RSA NETWITNESS® LOGS AND PACKETS

Visibility, Analysis and Action

OVERVIEW

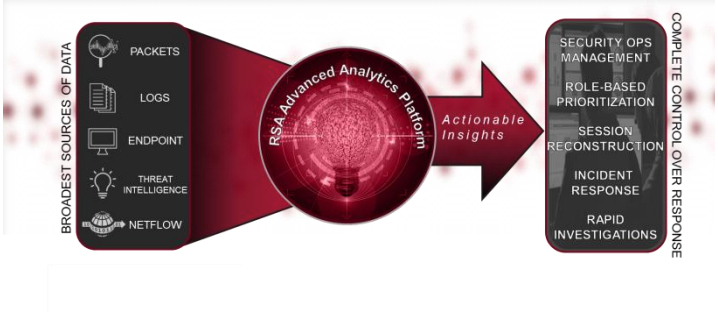
Security teams need to evolve to stay in front of attackers and the latest threats, but in recent years this has become much more difficult. Attackers continue to advance and use sophisticated techniques to infiltrate organizations which no longer have well defined perimeters. Attackers spend significant resources performing reconnaissance to learn about organizations and develop techniques specifically designed to bypass the security tools being used.

The sophistication of threat actors and the expanding attack surface make it nearly impossible for security teams to discover and understand compromises quickly enough to respond before they impact the business.

RSA NetWitness Logs and Packets provides pervasive visibility with advanced analytics - including real-time behavior analytics - to detect and investigate sophisticated attacks. Visibility is provided across:

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

RSA NetWitness Logs and Packets unique architecture captures and enriches data sources with security context in real-time. Additionally, threat intelligence is applied to the enriched data to identify high risk indicators as APT domains, suspicious proxies or malicious networks. This method of processing large data sources in real-time provides analysts with security insight into their entire environment from on-premise to cloud.

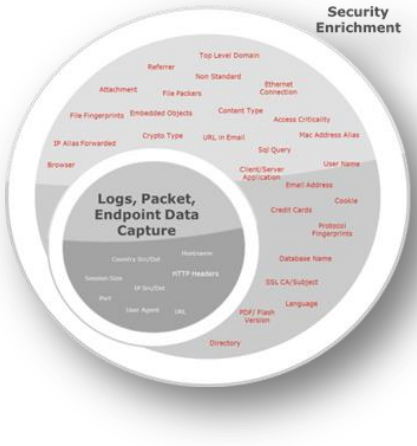


Analysts can now detect and investigate sophisticated attacks and truly understand the full scope of the attack by leveraging advanced analytics which apply our unique combination of behavioral analysis, data science techniques and threat intelligence to iteratively discover known and unknown attacks. RSA NetWitness Logs and Packets enables enterprises to connect incidents in real time and across a long time horizon which means an attack can be fully identified and understood before there is impact to the business.

NETWORK MONITORING AND FORENSICS

RSA NetWitness Logs and Packets captures and enriches full network packet data alongside other data types, such as logs, NetFlow and endpoint. RSA NetWitness Logs and Packets captures full network packets, which means an attack can be reconstructed to fully understand the full scope of the attack and in turn implement an effective remediation plan to stop the attacker from achieving their objective. It processes the data types at time of capture as follows:

- **Data enrichment** – Associates normalized and intuitive metadata to raw data so the security analyst can focus on the security investigation instead of data interpretation.
- **Apply threat intelligence –** Threat intelligence is applied and correlated to the raw data at time of capture to quickly identify sophisticated attacks early.
- **Parse and Sessionize Raw Packet Data –** Raw packet data is parsed and sessionized at capture time so it's faster to retrieve and reconstruct the event during an investigation.



The ability to process the data in real-time as indicated above enables security operations team to detect earlier and investigate more effectively and faster.

For example, in a Spear Phishing attack, the attacker implements a series of steps across the kill chain.

By using RSA NetWitness Logs and Packets, a security operations team will have full visibility across the kill chain as shown below.

