RSA® Security Analytics

THREAT DETECTION WITH EVENT STREAM ANALYSIS

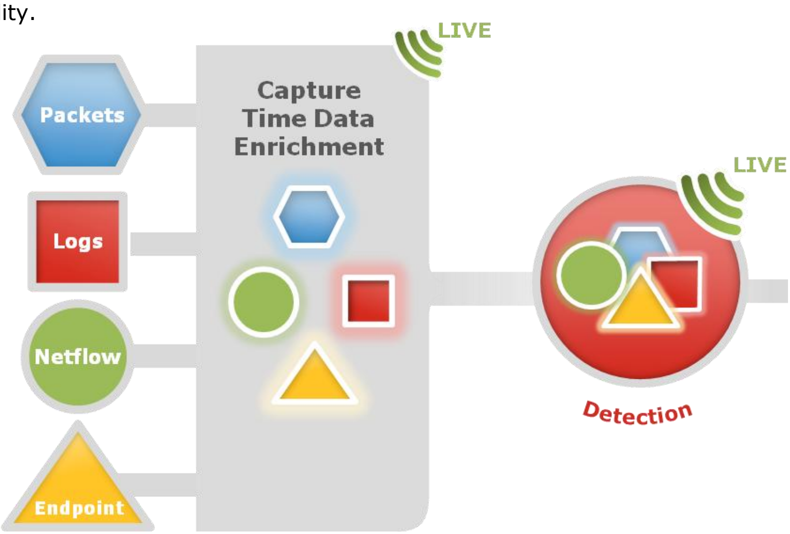
HIGHLIGHTS

Event Stream Analysis

- Detect sophisticated attacks using a powerful event processing engine that allows for real-time correlation of packet, log, endpoint and NetFlow data
- Increase speed and precision by correlating enriched data across multiple sessions and sources of telemetry
- Leverage the RSA Incident Management module to enable prioritized and streamlined investigation and response workflows

TIMING IS EVERYTHING WHEN IT COMES TO THE IDENTIFICATION OF THREATS

The clock is ticking when it comes to the timely identification, investigation and remediation of advanced threats and other anomalous security activity. The attack surface is expanding and client environments are becoming increasingly out of the control of the security team. **Attackers are increasing their skills and compromising environments faster than security teams can defend against them. The effectiveness of security teams is challenged as many are encountering staff shortages, investigations taking hours to weeks; lacking the speed and precision need to accurately prioritize incidents, investigate and determine how to take action.** In addition, with the overwhelming amount of data that needs to be collected and analyzed, security teams find themselves struggling to get value from the data they already consume while simultaneously being driven to collect even more data to expand their visibility.



Graphic: ESA engine is represented by Detection in this segment of the Security Analytics architecture

CORRELATION AND DETECTION IN REAL-TIME

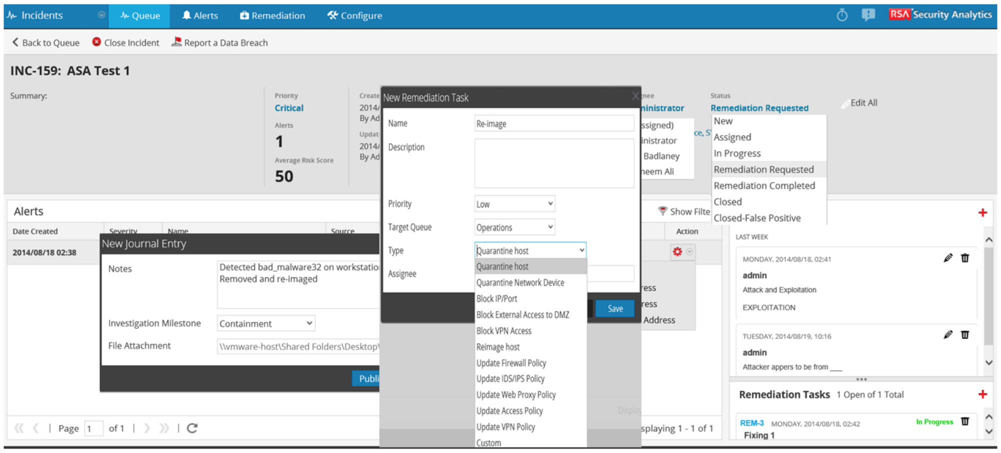
RSA Security Analytics' Event Stream Analysis (ESA) Module is a powerful analytics and alerting engine that enables the correlation and prioritization of multiple event types. Not limited to just analyzing log data, ESA can consume and analyze meta data from log, packet, NetFlow, and endpoint sources using rules delivered out of the box or by creating custom rules using the underlying event processing language - or the rule builder wizard. Rule outputs can be tagged at run time with a variety of enrichment data to provide the level of context an analyst needs to more efficiently detect and investigate a threat. For example, an alert containing a username may be tagged with enrichment data from an identity management system that categorizes that user as being from a partner or contractor, thereby providing additional context to that alert.

