Introduction to Threat Hunting - Overview

Brian Olliff

Defensive Engineering Instructor

Key Concepts

+ **Fundamentals of Threat Hunting**

+ **Threat Hunting Preparation**

MAJOR TOPICS

- Threat Hunting Overview
- Common Terms
- Frameworks/Models
- Organization Preparation

LEARNING OUTCOMES

- Understand what threat hunting is, and why it’s important
- Be able to use different strategies for effective hunting
- Understand common terminology and frameworks associated with threat hunting
- Be able to ensure an organization is prepared for hunting threats

PREREQUISITES

- Understanding of basic cybersecurity topics
- Knowledge of different types of attacks and attacker methods
- Fundamental understanding of IT logging

Let’s Get Started!

Introduction to Threat Hunting

+ Starting with overview of threat hunting and its importance
+ Strategies and terminology
+ Organization preparation

Threat Hunting Overview

What is Threat Hunting?

- Proactively looking for threats in infrastructure
  - Using logs from endpoints, network devices, authentication systems, etc
- Proactive vs reactive
  - Reactive - alerts from EDR, SOC, SIEM, IPS, etc
  - Proactive - searching through logs for indicators of compromise
  - Reactive methods are insufficient for advanced threats
- Uses “assumption of breach”
- Does not replace alert-based detections
  - Defense-in-depth

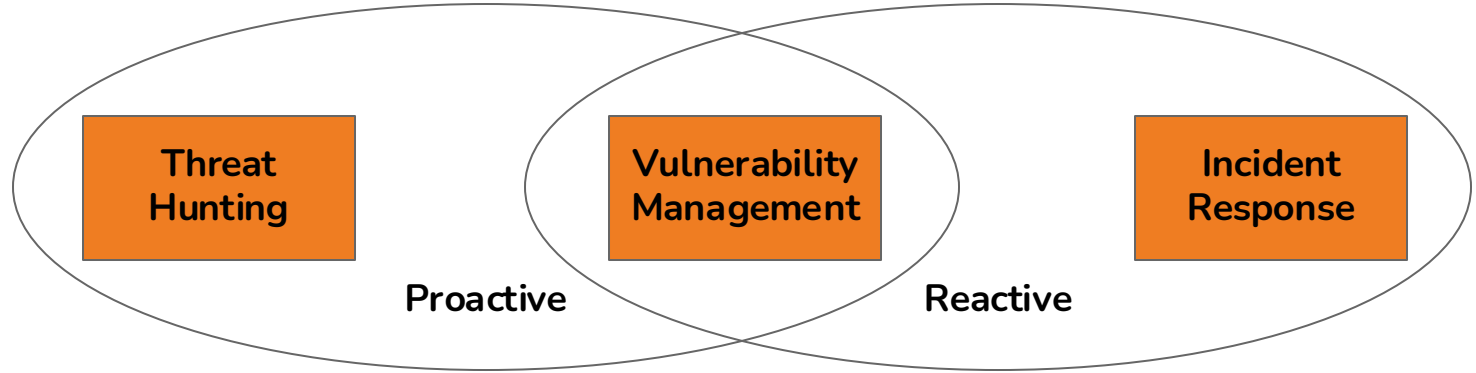
Assume Breach

- Investigating and analyzing assuming threat actor on network
- Requires many other assumptions and hypotheses
  - System that may be compromised
  - How system may be compromised
  - Threat actor involved
    - Adversary TTPs
- Not necessarily reacting to any threat or alert

Incident Response

- **Threat hunting ≠ incident response**
  - TH is a passive activity
  - IR is an active activity
- Threat hunters and incident responders work closely together
  - Hunters discover threats and relay information to responders
  - Responders often gather additional information to provide to hunters
    - Hash values, memory dumps, disk images, file contents, etc
    - Additional indicators for new threat hunts
- Responding to threats alters data on systems
  - Could affect in-progress hunt

Tools & Methods



Data Analytics

Automation & Orchestration

TTPs

Manual Analysis

Intelligence Information

Vulnerability Feeds

Threat Hunting Goals

- Detect advanced threats in infrastructure
  - “Routine/common” threats often detected by monitoring
- Advanced threats
  - Nation-state actors
  - Insider threats
  - New/advanced malware
- Reduce time that attackers are in network
  - Attempt to identify threats in early stages
  - Less time to cause damage, exfil data, etc

Importance of Threat Hunting

Dwell Time

- Amount of time adversary is on network undetected & retains access
  - Gather/exfil data, collect creds, lateral movement/privesc, deploy other tools
- Impacted by multiple factors
  - Detection of intrusion before goals achieved
  - Attacker achieves their goal(s), or detonates “noisy” payload
- 2022 - 16 days, 2023 - 10 days
  - According to Mandiant report
- Why is this important?

