Intrusion Analysis Overview

Brian Olliff

Defensive Engineering Instructor

Topics

IR Planning & Process
Sharing Information
IR Teams
Artifacts
Threat Hunting
MITRE ATT&CK

Learning Objectives

- Understand what incident response is and its components
- Understand incident response planning
  - Policy contents and steps
- Be able to explain incident response process and steps
- Understand incident response information sharing
  - VERIS standard
- Understand threat hunting process and phases
- Understand MITRE ATT&CK and how it can be used
  - Incident response and threat hunting

Incident Response Planning

Incident Response

- Evaluating, analyzing, and responding to events and incidents
- Complex response processes and activities
- Multiple guides & resources available
- NIST SP 800-61
  - Computer Security Incident Handling Guide
- Event vs incident
  - Event - “any observable occurrence in a system or network”
  - Incident - event that violates security policies or standard practices

Incident Response Plan (IRP)

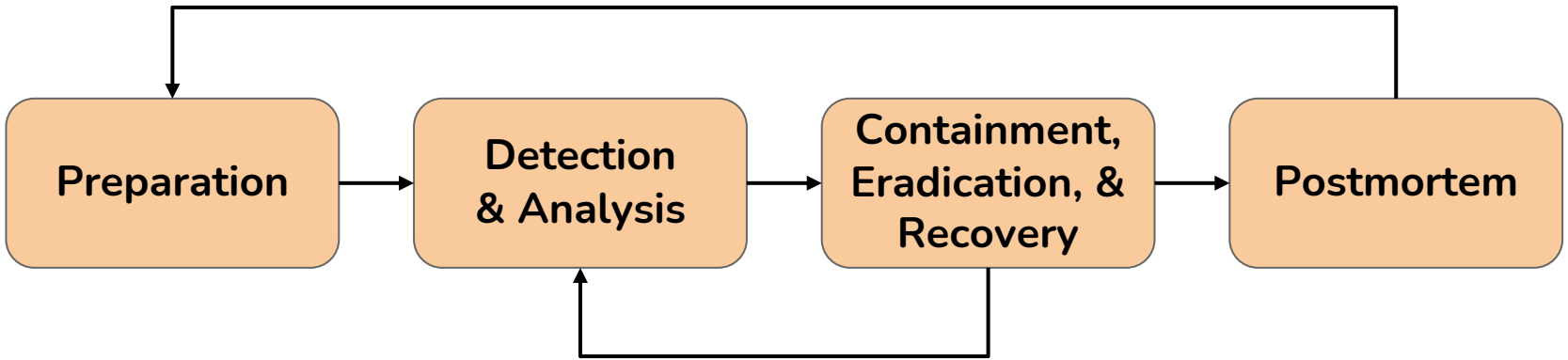
- Predetermined plan on how to handle different types of incidents
  - Structured approach to incident response
  - Helps to reduce the impact of incidents
  - Lessons learned helps improve response process
- SP 800-61 - incident response plans, policies, & procedures
- IRP components
  - Overall strategies and goals
  - Organizational approach - runbooks/playbooks, automation & orchestration
  - Communication plans
  - Metrics to measure effectiveness of incident response
  - Potential future plans for improving responses

Incident Response Policies

- Help to ensure plan fits with organizational goals
- Provide guidance on future plan development
- Policy components
  - Overall objectives and purpose of policy
  - Scope
  - Definition of terms (events, incidents, severity, etc)
  - Organizational structure and responsibilities in IR
  - Severity prioritization
  - Performance measurement guidelines
  - Contact information/forms and reporting guidelines

Incident Response Process

Incident Response Phases



Preparation Phase

- Creation and training of IR team(s)
- Deployment of tools, security controls, countermeasures, etc
  - Based on needs of org and risk analysis/assessments
- Location and systems for SOC and IRT
  - Monitoring, communication, response capabilities, etc
- Ensuring appropriate hardware and software procured and deployed
- Appropriate systems in place for detection and response
  - Host-based & network based controls
- User awareness training development

Detection & Analysis Phase

- Many attacks and breaches can go undetected for days, weeks, months
- Requires effective controls/tools to examine network “blind spots”
  - Preplanned processes and procedures
- Profile infrastructure and define baselines/normal behavior
- Log collection, correlation, and analysis
  - From hosts, devices, & network (using packet sniffers)
  - Events filtered effectively as needed
  - Proper time synchronization is important
- Appropriate resources and references used
  - Internal knowledge base, Internet resources, intelligence data, other analysts
  - Knowledge of types of attacks, attack vectors, and attackers

Detection & Analysis Phase

- All necessary steps defined in processes and procedures
  - Especially processed to recognize potential incidents
- Incident documentation as needed
  - Including IOCs, actions taken, results from analysis, etc
- Prioritize incidents based on established processes
- Effective communication
  - Between analysts/responders
  - With leadership and rest of organization

Containment, Eradication, & Recovery Phase

- Based on information/intelligence gathered in analysis phase
  - Identification of hosts involved
  - Containment strategy choice to effectively eradicate and recover
- Appropriate strategy determined by:
  - Potential damage to organizational resources
  - Evidence preservation requirements
  - Affected systems and services
  - Required time, effort, resources to implement
  - Strategy effectiveness (partial or full containment)
  - Solution duration (permanent, temporary, emergency)

Post-Incident Activity Phase (Postmortem)

