Security Intelligence in Action: A Review of LogRhythm's SIEM 2.0 Big Data Security Analytics Platform

Dave Shackleford, Voodoo Security and SANS
Dave is the founder and principal consultant with Voodoo Security, a SANS analyst, instructor and course author, and a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert, and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security.

He is the co-author of "Hands-On Information Security" from Course Technology as well as the "Managing Incident Response" chapter in the Course Technology book "Readings and Cases in the Management of Information Security." Recently, Dave co-authored the first published course on virtualization security for the SANS Institute.

Dave currently serves on the board of directors at the Technology Association of Georgia's Information Security Society and the SANS Technology Institute.
Introduction

• Why do organizations leverage security logs and event data?*
  – Detecting and tracking suspicious behavior
  – Supporting forensic analysis and correlation
  – Preventing incidents
  – Achieving/proving compliance with regulatory requirements

• Logs are an excellent starting point for effective security event management

The Threat Landscape

- Threats are more advanced than ever
  - Phishing and social engineering
  - Advanced malware
  - “Low and slow” attack styles
  - Subtle behavioral patterns

- Lots of examples:
  - South Carolina SSN breach
  - RSA → Lockheed Martin

Hack of South Carolina network exposes SSNs for 3.6 million taxpayers

Ars Technica. 10/26/2012
• Attacks are more difficult to detect these days
  – Malware is custom, avoids signatures
  – Memory resident attack code
  – Use of built-in commands
  – Longer attack periods

• Analysts have too much data to sift through – how do we detect and respond to attacks?
Drowning in “Big Data”?

- Attacks leave multiple footprints
  - Network, system and application logs
  - Security events
  - Access / authentication
  - Seemingly innocuous actions

- Traditional malware protection can’t connect the dots

- Analysts have too much data to sift through

- How do we detect and respond to attacks?
The LogRhythm Review

• Focused on the following aspects:
  – User Interface and Ease of Use
  – Deep-dive Searching and Event Drilldown
  – Unique Analysis Capabilities
  – Advanced Features
  – Knowledge Modules

• A virtualized demo environment was set up for the review
LogRhythm Interface: General Analysis

- Includes fundamental operations for security analysts
- Options include:
  - Aggregation of logs and events
  - Aggregation with audit, operations, and security logs
  - Breakdowns of event categories
  - Logs by type
  - Logs by traffic direction
- Basic analysis capabilities
LogRhythm Interface: Time Analysis

- Breakdown of logs and events by time of event occurrence
- Further broken down by:
  - Type
  - Direction of traffic
  - Granular time options
LogRhythm Interface: Statistical Analysis

- Granular data analysis and reporting on events
- **Categories:**
  - Log source statistics
  - Origin login stats
  - Host stats (system/user info)
  - Affected hosts
  - Affected applications
  - Vendor Message IDs
- **Very useful for reporting**
LogRhythm Interface: TopX Analysis

- TopX views are open, flexible containers that can be populated with the top events from numerous categories
- Examples:
  - 10 inbound/outbound packet types
  - Top 10 user accounts appearing in log events
  - Top 20 domain names present in events
An Example Dashboard
Lists

- Lists are logical groupings of multiple data types or rule aspects
- Simplifies rule creation & investigations by grouping common items together
LogRhythm’s search and analysis features were the heart of the review.

Distinguishing characteristics:
- Ease of access to drilldown functions and capabilities
- Access to wide data sets
- Levels of drilldown and access to event data quickly and simply
- Usefulness of reports and analytics tools
Event Drilldown

- Intuitive view of events and reports
Network Visualization

- It may be useful to visualize events from a network perspective to understand context and relationships.
Analysis: Tail

- The Tail feature creates a view of specified logs that updates in real time.
Another Tail Example

- Tracking Meaningful Network Events
Analysis: Investigations

- More in-depth analysis
- Intuitive wizard helps select:
  - Log and event sources
  - Time and date ranges
  - Specific systems, lists, and other rule criteria
- Review results: This feature was simple to use and provided a huge amount of excellent data and analysis
Investigation Example

- Defined list of blacklist hosts
- Started an investigation from the list
- Looked up and analyzed:
  - Traffic patterns and direction
  - Hosts involved
  - Affected applications
- IT groups can target their response and remediation with greater accuracy
Investigation Example (cont.)

![Image of Log/Event Analyzer](image)

<table>
<thead>
<tr>
<th>Value</th>
<th>Count</th>
<th>KB In</th>
<th>KB Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>CENTAURUS</td>
<td>370</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ANTUA</td>
<td>788</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MENSA</td>
<td>404</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SD_SN_MAIL1</td>
<td>117</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UK_SN_MAIL1</td>
<td>110</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NY_SN_MAIL1</td>
<td>106</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>180.156.103.19</td>
<td>69</td>
<td>0</td>
<td>113.3</td>
</tr>
<tr>
<td>NEPTUNE</td>
<td>67</td>
<td>2.0</td>
<td>0.0</td>
</tr>
<tr>
<td>192.168.169.104</td>
<td>60</td>
<td>24,748,383</td>
<td>26,247.1</td>
</tr>
<tr>
<td>502.110.10.185</td>
<td>56</td>
<td>74,404,150</td>
<td>76,996.2</td>
</tr>
</tbody>
</table>

