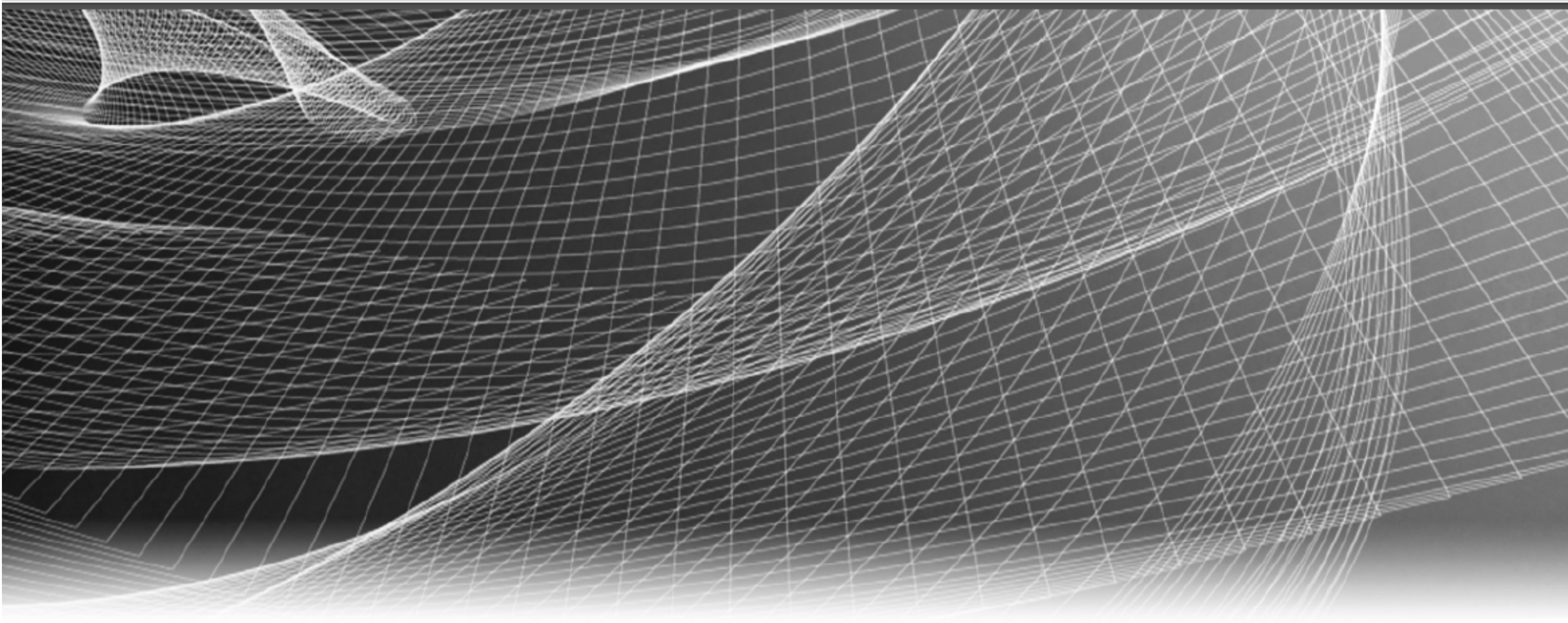

RSA Security Analytics

Investigation Model

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

Investigation Model

The Investigation model organizes content, with the purpose of delivering an accurate path to information security incident response. This is a hierarchical model, four levels deep.

The Investigation Feed uses this model.

Threat

- Attack Phase
  - Reconnaissance
  - Delivery
  - Exploit
  - Installation
  - Command and Control
  - Action on Objectives
    - Lateral Movement
    - Data Exfiltration
    - Data Sabotage
    - Denial of Service
- Malware
  - Remote Access Trojans
  - Crimeware
  - Web Shells
  - Key Loggers

Identity

- Authentication
- Authorization
- Accounting
- Behavior Analytics
  - Entity Monitoring
  - User Mapping

Assurance

- Governance
  - Active Violations
  - Enforcement
- Risk
  - Vulnerability Management
  - Organizational Hazard
  - Enterprise Intelligence
- Compliance
  - Corporate
  - Audit

Operations

- Situation Awareness
- Event Analysis
  - Application Analysis
  - Protocol Analysis
  - File Analysis
  - Flow Analysis
  - Filters

Note: The current Advanced Security Operations Center (ASOC) Incident Response model is described in Live Content Search Tags.

Model Hierarchy

The objective of each category is to catalog existing and upcoming content with an Incident Response service-based approach. This is done to maintain mission critical revenue, protect customer data and branding, as well as to drive information security programs forward in response maturity.