- Lessons learned, evidence retention and use
- Documentation and review of what happened, where, & when
- Review of responder/staff activities
- Verification of procedure effectiveness, and review of whether followed
- Identify what could have been done differently
  - Any actions that inhibited response or recovery
  - Information sharing that could be improved
  - Events that could have been identified sooner
  - Any additional tools or resources that may be needed
- Acknowledge actions that went well and contributed to recovery efforts

Information Sharing

Information Sharing

- Often necessary to communicate with outside parties
  - During and after response and resolution
  - Law enforcement, media, third-party expertise, ISPs, etc
- IOC (indicator of compromise) sharing with industry peers
  - Automated through some security controls
  - Manual processes
- ISAC - Information Sharing and Analysis Center
  - Private-sector, critical infrastructure organizations/government institutions
  - Exist for various industry types - communication, aviation, electricity, etc

Information Sharing Policies

- Information sharing should be included in incident response plan
- Sharing process with internal resources & departments
  - Public relations
  - Legal department (esp important)
  - Senior leadership
- Any data shared with outside resources should be coordinated
  - Avoid sharing sensitive information
  - Unnecessary data leakage could impact incident, cause further loss
- Document information sharing
  - What, with whom, when, etc

Vocabulary for Event Recording and Incident Sharing (VERIS)

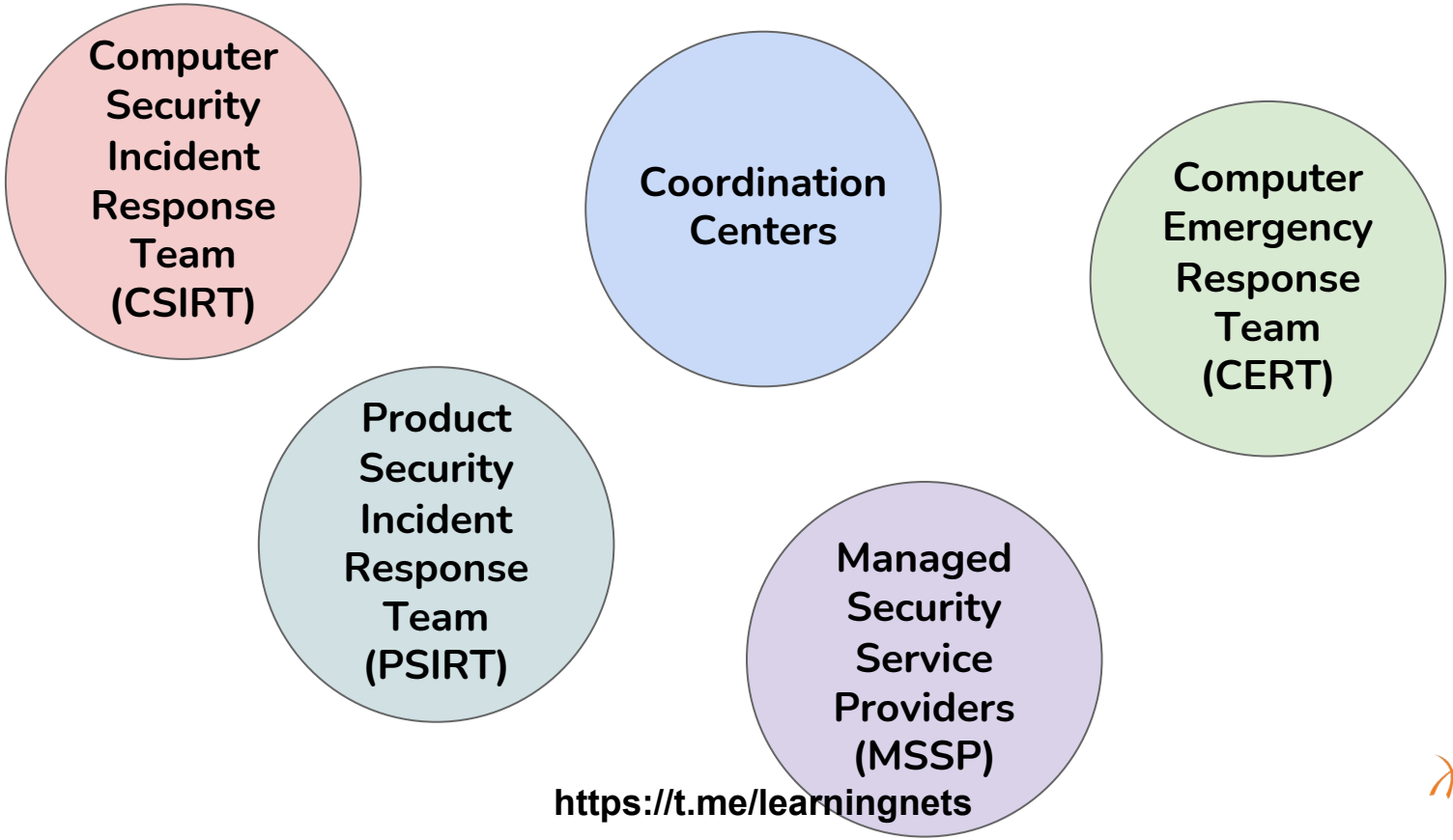
- Standardized language used to describe security incidents
  - Used for both internal documentation and information sharing
- Schema divided into five sections
  - Incident Tracking
  - Victim Demographics
  - Incident Description
  - Discovery & Response
  - Impact Assessment

VERIS

Incident Tracking	Victim Demographics	Incident Description	Discovery & Response	Impact Assessment
• Incident ID • Source ID • Incident confirmation • Incident summary • Related incidents • Confidence rating • Incident notes	• Victim ID • Primary industry • Country of operation • State • Number of employees • Annual revenue • Locations affected • Notes	• Actors • Actions • Assets • Attributes	• Incident timeline • Discovery method • Root causes • Corrective actions • Targeted vs opportunistic	• Loss categorization • Loss estimation • Estimation currency • Impact rating • Notes

