FROM SIEM TO SOC: CROSSING THE CYBERSECURITY CHASM

Mike Ostrowski

VP
Proficio
@proficioinc
EXPERIENCE FROM THE CHASM

- Managed Detection and Response Service Provider
- Three Global Security Operations Centers
- Both Cloud Based SIEM / SOC and Hybrid SIEM / SOC
- Operate over 18 SIEM platforms in our SOCs
- Co-Manage many SIEM platforms for Clients plus SOC-as-a-Service
- Experience with SIEM, SOC, Threat Intel, Incident Response, UBA, and AI
HIGHLIGHTS WE WILL COVER

- SIEM Foundation
- SIEM Optimization
- SOC People, Process, and Technology
- SOC Metrics
- SOC Total Cost of Ownership Comparison
- Apply Lessons Learned
• Define your Log Sources
• Perform Asset & Policy Business Context Modeling
• Define Incident Definitions, Categorization, & Response Actions
• Define Use Cases to Detect, Validate & Respond
  • Detect Indicators of Attack, Indicators of Compromise, or Policy Violations
  • What log or data sources are useful
  • How will suspicious Indicators be validated, investigated, and enriched for triage and response escalation actions
• Create SOC Workflow to enrich data for Analyst review, process for validation & triage
• Create Run Book for escalation and incident lifecycle management
**USE CASES MAPPED TO KILL CHAIN**

- Cyber Kill Chain is an excellent map for Use Case development
- ‘Zero Trust’ Model required visibility across the entire chain and enterprise
- Early threat discovery and rapid containment are critical

<table>
<thead>
<tr>
<th>Delivery</th>
<th>Exploitation/Installation</th>
<th>C2</th>
<th>Pivot</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Client Compromise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>Downloader</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Attachment</td>
<td>Remote Access Tool</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive-By</td>
<td>Exploit Kit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive-by Download</td>
<td>OS Modification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosted Services</td>
<td>Credential Attack</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Exploit</td>
<td>Backdoor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosted Services</td>
<td>Client Application Exploit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Connection</td>
<td>Webshell</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Connection</td>
<td>Account Modification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partner Connection</td>
<td>Modification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Accounts</td>
<td>Application Modification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Remote Interaction**
- Shell Access
- Rem. Desktop Session

**Exfiltration**
- Email Exfiltration
- Web Transfer
- File Transfer

**Credential Abuse**
- Credential Dumping
- Account Modification

**Lateral Movement**
- Network Recon
- Remote Administration

**Steal**
- Obtain PII
- Maintain Presence
- Obtain IP

**Modify**
- Sabotage
- Create Advantage

**Destroy**
- Destroy IP
- Destroy Services
- Destroy Equipment

**Access Logs**
- UTM/NGFW
- Firewall
- IDS/IPS
- Email Gateway

**Operating System**
- Application
- HIDS/HIPS
- File Integrity
- Anti-Virus

**UTM/NGFW**
- Firewall
- Webfilter
- IDS/IPS

**Access Logs**
- UTM/NGFW
- Firewall
- IDS/IPS
- HIDS/HIPS
- Operating System

**HIDS/HIPS**
- File Integrity
- Operation System
- Application
- Database
- Application Control
SIEM OPTIMIZATION

• Enable **Automated Alerts** that are ticketed to Incident Responders & Operations teams

• Create ability to assign **Analyst Action Required** alert investigations by SOC Analysts

• Create SOC workflow to **ENRICH DATA FOR HUMAN VALIDATION AND TRIAGE**

• Detect: Validation / Investigation / Triage / Escalation – Ticketing

• Respond: Containment / Incident root cause investigation / Incident Scope investigation

• Remediate: Lifecycle management / Change or Add Control, Detection, or Compensation
CREATE SOC WORKFLOW IN YOUR SIEM
SAMPLE ESCALATION

**Security Team**

**Triage and Ticket to Network Team**

**Use Case Auto-Assign Incident Criticality Based on Asset Model and Incident Classification**

**Triage and Ticket to Desktop Team**

**Auto Generate Incident Response Classifications Based on Use Case**

**Data Enrichment for SOC Analyst and Responders**

**SOC Analyst Analysis of Event and Research Source**

**SOC Analyst Manual Response Recommendation**

---

To: security@case.com
Cc: Firewall@case.com; Web_Dev@case.com

On: 2018-03-20 10:00

Subject: ProSOC Alert Notification - 2018-03-20T10:00 - Short - Multiple Trojan Activity Signatures Triggered

---

**SOCO Command Team**

**Severity Check:**

- **Criticality:** High
- **Severity:** Unspecified
- **Data Center HIP Check:** Failed - Not HIP Compliant
- **Public Asset Check:** Failed - Not HIP Compliant
- **Critical Asset Check:** Failed - Not HIP Compliant

**ProSOC has detected multiple unique Short "Trojan activity"-cluster events between a source and destination IP address that could indicate an anomalous. Details of the event are as follows:**

