RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

MATTERS

SESSION ID: TECH-F02

FROM SIEM TO SOC: CROSSING THE CYBERSECURITY CHASM

Mike Ostrowski

VP
Proficio
@proficioinc

EXPERIENCE FROM THE CHASM

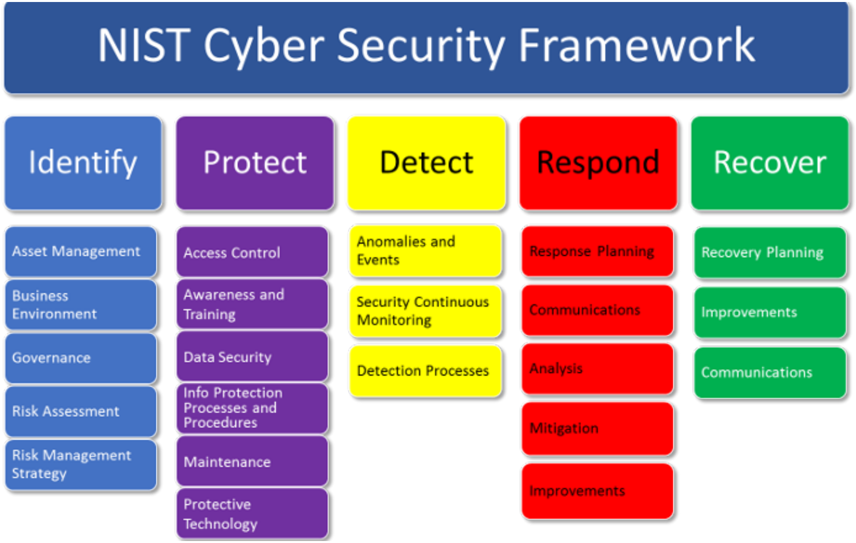
- Managed Detection and Response Service Provider
- Three Global Security Operations Centers
- Both Cloud Based SIEM / SOC and Hybrid SIEM / SOC
- Operate over 18 SIEM platforms in our SOCs
- Co-Manage many SIEM platforms for Clients plus SOC-as-a-Service
- Experience with SIEM, SOC, Threat Intel, Incident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

