MANDIANT

YOUR CYBERSECURITY ADVANTAGE

HUNT MISSION WORKSHOP

PARTICIPANT GUIDE

Contents

Welcome and Introduction

Overview/Setting Expectations

- Formalize a hunt mission framework with an intelligence led approach
- This framework can be the foundation of future workflows
- Develop an understanding of inputs and outputs into different phases of a hunt mission
- Identify gaps and operational pre-requisites

Agenda

Title	Purpose and Description
Introductions and Objectives	Introduce presenter and learners/Set expectations and identify objectives
Foundations of Intel-Led Hunting	Realizing Operational and Business Value (Hunt Value Model)
Framework Overview and Operational Drivers	Understanding the six core drivers of an effective intelligence-led process
Workshop Exercise #1 (WE1)	Enrichment of a Threat Hunt Mission
Understanding of "Assess" & "Acquire" Phases	Drivers for Scoping and Searching the Hunt Mission
Workshop Exercise #2 (WE2)	Applying the "Assess" & "Acquire" phases
Understanding "Analyze" & "Action" Phases	Drivers for interpreting and communicating outputs
Workshop Exercise #3 (WE3)	Applying the "Analyze" and "Action" phases
Wrap-up	Final discussion and closing comments

Module 1: Foundations of Intel-Led Hunting

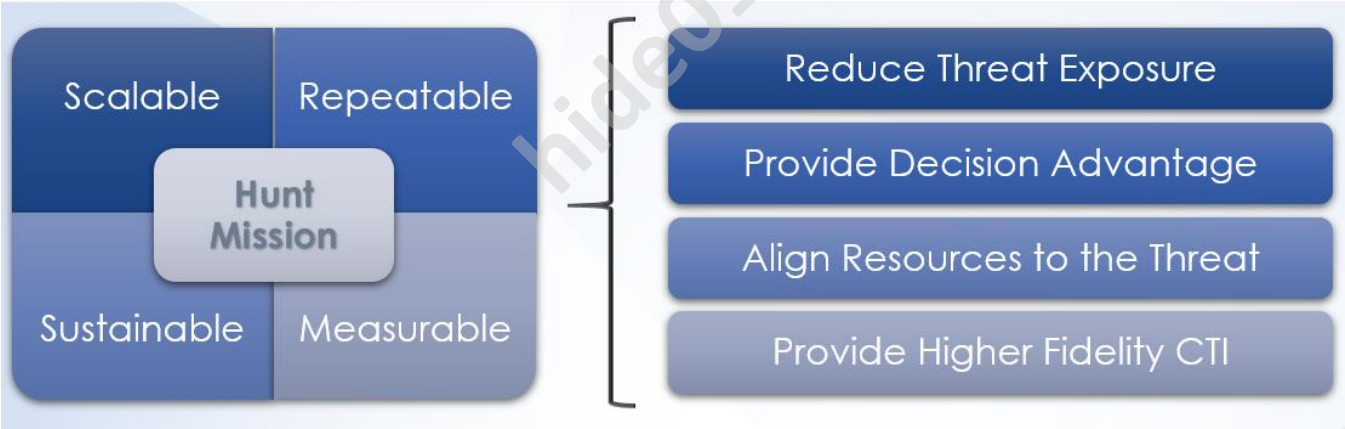
Objectives

- Define hunting
- Bridge the divide with hunting
- Realize operational and business value (Hunt Value Model)
- Integrate hunt capability into conventional cyber security operations
- Operational drivers (core hunt capabilities)
- Gap analysis and/or desired end-state

Threat Hunting Is…

The methodical, use case driven, proactive identification of cyber threats within a computing environment or infrastructure.

Defining the Hunt Mission



A hunt mission is scalable, repeatable, measurable, and sustainable. The goals of hunting are to reduce threat exposure, provide decision advantage, align resources to the threat, and to provide higher fidelity Cyber Threat Intelligence (CTI)