AV/EDR Limitations

- Systems work based off *pre-determined* detection rules
  - Signatures
  - User behavior
  - File hashes/filenames
- If attack doesn't match rule, security control isn't aware
- No alerts or actions if detection rule isn't triggered
- Require constant updating for awareness of new malware/attacks/tools

- Should still be used, but will not detect all threats

Better Defenses

- Threat hunting can discover many other security issues
  - Priority vulnerabilities that need remediation
  - Misconfigurations on endpoints
  - Unapproved software on workstations
  - Access issues
- All data found during hunt can be used to improve security of org
  - Adjustments of security controls
  - New security controls that need to be implemented
  - Improvements to logging infrastructure
  - Additional signatures/rules for detection systems

When to Hunt

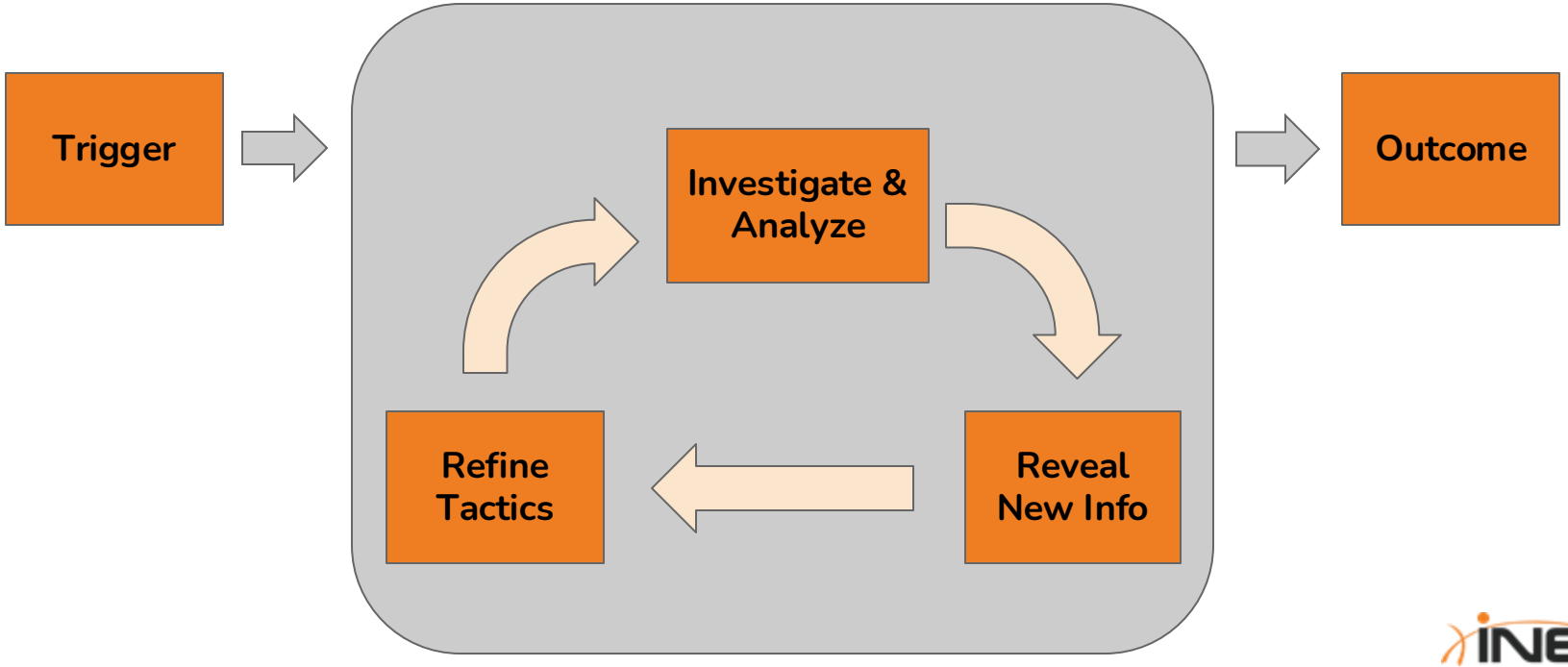
- Orgs with threat hunting teams often have scheduled hunts
  - Routinely performed based on various hypotheses
- New intelligence received about potential threat
  - Attacks against similar organizations/same industry
  - Actively exploited vulnerabilities in software/systems org uses
- SOC/IR teams report incident
  - Active incident that requires additional hunting
  - Anomalous activity on network
- Additional IOCs identified as part of previous hunt
- After completion of risk assessment
  - Verify riskiest assets/systems are secure