Incident Response Teams

Types of Incident Response Teams



Computer Security Incident Response Team - CSIRT

- Typically works closely with infosec/IT teams
  - Smaller organizations may combine
- Aspects of creating team
  - What is the team responsible for?
    - "Customer", scope, coverage
  - Support of leadership and management
  - Appropriate budget allocated
  - Placement of CSIRT in organization hierarchy
  - Central or distributed?
  - Established policies and procedures
  - Value provided to organization - "return on investment"

CSIRT Policies

- How to handle and classify incidents
- Classification and protection of data and information
- Communication and information dissemination
- Record handling (retention and destruction)
- Acceptable encryption
- Engagement with outside parties
- Outsourcing options
- Others as organization needs

Product Security Incident Response Team - PSIRT

- Responsible for vulnerabilities/incidents in org's products/services
- Additional challenges
  - Vulnerability chaining
    - Analysis can be very challenging
    - May change priority of vulnerability remediation
  - "Theoretical" vulnerabilities
  - Secure coding practices (software development lifecycle)
  - Third-party software used in product (supply chain)

National Teams

- National CSIRTs or CERTs (Computer Emergency Response Team)

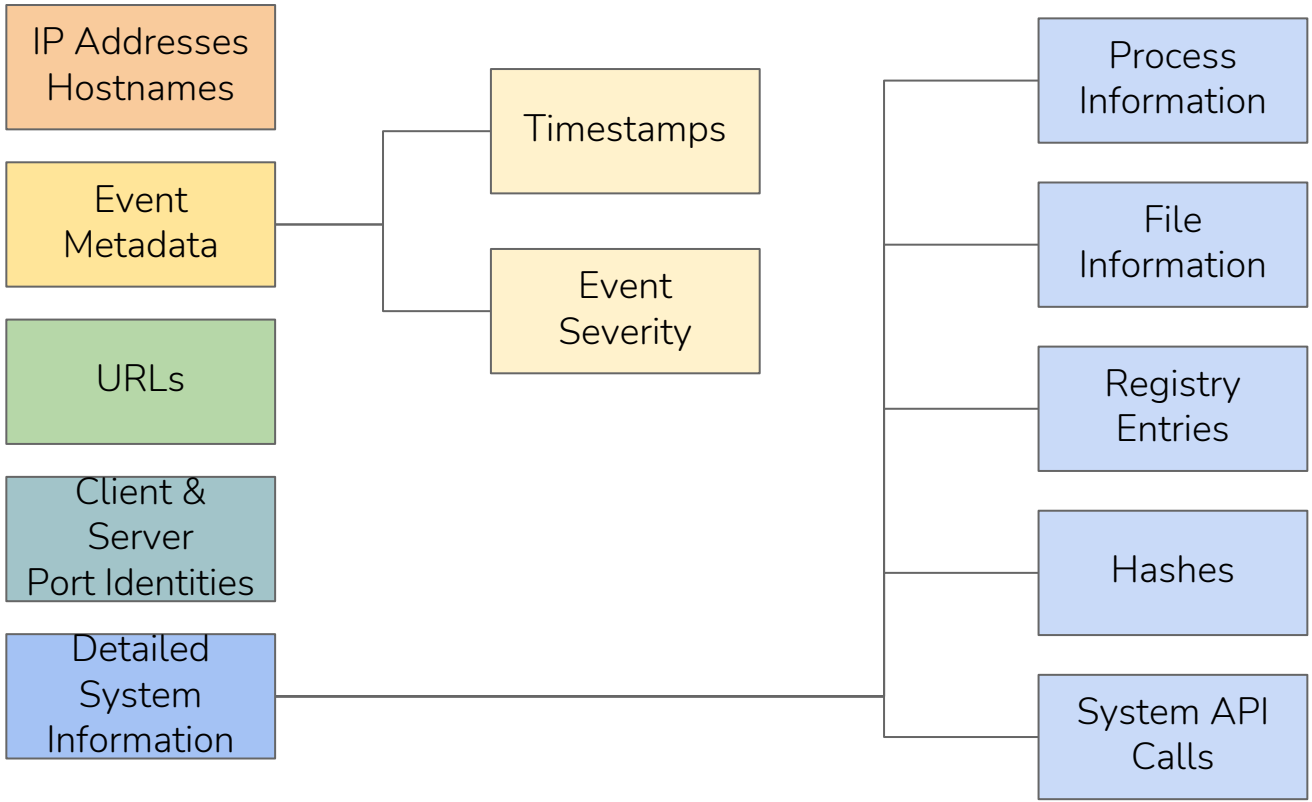
- Provide vulnerability information, awareness training, best practices, etc
- Goal of protecting gov, citizens, critical infrastructure, other organizations