Benefits of Hunting

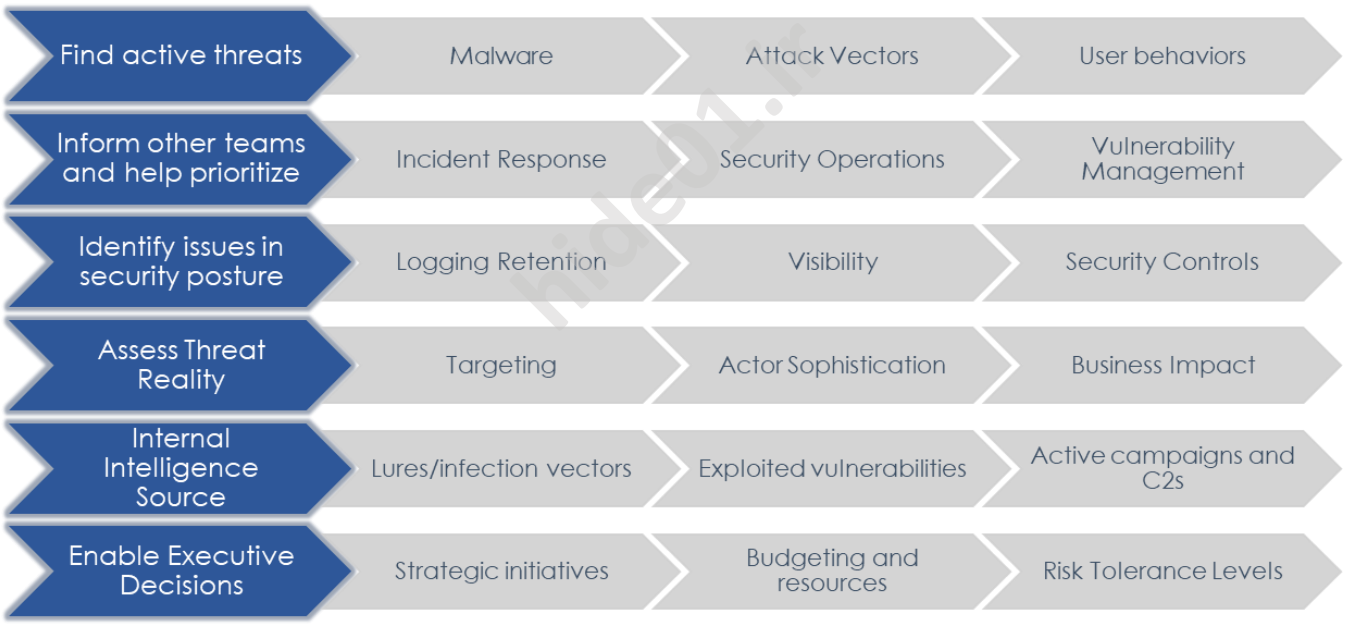
- Identify previously undiscovered activity
- Evolve monitoring and detection
- Identify attacker Tactics, Techniques, and Procedures (TTP)
- Bridge automation and analysis

- Reduce attack surface and threat exposure
- Define baseline operating environment
- Increase visibility of attacker activity
- Validate security controls

Key Characteristics

- Intelligence-led
- Proactive
- Analyst-centric
- Iterative
- Methodology-focused
- Integrated

Intelligence-Led Value Model



Active Threats

- What threats to the business will hunting identify?
- What techniques are popular by malware?
- Are there risky user behaviors?

Inform other teams

- How do hunting results get communicated out to other teams?

- Hunting results can inform other teams and help prioritize tasks; reduce the time to detect by IR; generate alerts; increase situational awareness; and streamline vulnerability management. Socialize these findings and intelligence across stakeholders.

Identify security posture issues

- How does hunting help you identify issues and your security posture?
- What are your logging retention practices? You may identify that you need to hunt back further than data has been collected and you can address this.
- Do you have visibility in your network for hunting? You might pinpoint an area of the network that has been overlooked and is not being monitored.

Threat Reality

- Are you focusing on the right thing?
- With hunting you assess the threat reality – who is targeting you, what level of sophistication they have, and what the impact to your organization would be if an attacker were successful.

Internal Threat Intelligence

- Have you created intelligence specific to your org?
- Through hunting, you can build out your own internal intel. Document what has targeted you and specific lures. This may be used for future hunts and detection.
- Who in the org is targeted? It may not always be the executives – it may be people who work in specific functions, like the financial org with users that use a specific application for moving money, or customer service.

Executive Decisions

- How can hunting enable executive decisions?
- Hunting helps you advocate for resources, like additional monitoring, new tools to best protect your network, or personnel.