This content strategy focuses on highlighting key pieces of information within an Enterprise network and log capturing environment and strives to make this data readily available for consumption and dissemination. This model aims to aid in the discovery of the preliminary and often responsive data mining tasks related to information security services.

Threat

The Threat category accounts for content that may directly lead to security incident investigations when observed on a high value corporate asset or target.

- Attack Phase
  - Reconnaissance
  - Delivery
  - Exploit
  - Installation
  - Command and Control
  - Action on Objectives
    - Lateral Movement
    - Data Exfiltration
    - Data Sabotage
    - Denial of Service
- Malware
  - Remote Access Trojans
  - Crimeware
  - Web Shells
  - Key Loggers

Examples

Rule	Categorized with meta keys
RDP Traffic Same Source to Multiple Destinations	Investigation Category (inv.category) = “Threat" Investigation Context (inv.context) = “Attack Phase" Investigation Context (inv.context) = “Action on Objectives" Investigation Context (inv.context) = “Lateral Movement"

If the source host in question is identified as being compromised, we can apply this activity to an attack phase describing pivoting within an environment.

Rule	Categorized with meta keys
Zusy Botnet	Investigation Category (inv.category) = “Threat" Investigation Context (inv.context) = “Malware" Investigation Context (inv.context) = “Remote Access Trojan" And: Investigation Category (inv.category) = “Threat" Investigation Context (inv.context) = “Attack Phase" Investigation Context (inv.context) = “Command and Control"

The distinction in specific malware situates this content in the family-type malware subtag.

Attack Phase

The intent of attack phase content is to assist incident response practitioners with the escalation, remediation or classification of observed indicators of compromise activity. This content makes use of organized threat intelligence and provides a template for incident response operations tasked at monitoring and detecting indicators in a given dataset. The attack phases are a procedural set of stages that can be carried out in a variety of ways and over a long period. An example of attack phase content would be a rule that leverages any of the stages listed below.

- **Reconnaissance**: attacker attempts to gain information about the target before the attack begins.
- **Delivery**: the attacker sends the malicious code to the victim.
- **Exploitation**: the actual execution of the exploit (only relevant when the attacker uses an exploit).
- **Installation**: the installation of malware onto the affected computer.
- **Command & Control (aka "C2")**: the attacker creates a command and control channel in order to continue to operate internal assets remotely.
- **Action on Objectives**: the attacker performs the steps to achieve actual goals inside the victim’s network. Possible sub-values are as follows:
    - Enumeration
    - Lateral Movement:
    - Data Exfiltration:
    - Data Sabotage:
    - Denial of Service (aka "DDoS"):

Malware

While some known malicious behavior can be attributed to actors that have high-end intelligence, suspicious behavior can be classified independently of threat portal intelligence. Taking this approach eliminates the downside of associating a certain behavior to one actor only and better permits NetWitness Suite to detect new threats or TTP not already defined.

Breaking malware into certain family types helps content engineers to easily update any parsers or application rules that may reference a new malware variant. Response priorities can differ amongst organizations in relation to the diversity of malware types.

- **Remote Access Trojans**: Remote Access Trojans are an obvious indication that your network is actively compromised. ASOC Analytical Services recommends high response priorities be set when a remote access Trojan signature is generated
- **Crimeware**: Crimeware is currently a huge part of the Internet. Thus, it deserves a place in a response program’s standard operational intake and remediation efforts. Heightened awareness on this malware type would be logical within organizations saturated with confidential identity and financial-based information.
- **Web Shells**: Web shells are an obvious indication there is active compromise. Content related to web shells should be highlighted and escalated with a sense of urgency.
- **Key Loggers**: Key loggers can be packaged up in exploit kits or delivered via spyware. Key logger content can take the form of intrusion detection signature identification numbers, or antivirus filename matches based off Virus Total analysis. Examples are aimed at identifying key loggers that do not solely utilize packet capture.

Identity

The Identity category accounts for content used in the identification or mapping of users and entities.

Identity content data is heavily utilized in response operations for validation of a particular IP address and associated end user. It classifies specific evidentiary logs to assist in incident response, and provides a means to create a baseline for NetWitness Suite.

- Authentication
- Authorization
- Accounting
- Behavior Analytics
  - Entity Monitoring
  - User Mapping

Examples

Rule	Categorized with meta keys
Account Created	Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Authorization" And: Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Assurance" Investigation Context (inv.context) = “Compliance" Investigation Context (inv.context) = “Audit"

This rule is used to highlight any accounts created in a collection. The data represented in the t escalation can be intelligence that is utilized during the corporate auditing process.