CENTRALIZED WORK QUEUE FOR PRIORITIZED WORKFLOW

As ESA alerts are triggered as a result of meeting certain rule conditions, incidents can be automatically created, prioritized, and assigned from within the native Incident Management (IM) queue of ESA. The Incident Management queue gives analysts the ability to rapidly identify, triage, investigate and respond to security incidents. This allows an analyst to focus on the most important incidents using prioritized and categorized risk-scores. Instead of switching between various incident management tools and consoles, with a single click analysts can conduct an investigation all within one solution. This functionality makes the comprehensive visibility provided from packets, endpoints, logs and NetFlow highly actionable, leading to faster and more accurate incidence response workflows.

- RSA Live delivers over 100 ESA rules correlating network packets, logs, NetFlow, and endpoint data.

- Provides a set of alert aggregation rules to enable customers to tailor incident management to their own workflows.



INC-159: ASA Test 1

Summary:

Priority: Critical

Alerts: 1

Average Risk Score: 50

Status: Remediation Requested

Alerts

Date Created	Severity	Name	Source
2014/08/18 02:38			

New Journal Entry

Notes: Detected bad_malware32 on workstatio
Removed and re-imaged

Investigation Milestone: Containment

File Attachment: \\vmware-host\Shared Folders\Desktop\

New Remediation Task

Name: Re-image

Description:

Priority: Low

Target Queue: Operations

Type: Quarantine host

Assignee:

LAST WEEK

MONDAY, 2014/08/18, 02:41
admin
Attack and Exploitation
EXPLOITATION

TUESDAY, 2014/08/19, 10:16
admin
Attacker appers to be from ___

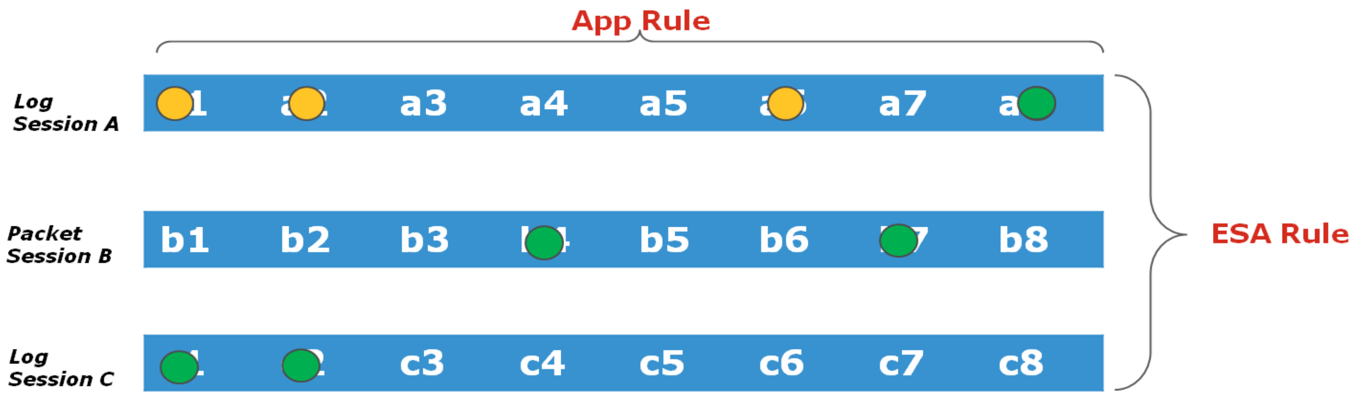
Remediation Tasks 1 Open of 1 Total

REM-3 MONDAY, 2014/08/18, 02:42 In Progress
Fixing 1

Example: Incident shown in the Incident Management module

HOW DOES THE EVENT STREAM ANALYSIS ENGINE WORK?

Starting at the foundation layer within the RSA Security Analytics' infrastructure, collected log, packet, NetFlow, and endpoint data gets consumed and parsed into metadata. This metadata is then forwarded to the ESA engine which then processes it against its rule set. All ESA alerts are then pushed to the Incident Management queue. An ESA rule is different than a typical SIEM correlation rule in part because it correlates metadata across multiple sessions versus within just a single session:



🟡 ***An app rule can correlate meta data within a single session***

🟢 ***An ESA rule can correlate meta data across multiple sessions***

Using this level of visiblity and analysis, ESA can detect malicious activity across multiple sources of telemetry that would otherwise go undetected. Combined with RSA Security Analytics' data consumption and capture time data enrichment, ESA is a key component offering superior incident detection functionality. This leads to security hunters spending less time digging through mounds of data and more time focusing on detecting and investigating the activity that matters most in their enterprise.

APPLIANCE MODEL

SKU	SA-S4H-MAL
Processor	Dual Eight Core, 2.6GHZ
RAM	96GB
Power	750W Redundant
Form Factor	1U, Full Depth
Maximum Weight	44 lbs

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

EMC believes the information in this document is accurate as of its publication date. This information is subject to change without notice