Threat Hunting Strategies

Phases of Threat Hunting

- Trigger
  - Reason for the hunt
  - Usually in form of hypothesis
- Investigation
  - Using hypothesis, search data for supporting evidence
  - Hypothesis may be adjusted during hunt, based on found evidence
- Resolution/outcome
  - What was the outcome of hunt?
  - Hypothesis true?
  - Communication and reporting of information
  - May pivot into new hunt

Threat Hunting



Types of Hunts

- Structured
  - Begins with searching for specific TTPs
  - Hypothesis based on attacker's method
  - Hunt based on possible symptoms of that type of attack
- Unstructured
  - Typically starts with IOCs and searching logs for them
- Situational
  - Focused on specific resources or systems in organization
  - Often starts with risk assessment - hunt based off those findings

Threat Hunting Terminology

Threat

- Any potential negative impact (or danger) to an asset
  - Asset - any item owned by individual or organization
- Threat actor - entity taking advantage of vulnerability/risk
- Threat/attack vector - path used to perform attack
- Types of threats
  - Natural disasters
  - Virus/malware
  - Data breach
  - Denial of service (DoS)
  - APTs

APT

- Advanced Persistent Threat
  - Used to refer to groups or types of malware
- Attacker group with significant resources, infrastructure, capabilities
  - Long-term detection evasion
  - Multi-stage attacks
  - Quick use of zero-days
  - Custom zero-days
- Different naming conventions
  - APT/UNC/FIN# - **APT29** (Mandiant/Google)
  - Animal names - **Cozy Bear** (CrowdStrike)
  - Weather events - **Midnight Blizzard** (Microsoft)

https://attack.mitre.org/groups/G0016/

TTPs

- Tactics, Techniques, and Procedures
- Methods or patterns used by threat actors
- Tactics
  - High-level description of behaviors and strategies
- Techniques
  - More specific methods describing how tactics can be implemented
- Procedures
  - Sequence of activities using specific techniques to carry out attacks
  - Can be tailored for different threat actors/groups

IOCs and Hashes

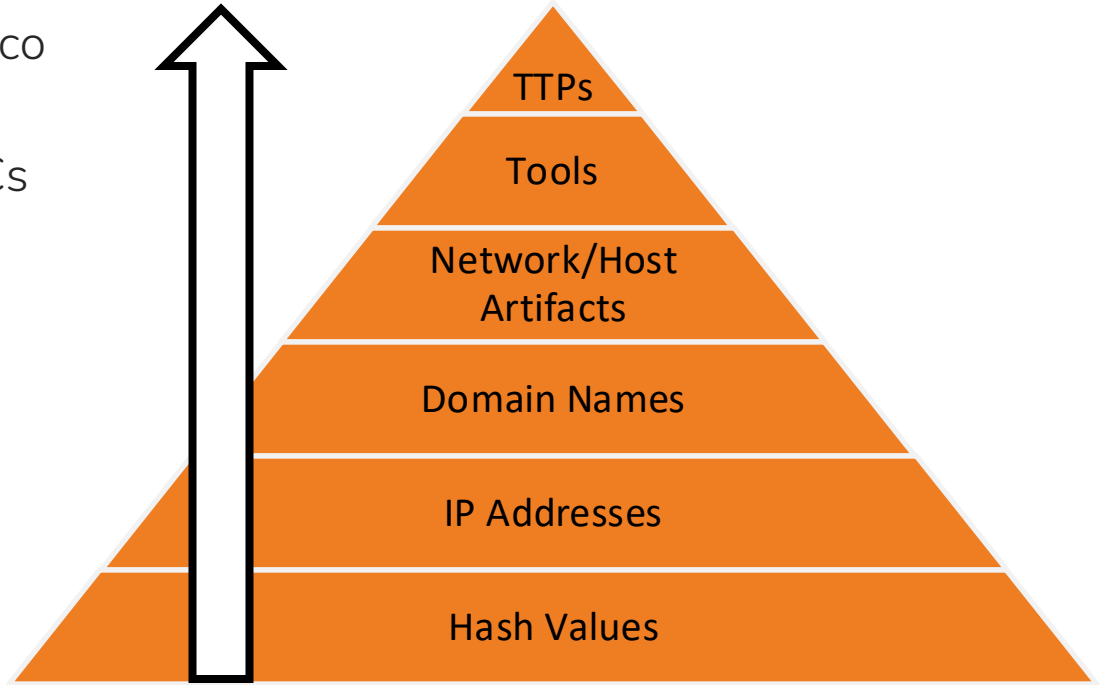
- Indicators of Compromise
  - Artifacts that may indicate presence of malicious activity
    - File hash, IP address, domain name, filename, strings, etc
    - Behavioral & other anomalous activity
  - Included in threat intelligence reports