Coordination Centers and MSSPs

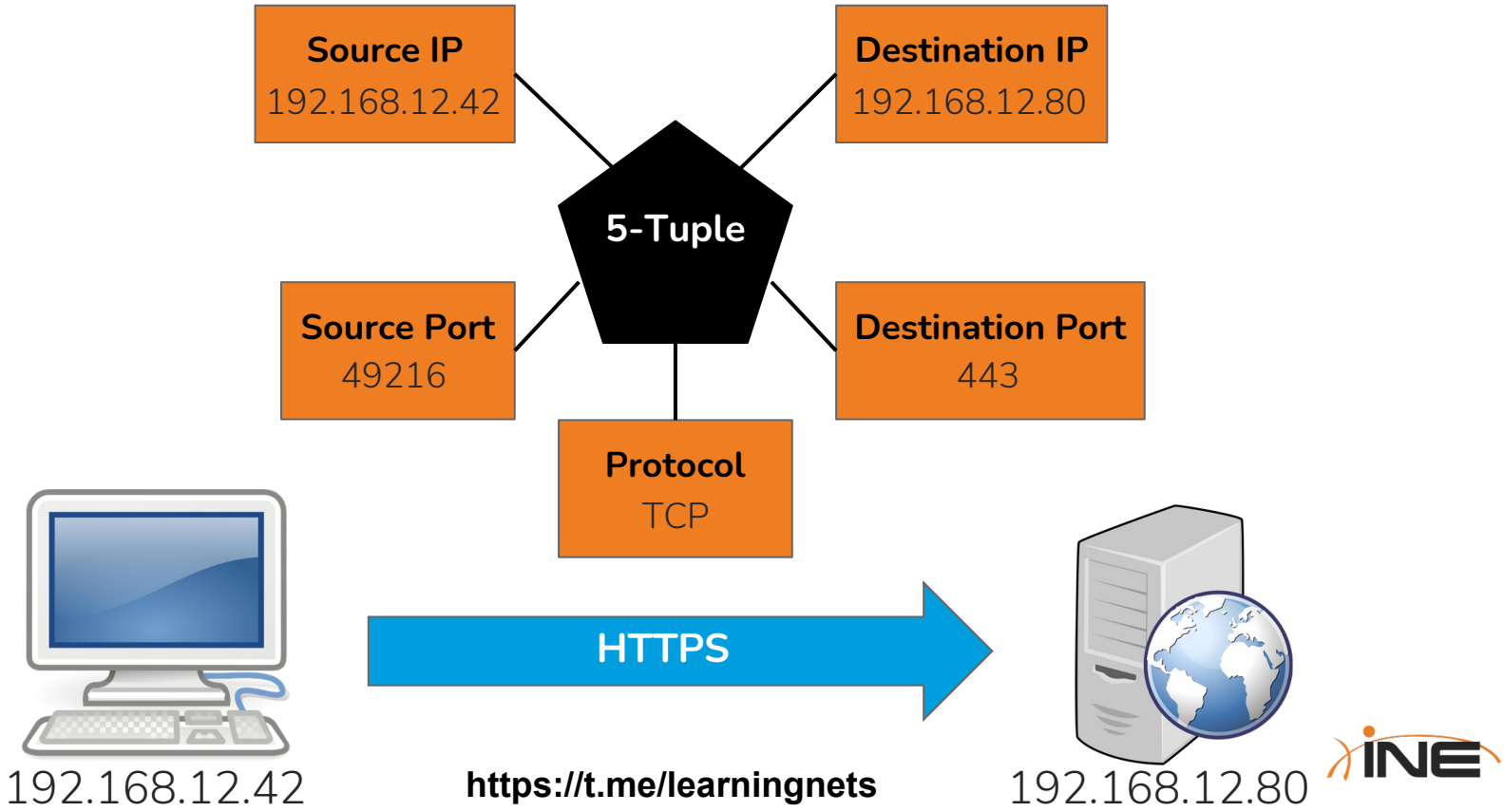
- Coordination centers
  - Help to coordinate activities between multiple organizations
    - Vendors, hardware & software providers, security researchers, etc
    - Vulnerability disclosures and remediation
    - Monitoring and analysis
- Managed security service providers (MSSPs)
  - Outsourced incident response and managed security services
  - Similar tasks to other CSIRTs, but for external organizations (customers)
  - MDR - managed detection and response
- Cisco Incident Response Service
- Cisco managed security service

Security Event Artifacts

Common Artifacts



5-Tuple

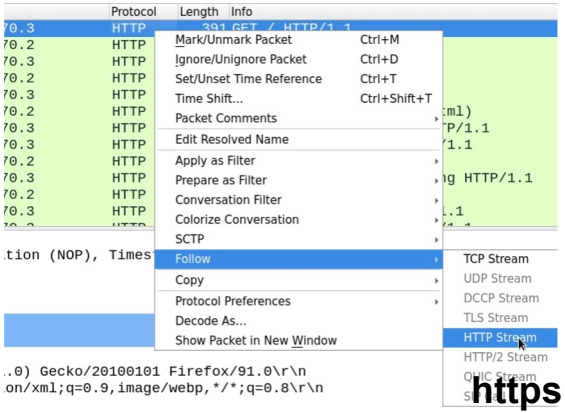

Source IP
192.168.12.42
Destination IP
192.168.12.80
5-Tuple
Source Port
49216
Destination Port
443
Protocol
TCP
HTTPS
192.168.12.42
https://t.me/learningnets
192.168.12.80

Protocol Analysis

- TCP, HTTP(S), TLS, SSH, DNS, etc
- Modern security controls understand how protocol is supposed to work
  - IDS/IPS, traditional firewalls, NGFW
  - Inspect protocol headers to ensure compliance with protocol
- Header analysis provides better protection than signatures
  - Looks for anomalies or misuse in protocol
    - Compares captured traffic to “normal” for protocol
  - Can detect known and unknown attacks
  - More difficult for attackers to evade

