

# CI/CS WORKSHOP

## THE COMMUNITY TOGETHER



Researchsoc

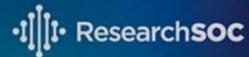


CICoE<sup>PILOT</sup>

# Developing a Network Monitoring Strategy

Scott Orr, SOC Operations Manager, OmniSOC  
Mark Krenz, CISO, ResearchSOC

**CI/CS WORKSHOP**



# Compromise is Inevitable

**Attacker** only has to be successful **once**, but  
the defender has to stop **100% of attacks**

Source: Ben Johnson, [Threat Hunting as a Culture \(HaaC\)](#) SANS Threat Hunting & Incident Response Summit, 2016

# So game over...



Source: <https://mindtheflap.files.wordpress.com/2018/03/sherlock-wrong-qif.gif?w=676>

CI/CS WORKSHOP

•|||• ResearchSOC | ☀️ CI CoE PILOT

# Compromise is Inevitable but...

**Attacker** only has to be successful **once**, but  
the defender has to stop **100% of attacks**  
**But...**

Once the attacker is in your environment, **they**  
**should have to be 100% perfect**

Source: Ben Johnson, [Threat Hunting as a Culture \(HaaC\)](#) SANS Threat Hunting & Incident Response Summit, 2016

# Phases of Attack - Cyber Kill Chain



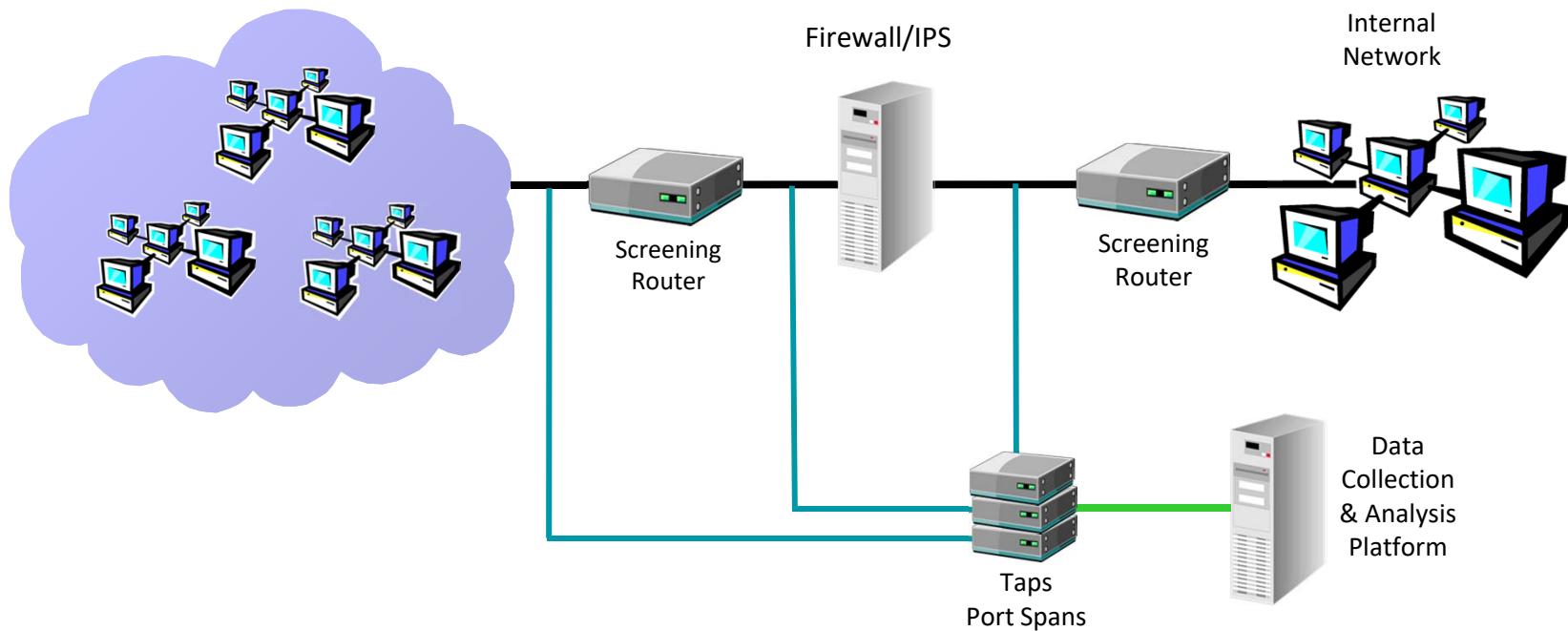
Source: <https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