- Hashes
  - Unique value that represents “digital fingerprint” of file
  - Generated by running file through hashing algorithm
  - MD5, SHA256/512, etc

Pyramid of Pain

Pyramid of Pain

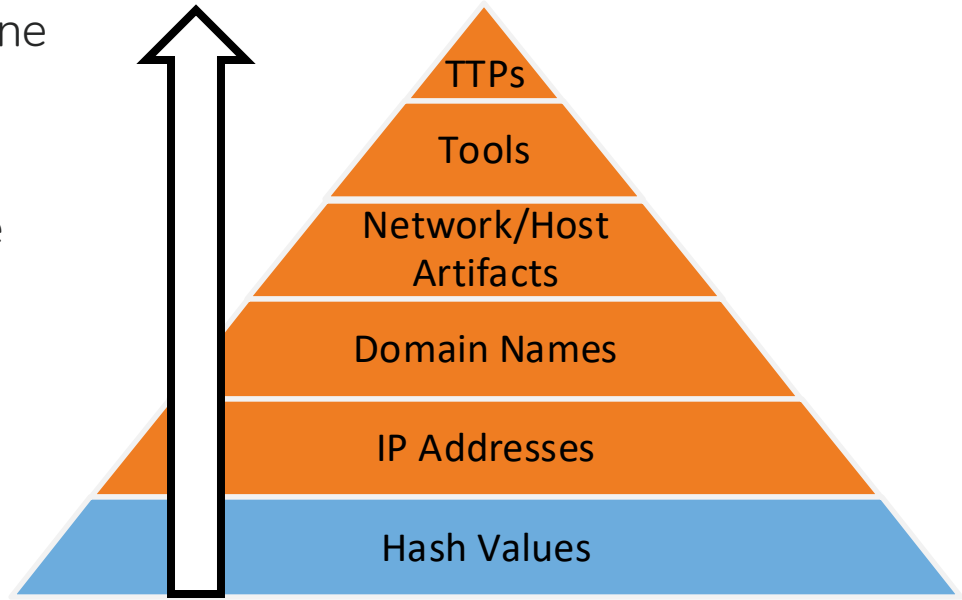
- Created by David Bianco
- Shows the difficulty in obtaining different IOCs
- Also level of effort for attacker to change



Hash Values

- Very easy to discover and use
- No question of compromise if one found

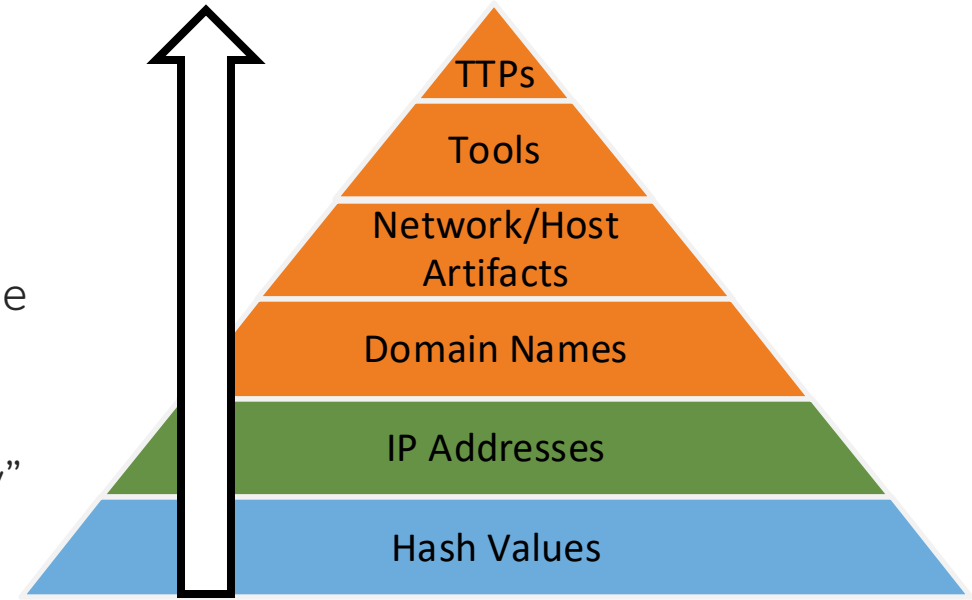
- Trivial for an attacker to change
- *Any* change to file results in completely different hash



