Day in the Life of the SOC
Security Operations Center at WSU

Jim Walsborn
Security Operations Manager
Washington State University

Other Team members:
Rebecca Solen
Brian Hall
Zvikomborero Masike (Intern)

Currently Recruiting for Security Analyst III (Apply!)
Overview

• Introduction
• In the Morning
• Incident Response
• Education
Introduction

Cybersecurity is a Lifestyle

• Why it’s a lifestyle
  • Failure is inevitable
  • Threat intelligence
  • Incident Response
  • Documentation
  • No friends
In The Morning
There’s rarely a dull day, but some are quieter than others

- Threat Intelligence
  - Feeds
  - Indicators of Compromise
    - Hashes
    - IP addresses
    - Yara
      - Primarily used in malware research and detection. A description is essentially a YARA rule name, where these rules consist of sets of strings and a boolean expression.
  - XQL (XML Query Language) (XML=extensible markup language)
  - SPL (Search Processing Language)
    - Putting it all together
In The Morning
Continued

• Workflow
  • Watching different systems, moving through all the tools
    • Patching
    • PCI (Payment Card Industry)
    • Various SPL Dashboards
    • Endpoint Incident counts assessments
    • Information Security Services Jira Service Desk
    • Email Security
Incident Response

• Assess True Positive Vs. False Positive
  - FP
    • Usually requires some type of whitelisting, exception or exclusion
  - TP
    • Analyze and understand Incident
    • Contact department Area Technical Officer/helpdesk depending upon local Incident Response Plan
    • Remediation
    • Lessons Learned discussion within the SOC

• 24/7
  - Incident Response happens throughout the day everyday
Incident Response
Continued

• End User Reported Incidents
  - Usually require more in-depth analysis
  - Phishing campaigns
  - Coordination between departments
  - Remediation
  - Documentation and Lessons learned
All Together

Threat Intelligence

Documentation/Lessons Learned

SOC Analyst Gathered & Dynamic

Remediation

Systems (Firewalls, Endpoint Security)

Incident Response

Threat Hunting for evidence of Compromise
Education

• Love to Learn
  - New threats = new security
  - All systems all protocols

• Practice Your Cybersecurity Skills

• Engage in the Cybersecurity Community
Questions?

• Contact info
  - Jim.Walsborn@wsu.edu (love collaborating and sharing information)