RSA® Security Analytics

Discover & Investigate Threats.

THE ANALYTICS

HIGHLIGHTS

The Analytics

- Proven, patented analytics for threat detection and investigations
- Provides the industry's most comprehensive and understandable analytical workbench
- Applies business context to security investigations
- Fuses threat intelligence with both packet and log data at the point of capture
- Automates the generation of compliance reports and enables long term forensic analysis

Analytic Modules Include:

- Investigation
- Live
- Reporter
- Alerter
- Warehouse
- Administration

AFTER DATA COLLECTION, IT'S ALL ABOUT THE ANALYTICS

The data is collected. Now what? You require the ability to look at all this data with the minimum amount of manual effort, detect abnormal activity, analyze potential threats, and do a more detailed investigation of those threats that pose the biggest risks. When you need clarity and definitive answers to your most challenging security questions, you need a deeper level of detail and the agility to quickly examine application layer sessions and events in a way that is easy to comprehend– and this needs to be done in a matter of minutes, not hours or days.

The core analytic system in RSA Security Analytics provides security teams with an analytic workbench that they can use to discover and investigate threats, also allowing analysts to then automate routine analyses so they can focus on generating new intelligence or insight into their IT environment. The end state for your enterprise is comprehensive situational awareness and compliance management - all reusing the same captured data for short term and longer term archiving and analysis purposes.

RSA

EMC²

The Security Analytics Dashboard

- Seamlessly move among analytic views
- Centralizes analysis with consolidated browser based dashboard
- Personalize based on the analyst's preferences

THE ANALYTIC MODULES

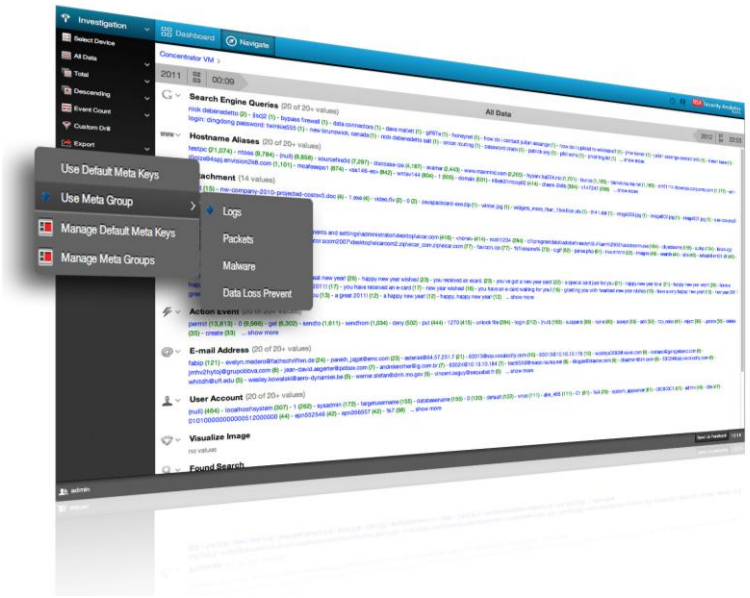
INVESTIGATION

Leveraging proven analytical capabilities, the Investigation module is the primary investigative tool for the security analyst. Investigation provides free-form contextual analysis on massive volumes of data managed by the RSA Security Analytics infrastructure. Unlike other products that display network or log traffic in the context of confusing nomenclature, the Investigation module uses the solution's patented metadata framework to organize the data in a clear and navigable way. The metadata framework is based on a lexicon of nouns, verbs and adjectives — characteristics of the actual application layer content and context parsed by Security Analytics at the time of capture. The metadata from both packets and logs is normalized so the analyst can focus on the security investigation instead of data interpretation.

With its customizable browser-based user interface, Investigation lets analysts view their data in unlimited dimensions for comprehensive situational awareness. In other words, Investigation allows an analyst to "remove the hay" until only "needles" (likely bad activity) remains - allowing the analyst to quickly filter the collected data, in order to focus on generating new intelligence.