This means that security analysts can investigate the attacker at each stage of the cyber kill chain as follows:

- **Delivery** – Targeted E-Mail attachment, Embedded Links
- **Exploitation** – Opening of targeted malware of the endpoint, installation and hooking into the system
- **C2** – Malware beaconing
- **Action** – Data Exfiltration, Lateral Movement, Disruption

Attacker's actions are fully reconstructed with RSA NetWitness Logs and Packets and this helps the security operations team to put an effective remediation plan in place.

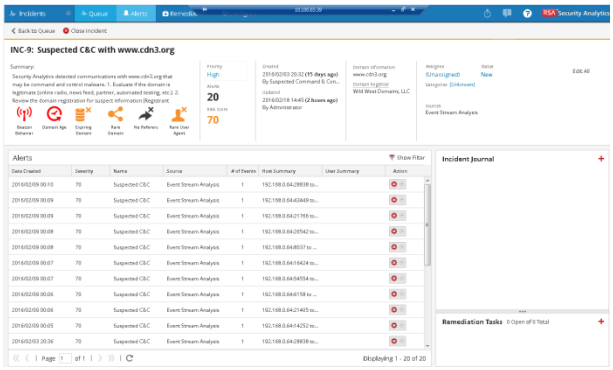
CORRELATE, DETECT AND RESPOND IN REAL TIME

The Event Stream Analysis (ESA) module is a powerful analytics and alerting engine that enables correlation across multiple event types. ESA can consume and analyze metadata from log, packet, NetFlow, and endpoint sources using rules delivered out of the box or by creating custom rules using the underlying event processing language – or the rule builder wizard. The ESA capability helps analysts gain visibility and alert on the attacker TTPs as they move across the kill chain.

BEHAVIOR ANALYTICS

The RSA NetWitness advanced analytics engine detects attack activities based on behavior analytics to speed threat detection and response. The engine uses modular machine learning techniques – it requires no advanced knowledge of specific attacks and does not rely on signatures, rules, or analyst tuning. By observing traffic in the enterprise, the real-time behavioral analytics engine identifies specific anomalous activity through traffic behavior and creates incidents for investigation. The real-time behavior analytics engine delivers Behavior Analytics capabilities that help enterprises identify high risk activity, speed detection of threats, and focus response.

For example, a series of attacker actions and a combination of anomalous activities by users and entities could be leading indicators of Command and



Control (C2) communications which will require further investigation and counter strike to stop the attacker. By having access to the right data, profiling attacker's behavior and detecting anomalies utilizing machine learning, RSA NetWitness Logs and Packets automates C2 detection.

Similarly, detection of lateral movement in a windows environment can be automated using advance analytics. In this case by actively monitoring Windows credential harvesting services, suspicious login activity and explicit logins could help in detecting an attacker's attempt at moving laterally across the organization.

Once alerts are triggered in ESA, the RSA NetWitness Incident Management capability provides the response workflow to assign, triage, investigate and remediate the incident.

ACTIONABLE THREAT INTELLIGENCE

RSA delivers threat intelligence to customers via RSA Live. The threat intelligence delivered by RSA Live is actionable and helps customers detect the latest threats. RSA Live converts threat intelligence into feeds for enriching raw data and correlation rules for

detecting the sophisticated attacks. RSA Live threat intelligence is generated by a combination of RSA Research and Incident Response teams, engineering and external sources.

RSA LIVE CONNECT

Threat actors have collaborated amongst themselves to work through the defensive measures that enterprises have implemented. They are really good at sharing and have created an 'open market' for hacking services, botnets, malware and exploits. To counter this, enterprises need to collaborate and share intelligence in order to reduce the time from when the first attack is observed to awareness across the community. This is critical in reducing the dwell time of the attackers and preventing the attackers from compromising an organization's operations and intellectual property.

RSA Live Connect enables organizations to utilize and operationalize real-time, crowd sourced threat intelligence from the RSA Community. Analysts will gain time sensitive insights into emerging threats that target their Enterprise from peer analysts as well as public and commercial partners. In addition, analysts can provide anonymous risk assessment of threat intelligence after investigation.

By connecting security teams and their insights on threats, RSA Live Connect dramatically reduces the time from when the attack is first observed to general awareness across our community.