Packet Captures

- Interception and logging of packets for further analysis
  - Can be used to analyze protocol headers
- Also called *sniffers*
- Wireshark one of most popular
  - Protocol-decoding features and filtering to assist analysis
  - Ability to *follow* TCP stream




```
GET / HTTP/1.1
Host: demo.ine.local
User-Agent: Mozilla/5.0 (X11; Linu
Accept: text/html,application/xhtm
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 302 Found
Date: Wed, 02 Mar 2022 18:11:27 GM
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.2
Location: portal.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

GET /portal.php HTTP/1.1
```

File Hashes

- Unique value that represents “digital fingerprint” of file
- Generated by running file through hashing algorithm
- Key component of several types of security event logs
- Used to identify malicious or potentially malicious files
- Cisco AMP for Endpoints/Networks (Cisco Secure Endpoint)
  - Examines, records, tracks, sends files to cloud, creating SHA-256 hash
  - Compares hash to local cache
    - If not present, sends to cloud for analysis (or another appliance)

False Positives

- False positive
  - Security control triggers alert, but no malicious activity is present
  - Benign triggers
  - Can lead to alert fatigue - too many alerts, leads to overlooking real incident
- False negative
  - Malicious event that is not detected or alerted by security control
- True positive
  - Successful identification of malicious event
- True negative
  - Correct identification of normal, acceptable, non-malicious event

Regular Expressions

Regex Basic Matching

\	Escape character ([] {} () ^ $. | * + ? \ -)
.	Match anything (except line breaks)
\d & \D	Any digit (and any non-digit)
\w & \W	Any “word” (and any non-word) (letter, digit, _)
\s & \S	Whitespace (and non-whitespace)
[...]	Character class [a-z], [A-Z], [0-9]
\b & \B	Word boundary (and non-word boundary)
^	Match at beginning of line (or NOT inside [...])
$	Match at end of line

“Quantifiers”

*	Zero or more repetitions (ab* matches “a” or “abbbbbb”)
+	One or more repetitions (ab+ matches “ab” or “abb”, not “a”)
?	Zero or one instances (ab? matches “aa” or “ab”)
{x}	Exactly x instances ([0-9]{3} matches “526”, not “76” or “2562”)
{x, }	At least x instances ([0-9]{2,} matches “42” or “23552”, not “5”)
{x,y}	Between x and y instances ([0-9]{1,3} matches “1” or “642”, not “2342”

Character Grouping

()	Groups characters for matching
x|y	Match “x” or “y”
(A|a)	Matches “A” or “a”
(Mon|Tues)day	Matches “Monday” or “Tuesday”
\b(cat|dog)s\b	Matches “cats” or “dogs” as their own word

Threat Hunting Overview

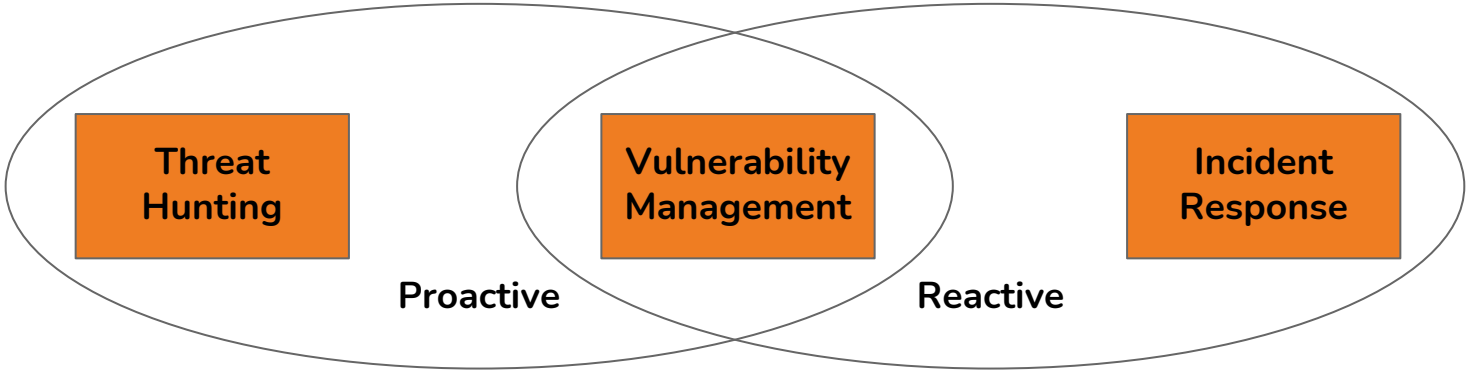
Threat Hunting

- Process of proactively looking for intrusions on network
- No security control is 100% effective
  - Can’t detect everything, can’t block everything
- Requires deep knowledge of infrastructure
  - Usually specialized tools
  - Frequently use MITRE ATT&CK framework
- Typically performed by senior SOC analysts
  - Dedicated team
  - Depends on organization