Investigation Highlights:

- Meta Groups highlight interest areas based on investigation or analysis requirements
- Easily separate and organize analyst focus by use case
- Quickly identify and organize items of interest for analysis
- Events are reconstructed and presented in the best view as determined by the system
- View many different types of logs using the same investigative interface



LIVE

RSA Live is a threat intelligence delivery system that elevates your security by minimizing the time it takes to identify, assess and respond to incidents. RSA has partnered with the most trusted and reliable providers in the global security community, along with RSA's own intelligence generated by the RSA FirstWatch℠ team, to deliver the most pertinent threat intelligence. RSA Live operationalizes threat intelligence data by fusing it with the organization's network and log data in real-time directly in Security Analytics. This allows analysts to better understand

what types of events to be looking for based on hacker activity and tools. Additionally, it helps level the playing field by taking advantage of the intelligence already discovered by the broader security community.

Live Highlights:

- Operationalizes advanced threat intelligence and content from the global security community & RSA FirstWatch

- Aggregates & consolidates the most pertinent information and fuses it with your organization's data

- Automatically distributes correlation rules, blacklists, parsers, views, & feeds

- Threat intelligence sources include core content for common protocols/C&C Reports, Zero-Day indicators, RSA Security Threat Blacklist, Suspicious proxies and Malicious networks

REPORTER & ALERTER

By having every session, log, communication, service, application and user activity recorded, reconstructed and exposed for analysis, the possibilities are endless as to what can be done using the Reporter and Alerter modules. Zero day malware, botnets, hacker tool activity, policy evasion tactics, data exfiltration, anomalous communications, compliance gaps, and other activities occurring on your network can become readily visible through Reporter and Alerter's rule based approach. These modules use an interactive dashboard for viewing alerts, charts, and provide hundreds of standard security and compliance reports and alerts. Built in compliance reports include (but are not limited to) ISO27002, Basel II, PCI, SOX, HIPAA, FISMA, FERPA, FFIEC, GLBA, NISPOM, NERC, SSAE 16, Bill 198 and GPG13.

Reporter and Alerter Highlights:

- Build your own custom alerts, queries, reports and rules with ease.

- Generate reports from the long-term retained data stored in the Warehouse

- Extensive library of compliance reports mapped to common regulations

WAREHOUSE

The RSA Security Analytics Warehouse enables long term retention and analytics of security information and scales to meet the data management needs of even the largest organizations. The Warehouse is designed to scale computing power along with capacity, enabling the analysis of the data where

Warehouse Highlights:

- Leverages Hadoop technology for linear scaling and intensive data analytics

- Free text searching enables powerful retrieval of documents, information within documents or metadata about documents

- Query and analyze large retained data sets using HIVE and PIG, Hadoop querying languages

it is stored, thus eliminating the time intensive and costly process of moving data from storage and into the analysis system. Raw free text search functionality enables analysts to interact with their data in a way that is similar to a web search and more advanced queries, including correlations, can be written or scripted using HIVE and PIG languages to perform deeper analysis of the retained data.

ADMINISTRATION

When it comes to managing the configuration and performance of your Security Analytics system, the Security Analytics Administration module is designed to allow the analyst to spend more time conducting investigations and analysis while minimizing the effort and time it takes to manage the environment itself. Easily update configurations across your enterprise and upgrade multiple devices at once by grouping devices for administration or data access. Additionally, the administration module allows for the ability to upload intelligence feeds to a single device, a group of devices or all devices easily and quickly. Finally, timeline charts help gain quick insight into historical statistical performance information.

Administration Highlights:

- Drag and drop custom metric charts

- Timeline charts provide insight into historical statistical information

- Group devices for efficient management of your environment

- Consume, distribute, and integrate custom feeds of your choosing

- Role and Permissions management