ENDPOINT VISIBILITY AND ENRICHMENT

RSA NetWitness for Endpoint provides visibility into endpoints by leveraging unique behavior analytics to flag anomalous activity, provide machine suspect scores and block/quarantine suspicious processes.

RSA NetWitness Logs and Packets and the RSA NetWitness Endpoint product are tightly integrated. Events generated by RSA NetWitness Endpoint are ingested by RSA NetWitness Logs and Packets and correlated against packet, log and NetFlow data to detect sophisticated attacks.

Additionally, as part of an investigation or when an incident is triggered, RSA NetWitness Endpoint provides the source of endpoint enrichment for RSA NetWitness. A security analyst can contextually link into RSA NetWitness Endpoint from RSA NetWitness Logs and Packets by right clicking, and vice-versa.

SIEM AND BEYOND

SIEM solutions have been around for many years and they were designed primarily for two objectives:

1. Collect, analyze, report and store log data from hosts, applications and security devices to support security policy compliance management and regulatory compliance initiatives
2. Process and correlate in real time event data from security devices, network devices and systems to identify security issues that pose the biggest risk to an organization

While most SIEM solutions have met objective number 1, a big majority of these solutions struggle to meet objective number 2. These SIEM solutions do not have the scale and real-time analytics capabilities for identifying issues that can compromise an organization before an attacker achieves their objective.

RSA NetWitness Logs and Packets has SIEM capabilities for the compliance use cases with pre-built templates for a majority of the regulations such as SOX, PCI or HIPAA.

However, RSA NetWitness Logs and Packets goes beyond the baseline SIEM capabilities. With scale and analytic capabilities, RSA NetWitness Logs and Packets will spot sophisticated attacks in real-time. Additionally, the unique correlation across logs, packets, NetFlow and endpoint enables analysts to comprehensively investigate and reconstruct the event.

SECURITY OPERATIONS ORCHESTRATION

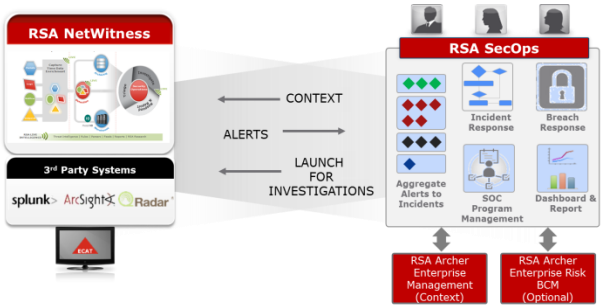
A Security Operations Center (SOC) is comprised of people, process and technology. The orchestration of people, process and technology increases the effectiveness of the overall SOC program. Investing in technology and considering how the three aspects of the SOC work together is an effective strategy.

Orchestration and framework can increase the return on investment and maximize the value of resources in a SOC implementation, reducing the time taken to respond to incidents.

RSA NetWitness SecOps Management (SecOps) provides the orchestration and framework for the SOC. It integrates with RSA NetWitness Logs and Packets and RSA NetWitness Endpoint and other third party security monitoring systems, aggregating events/alerts/incident and managing the overall incident response workflow. The workflow and capturing incident information is aligned with industry best standards such as NIST, US-CERT, SANS and VERIS.

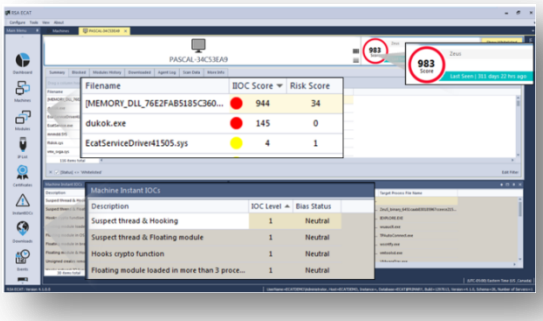
RSA SecOps caters to multiple personas within the SOC from the analysts, incident coordinators, SOC manager and CISO, providing a view on the overall effectiveness of the SOC program.

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.