# Time to Detect

- System/credential compromise ≠ Attacker mission accomplishment
- How long do attackers need once inside to **succeed?**
  - Elevate access/Install backdoors/Cover tracks
  - Lateral movement: Recon/Compromise additional systems
  - Locate/Exfiltrate target data!
- Average time to detect (dwell time): 56 days\*
- Goal: Detect/Respond/Recover before attackers achieve their goals

\*Source: [Mandiant M-Trends 2020 Report](#)

# Network Sensors



# Network Data Capture

- Full Packet Content
- Extracted Content
- Session
- Statistical
- Transaction

# So much data!!!



Source: <https://www.drsanders.com/wp-content/uploads/2014/12/Drowning-in-Paperwork.jpg>

# Netflow Data

- Keeping all network packet capture data is expensive
  - Storage
  - Ability to search
  - Privacy
- Netflow provides network traffic summaries
  - Sessions/Services/Protocols
  - Session duration
  - Session packet and byte count

# Zeek Network Security Monitor

- Collects and analyzes network data via passive taps
- Includes modules (analyzers) to examining application layer services
  - DNS
  - SMTP
  - HTTP/HTTPS
- Can be customized to act as a Network Intrusion Detection System (NIDS)

# Network Intrusion Detection/Protection Systems

- NIDS alerts when (potential) malicious network activity detected
- Signature-based Rules
  - Known Network/Service Attacks
  - Unexpected Services
  - Spoofing
  - Content (e.g. Web Data)
  - Policy Violations
- Behavioral-based Rules
  - Port Scans
  - Denial of Service
  - Worms
- Intrusion Protection Systems (NIPS) can dynamically block when rules are triggered

# Data Collection Starting Point Examples

- Network/Service Data
  - Netflow
  - Zeek
- NIDS/NIPS
  - Snort / Suricata
- Next-Gen Firewalls (NGFW):
  - Cisco ASA FirePower
  - Palo Alto devices

# So many places to check...



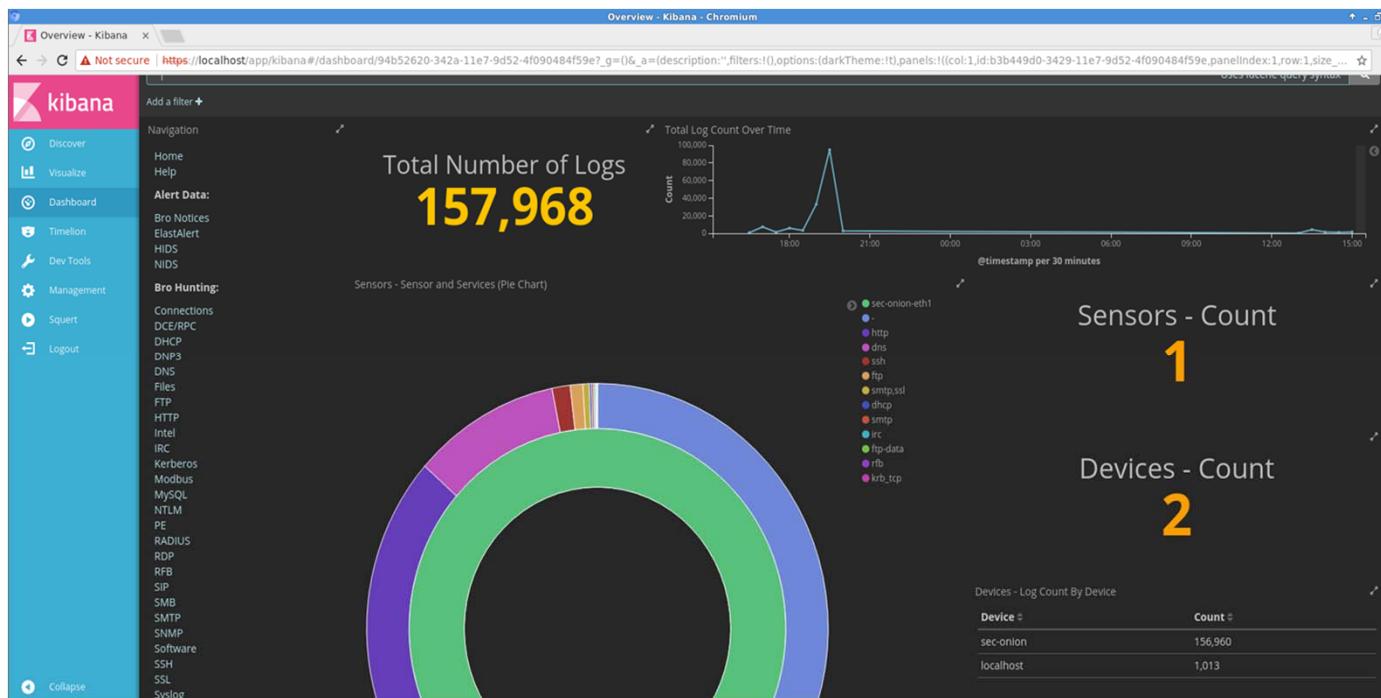
Source: <https://memegenerator.net/instance/72618553/sixth-sense-boy-i-see-data-everywhere-and-they-are-very-big>

