Using SIEM for Real-Time Threat Detection

Presentation to ISSA Baltimore

Joe Magee
CTO and Co-Founder
March, 27 2013
About us

Vigilant helps clients build and operate dynamic, business-aligned security monitoring, threat detection and incident response capabilities.

- Focused on the enterprise-wide “intelligence” layer of security
- Specialized in SIEM since 2003
- Pioneered a “co-sourced” model for SIEM management
- Vendor-agnostic

www.thevigilant.com
Agenda

- What’s the potential for SIEM as a threat detection platform?
  - SIEM’s strengths as a platform

- Threat Intelligence
  - Challenges with consuming threat intelligence data
  - Choosing the right threat intelligence

- Solution architecture
  - Benefits of marrying SIEM and Threat Intelligence Data
  - SIEM Use Cases
  - SIEM Case Study
Today’s cyberthreat challenge

THEN...

ATTACKS
- Orchestrated by smaller groups
- Aimed at as many victims as possible
- Targeted specific device types
- Aimed to disrupt network productivity

DEFENSE
- GOAL: KEEP BAD STUFF OUT
  - Protect at the perimeter
  - All assets treated equally
  - Used signature-based tools

WE NEED:
- Smarter alerts
- Prioritization
- Better incident analysis & handling

GOAL: MINIMIZE DAMAGE
- Assume you are always infiltrated
- Risk-focused on critical data & assets
- Layered defenses, advanced correlation, transaction-oriented monitoring
Benefits of SIEM Technology

SIEM technology in the organization offers many benefits including:

- Single pane of glass for all security event data monitoring
- Operational efficiency in Security Operations and Incident Response
- Regulatory compliance reporting
- Detection of policy violations and associated threats
- Fraud and business risk mitigation

The Most Successful SIEM Implementations marry referential data sources with real-time data to enable true business context and actionability.
SIEM: Powerful “security intelligence” technology

SIEM provides rich real-time support for detecting and responding to infiltrations...

- Provide visibility into security status of key IT assets
- Identify indications of fraud or other cybercrime
- Reduce risks associated with new technologies & services

#### Business Risk Management

- Produce audit-related reports
- Demonstrate adherence to policy & regulations
- Monitor controls to remediate audit findings

#### Compliance & Audit Support

- Improve staff efficiency through log aggregation
- Improve incident response through automation
- Accelerate remediation through improved workflow
- Enable post-incident forensics
- Validate effectiveness of security controls

#### Real-Time IT Security Management & Operations

- Improve staff efficiency through log aggregation
- Improve incident response through automation
- Accelerate remediation through improved workflow
- Enable post-incident forensics
- Validate effectiveness of security controls
Threat intelligence...?

Is this information really intelligent?

- Too much data, too many sources
- Tied to specific security devices
- Inefficient to utilize
- Lacks contextual information

Can SIEM be used to help solve this problem?
Threat intelligence data quality issues

Typical Open Source Feeds used in threat intelligence integration

<table>
<thead>
<tr>
<th>Open Source Feeds</th>
<th>Average Records/Day</th>
<th>% Filtered Based on IP White Lists</th>
<th>% Filtered Based on Validation Techniques</th>
<th>% Filtered Based on Reputational History</th>
<th>Actual Percentage of Data Used</th>
<th>Intelligence Source Feed Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRI Malware Threat Center</td>
<td>800</td>
<td>20%</td>
<td>43%</td>
<td>8%</td>
<td>29%</td>
<td>Feed source not used due to data relevancy</td>
</tr>
<tr>
<td>SAN ISC - DShield</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Malware Domain List</td>
<td>1214</td>
<td>25%</td>
<td>10%</td>
<td>10%</td>
<td>55%</td>
<td></td>
</tr>
<tr>
<td>Zeus Tracker</td>
<td>380</td>
<td>18%</td>
<td>65%</td>
<td>2%</td>
<td>15%</td>
<td></td>
</tr>
<tr>
<td>SpyEye Tracker</td>
<td>480</td>
<td>12%</td>
<td>75%</td>
<td>3%</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>Project HoneyPot</td>
<td>5300</td>
<td>25%</td>
<td>62%</td>
<td>3%</td>
<td>10%</td>
<td></td>
</tr>
</tbody>
</table>

| Averages                | 1635                | 20%                                | 51%                                      | 5%                                       | 24%                           |                                                                    |
| Totals                  | 8174                | 1635                               | 4169                                     | 425                                      | 1945                          |                                                                    |

- Many feeds report data that is either aged or is not currently tied to active malware participation.
- Much of the IP data reported is associated with major hosted servers (i.e. Yahoo, Google).
- Filtering and validation is absolutely necessary to ensure that data leading to identification of a security incident is valid.
Turning threat information into threat intelligence

- **INFORMATION:** Knowledge communicated or received concerning a fact or circumstance.
  - High quality data
  - Analytical risk scoring
  - Available to the right people
  - Supported by contextual information and research tools
  - Am I getting the right data?
  - Is it accurate and easy to use?
  - What needs attention first?
  - What resources will be impacted by this threat?
  - Who needs to use it?
  - What is the most effective integration point?
  - Is the data relevant to us?
  - Can I quickly construct a picture of what’s occurring?
  - Can I easily get additional information and support?