Logs by Time

- Logs
- Avg Logs

<table>
<thead>
<tr>
<th>Logs by Time</th>
<th>KBytes by Time</th>
<th>Items by Time</th>
<th>Origin Host by Logs</th>
<th>Origin Host by KBytes</th>
<th>Origin Host by Items</th>
<th>Origin Host by Logs</th>
<th>Origin Host by KBytes</th>
<th>Origin Host by Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/29/2012 3:27:00.000 PM</td>
<td>10/29/2012 3:44:00.000 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Aggregate Log/Event List

- First Normal Date
- Last Normal Date
- Count
- RBP
- Log Source Entity
- Log Source Type
- Classification
- Common Event
- Direction

© 2012 The SANS™ Institute - www.sans.org
Advanced Intelligence Engine

• Many of the more sophisticated analytics capabilities in the product are found in the AI Engine
• Concentrates on behavioral profiles and advanced correlation between widely disparate data and event sources
• Real-time analysis, detection and response, and support for rapid drill down and forensic analysis
• Better “big data” analytics
### AI Engine Rule Manager

- **Pre-built rules include Connections, Behavior, Critical Events, etc.**

<table>
<thead>
<tr>
<th>Action</th>
<th>AI Engine Rule Name</th>
<th>Rule Status</th>
<th>Restart</th>
<th>Activation</th>
<th>Expiration</th>
<th>Data Segregation Mode</th>
<th>Alarm Status</th>
<th>EDF</th>
<th>FPP</th>
<th>Suppress For</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Behavior: Config Change Followed By new warnings/errors/criticals</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Disabled</td>
<td>None</td>
<td>None</td>
<td>Medium-Medium</td>
<td>1 Hour</td>
</tr>
<tr>
<td></td>
<td>Behavior: Baseline Target Hosts</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Disabled</td>
<td>None</td>
<td>None</td>
<td>Medium-Medium</td>
<td>1 Minute</td>
</tr>
<tr>
<td></td>
<td>Behavior: Malware Phishing Home</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Disabled</td>
<td>None</td>
<td>None</td>
<td>Medium-Medium</td>
<td>1 Hour</td>
</tr>
<tr>
<td></td>
<td>Behavior: User from non-whitelisted location accessing non-whitelisted objects</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Connection To Krom Blacklisted Domain</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Critical Windows Event Logs II</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>None</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
</tr>
<tr>
<td></td>
<td>Data Leakage to Non-Operating Countries</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>None</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
</tr>
<tr>
<td></td>
<td>External: Account Attack - Account Probe On Multiple Hosts</td>
<td>Enabled</td>
<td>Needed</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Attack - Account Scan On Single Host</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Attack - Brute Force From A Single Origin Host</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Attack - Brute Force From Distributed Origin Hosts</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Account Probe On Multiple Hosts</td>
<td>Enabled</td>
<td>Needed</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Account Scan On Single Host</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Brute Force From A Single Origin Host</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Brute Force From Distributed Origin Hosts</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>5 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Concurrent Authentication From Multiple Cities</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>3 Hours</td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Concurrent Authentication From Multiple Countries</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1 Day</td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Concurrent Authentication From Multiple Regions</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>3 Hours</td>
</tr>
<tr>
<td></td>
<td>External: Account Compromised - Concurrent VPN Authentications From Same User</td>
<td>Enabled</td>
<td>Needed</td>
<td>N/A</td>
<td>None</td>
<td>Enabled</td>
<td>Low</td>
<td>Medium-Medium</td>
<td>30 Minutes</td>
<td></td>
</tr>
</tbody>
</table>

© 2012 The SANS™ Institute - www.sans.org
• Rules can be added/modified easily

• Behavioral rules can be developed

• Examples:
  – Behavior: Baseline Target Hosts
  – External: Account Compromise: Account Scan on Multiple Hosts
AI Engine Rule Wizard

- Graphical representation of rule elements
  - Choose those “present” or “not present”
- This facilitates the behavioral baselines and whitelisting capabilities within LogRhythm’s engine
- Simple example was to look at target hosts that experience configuration changes
AI Engine Rule Wizard
Behavioral Analysis

• What is “normal”?
• LogRhythm helps define this with behavioral whitelisting and profiling capabilities
• As events are collected, they can be stamped as “normal” or “not normal” once a baseline is established
Behavioral Analysis (cont.)