Integration into Security Operations

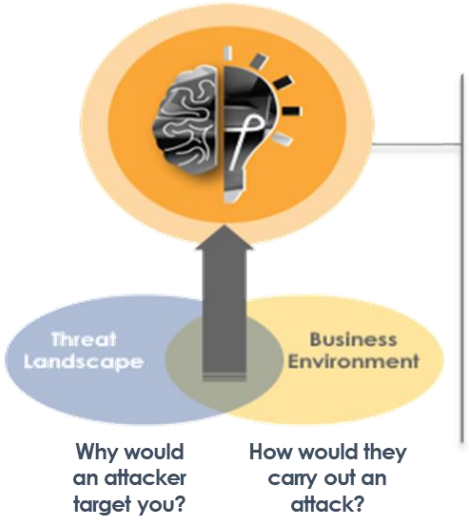
Inputs	Operation Areas	Outputs
Compliance issues made available as input into the hunt hypothesis process	Compliance Gaps	Significant gaps shared with EIM for remediation by the appropriate group systems/services.
Control issues made available as input into the hunt hypothesis process	Control Gaps	Significant gaps shared with SecEng; highlighted instances where risk is heightened
Event/Incident reports and CTI (with emphasis on threats found outside of detections)	Threats, TTPs, & Blind Spots	Enriched context with adversary information and judged motivation
Understanding of current security content logic; drive for enhancement of monitoring	Security Content	Automation of acquisition for hunting; new content logic shared with IR

Knowledge of Threat Landscape

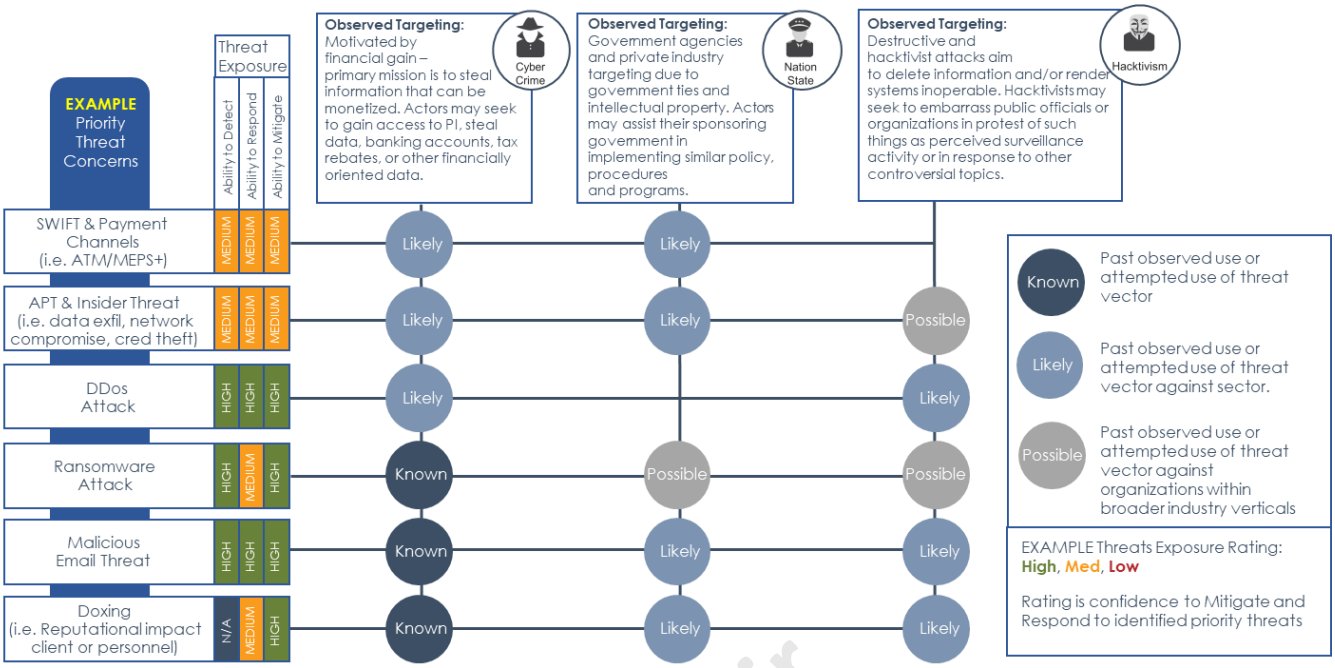
Understanding business drivers and the security controls in place to mitigate risk is key to defining your threat landscape and threat profile.

