connect relies on threat intelligence provided by the community and is hosted in the cloud. According to RSA, RSA Live Connect collects, analyzes and assesses community threat intelligence from various sources, which include RSA NetWitness Logs & Network and RSA NetWitness Endpoint Insights. Using RSA Live Connect can aid security analysts during an investigation. RSA Live Connect includes detection of suspicious IP addresses. These IP addresses are known for either having suspicious communications or being the origin of malware.

New Features

RSA NetWitness UEBA Essentials

RSA NetWitness User and Entity Behavior Analytics (UEBA) Essentials, available as part of RSA Live, detects suspicious behavior by monitoring behavior changes that stem from misuse of user accounts, either by insider threats or external attackers. The User Login Baseline rule, for example, alerts to suspicious behavior as evidenced by a user attempting to log in differently than usual (baseline), such as attempting multiple logins across different servers, which may indicate an attempt of lateral movement across the organization.

RSA NetWitness Endpoint Insights

RSA NetWitness Endpoint Insights is a feature that continuously monitors endpoint activity and provides visibility into an organization’s endpoints (Windows, macOS and Linux across physical and virtual infrastructure). This feature, accessed under Hosts in the Investigate view, has been integrated into the RSA NetWitness Platform to provide a single view for security analysts. It provides an overview of all the hosts on which the endpoint agent is installed. See Figure 1.

Security analysts can then quickly drill down on the hosts to get an overview of various information, such as users logged in, IP addresses, security configurations and processes running. See Figure 2.

In addition, the new RSA NetWitness Endpoint Insights can perform windows event log collection for better ease of deployment and forward to configured RSA NetWitness Log Decoders.
Walkthrough of RSA NetWitness Views

In this section, we will cover the user interface of RSA NetWitness Platform and highlight various functionalities.

**Respond View**

In the Respond view, security analysts of all tiers and incident responders can view and investigate prioritized results for incidents from different sources, such as ESA rules, RSA NetWitness Endpoint, RSA NetWitness UEBA Essentials or ESA Analytics module for Automated Threat Detection. Analysts can also view a list of alerts and indicators of compromise that the RSA NetWitness Platform has received—all in one place. See Figure 3.

Once a security analyst decides to initiate an investigation, he or she can get a quick look at all relevant content related to the attack and its breadth by using the Nodal view. This view includes information such as source and destination IPs communicating, respective MAC addresses, and the interconnection between them (communication to/with).

The security analyst can then quickly identify other enriched context for this specific incident such as related lists, incidents and alerts, Archer asset criticality information, RSA NetWitness Endpoint machine score and relevant indicators of compromise. See Figure 4.

**Investigate View**

Investigate view is the primary entry point for deconstructing events of interest. In this view, security analysts can drill down using different metadata and various options such as time range, meta group, query and profile.

Different event views in Investigate view allow security analysts to view packet and log data that includes metadata, event types and service types collected for various events. Also in this view, security analysts can query events and filter them using time-range settings and profiles.
Another function in this view is Malware Analysis, which provides a user interface for conducting malware analysis via a customizable dashboard. See Figure 5.

**Monitor View**

Monitor view combines multiple charts and graphs into a single view, creating an overview of various components considered to be important. Users can customize these dashboards to meet their organization’s needs and perform day-to-day operations. Monitor view also has the capability to manage rules and reports, so security analysts can create reports to query on log and packet data to customize reports and charts. See Figure 6.

**Configure View**

In the Configure view, the Live Content tab provides the capability to subscribe to RSA Live, which is the component that manages communications and synchronization between the RSA NetWitness Platform and a list of live content that an organization can subscribe to for updates. Security analysts can view details, subscribe to resources and deploy them to services in case of a matching resource. The Incident Rules tab allows security analysts to create and manage aggregation rules that are used when automating the incident creation process. In addition, the Incident Rules tab enables analysts to manage ESA rules and deployments. See Figure 7.
**Admin View**

From the Admin view, administrators can manage services that perform a unique function, such as collecting logs or archiving data. Administrators can also review event source types that RSA NetWitness solutions have discovered and the system’s level of confidence in how accurately they were identified. Moreover, administrators can define global system settings, such as notifications and audit logging settings, and manage user accounts. The health of the system can be reviewed in the Admin view as well. See Figure 8.