# Security Information and Event Management (SIEM)

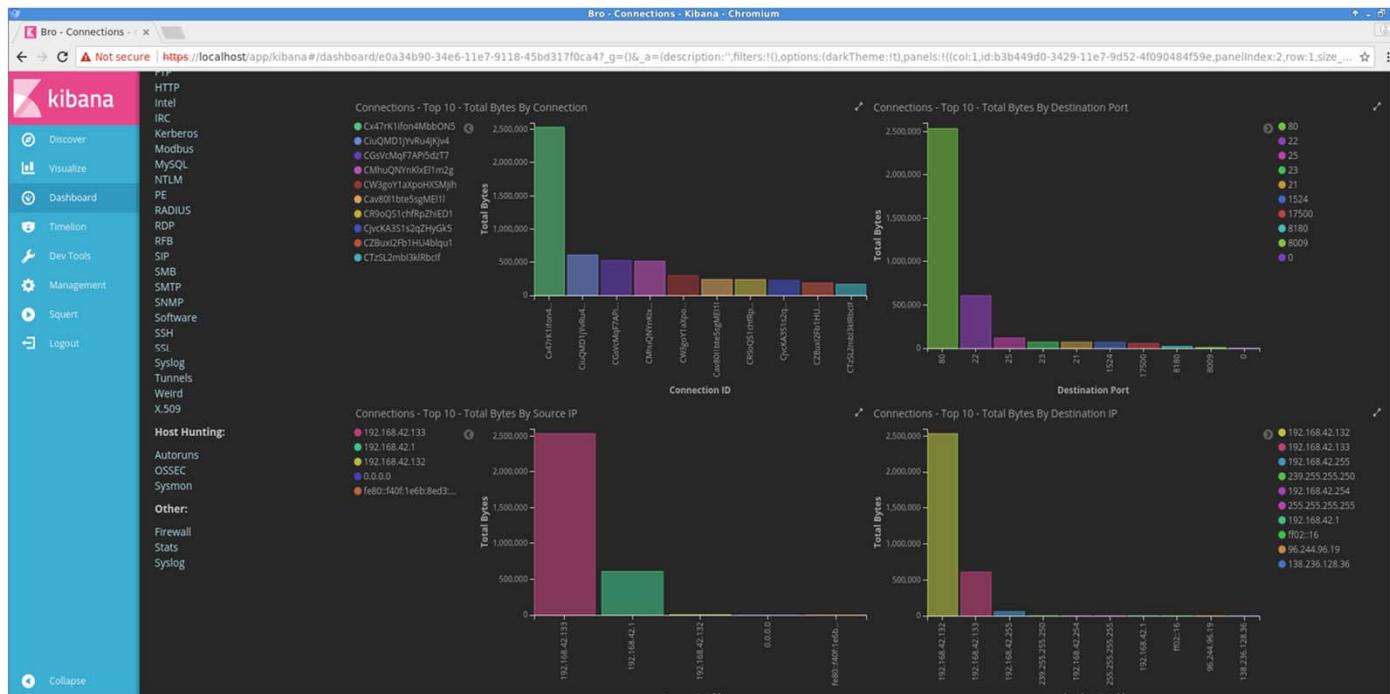
- System used by SOCs to analyze security related data
- Components/Capabilities
  - Data aggregation
  - Correlation
  - Alerting
  - Dashboards
  - Forensics
  - Compliance
  - Data retention
- Examples: Elastic, Splunk