SIEM FOUNDATION

- 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

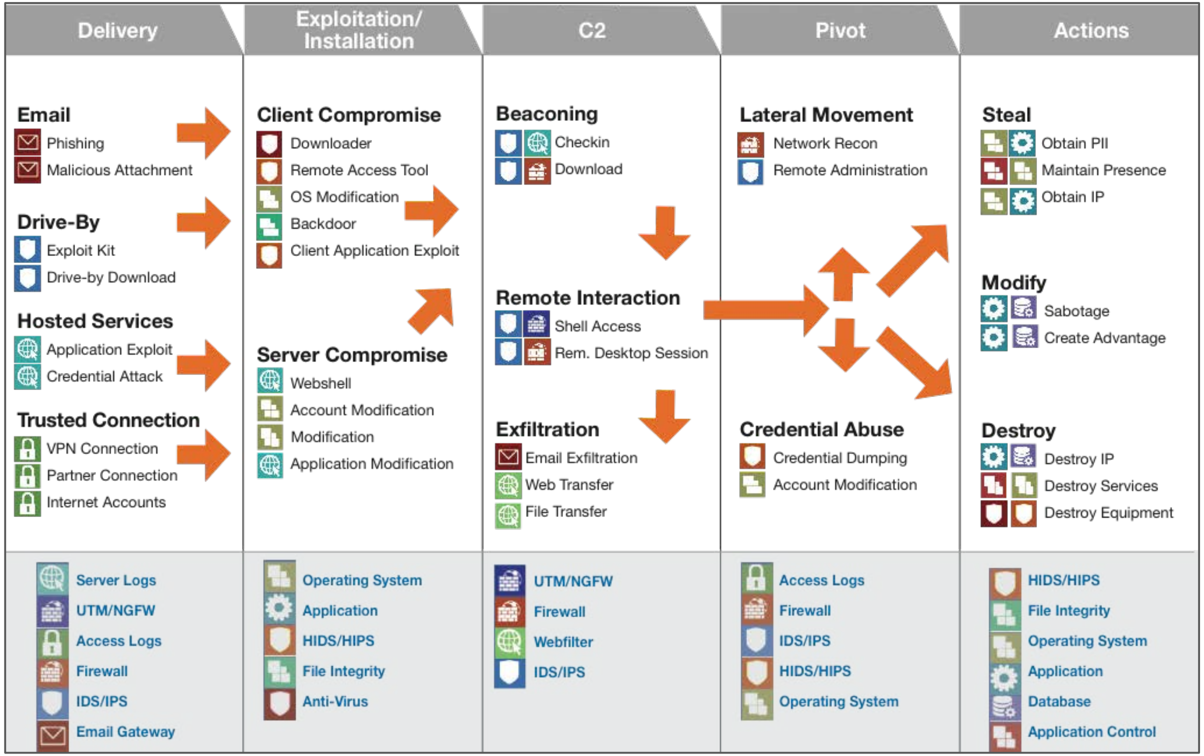


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

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



Delivery

Email
- Phishing
- Malicious Attachment

Drive-By
- Exploit Kit
- Drive-by Download

Hosted Services
- Application Exploit
- Credential Attack

Trusted Connection
- VPN Connection
- Partner Connection
- Internet Accounts

Server Logs
UTM/NGFW
Access Logs
Firewall
IDS/IPS
Email Gateway

Exploitation/ Installation

Client Compromise
- Downloader
- Remote Access Tool
- OS Modification
- Backdoor
- Client Application Exploit

Server Compromise
- Webshell
- Account Modification
- Modification
- Application Modification

Operating System
Application
HIDS/HIPS
File Integrity
Anti-Virus

C2

Beaconing
- Checkin
- Download

Remote Interaction
- Shell Access
- Rem. Desktop Session

Exfiltration
- Email Exfiltration
- Web Transfer
- File Transfer

UTM/NGFW
Firewall
Webfilter
IDS/IPS

Pivot

Lateral Movement
- Network Recon
- Remote Administration

Credential Abuse
- Credential Dumping
- Account Modification

Access Logs
Firewall
IDS/IPS
HIDS/HIPS
Operating System

Actions

Steal
- Obtain PII
- Maintain Presence
- Obtain IP

Modify
- Sabotage
- Create Advantage

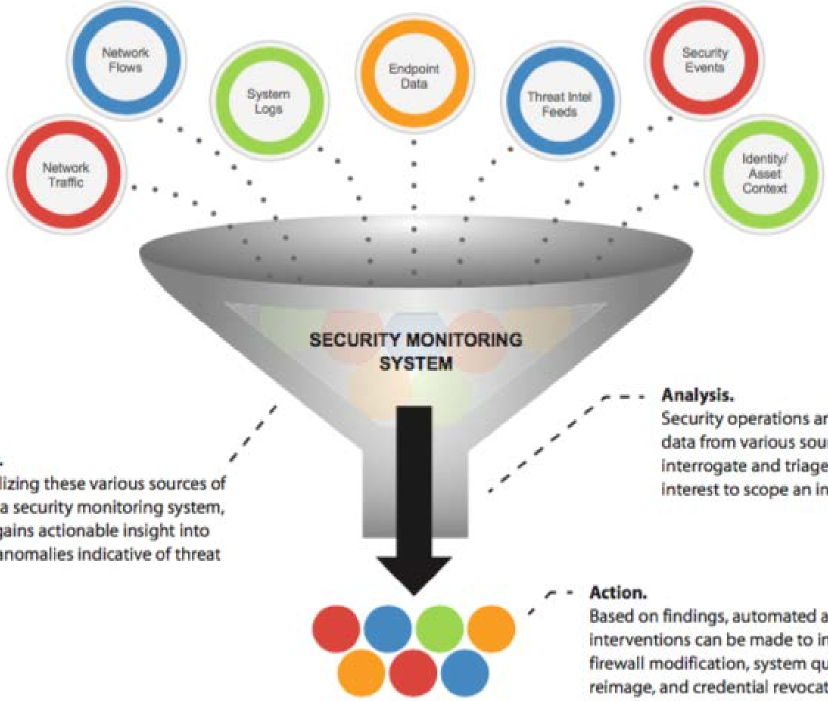
Destroy
- Destroy IP
- Destroy Services
- Destroy Equipment