---

**Threat Hunting Investigation: Encoded Reverse Shell**

A shell is piece of software that an attacker uses to execute code or a command on a remote system. A reverse shell uses remote systems to connect back to an attacker who is waiting for a connection. After a malicious piece of software or code is executed on the victim machine by any means, such as a malicious file, the reverse shell tries to connect back to the attacker machine. Then, the attacker can execute more commands on the victim’s machine and attempt to move laterally throughout the network environment.

Injection is such a common vulnerability that it’s the No. 1 risk in the OWASP Top 10 Most Critical Web Application Security Risks.\(^2\) **Command injection** is an attack that aims to execute arbitrary commands on the host OS via a vulnerable application. Command injection attacks are enabled by applications that pass unsafe user-supplied data input (forms, cookies, HTTP headers, etc.) to a shell on the system. In such attacks, the attacker-supplied OS commands are usually executed with the privileges of the vulnerable application.\(^3\)

There are two approaches to handling such incidents:

- Leverage out-of-the-box RSA NetWitness Platform detection capabilities and threat content by creating an incident in the Respond view and working through the Nodal view and context hub.
- Take a threat hunting approach. We used this approach in this paper.

---


\(^3\) [www.owasp.org/index.php/Command_Injection](http://www.owasp.org/index.php/Command_Injection)
For our scenario, we’ll enlist a web server with a command injection vulnerability that the attacker will exploit. Afterward, the web server will execute the payload and connect back to the attacker, as shown in Figure 9.

We simulated this attack using a vulnerable web application and capturing the network traffic. Using RSA NetWitness Platform’s capabilities, we uploaded the packet capture file (pcap) to the RSA NetWitness Platform and then used the Investigate view to drill down on the attacker’s malicious activity.

We first created an encoded Python reverse shell that uses msfvenom⁴ to execute a command that delivers an encoded payload. After injection and execution, the payload tried to connect back to the attacker device at IP 192.168.56.101 on port 443. After capturing the network packets, we uploaded the file to the RSA NetWitness Platform to be digested by the packet decoder. Next, we looked for suspicious activities using Navigate view, where we found suspicious meta keys. See Figure 10.

In the Navigate view, we can see the different meta groups into which this packet capture was classified. Two of the more interesting values of the meta keys are “long connection” and “ratio high transmitted” under session analysis:

- **Long connection.** Long, extended outbound connections may be an indicator of active data exfiltration.
- **Ratio high transmitted.** Between 75 percent and 100 percent of the session payload is transmitted outbound.

---

⁴ www.offensive-security.com/metasploit-unleashed/msfvenom/

---

*SANS Analyst Program | Automate Threat Detection and Incident Response: SANS Review of RSA NetWitness Platform*
To view these events, we select on the Events view tab. See Figure 11.

By double-clicking on the first event, we get a new window that reconstructs the raw network packets’ content, giving visibility to the complete request/response event payload. See Figure 12.

As shown in Figure 9 on the previous page, the attacker has injected the encoded Python payload that was created in the request. Because the payload is encoded, we can decode it without having to leave the RSA NetWitness Platform.

We click on Event Analysis, where we can highlight the payload and decode the selected text to get the output shown in Figure 13.

We also have other options, such as exporting the events as logs, PCAPs or files to analyze further with third-party tools. The event analysis window shows the requests and responses, and affords us the possibility of performing URL and base64 decoding. See Figure 14.
We can see that the decoded Python payload tries to connect back to the attacker machine on 192.168.56.101 and port 443. Going back to the previous screen, we can see the events that the attacker sent to the compromised web server. See Figure 15.

