Hunting for the Undefined Threat: Advanced Analytics & Visualization

Joshua Stevens

Enterprise Security Architect
Hewlett-Packard
Cyber Security Technology Office
Defining the “Hunt Team”
Cyber Defense Evolution

**Point Solutions**
Ad-hoc monitoring per device console

**SIEM/SOC**
Real-time monitoring of known threats

**Log Mgmt**
Centralized ad-hoc monitoring

**Threat Intel**
Track known adversary IOCs, TTPs, intent

**Hunt Teams**
Find unknown threats, understand new adversary TTPs

1995

2000

2003

2006

2013
‘Hunt’er Skillsets

Cyber Security
- Intrusion Analysis
- Malware Analysis
- Threat Intelligence

Data Science
- Data Management
- Data Visualization
- Statistics
- Programming

Mindset
- Desire to learn
- Creative
- Analytical
- Red team

Hunter
Hunt Processes

Unstructured Hunt
- Exploratory data analysis
- Pattern discovery

Structured Hunt
- Identify and search for indicators of compromise

Real-time Monitoring
- Create or modify detection methods
The Need for “Data” and Security Analytics
Hiding in Plain Sight

Known Threat

- Matches a signature
- Goes to a bad place
- Works in the clear
- Unauthorized use
- Outside of baseline
- Within monitored infrastructure

Unknown Threat

- New behavior
- Goes to an approved place
- Works encrypted
- Authorized use
- Inside of baseline
- Outside monitored infrastructure

Bad guys know how to stay inside the bell curve!
Security Analytics Comes in Different Flavors

- **Big Data Scale**
  - Exponential Decay + Risk Aging
  \[ N(t) = N_0 e^{-Mt} \]
  - Naive Bayes + Classification
  \[ p(C|F_1, \ldots, F_n) \]

- **Unstructured Context**
  - Cosine Similarity + Relationship
  - K Means Clustering + Ans.

- **Structured Analysis**

- **Enterprise Log Data**
A 13-billion Event Prototype
Security Analytics Prototype

Anomaly Detection

Vertica Data Store

Distributed R (models)

Causal Analysis

What-If Analysis

Cluster Analysis

Security Analytics

Vertica Data Store

Hadoop

Raw Events

Connectors

Normalized events

SIEM Correlation

Prototype

Kafka/Storm

Ingested events

SIEM Logging

Syslog

Files
5 Hunt Team Use Cases
Case 1: Cluster Analysis for Hunt Team Managers
Less VPN traffic and more IPS traffic reveals blind spots
Apply Categorization

SIEM categorization and destination port surfaces hostile events.
Case 2: Track Anomalies for Security Analysts
View: Events by High Severity Rating and Volume
Change View to Destination Type

Display trend of unique destinations visited
Apply Anomaly Chart

Graph filtered from billions of events

Anomalous Event

Uncover unique event, alerting next level of investigation.
Case 3: Analyze the Haystack for the Hunt Team
View: IPS Events for 45 days

Device Severity
- High
- Medium
- Unknown
- Very-High
Filter on the Return Traffic

Display IPS evasion, recurring pattern and gaps in visibility.
Case 4: Behavioral Analysis for the Hunt Team
View: Non-Security Events in the Environment

Category Device Type
- Applications
- Content Security
- Database
- Firewall
- Host-based IDS/IPS
- Mainframe
- Network Monitoring
- Network-based IDS/IPS
- Operating System
- Policy Management
- Security Management
- VPN
A Typical View of VPN Logging by Source

| Source Address | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|----------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 192.168.20.32  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.20.1...| o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.20.1...| o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.21.56  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.22.10  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.22.10  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.22.10  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.80.91  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.80.10  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.80.93  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.80.93  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.99.96  | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.100... | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.101... | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.104... | o | o | o | o | o | o | o | o | o | o |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Category Device Type: VPN
Overlay VPN Source with Recon Events

| Source Address | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|----------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 192.168.33.2   |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.20.1   |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.20.1   |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.21.86  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.22.10  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.40.1   |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.50.91  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.50.10  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.50.23  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.50.98  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Category Device Type: VPN

Overlay VPN Source with Recon Events

| Source Address | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|----------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 192.168.10.10  |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.10.1    |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 192.168.10.4    |   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Category Device Type: Recon

Correlate two sources of information to identify atypical behavior.
Case 5: Advanced Analysis for the Hunt Team
Drilldown Reveals Subtle Patterns

Horizontal line denotes large scale brute force attempts

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Device Type</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.100:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.99:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.104:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.105:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.199:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.101:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.103:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
<tr>
<td>10.0.111.39</td>
<td>10.0.20.102:22</td>
<td>Operating System</td>
<td>Failure</td>
</tr>
</tbody>
</table>
In Closing

- Defining the “Hunt Team”
- Leveraging “Data” and Security Analytics
- An internal analytics prototype
- Use cases for the hunt team
Apply What You Have Learned Today

1 Week
Give Analysts 4 hours/week for unstructured hunting

3 Months
Build data science skills into your hunt team

6 Months
Feedback lessons learned into other operational teams

1 Month
Identify relevant data to begin hunting

4 Months
Implement a Hunt practice
Incorporate use cases