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

Tools & Methods



Data Analytics

Automation & Orchestration

TTPs

Manual Analysis

Intelligence Information

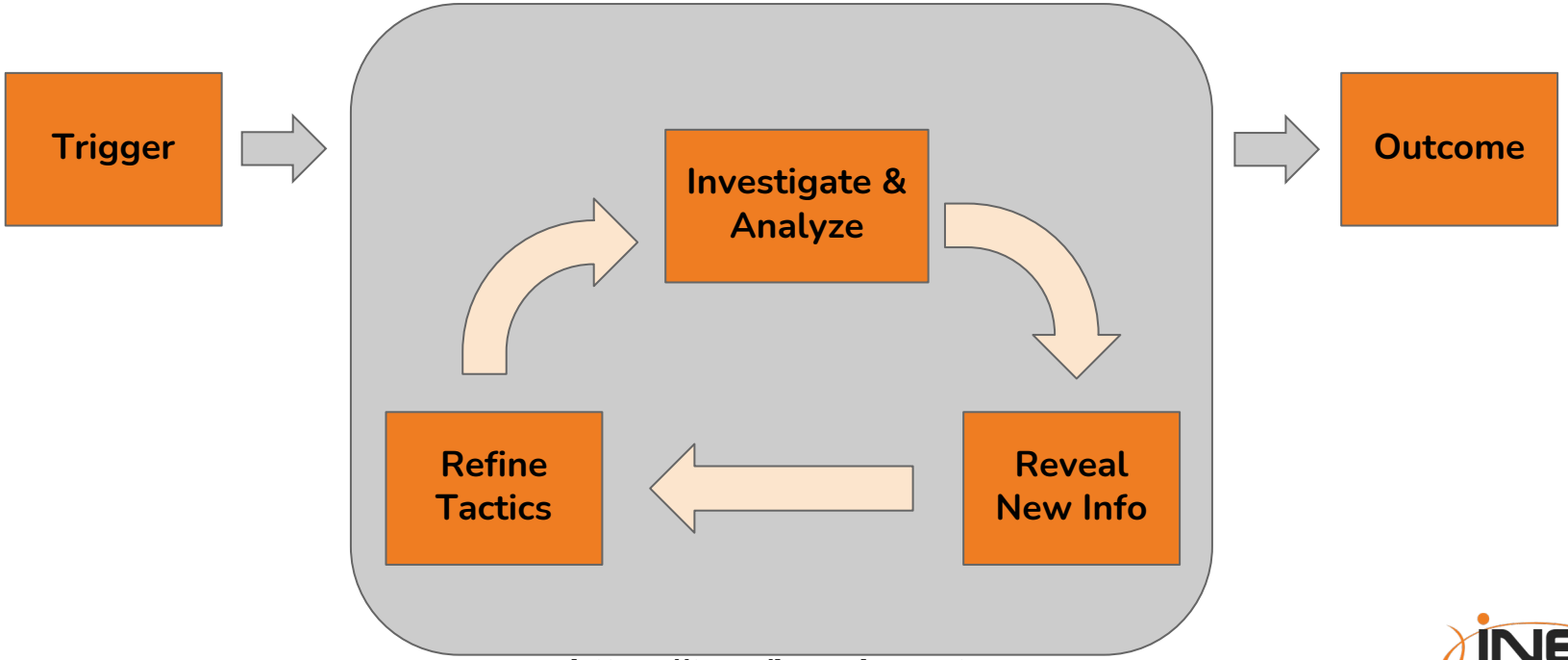
Vulnerability Feeds

Active Defense

- Use of honeypot(s) and honeynet(s) as defense mechanism
  - Intentionally vulnerable system(s), isolated from rest of network
  - Used to actively respond to attackers upon detection
- Not the same as threat hunting, but can be used in process
  - Decoy system logs can provide guidance on where/what to hunt
  - Instead of looking at all logs across systems
- Can be detected if not implemented correctly
  - No obvious default passwords
  - Dynamic CPU/memory usage, mouse movements, clipboard usage, etc
  - Multiple systems with different purposes
- Only useful if attackers interact with them