**Source Address:** 4.7.145.55
**Destination Address:** 4.7.145.20

**Short Cluster:** Trojan activity

**DNS/Website: Smart**

**Discoverer:** Smart

**SOCO Command:** Signatures

**E1 VAR E SERVER Whitebox Conversion - apm http POST**

**E1 VAR E SERVER allow alert include PHP-friendly option in url**

**E1 VAR E SERVER allow alert include PHP-friendly option in url**

**E1 VAR E SERVER PHP Commands or HTTP POST**

**Discoverer:** Triaging

**Discoverer:** Smart

**Item:** Administrative

**Triaging Team:**

- **E1 VAR E SERVER Whitebox Conversion - apm http POST**
- **E1 VAR E SERVER allow alert include PHP-friendly option in url**
- **E1 VAR E SERVER allow alert include PHP-friendly option in url**
- **E1 VAR E SERVER PHP Commands or HTTP POST**

**Discoverer:** Triaging

**Discoverer:** Smart

**Item:** Administrative

**Triaging Team:**

We observed that Short has detected the traffic from source address [4.7.145.55] towards the destination address [4.7.145.20], triggering multiple signatures relating to PHP web services. From the signatures observed, this appears to be a result of exploitable user data, as the response activity is localized to Short. An exploitation onto the requested URL from targeting and unpatched URL directed showed relation to PHP CGI Scanning. A lookup on the source address was found to be pre-located in California, California, Pennsylvania in the United States, and was recently reported for abuse activity, likely for web app attack. It is advisable to check the fingerprint of the traffic behind it.

https://www.abuseips.net/lookup/4.7.145.55 - info about source address

https://www.abuseips.net/lookup/4.7.145.20 - info about destination address

**ProSOC Reconciliation Team:**

This risk triggers on the unique "Trojan activity" signatures between a source and destination IP address pair in a short period of time. This can be an indicator of command and control activity. Please secure the system modulated for compromise. This is an unexplained activity, blocking the host in the interim should be considered.

*Regards,*
WHAT THE SIEM VENDORS DON’T SAY?

SIEM is Just a Tool

People are Required

Without Airtight Processes, it Won’t be Effective
SOC STAFFING

Infrastructure Management
- SIEM
- Log Collection
- Log Storage

Content Author
- creates & tunes Use Cases continuously

SOC Analyst Tier 1
- monitors, validates, investigates, & triages

Security Engineer
- advanced analysis, response, post incident investigation & remediation

Threat Hunter
- looks for the unknown and stays current with emerging threats

Threat Intelligence Manager
- stays current with fast moving emerging threats

Incident Responder
- Containment / IR root cause investigate / scope investigate

Manager
- manages the teams and KPI metrics
Sample Metrics for 100M Log Events per day

- 1,000 Alerts or Notables without tuning Use Cases for SOC Analyst to Investigate
- Goal is <2-3 Actionable Alerts with context, triage, and IR guidance
- Without Excellent SOC Workflow: Average SOC Analyst performs 10-15 Investigations day
- Requires 4 SOC Analysts per 24 hours or 8 SOC Analysts for 24x7x365
- With optimized SIEM and SOC: Average SOC Analyst performs 25-30 Investigations per day
Total Economic Impact Study on ROI of SOC-as-a-Service

Key Quantifiable Benefits include:

- Avoided cost of staffing to achieve the same services valued at $845,530
- Improved staff productivity valued at $182,907
- Avoided cost of retired security tools valued at $179,856
- Incremental projects provided by existing in-house team valued at $70,999
- Reduced cost of minor security breaches totaling $111,908
ADVANCEMENTS IN SIEM/SOC AUTOMATION

Extending Discovery
- UEBA – Use Cases
- Application Aware - both cloud and on premise

Machine Enhanced Human Decision Making
- Machine Learning
- Artificial Intelligence

Incident Response Orchestration
- Automated Containment
- Guided Playbook

Business Intelligence of Security for the Boardroom
1. List Your Goals
   - MTTD, MTTC, MTTR, and Visibility Mapping of Your Environment
   - How will Map to your Cybersecurity Framework (NIST Identify, Protect, Detect, Respond, Recover)

2. Build a Scope & Resource Model for SIEM and SOC
   - What logs will you collect, this will drive your resource model requirements
   - Define critical Use Cases
   - Engage stakeholders and executive management

3. Build a Total Cost of Ownership Comparison Model
   - This will drive budget and in-house or outsource decisions

4. Define KPI’s and What is Presented to the Board
   - What are your Security Program Key Performance Indicators
Crossing the Chasm

- Enable business context modeling in Use Cases for Situational Awareness and Response
- Enable 5 to 10 use cases per log source and operational area – focus on kill chain discovery
- Integrate threat intelligence with use cases
- Enable SOC workflow application with full life cycle of an event management
- Enable Automated and Orchestrated Incident Response
- Measure and manage by KPI’s
THANK YOU!

Mike Ostrowski | VP | Proficio
mostrowski@proficio.com