Rule	Categorized with meta keys
Logon Success	Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Authentication" And: Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Assurance" Investigation Context (inv.context) = “Compliance" Investigation Context (inv.context) = “Audit"

This rule is used to highlight any successful account authentications in a collection. The data represented in this content can also be utilized during the auditing process.

Rule	Categorized with meta keys
Multiple Account Lockouts From Same or Different Users	Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Authorization"

Detects multiple account lockouts reported for a single or multiple users within a given time window.

Authentication

Authentication is the act of giving a user access to secure systems based on user credentials that imply authenticity. For example, the act of logging onto a system. The ways in which someone may be authenticated fall into three tags, based on what are known as the factors of authentication: something the user knows, something the user has, and something the user is.

Authorization

The process of enforcing policy as in available activities, resources, services or overall user access. For example, elevated privilege, password modifications, distribution lists, and lockout activity.

Rule	Categorized with meta keys
Windows account disabled	Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Authorization"

The above rule tags all accounts disabled in a windows collection.

Accounting

The accounting tag contains content that measures resources utilized by a given user. This can include any of the following:

- the amount of data a user has transferred during a session
- remote access session information
- file share activity
- the overall audit of a user footprint

Rule	Categorized with meta keys
IP Profiling	Investigation Category (inv.category) = “Identity" Investigation Context (inv.context) = “Accounting"

The above content summarizes activity on a network based on a list of source IP addresses. The report includes bandwidth utilization, risk alerts, threats, top destinations, OS types, browsers and clients

Behavior Analytics

The goal of behavior analytics is to determine base lines in user behavior. Base lines are necessary for determining abnormality within overall network utilization. Behavior Analytical content helps to promote data science and user- and entity-based analytics. Within NetWitness Suite, a variety of content has already been utilized in ESA proof of concepts, which visualized host and user relationships based on MAC address, IPv4, hostname and username data from specific windows, DHCP and VPN logs.

- **Entity Monitoring**: An example of content in this subgroup could be the monitoring of the various types of administrator accounts on a corporate network. Many organizations have exclusive user names for these elevated accounts, or bind them to an associated group within active directory. Collecting, cataloging and embedding this enterprise intelligence within the content model is essential in maintaining a security program.
- **User Mapping**: Between employees adding their own devices to a network, and having multiple users on a machine, asset management can quickly become a difficult task for analysts. Any data that represents entity correlation can be stored and cataloged in this subgroup. The underlying function of this content is to associate and identify end users while they access the network.

Assurance

The Assurance category contains content that:

- determines the corporate security posture (governance)
- adheres to internal and external audits (compliance)
- manages overall risk within the enterprise (risk)

The governance, risk, and compliance aspects of security are paramount in enabling customers to alleviate and fulfill industry requirements.

Examples

Rule	Categorized with meta keys
BYOD Mobile Web Agent Detected	Investigation Category (inv.category) = “Assurance" Investigation Context (inv.context) = “Risk" Investigation Context (inv.context) = “Compliance" Investigation Context (inv.context) = “Corporate"

The above rule detects web browsing agents not issued during standard corporate deployments, adding to the summary of overall risk exposure.

Rule	Categorized with meta keys
Proxy Anonymous Services	Investigation Category (inv.category) = “Assurance" Investigation Context (inv.context) = “Risk" Investigation Context (inv.context) = “Organizational Hazard"

The above rule detects the use of common proxy services, by using a list of domains matched against alias host.

Rule	Categorized with meta keys
Config Changes	Investigation Category (inv.category) = “Assurance" Investigation Context (inv.context) = “Compliance" Investigation Context (inv.context) = “Audit"

The above rule highlights any modifications to infrastructure in support of Compliance reporting which may assist during audit.

Governance

Governance content spawns an action for the associated escalation contact. Incident Management is the determined mindset of this category. Content that enables an act of remediation, or the education an end user is in this subgroup. An example of this could be corporate misuse of an asset, which can be carved from an organization's acceptable use or information security policies.

This subgroup identifies behavior that violates an agreement, either employee or corporate.

- **Active Violations**: Misuse of corporate resources. For example, attempting to access a specific category that is blocked. Or, HR violations based on a data loss prevention escalation. Violations often warrant an action by the security analyst or response team escalations to a risk-based organization.
- **Enforcement**: Enforcement is designated for content used in the identification of expected nefarious or delinquent behavior outside of known policies. This subgroup identifies the behavior that an incident response team should consider in remediation of a given violation. This could be in the form of user education of investigation escalation.