- Based on inclusion/exclusion filters, time and date stamps, log source information
Knowledge Modules

- "Expert system" for security and compliance analysis
- Features include:
  - Auditor-approved frameworks that map all in-scope devices and applications
  - Out-of-the-box alerts, investigations and reports
  - A combination of exception-based alerting with compliance assurance reporting
Alerting

- Basic and custom events/categories

![Common Event Properties window with associated knowledge base artifacts highlighted.](image-url)
Reporting

• Huge number of reports
  – Compliance-specific, out of the box
• Also includes a “knowledge base”
Knowledge Base Modules

<table>
<thead>
<tr>
<th>Action</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Object Collection · Report Templates · Log Summary</td>
<td>This module contains all of the log summary report templates</td>
</tr>
<tr>
<td></td>
<td>Object Collection · Report Templates · All</td>
<td>This module contains all of the report templates</td>
</tr>
<tr>
<td></td>
<td>LogRhythm High Availability (HA)</td>
<td>This module contains objects required in support of LogRhythm High Availability appliance deployments.</td>
</tr>
<tr>
<td></td>
<td>Compliance · ND</td>
<td>The module components that are part of the ND compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · NERC</td>
<td>The module components that are part of the NERC compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · DoD 8500.2</td>
<td>The module components that are part of the DoD 8500.2 compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · ISO 27001</td>
<td>The module components that are part of the ISO 27001 compliance package</td>
</tr>
<tr>
<td></td>
<td>Object Collection · Lists · Default Accounts</td>
<td>This module contains lists of default accounts for various operating systems.</td>
</tr>
<tr>
<td></td>
<td>LogRhythm Required Objects</td>
<td>The module components that are part of every LogRhythm deployment</td>
</tr>
<tr>
<td></td>
<td>Compliance · PCI DSS</td>
<td>The module components that are part of the PCI DSS compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · SOX COSO</td>
<td>The module components that are part of the SOX COSO compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · HIPAA</td>
<td>The module components that are part of the HIPAA-compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · FISMA</td>
<td>The module components that are part of the FISMA compliance package</td>
</tr>
<tr>
<td></td>
<td>Compliance · GLBA</td>
<td>The module components that are part of the GLBA compliance package</td>
</tr>
</tbody>
</table>

**Compliance · NERC CIP**

The module components that are part of the NERC CIP compliance package

**Module Objects**

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Rule</td>
<td>NERC CIP · Alarm On Compromise</td>
<td>NERC CIP Compliance to Alarm when a compromise has been detected</td>
</tr>
<tr>
<td>Alarm Rule</td>
<td>NERC CIP · Alarm On Malware</td>
<td>NERC CIP Compliance to Alarm when malware has been detected</td>
</tr>
<tr>
<td>Alarm Rule</td>
<td>NERC CIP · Alarm On Attack</td>
<td>NERC CIP Compliance to Alarm when an attack has been detected</td>
</tr>
<tr>
<td>Investigation</td>
<td>NERC CIP · Network Connection Summary</td>
<td>This investigation is used to meet NERC CIP Regulations 5.R1.6.5-R2.2.5-R2.4.6-R2.2.7-R2.2.7 and 7-R2.2.</td>
</tr>
<tr>
<td>Investigation</td>
<td>NERC CIP · Network Service Summary</td>
<td>This investigation is used to meet NERC CIP Regulations 5.R1.6.5-R2.2.5-R2.4.6-R2.2.7-R2.2.7 and 7-R2.2.</td>
</tr>
<tr>
<td>List</td>
<td>NERC CIP · Critical Cyber Assets</td>
<td>Devices that are part of the Critical Cyber Assets.</td>
</tr>
<tr>
<td>List</td>
<td>NERC CIP · Electronic Security Perimeter</td>
<td>Devices that are part of the Electronic Security Perimeter.</td>
</tr>
<tr>
<td>List</td>
<td>NERC CIP · Incident Reporting And Planning</td>
<td>Devices that are part of Incident Reporting and Planning.</td>
</tr>
<tr>
<td>List</td>
<td>NERC CIP · Incident Reporting And Planning</td>
<td>Devices that are part of Incident Reporting and Planning.</td>
</tr>
<tr>
<td>List</td>
<td>NERC CIP · Incident Reporting And Planning</td>
<td>Devices that are part of Malware Systems.</td>
</tr>
<tr>
<td>List</td>
<td>NERC CIP · Incident Reporting And Planning</td>
<td>Devices that are part of Malware Systems.</td>
</tr>
<tr>
<td>Report</td>
<td>NERC CIP · Account Management Activity</td>
<td>This report summarizes all account management activity for production systems.</td>
</tr>
</tbody>
</table>
Universal Descriptor Language

- UDL is a simple rule and module definition format that allows the LogRhythm software to create new reports, rule modules and correlation routines
  - Similar to Snort/Sourcefire VRT model
  - Community can share event data, correlation rules, and more
Conclusion

• Product was easy to use with highly advanced features

• New features in version 6.1 that deserve particular attention include:
  – User, system, and application behavioral event analysis
  – Out of box reporting and expert reporting modules
  – Ability to set standardized and custom alerts
  – Expert-driven knowledge modules to aid in analysis

• Should help IT teams to monitor more effectively and respond more quickly to advanced threats
Dave will be joined by Seth Goldhammer, LogRhythm’s Director of Product Management

Please use the on-screen tools in the Eluminate interface to submit a question
Acknowledgements

Thanks to our sponsor:

LogRhythm

And to our attendees:
Thank you for joining us today!