- **INTELLIGENCE:** A discipline that exploits a number of information collection and analysis approaches to provide decision-making guidance.
  - Enables Security Operations to:
    - Prioritize remedial action
    - Streamline incident handling
    - Prevent or minimize damage
Considerations for choosing feeds

- What integration points?
- Who will consume it?
- Are the feeds in the right format for your usage model?
- What range & categories of data will you need?
- What data sources are important to monitor for, and how will you detect them?
- What threats are important to monitor for, and how will you detect them?
- What analysis support does the provider offer?
- What does the provider do to enrich, update & validate?

© 2012 Vigilant, Inc. – not for duplication or distribution

3/28/2013
The more advanced your SIEM deployment is, the more value you can get from threat intelligence.

Solution: SIEM infused with Threat Intelligence

Real-time threat detection requires:
- Typical IT security data sources
- Additional, commonly available data
- Appropriate external threat intelligence, directly into SIEM, or secondarily through other source devices

Asset, HR, and other business data enable risk-aware monitoring, insider threat and privileged user monitoring, fraud detection, and other advanced use cases.

Commonly-accessible data sources are needed to provide the foundation for threat detection use cases.
# Top ten intelligence use cases for SIEM

<table>
<thead>
<tr>
<th>Detection Activity</th>
<th>Threat Feed Data</th>
<th>Real Time Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Detect Outbound Browser Activity to known CC &amp; Malware drop sites IP/Domains</td>
<td>Domain, URI, IP Address</td>
<td>Web Proxy Logs, Firewall Logs</td>
</tr>
<tr>
<td><strong>2.</strong> Detect Outbound Network Activity to known CC &amp; Malware drop sites IP/Domains</td>
<td>Domain, URI, IP Address</td>
<td>Firewall Logs, Netflow Traffic</td>
</tr>
<tr>
<td><strong>3.</strong> Detect Inbound Network Activity from CC &amp; Malware drop sites IP/Domains</td>
<td>Domain, IP Address</td>
<td>Firewall Logs, Webserver Logs</td>
</tr>
<tr>
<td><strong>4.</strong> Detect Outbound Network Activity to Dyn-Dns Hosts</td>
<td>DYN-DNS</td>
<td>DNS Logs, Firewall Logs</td>
</tr>
<tr>
<td><strong>5.</strong> DNS Queries to non standard TLD</td>
<td>DNS, TLD</td>
<td>DNS Logs</td>
</tr>
<tr>
<td><strong>6.</strong> Inbound Phishing attempts against organization webservers</td>
<td>Domain, IP Address</td>
<td>Web Server Logs</td>
</tr>
<tr>
<td><strong>7.</strong> Email from Known Phishing Servers</td>
<td>Email</td>
<td>SMTP Logs, Exchange Logs</td>
</tr>
<tr>
<td><strong>8.</strong> Infected User Accessing a Critical Asset</td>
<td>Domain, URI, IP Address</td>
<td>Suspicious User Active List</td>
</tr>
<tr>
<td><strong>9.</strong> Accepted Outbound Firewall Connections to Identified Malicious sites</td>
<td>Domain, IP Address</td>
<td>Firewall Logs</td>
</tr>
<tr>
<td><strong>10.</strong> Infected Host has not triggered an Anti Virus Alert</td>
<td>Domain, IP Address</td>
<td>Anti-Virus</td>
</tr>
</tbody>
</table>
Case Study: Regional Retail Chain

- **CUSTOMER PROFILE:**
  - Retail convenience store chain in US mid-Atlantic region
  - 16,000 employees; $5.89B revenue; Forbes largest private companies list

- **KEY BUSINESS OBJECTIVE:**
  - To establish SIEM-based monitoring that is more actionable through correlation with external threat data.
  - To identify threats that may already exist within their environment

- **SOLUTION:**
  - Build an internal threat intelligence capability by leveraging third party feed providers (multiple providers)
  - Integrate the feed data into SIEM for the purpose of real-time correlation and alerting.

- **BENEFITS:**
  - Organization was able to identify and quarantine a number of systems that were compromised that had Anti Virus running and were behind a firewall/proxy.
  - Organization was able to prioritize the focus of their incident response team on alerts that were actionable and of high priority to the group.
QUESTIONS / DISCUSSION

Joe Magee  
CTO and Co-Founder

- Office Number: (201) 324-1800 x202
- Cell Number: (617) 921-8671
- Email: jmagee@thevigilant.com