Source: [https://en.wikipedia.org/wiki/Security\\_information\\_and\\_event\\_management](https://en.wikipedia.org/wiki/Security_information_and_event_management)

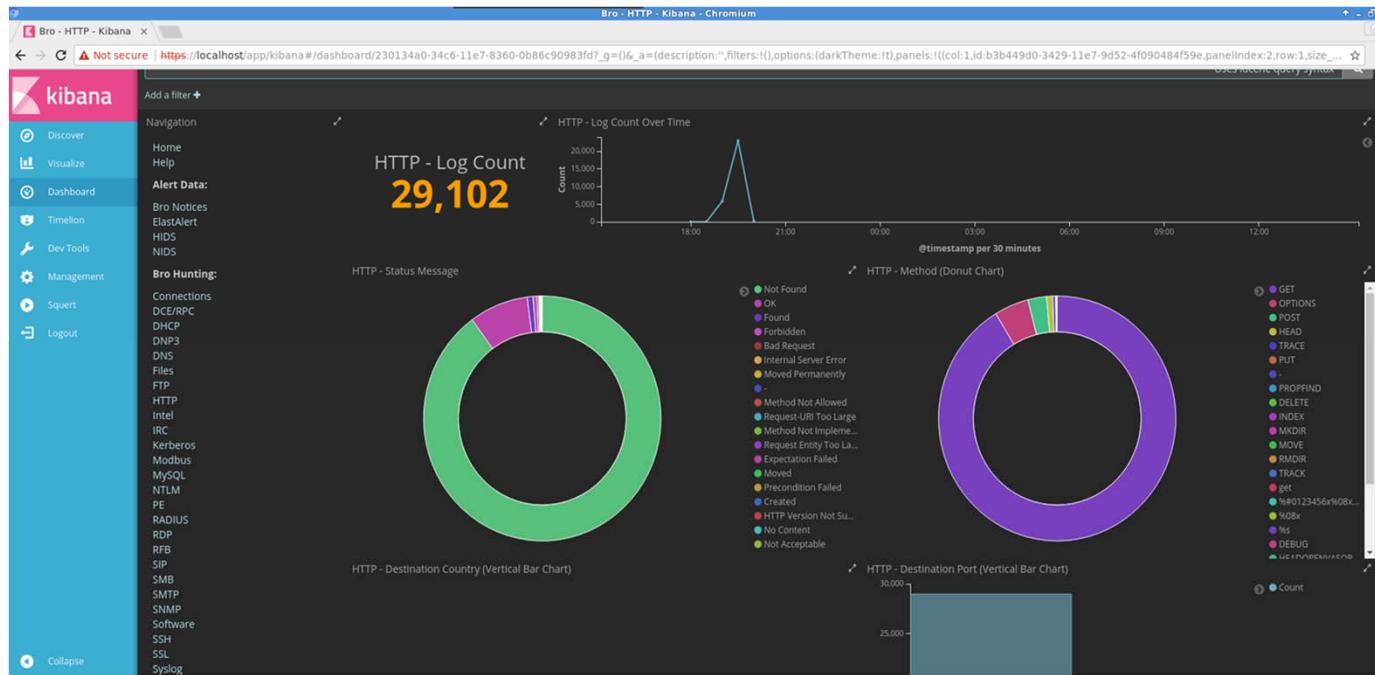
# Security Onion Dashboard - Overview



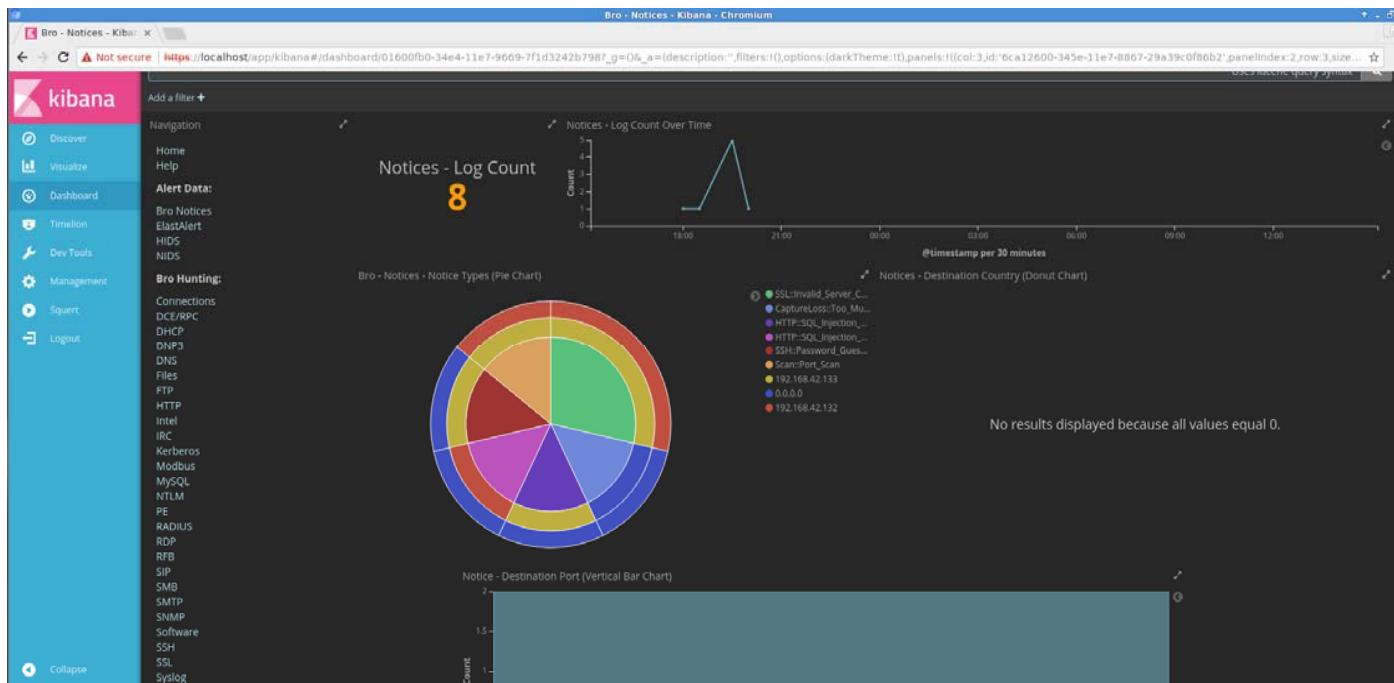