HIDS/HIPS
File Integrity
Operating 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



Visibility.
By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into possible anomalies indicative of threat activity.

Analysis.
Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

Action.
Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

SAMPLE ESCALATION

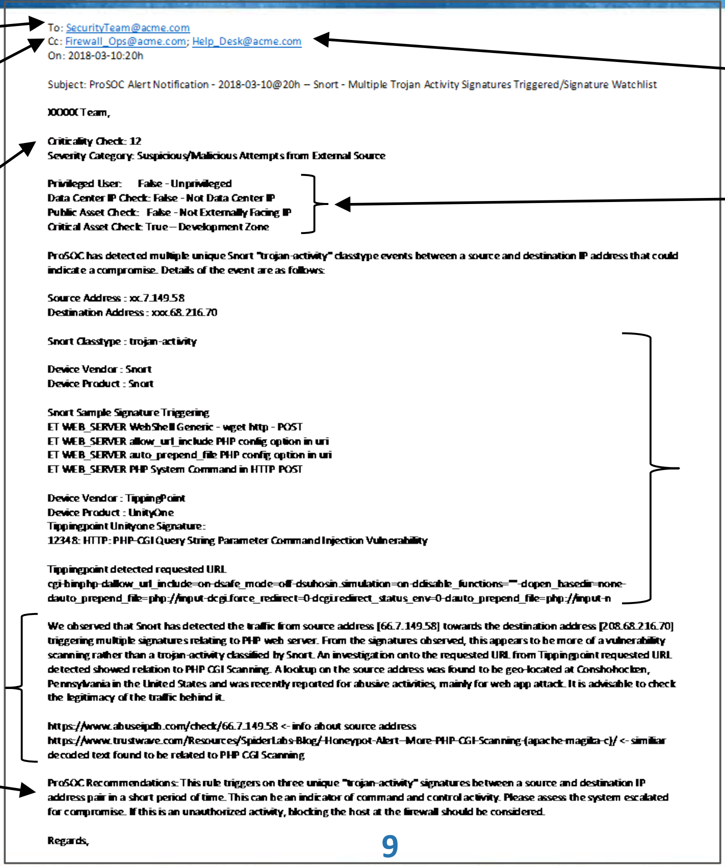
Security Team

Triage and Ticket to Network Team

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

SOC Analyst Analysis of Event and Research Source

SOC Analyst Manual Response Recommendation



To: SecurityTeam@acme.com
Cc: Firewall_Ops@acme.com; Help_Desk@acme.com
On: 2018-03-10:20h

Subject: ProSOC Alert Notification - 2018-03-10@20h – Snort - Multiple Trojan Activity Signatures Triggered/Signature Watchlist

XXXXX Team,

Criticality Check: 12
Severity Category: Suspicious/Malicious Attempts from External Source

Privileged User: False - Unprivileged
Data Center IP Check: False - Not Data Center IP
Public Asset Check: False - Not Externally Facing IP
Critical Asset Check: True – Development Zone

ProSOC has detected multiple unique Snort "trojan-activity" classtype events between a source and destination IP address that could indicate a compromise. Details of the event are as follows:

