THE EVOLUTION OF SIEM

WHY IT IS CRITICAL TO MOVE BEYOND LOGS

Despite increasing investments in security, breaches are still occurring at an alarming rate.

Traditional SIEMs have not evolved to meet the security challenge.

Log-centric SIEMs can’t defend against attacks.

RSA® NetWitness® Logs and Packets addresses the gap left by log-centric SIEMs.

.....Analytics are critical. RSA NetWitness Logs and Packets can help us determine standard behavior, and what’s one standard deviation away, or two standard deviations away, so that we have better visibility into what potential attackers are doing.

JIGAR KADAKIA
PARTNERS HEALTHCARE

---

(SOURCE: VERIZON BREACH REPORT 2014)
BEGINNING STATE

REALITY OF LIVING IN THE PRE-EVOLUTION SECURITY WORLD

DESPITE INCREASING INVESTMENTS IN SECURITY,
BREACHES ARE STILL OCCURRING AT AN ALARMING RATE.

Whether the result of cyber criminals sending phishing or malware attacks through company emails, nation states targeting an organization’s IP, or insiders misusing sensitive data, we live in a world where prevention of breaches has become impossible. Successful attacks bypass each layer of prevention that we have put in place because they often use valid user credentials, trusted access paths, or new exploits, thus going unnoticed by our preventative controls.

GIVEN THE SPEED AT WHICH CYBER CRIMINALS ARE ABLE TO CREATE NEW SECURITY THREATS,
COMPANIES MUST CHANGE THEIR APPROACH TO SECURITY.
SIEM systems were originally intended for compliance and log management. Later they were used to detect and investigate attacks. However, log-centric SIEMs have several flaws that make it difficult to detect successful attacks and even more difficult to investigate them.

Log-centric SIEMs give security personnel some level visibility of what is going on across the enterprise by connecting the dots between anomalies within the different layers of defense via logs. However, logs lack deep visibility and detail to understand what is truly happening in an environment.

IN FACT, 99% OF SUCCESSFUL ATTACKS WENT UNDISCOVERED BY LOGS.

(SOURCE: VERIZON BREACH REPORT 2014)
Since companies have no choice but to allow some traffic to pass through all layers of defense in order to do business, traffic will need to flow through preventative controls. Logs only tell part of the story of what traffic makes it through. Log-centric SIEMs can only report on what the preventative controls have identified. However, they are unable to detect and investigate attack techniques such as unusual client activity, protocol anomalies, unauthorized connections, and suspected malware activity.

As organizations add more preventative controls, the amount of data and events generated can overwhelm even the most mature security teams. This leads to even more noise, increasing the likelihood that the signals (clues about an attack) will get lost or take too long to spot.

In fact, **83% of cyber-espionage breaches took weeks or more to discover**, while **67% took months to discover, with 5% going unnoticed for years**.
RSA NetWitness Logs and Packets addresses the log-centric SIEM problem in a very unique way.

By capturing raw packet data and amplifying the value of this data with Capture Time Data Enrichment and machine learning methodologies that distinguish anomalous behavior, RSA NetWitness Logs and Packets will spot advanced threats that bypass preventative controls. Unlike a traditional SIEM, RSA NetWitness Logs and Packets provides deeper visibility and security context to reconstruct events and attacker TTPs (Tactics, Techniques and Procedures) to stop the attackers before they compromise the organization. Ultimately, RSA NetWitness Logs and Packets helps spot anomalous behavior of threat actors versus legitimate users and investigate these attacks.
SURVIVAL OF THE FITTEST
THIS IS WHAT YOUR SIEM WAS MEANT TO BE

**RSA NETWITNESS LOGS AND PACKETS**

Is the only platform that can correlate security data across logs, packets, and endpoints with real-time behavior analytic capabilities to speed detection and response.

Event correlation can now occur between a mix of logs, packets, and endpoints that enables analysts with leading indicators and in-depth views of threats that bypassed preventative controls. This offers organizations a unified platform to speed detection and response, investigations, compliance reporting, and behavior analytics to spot anomalous behavior.

With **RSA NETWITNESS LOGS AND PACKETS**, security teams can go from an alert to investigation to response faster and with more detail than any other tool.