# SO Dashboard – Zeek Connections



# SO Dashboard – Zeek HTTP



# SO Dashboard – Zeek Notices

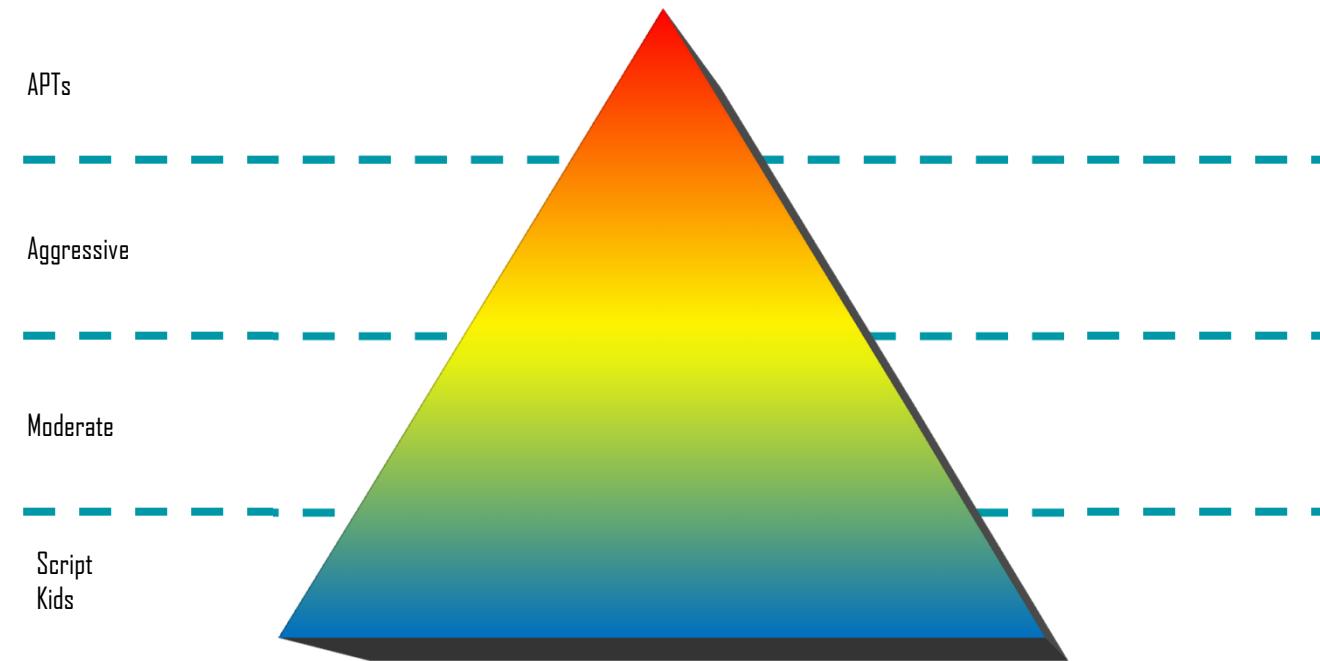


# Detective Mode: On



Source: <https://media.giphy.com/media/3o7TKVSE5isogWqnwk/giphy.gif>