ARCHITECTURE

The RSA NetWitness Logs and Packets architecture is designed so that customers get security insight in real time when detecting and investigating incidents. As such, at capture time, data sources are sessionized and security enriched at wire speeds. Additionally, analytics such as behavior analysis are performed as streams of data sources are captured in real time. This means that events are being analyzed in real time, speeding the detection and alerting of anomalous activities.



From an investigation perspective, retrieval and reconstruction of sessions is faster since the raw data is parsed and indexed. This allows security analysts to retrieve the raw data quickly and reconstruct sessions.

The architecture consists of three functional components: capture, analysis and server. It is a modular architecture allowing customers to scale the RSA NetWitness Logs and Packets deployment based on capture or analysis performance requirements. From a deployment perspective, RSA NetWitness Logs and Packets can be deployed in both physical, cloud and virtual environments.

The following table provides a summary of the RSA NetWitness components.

Component	Description
Security Analytics Server	Web UI and management server, primary user interface.
Decoder	Captures and stores raw data. Decoders are specific to Logs and Packets. Creates metadata of raw data capture and enriches with security context.
Concentrator	Stores and indexes metadata for fast queries and retrieval of raw data capture.
Hybrid (Decoder / Concentrator)	Decoder / Concentrator combination in a single appliance for branch monitoring. Hybrids are specific to Logs and Packets.
Event Stream Analysis (ESA)	Real-time correlation and analysis engine across logs, packets, endpoints and NetFlow.
Broker	Facilitate queries across a multi-site deployment of Concentrators and Decoders.
Archiver	Long term retention and compression of log data for compliance reporting.
Virtual Log Collector (VLC)	Virtual instance of a log collector for remote sites to forward logs to the Decoder.

HARDWARE SPECIFICATIONS

The following is a summary of HW specifications for the various RSA NetWitness components.

Specification	Hybrid (Decoder / Concentrator)	Event Stream Analysis (ESA)	Core Components (SA Server, Decoder, Concentrator, Archiver, Malware Analytics)
Model	Dell PowerEdge R730xd	Dell PowerEdge R630xl	Dell PowerEdge R630xl
Processor Type	Intel Xeon E5 -2680v3	Intel Xeon E5 -2680v3	Intel Xeon E5 -2667v3
Processor Speed Cache # of Cores # of Processors # of Threads	2.5 GHz 30 MB 12 2 24	2.5 GHz 30 MB 12 2 24	3.2 GHz 20 MB 8 2 16
Total Memory	128 GB	256 GB	128 GB
Internal Disk Controller Type	Dell PERC H730	Dell PERC H730	Dell PERC H730
External Disk Controller Type	Dell PERC H830	Dell PERC H830	Dell PERC H830
SAN Connectivity (HBA) – Optional	Emulex 2X8Gb Fiber	Emulex 2X8Gb Fiber	Emulex 2X8Gb Fiber
Remote Management Card	iDRAC8 Enterprise	iDRAC8 Enterprise	iDRAC8 Enterprise
Drives	Total – 14 Drives • 4 X 1TB, 3.5" HDD • 8 X 6TB, 3.5" HDD • 2 X 800GB, 2.5" SSD	Total – 6 Drives • 2 X 1TB, 2.5" HDD • 4 X 2TB, 2.5" HDD	Total – 6 Drives • 2 X 1TB, 2.5" HDD • 4 X 2TB, 2.5" HDD
Chassis	2U	1U	1U
NIC Card	On Board • 2 X 10 Gb Copper • 2 X 10 Gb & 2 X 1Gb Copper * Other Options Available	On Board • 2 X 10 Gb Copper • 2 X 10 Gb & 2 X 1Gb Copper * Other Options Available	On Board 2 X 10 Gb Copper 2 X 10 Gb & 2 X 1Gb Copper * Other Options Available
Dimensions	H: 8.73 cm (3.44 in.) x W: 44.40 cm (17.49 in.) x D: 68.40 cm (26.92 in.)	H: 4.28 cm (1.68 in.) x W: 48.23 cm (18.98 in.) x D: 75.51 cm (29.72 in.)	H: 4.28 cm (1.68 in.) x W: 48.23 cm (18.98 in.) x D: 75.51 cm (29.72 in.)
Power	1100W Redundant	1100W Redundant	1100W Redundant