  For example, the release of an enterprise confidential e-mail to someone outside of the Corporation based on Human Resources or a legal team's request.

Risk

Risk is defined as intelligence one may discover about the Enterprise, which may be useful within the incident response life-cycle. This can be escalation contact information, server specifics, or business intelligence.

Rule	Categorized with meta keys
Shadow IT User	Investigation Category (inv.category) = “Assurance" Investigation Context (inv.context) = “Risk"

The above content reports on suspected shadow IT usage within the organization.

- **Vulnerability Management**: Content such as vulnerable pieces of software, or updates on patches.
- **Organizational Hazard**: This subgroup consists of content that can be attributed to potentially enabling a compromise. For example, this could be passwords stored in a plain text file on the desktop of a shared administrator server. Further examples might include users using the same logon/FOB; this is an

operational security failure. Additional content that would contribute to organizational hazard are instances of shadow IT.

- **Enterprise Intelligence**: Content that assesses your network and business processes. The more you know about the business itself, the better suited you are to defend it. This content could be related to high value assets or targets, or simply security infrastructure.

Compliance

The Compliance tag contains Information that may be subject to audit, or content that may contribute to readily accessing answers to important questions. Content here promotes information transparency about the security program. More importantly, the compliance section can be considered as information which supports Incident Response. Content examples can include confirming whether systems adhere to corporate compliance via installed security controls.

Rule	Categorized with meta keys
Access to Compliance Data	Investigation Category (inv.category) = “Assurance" Investigation Context (inv.context) = “Compliance"

This content is used to report on any activity related to the handling of sensitive data or restricted hosts.

- **Corporate**: content related to determining a fully IT-compliant entity or user, and required in a successful security program. This is also a task that analysts take in response to disreputable activity. In any instance of escalation, one of the first items to determine is if the security controls in place have failed.

  This type of content can be used to drive security programs forward, more intelligently occupy IT-security budgets, and enable more rapid incident response.

- **Audit**: content that concerns reporting based on industry standards related to fiduciary auditing compliance (at both the state and federal level).

Operations

The Operations tag accounts for content used to aid in systematic analysis of enterprise data. This could be in the form of daily reports, dashboard visuals or the management lifecycle of customer-specific data. Most importantly, it is the content which constitutes the initial inspection of log and session collections. This is important content to deliver to an analyst because it is a prerequisite for understanding situational context.

Examples

Rule	Categorized with meta keys
Only ACK Flag Set in Session Containing Payload	Investigation Category (inv.category) = “Operations" Investigation Context (inv.context) = “Event Analysis" Investigation Context (inv.context) = “Protocol Analysis"

Above rule alerts when a session containing payloads have only ACK flag set.

Rule	Categorized with meta keys
NGINX HTTP Server	Investigation Category (inv.category) = “Operations" Investigation Context (inv.context) = “Event Analysis" Investigation Context (inv.context) = “Application Analysis"

The above rule detects web servers running NGINX, which is often used for malicious purposes.

Rule	Categorized with meta keys
Attachment Overload	Investigation Category (inv.category) = “Operations" Investigation Context (inv.context) = “Event Analysis" Investigation Context (inv.context) = “File Analysis"

The above rule looks for more than 4 attachments in a single session.

Situation Awareness

Comprehensive cyber situation awareness involves three key areas: computing and network components, threat information, and mission dependencies. It has added a new dimension of required awareness to traditional business operations. With this awareness, negative situations can be recognized and managed as they occur. Examples of this type of content can be daily reports and charts for visualizing certain aspects of a collection.

Event Analysis

The event analysis tag is used to classify a majority of the deep packet inspection content available within Live. Alone, a piece of content here might not lead to an active investigation. However, in combination with additional indicators of compromise the collections may require immediate review. Non-standard and service-based analysis content resides in this tag.

This tag contains the following:

- **Application Analysis**: content used to identify applications.
- **Protocol Analysis**: content used to identify anomalous sessions and deviations from standards

- **File Analysis**: content focused on the ability of NetWitness Suite to inspect files and escalate based on irregular behavior.
- **Flow Analysis**: content classified based on directionality rules:
  - Outbound Communication with the Internet,
  - Inbound Web Application Communication,
  - Intra- and Inter-DMZ communications,
  - DMZ to Inside Communications,
  - Inside to Inside Communications,
  - B2B or Partner Communications,
  - Inbound SMTP Communications,
  - Inbound Other Applications,
  - Cleartext side of Inbound VPN Connections
- **Filters**: content labeled as noise, and therefore not stored in the index of an active collection.