# Threat Pyramid



Source: Tom Perrine, SDSC, Security as Infrastructure, USENIX LISA 1998

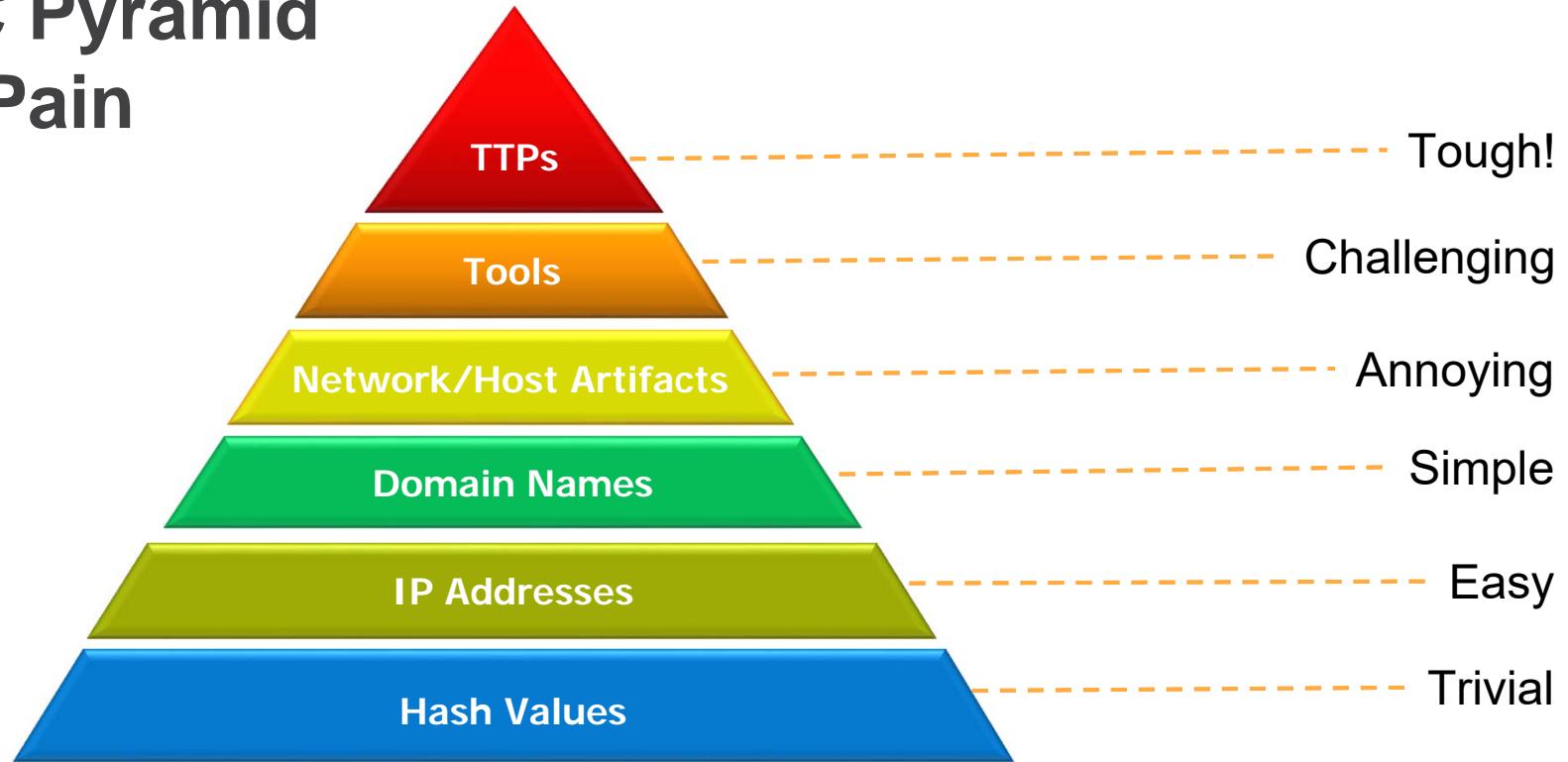
# Advanced Persistent Threats (APTs)

- State and Non-State Sponsored Intruder groups
- Advanced: Use of sophisticated tools/techniques
- Persistent:
  - Remain inside network for long period
  - External Command and Control (C2)
- Threat: Attackers with an agenda



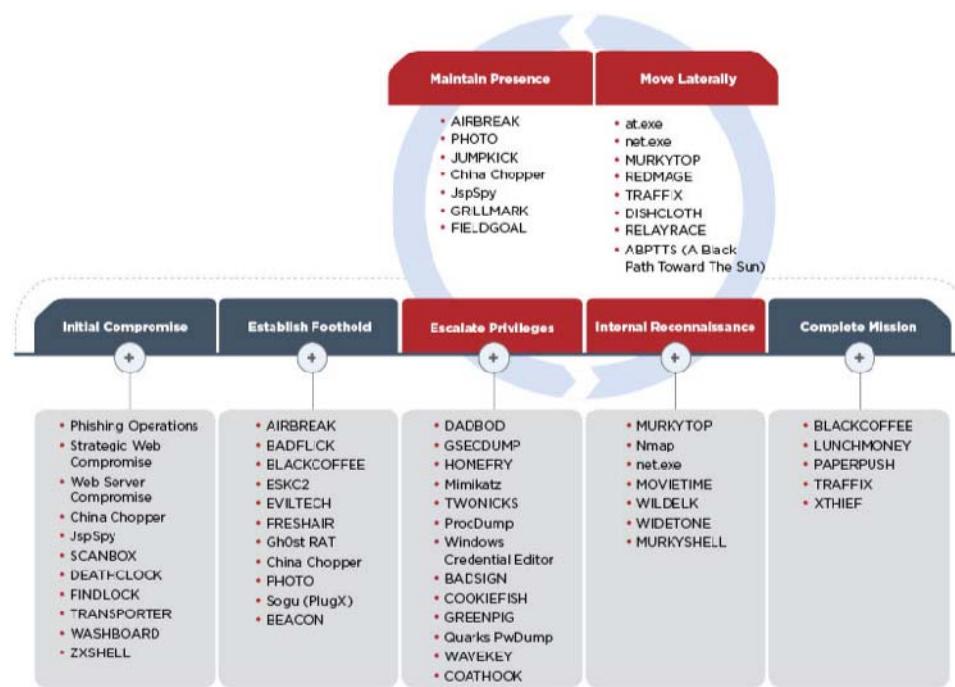
Source: <https://vignette.wikia.nocookie.net/bakerstreet/images/b/bc/MoriartyCrown.png/revision/latest?cb=20140113071813>