IP Addresses

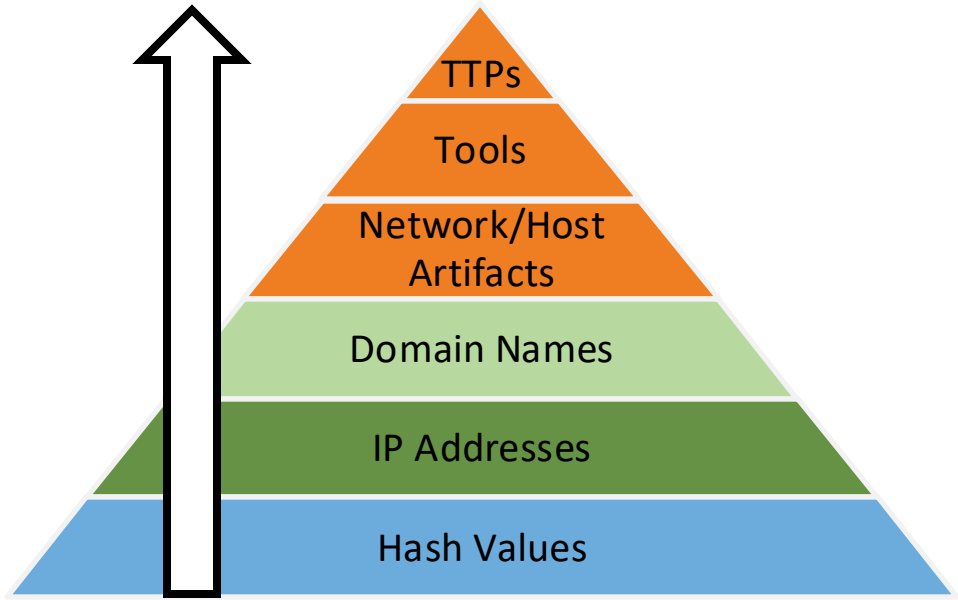
- One of most fundamental indicators
- If malicious IP found, near certainty of malicious activity

- Very easy for attacker to change
  - Especially if using domain names
- Many attackers use “temporary” IPs



Domain Names

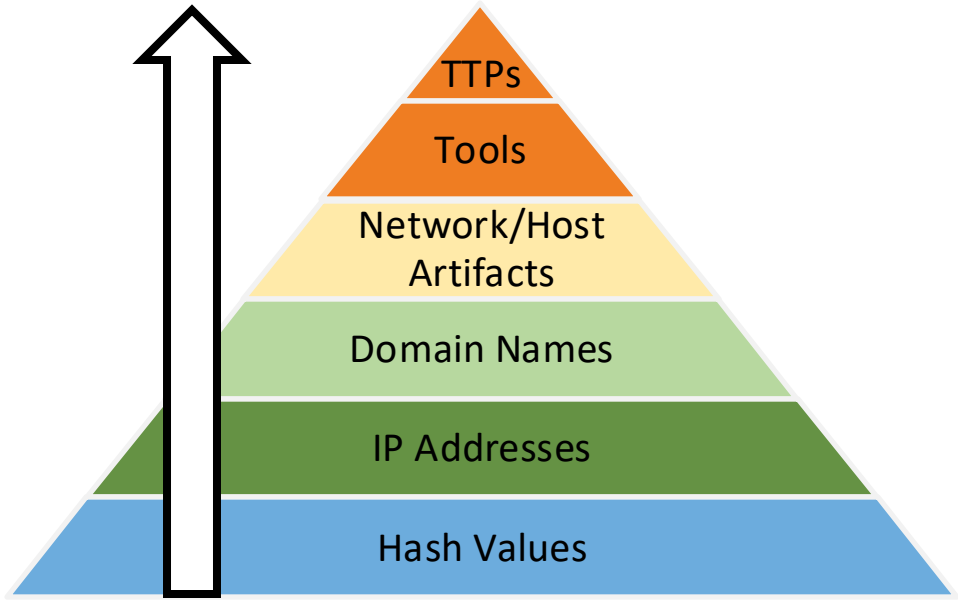
- Similar type of IOC as IPs
- More difficult for attacker to change
- Requires
  - Registration
  - Payment
  - Hosting
- May be delay in propagation