Threat Hunting Process

Threat Hunting



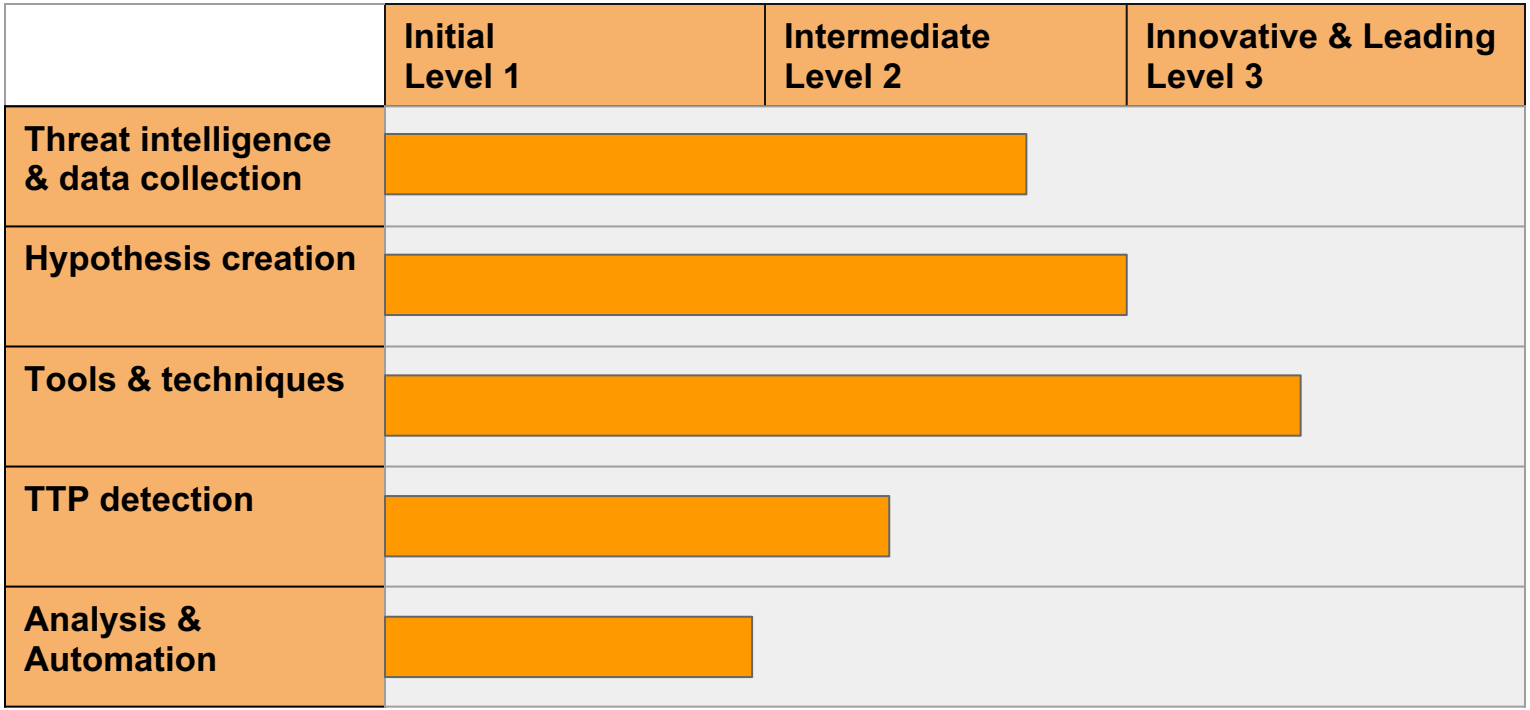
Threat Hunting Maturity

- Metrics
  - Threat intelligence and data collection
  - Hypothesis creation
  - Tools and techniques
  - TTP detection
  - Analytics and Automation
- Maturity levels
  - Initial
  - Intermediate
  - Innovative and leading

Threat Hunting Maturity

	Initial Level 1	Intermediate Level 2	Innovative & Leading Level 3
Threat intelligence & data collection	Limited intelligence and data collection	High collection of certain types of intel and data	High collection of many types of intel and data
Hypothesis creation	Responding only to existing alerts and logs	Combines traditional logs with other TTPs	Logs combined with TTPs and automated threat/risk scoring
Tools & techniques	Reactive alerts and searches	Simple tools and analytics, mostly manual	Advanced search capabilities, new tool creation
TTP detection	None, only reactive detections	IOC and new trend identification	Detection of TTPs, IOCs, with automation for future detection
Analysis & Automation	None	Limited analysis and automation	Automated tools to routinely detect future threats