# IoC Pyramid of Pain



Source: <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

# TTP Example: APT40



Source: <https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html>

# Where to start?

- NIDS Alerts
  - Newly encountered alerts
  - Recent alert spikes
- Deny lists
  - Known bad
  - Shared Threat Intelligence
- Allow lists
  - Anything not known to be good
  - Know thy environment
- Long Tail Analysis
  - Least occurring events
- Anomaly Detection
  - Baselines, Machine Learning

# Verify!!!



Source: <https://socprime.com/en/blog/deliver-ti-feeds-into-arcgis-without-false-positive-triggers/>

CI/CS WORKSHOP

••• ResearchSOC | CI CoE PLOT

# Event Analysis – Phase 1

- What do we know?
  - Can we corroborate what we see? Multiple data sources?
- What don't we know?
  - Is there more information available elsewhere? Can we get to it?

Source: General Colin Powell, [It Worked For Me](#)

# Endpoint Data

- System logs
  - User logins/logouts, Resource access requests, application accounting
- Performance metrics
  - CPU load, memory usage, disk usage, network usage
- Service transaction logs
  - Web server, email server, database server, DNS
- Host Intrusion Detection system(s)
  - Anti-virus
  - Firewall
  - Integrity checkers

# External Data Sources/Tools

- What kinds of info is out there?
  - Hashes
  - IP Addresses
  - Domain Names
  - URLs
- Threat Intel Sites?
  - Open Source
  - Commercial/Membership Sharing Sites
- Honeypots/Honeynets

# Event Analysis – Phase 2

- What do we know?
  - Can we corroborate what we see? Multiple data sources?
- What don't we know?
  - Is there more information available elsewhere? Can we get to it?
- What do we think happened?
  - Golden nuggets, prior experiences, hunches/instinct, collaboration
- Distinguish which from which.
  - Decision time! Confidence level?

Source: General Colin Powell, [It Worked For Me](#)

# Now what?



Source: <https://media.giphy.com/media/xT8qB3utUzMWqmpH20/giphy.gif>

# Notes on Incident/Threat Info Sharing

- We deal with a lot of sensitive data!
- Sharing Model: Traffic Light Protocol (TLP)
  - Classifying audiences that can receive information
  - White: Disclosure is not limited
  - **Green**: Limited disclosure, restricted to community
  - **Amber**: Limited disclosure, restricted to participant organizations
  - **Red**: Not for disclosure, restricted to participants only
- When in doubt – **RED!**

Source: <https://www.first.org/tlp/>

# Several Great Blogs and Video

## Blogs

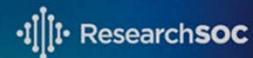
- [KrebsOnSecurity](#)
- [PaulDotCom](#)
- [Tao Security](#)
- [Schneier on Security](#)
- [Darknet](#)
- [ThreatPost](#)
- [SANS Cyber Defense](#)
- [SANS Digital Forensics and Incident Response Blog](#)
- [SANS Internet Storm Center \(ISC\)](#)

## Youtube Channels

- [SANS Institute](#)
- [SANS Digital Forensics and Incident Response](#)
- [SANS Pen Test Training](#)
- [Black Hat](#)
- [DEFCONConference](#)
- [Hackers Security](#)
- [IronGeek](#)

# Questions?

CI/CS WORKSHOP



CICoE  
PILOT

# Thank you!

Scott Orr, [smorr@iu.edu](mailto:smorr@iu.edu)

Mark Krenz, [mkrenz@iu.edu](mailto:mkrenz@iu.edu)

**CI/CS WORKSHOP**



CICoE  
PILOT