We can also see the reconstruction in the Event Reconstruction view by selecting View Text; this view allows us to see the commands injected by the user and the response in an easy-to-read, side-by-side format. See Figure 16.
Then we can see all the commands sent by the attacker and how the compromised web server responded. See Figure 17.

Conclusion

RSA NetWitness Platform offers a unique approach for detecting threats and providing a single view for incident detection and response. RSA NetWitness Platform leverages advanced data analytics, machine learning and behavior analytics to differentiate between the normal activity of a user, network or a system and any abnormalities. In addition, it inspects network packet sessions and log events for indicators of compromise and enriches data by adding context to the events. Enrichment features such as threat intelligence (RSA Live, RSA Live Connect) offer better insight into advanced threat actors and attacks that otherwise might not be easily detected.

The user interface took some time to get used to. However, throughout our review we were able to find all needed information in the documentation, and there are plenty of publicly available use cases examples that can aid users in discovering the rich features that the RSA NetWitness Platform has to offer both for detection and full incident investigation.

In conclusion, RSA NetWitness Platform is a modern SIEM that leverages machine learning and analytics technologies to give a security operations center (SOC) a good overview of its organization’s environment, while offering the capability to drill down and investigate events in a single view without having to leave the RSA NetWitness Platform.
About the Author

Ahmed Tantawy is a member of the GIAC Advisory Board and a SANS analyst. He currently holds GIAC Penetration Testing (GPEN), GIAC Web Application Penetration Tester (GWAPT) and Offensive Security Certified Professional (OSCP) certifications, as well as the HP ArcSight Administrator and Analyst certificates. Ahmed works primarily as a security operations engineer. His experience includes working on enterprise SIEM solutions and other enterprise security products, as well as leading a security operations center team in the financial sector. In addition, Ahmed has experience as a penetration tester and with ensuring PCI DSS compliance.

Sponsor

SANS would like to thank this paper’s sponsor:

RSA
<table>
<thead>
<tr>
<th>Event Title</th>
<th>City, Country</th>
<th>Start Date - End Date</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Rocky Mountain 2018</td>
<td>Denver, COUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2018</td>
<td>Austin, TXUS</td>
<td>Jun 07, 2018 - Jun 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud INsecurity Summit - Washington DC</td>
<td>Crystal City, VAUS</td>
<td>Jun 08, 2018 - Jun 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Milan June 2018</td>
<td>Milan, IT</td>
<td>Jun 11, 2018 - Jun 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud INsecurity Summit - Austin</td>
<td>Austin, TXUS</td>
<td>Jun 11, 2018 - Jun 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Crystal City 2018</td>
<td>Arlington, VAUS</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit and Training 2018</td>
<td>Munich, DE</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo June 2018</td>
<td>Oslo, NO</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2018</td>
<td>Manila, PH</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2018</td>
<td>Minneapolis, MNUS</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Canberra 2018</td>
<td>Canberra, AU</td>
<td>Jun 25, 2018 - Jul 07, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Vancouver 2018</td>
<td>Vancouver, BCCA</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Charlotte 2018</td>
<td>Charlotte, NCUS</td>
<td>Jul 09, 2018 - Jul 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh July 2018</td>
<td>Riyadh, SA</td>
<td>Jul 28, 2018 - Aug 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pittsburgh 2018</td>
<td>Pittsburgh, PAUS</td>
<td>Jul 30, 2018 - Aug 04, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS August Sydney 2018</td>
<td>Sydney, AU</td>
<td>Aug 06, 2018 - Aug 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Summer 2018</td>
<td>Boston, MAUS</td>
<td>Aug 06, 2018 - Aug 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Hyderabad 2018</td>
<td>Hyderabad, IN</td>
<td>Aug 06, 2018 - Aug 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Summer 2018</td>
<td>New York City, NYUS</td>
<td>Aug 13, 2018 - Aug 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Prague 2018</td>
<td>Prague, CZ</td>
<td>Aug 20, 2018 - Aug 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SEC487: Open-Source Intel Beta Two</td>
<td>OnlineCOUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>