Network & Host Artifacts

- User-agent strings
- Traffic on non-traditional ports
- Specific file/registry key
- Non-browser process on port 80/443

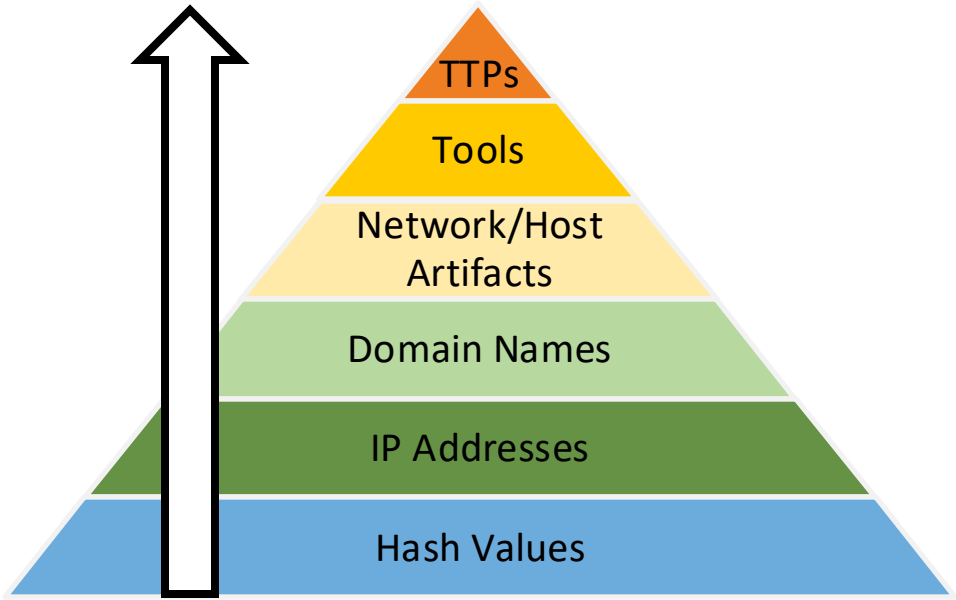
- Often requires attacker to reconfigure or recompile



Tools

- APT groups tend to use consistent set of tools
- Requires detection of specific artifacts of unique tools

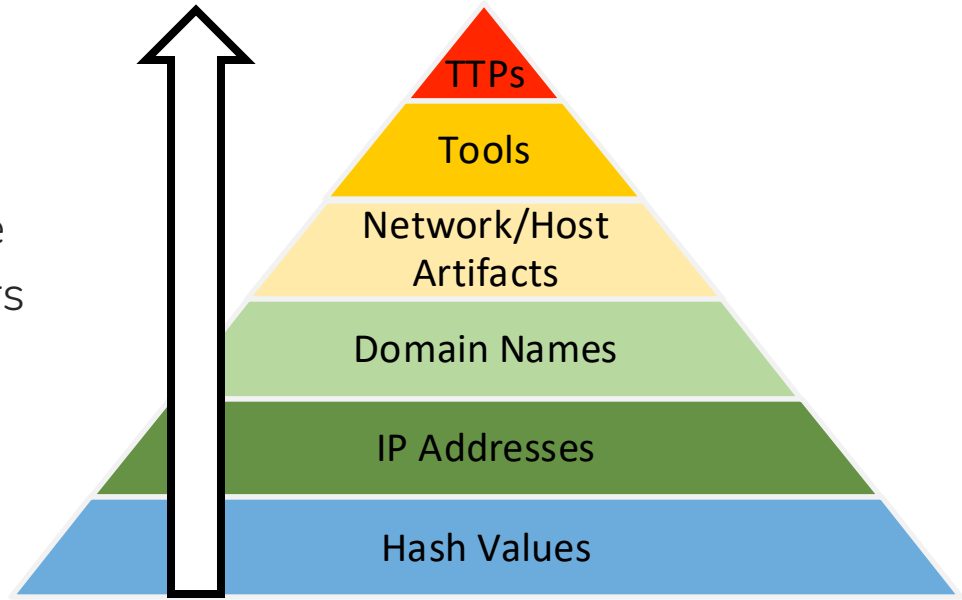
- Blocking specific tools requires adversaries to find/create new tools for same purpose