Source Address : xx.7.149.58
Destination Address : xxx.68.216.70

Snort Classtype : trojan-activity

Device Vendor : Snort
Device Product : Snort

Snort Sample Signature Triggering
ET WEB_SERVER WebShell Generic - wget http - POST
ET WEB_SERVER allow_url_include PHP config option in uri
ET WEB_SERVER auto_prepend_file PHP config option in uri
ET WEB_SERVER PHP System Command in HTTP POST

Device Vendor : TippingPoint
Device Product : UnityOne
Tippingpoint Unityone Signature:
12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability

Tippingpoint detected requested URL
cgi-binphp-dallow_url_include=on-dsafe_mode=off-dsuhosin.simulation=on-ddisable_functions=""-dopen_basedir=none-dauto_prepend_file=php://input-dcgi.force_redirect=0-dcgi.redirect_status_env=0-dauto_prepend_file=php://input-n

We observed that Snort has detected the traffic from source address [66.7.149.58] towards the destination address [208.68.216.70] triggering multiple signatures relating to PHP web server. From the signatures observed, this appears to be more of a vulnerability scanning rather than a trojan-activity classified by Snort. An investigation onto the requested URL from Tippingpoint requested URL detected showed relation to PHP CGI Scanning. A lookup on the source address was found to be geo-located at Conshohocken, Pennsylvania in the United States and was recently reported for abusive activities, mainly for web app attack. It is advisable to check the legitimacy of the traffic behind it.

https://www.abuseipdb.com/check/66.7.149.58 <- info about source address
https://www.trustwave.com/Resources/SpiderLabs-Blog/-Honeypot-Alert--More-PHP-CGI-Scanning-(apache-magika-c)/ <- similiar decoded text found to be related to PHP CGI Scanning

ProSOC Recommendations: This rule triggers on three 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 assess the system escalated for compromise. If this is an unauthorized activity, blocking the host at the firewall should be considered.

Regards,

Triage and Ticket to Desktop Team

Auto Generate Incident Response Classifications Based on Use Case

Data Enrichment for SOC Analyst and Responders

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 w/ emerging threats

Threat Intelligence Manager

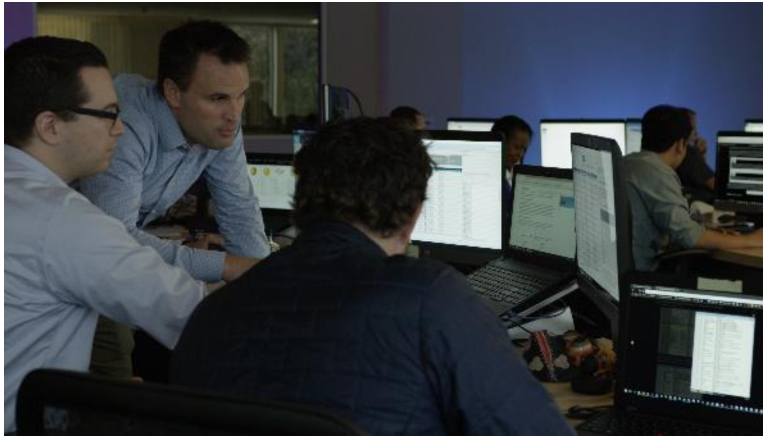
- stays current with fast moving emerging threats

Incident Responder

- Containment / IR root cause investigate / scope investigate

Manager

- manages the teams and KPI metrics



SOC BY THE NUMBERS

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

FORRESTER TEI REPORT

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

ROI

402%

NPV

967K

Payback

< 3

months

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

HOW TO APPLY THESE LESSONS

Preparation

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

HOW TO APPLY THESE LESSONS

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

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: TECH-F02

FROM SIEM TO SOC: CROSSING THE CYBERSECURITY CHASM

THANK YOU!

Mike Ostrowski | VP | Proficio
mostrowski@proficio.com