Threat Hunting Maturity

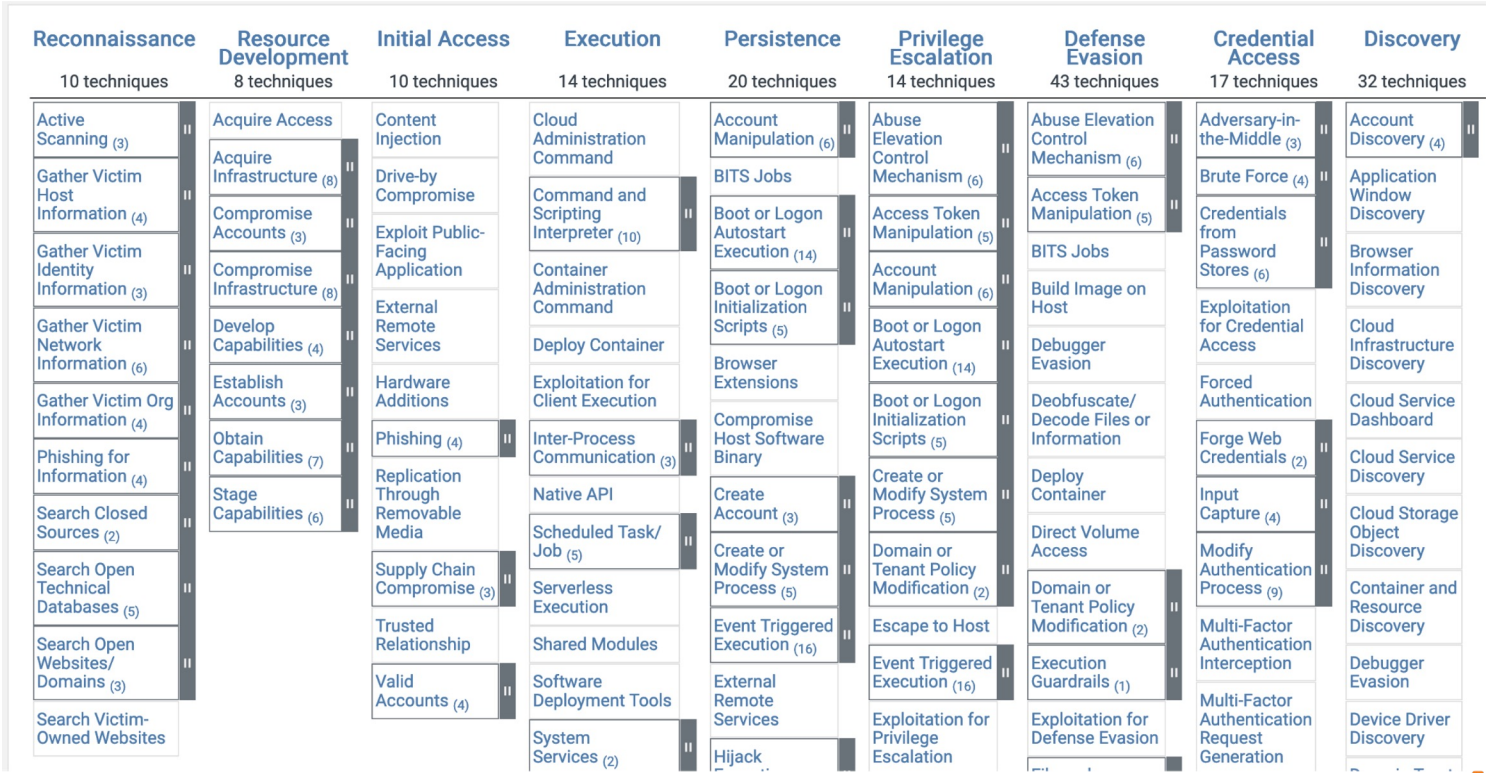


MITRE ATT&CK

MITRE ATT&CK

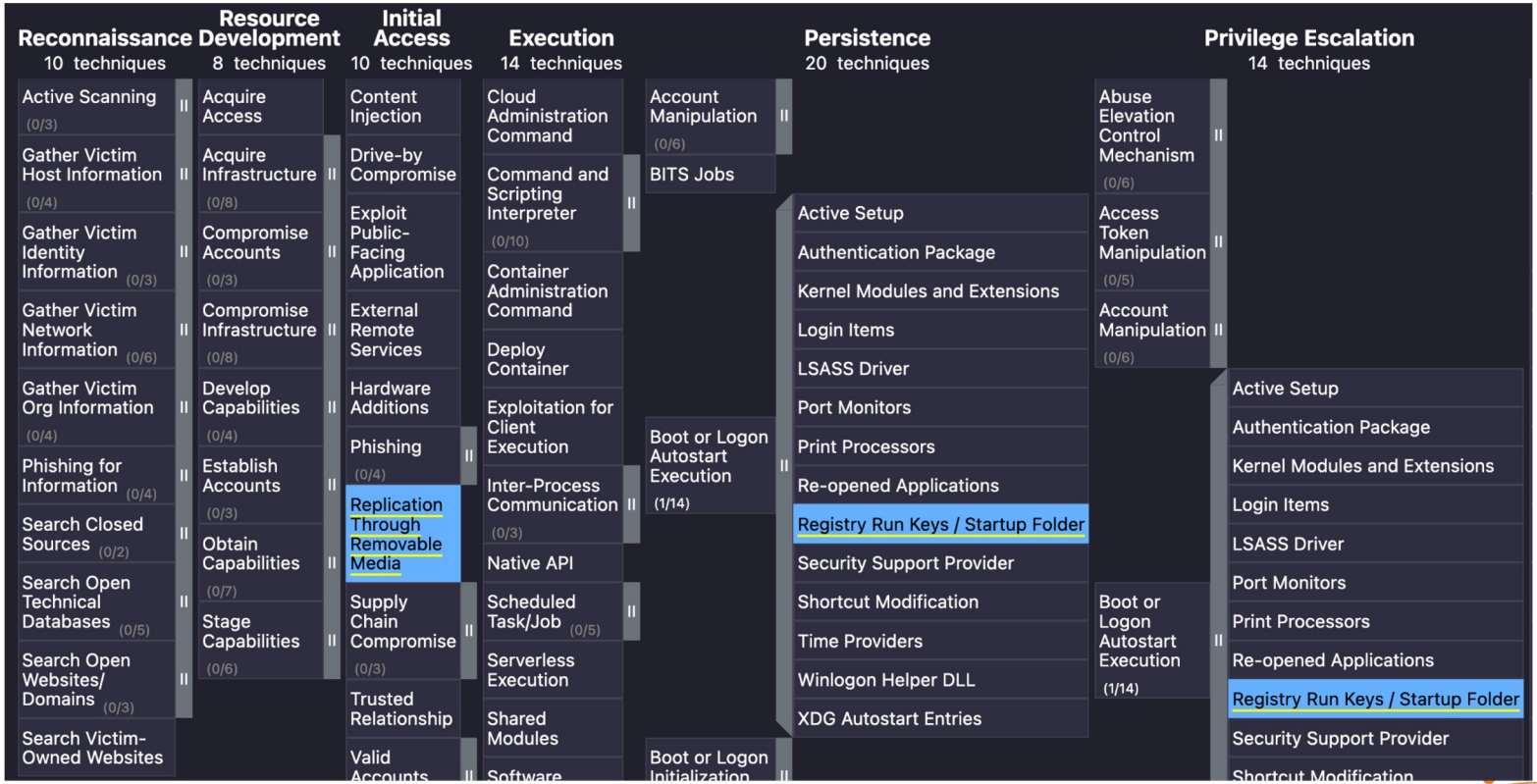
- **A**dversarial **T**actics, **T**echniques **& C**ommon **K**nowledge
- Used to understand & track adversary techniques during attacks
  - Commonly used for threat hunting
- Collection of multiple matrices
- PRE-ATT&CK
  - Tactics and techniques used while preparing for an attack
  - Now included as part of Enterprise Matrix
- ATT&CK Enterprise
  - Windows
  - MacOS
  - Linux
  - Cloud

Enterprise Matrix



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/ Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/ Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery
Search Open Websites/ Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery
			Software Deployment Tools	Hijack		Exploitation for Defense Evasion		
			System Services (2)					

Software Matrix Example



Adversary Emulation

- Assessment method used to test security controls
  - Tests against TTPs commonly used by threat actors
- Often used with threat emulation
- Open source tools available to automate process
  - Caldera - originally created by MITRE
  - Atomic Red Team - adversarial techniques mapped to ATT&CK
- Caldera
  - Core services, plug-ins and agents (Windows, macOS, and Linux)
  - Agents installed on systems and simulate different adversaries