TTPs

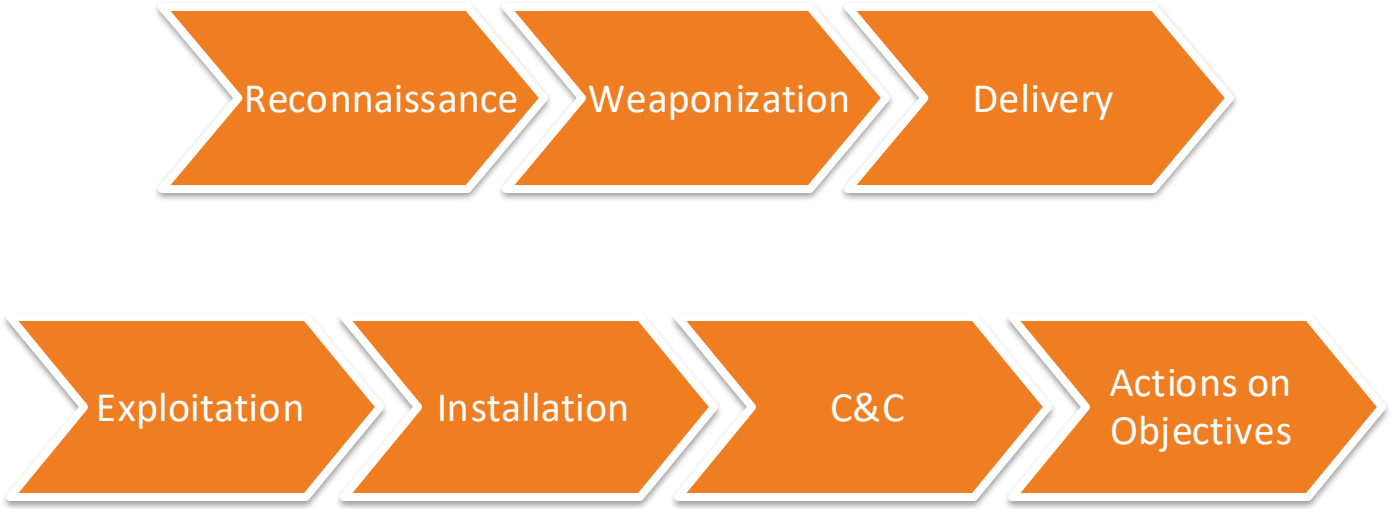
- Attacker's training, methods
- Detecting adversary **behavior**, not their **tools**

- If responding quickly, may force attackers to learn new behaviors



Cyber Kill Chain

Cyber Kill Chain



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Reconnaissance

- Attacker gathers information about target
- Passive and active methods
  - Internet searches
  - Email harvesting
  - Network scans

Weaponization

- Attacker creates deliverable payload
- May consist of
  - Remote access tool (RAT) or other backdoor
  - Encryption tools
  - Other malware downloader

Delivery

- Malicious payload sent to victim
  - Email
  - Watering hole attack (malicious website)
  - Drive-by download
  - Malicious USB drive

Exploitation

- Malicious payload is run on victim system
  - User opens email attachment
  - Visit to malicious website where malware downloads/runs
- Attacker may exploit other vulnerabilities using other methods
- Can be multi-step process
  - Original payload runs and downloads additional malware

Installation

- Additional tools installed via original RAT/backdoor
  - Encryption software
  - More complex malware
  - Command & control software
  - Exfiltration tools
- Any tools attacker needs to carry out objective

Command & Control

- Victim machine connects to attacker controlled infrastructure
  - May use well-known ports to evade firewall rules/detection
  - Traffic may be encrypted
- Allows additional commands and malware to be run
  - Attacker can further customize based on victim environment

Actions on Objectives

- Attacker accomplishes original goals based on all previous steps
  - Encryption and ransom demand
  - Data theft (and possible ransom)
  - Destruction of data or systems
  - Software disruption
  - Persistent access for further goals

MITRE ATT&CK

MITRE ATT&CK

- **A**dversarial **T**actics, **T**echniques, **& C**ommon **K**nowledge
- “Knowledge base of adversary tactics and techniques based on real-world observations”
- ATT&CK Matrix for Enterprise
  - Columns reflect tactics, which contain techniques
  - Over 230 techniques
  - Each contains explanation, procedure examples, mitigation, detection

Organization Preparation

Preparation

Threat Hunting Personnel

Data Collection

Aggregation & Analysis Tools

Appropriate Access

Threat Intelligence

Threat Hunting Teams

- Not necessarily a standard definition of team
  - Based on size of org, industry, systems, etc
- Ad-hoc hunter
  - Typically has multiple roles in IT/security
  - Hunts are more “task-oriented”
- Analyst and hunter
  - Most common in medium sized organizations
  - Security (SOC) analyst is also the threat hunter
- Dedicated hunting team
  - Most specialized
  - Several members whose sole purpose is threat hunting

