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.

43%

of

COMPANIES EXPERIENCED A DATA BREACH

Traditional SIEMs have not evolved to meet the security challenge.

99%

of

SUCCESSFUL ATTACKS WENT UNDISCOVERED BY LOGS

Log-centric SIEMs can't defend against attacks.

among

CYBER-ESPIONAGE BREACHES

83% TOOK WEEKS OR MORE TO DISCOVER

67% TOOK MONTHS TO DISCOVER

5% WENT UNNOTICED FOR YEARS

RSA Security Analytics addresses the gap left by log-centric SIEMs.

> "...You actually get more from Security Analytics than any other SIEM that I have."

BOB CHEONG
CISO / LOS ANGELES WORLD AIRPORTS

(SOURCE: VERIZON BREACH REPORT 2014)

RSA

1

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.

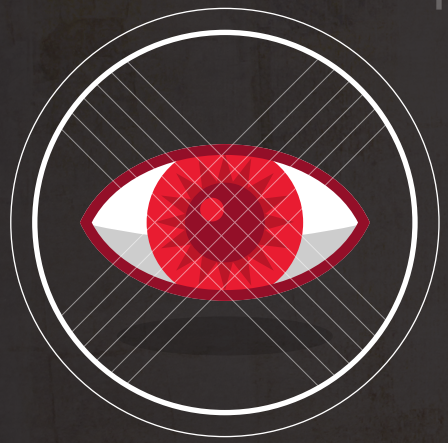
RSA

2

BRINK OF EXTINCTION

TRADITIONAL SIEMs HAVE NOT EVOLVED TO MEET THE SECURITY CHALLENGE

SIEM systems were orginally 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)

RSA

3

THE NEED TO EVOLVE

LOG CENTRIC SIEMs CAN'T DEFEND AGAINST ATTACKS

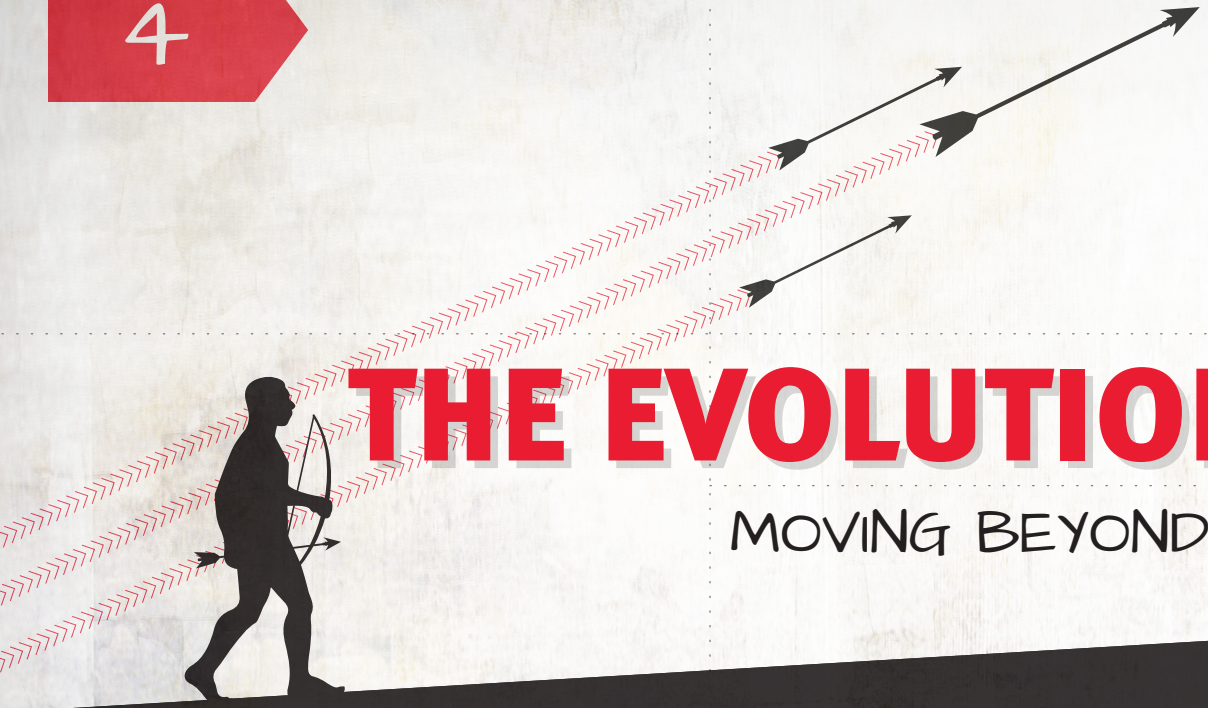
Since companies have no choice but to allow some traffic to pass through all layers of defense in order to do business, traffic will need to flow through preventative controls. Logs only tell part of the story of what traffic makes it through. Log-centric SIEMs can only report on what the preventative 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

4



THE EVOLUTION IS HERE

MOVING BEYOND LOG-CENTRIC SIEM

RSA SECURITY ANALYTICS ADDRESSES THE LOG-CENTRIC SIEM PROBLEM IN A VERY UNIQUE WAY.

It can ingest log data just like a traditional SIEM, but it can also tap into traffic bypassing preventative controls by ingesting raw packet data to achieve much deeper visibility and provide a comprehensive view of the entire organization. Better yet, it amplifies the value of this data with Capture Time Data Enrichment,

MAKING IT MORE EFFECTIVE FOR SPOTTING AND INVESTIGATING ATTACKS.

RSA

5

SURVIVAL OF THE FITTEST

THIS IS WHAT YOUR SIEM WAS MEANT TO BE

RSA Security Analytics
IS THE ONLY PLATFORM THAT CAN CORRELATE SECURITY DATA ACROSS LOGS AND PACKETS (AS WELL AS ENDPOINTS, NETFLOW, AND MALWARE ANALYSIS).

Event correlation can now occur between a mix of both log and raw packet data allowing the analyst in-depth views of events at the defensive perimeter as well as within the legitimate and unauthorized network traffic that bypassed preventative controls. This offers organizations a unified platform for incident detection, investigations, compliance reporting, and advanced security analysis.

WITH RSA SECURITY ANALYTICS, SECURITY TEAMS CAN GO FROM AN ALERT TO INVESTIGATION TO RESPONSE FASTER AND WITH MORE DETAIL THAN ANY OTHER TOOL.

> **I selected** the RSA Security Analytics solution to correlate logging events with egress traffic and match it with security intelligence feeds. This powerful correlation enables us to detect external and insider threats. Security Analytics has really improved our detection capability.
>
> **BOB CHEONG**
> CISO / LOS ANGELES WORLD AIRPORTS

RSA