Software and Systems

- Threat hunting requires data to be collected prior to hunt
- Logs from multiple systems ingested into central point (SIEM)
  - Also provides point for searching logs from multiple systems
  - Splunk & ELK stack
- Packet capture and analysis
  - Wireshark
- EDR systems
  - Provide additional data that may not be included in other logs
- Threat intelligence information
  - Data feeds, in-house team, third party vendor

Log Preparation

- Ensure appropriate logs are being collected and saved
  - Endpoints, servers, network devices, authentication systems, cloud, apps, etc
- Log retention
  - Logs must be kept for appropriate amount of time
  - Retention length varies by organization
  - May require large amount of storage
  - More logs = less retention (with equal amount of storage)
- May need additional software for more detailed logs
  - Sysmon (MS Sysinternals)

Infrastructure Logging

What To Log

- Account and group activity
  - Creation, deletion, modification
  - Log on/off - including source information
- Network traffic & devices
  - Firewall traffic - inbound and outbound
  - Internal network traffic as needed
- File activity
  - Especially any sensitive, proprietary information
  - File creation, modification, deletion
- Email systems
  - Any email filtering
  - Inbound and outbound mail

What To Log

- Endpoint event logs
  - Windows systems - PowerShell, system, application, Sysmon
- Applications
  - Any specific application logs that my be relevant to security
- Any public facing interfaces
  - Web servers
  - Remote access gateways
  - Email portals
  - Customer interface
  - APIs

Baselines & Known Good Configurations

- Measure of what is “normal” on endpoint/network
  - File hashes
  - Open network ports
  - Accounts on endpoint/permissions granted
  - File/directory permissions
- Used to compare against current state
  - If matches baseline - ✅
  - If does not match baseline - ❌
    - Further investigation to determine *why* and if malicious

Threat Hunting Maturity

Maturity

- **Standard method to measure organization's threat hunting abilities**

- Measured by multiple factors
  - Amount and quality of data that is collected
  - Frequency of data collection
  - Methods of analyzing collected data
  - Ability to add automation in analysis
- Hunting Maturity Model (HMM)
  - 0 - 4

Threat Hunting Maturity Model

Level 0 Initial	Level 1 Minimal	Level 2 Procedural	Level 3 Innovative	Level 4 Leading
Primarily automated alerting	Threat intelligence indicator searches	Follows analysis procedures created by others	Creates new data analysis procedures	Majority of successful data analysis is automated
Little/no routine data collection	Moderate - high routine data collection	High - very high routine data collection	High - very high routine data collection	High - very high routine data collection

Threat Hunting Mindsets

Intelligence Based Hunting

- Hypothesis to begin hunt starts with intelligence information
  - IPs, domains, hashes, filenames, email addresses, other IOCs
- Strategic
  - **Who?**, **Why?**, and **Where?**
- Tactical
  - **What?** and **When?**
- Operational
  - **How?**

Data Driven Hunting

- Driven mainly by internal data that may indicate malicious activity
  - Lower priority alerts
  - Detections based solely on aggregated data
- Does not typically start with definite “something bad is happening”
  - Provides potential starting point to create hypothesis

- **Still uses intelligence information**

Knowledge Based Hunts

- Relies more on hunters knowledge of available data
  - Logs and events
  - Network layout and architecture
  - Adversary TTPs
- Heavily uses frameworks (MITRE ATT&CK)
- Hypothesis created based on TTPs seen in the wild
  - Knowledge of TTPs helps to know **how** to look for suspicious activity

Attack Based vs Analytics Based

- Attack-based hunting
  - Searching for evidence whether or not attack has occured
  - **“Did <event> occur on the network?**

- Analytics-based hunting
  - **“Does anything in <system/network/data> look malicious or suspicious?”**

Introduction to Threat Hunting - Summary

Key Concepts - Recap

+ **Fundamentals of Threat Hunting**

+ **Threat Hunting Preparation**

Learning Outcomes Recap

- Understand what threat hunting is, and why it's important
- Be able to use different strategies for effective hunting
- Understand common terminology and frameworks associated with threat hunting
- Be able to ensure an organization is prepared for hunting threats

Next Steps

+ Continue with Threat Hunting learning path
+ Revisit courses or videos about threat actors and their motivations
+ Research more about Pyramid of Pain or Cyber Kill Chain
+ Practice navigating and using MITRE ATT&CK Matrix

Thank you!

Introduction to Threat Hunting

+ Fundamentals of threat hunting to build up to technical skill
+ Thank you for your time!