An organizational threat profile helps:

- Maintain regular situational awareness on threats, vulnerabilities, and risks to assets and operations
- Identify what is critical to your business operating model



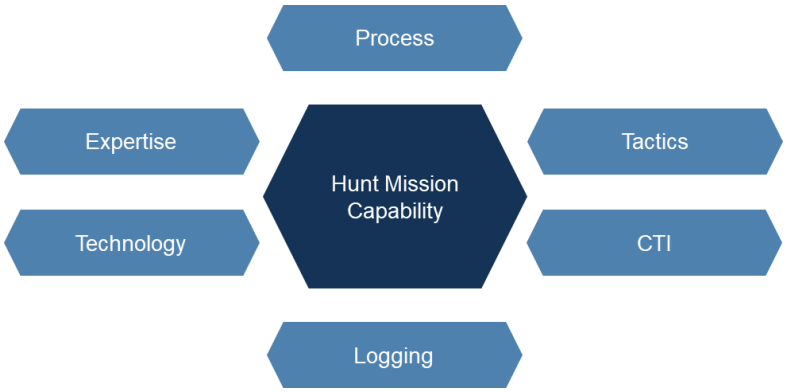
Example Threat Profile



Process Framework Overview & Operational Drivers

Operational Drivers

What should you have before you start?



Operational Drivers: Process

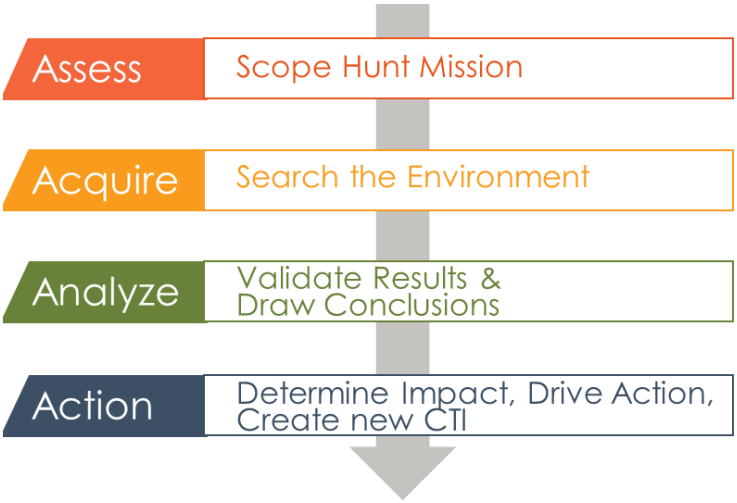
- Framework at a high-level
  - Use-case driven
  - Promotes consistency and repeatability
  - Structured yet flexible
  - Balances robustness with simplicity
- Set initial course of action
- Forms the basis of a SOP
- Does not impede creative nature of threat hunting
- Identifies input and output concepts

A formalized process allows hunt missions to be:

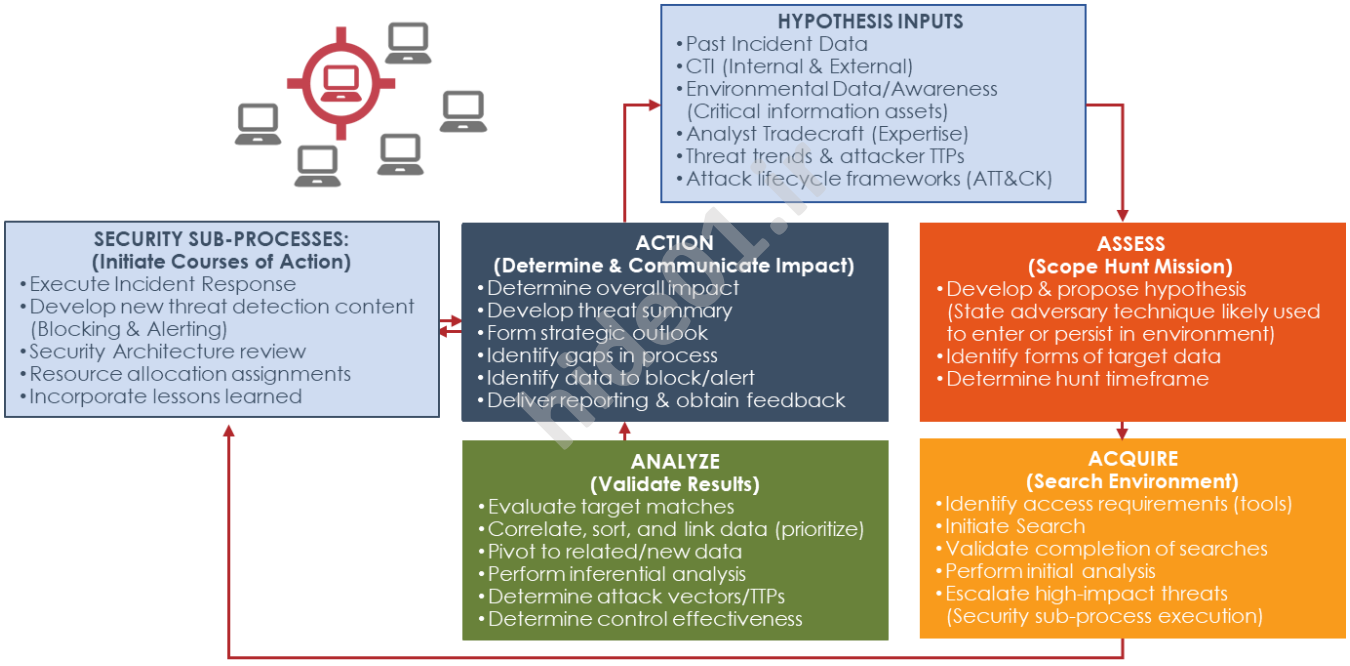
- Consistent
- Efficient
- Quantified

The framework provides a structure to:

- Ensure progress is measurable
- Facilitate coordination
- Maximize utilization of analyst time



Process: A4 Framework



Operational Drivers: Expertise

- Foundational skills possessed:
  - Knowledge of advanced threats
  - Technical (e.g., log/traffic analysis, malware analysis)
  - Data/Trend analysis
  - Critical thinking
  - Research & writing skills

- Expands these skills:
  - Identifying and confirming malicious activity through research
  - Ability to recognize not only malicious activity, but suspicious activity that could indicate something deeper afoot

Operational Drivers: Technology

- Enterprise Knowledge
  - Awareness of the IT environment
  - Level of understanding of the baseline security architecture
  - Deployment of defenses
- Business Knowledge
  - Critical systems, applications and data
  - Location, authorized user set
  - What are we monitoring today
  - Processes related to triaging and responding to incidents
- Log Access
  - Ability to access various logs in an efficient and timely manner
- Robust Querying and Retrieval Mechanisms
  - Searching large volumes must be feasible
  - Hunt missions often necessitate analysis over large data sets and timeframes
- Grouping and Sorting
  - Ability to regroup, sort, and link by various fields and calculate statistics

Operational Drivers: Logging

- Capture multiple data points
  - Enable deeper analysis to increase confidence
  - Enrich intel production
- Ensure overlap and source variety
  - Confirmation/validation of findings
  - Cross-correlation of disparate logs
- Retention period and logging levels
  - Build out infection chain
  - Historical analysis and trending to address potential target patterns

Understanding Data Sets

Log Data Sources

- Malicious egress activity?
- Phishing/Spearphishing campaigns?
- Resident malware on a system?
- Network reconnaissance?

Log Data Attributes

- What log data attributes enable event correlation?
- What log attributes [per source] are valuable for threat context?
    - Network-based:
    - Host-based:

What gaps might you have in your log sources?

Operational Drivers: Logging

Windows Hunting Scenario Example

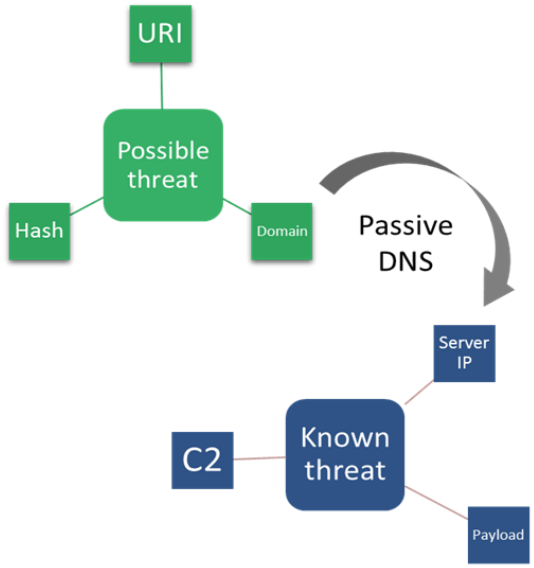
Hunt Category	Data/Log Sources	Example Techniques
Suspicious Files	File listings EDR, similar tools MS-Windows Sysmon	- Look for files created in suspicious directories - Known attacker file extensions - Known staging directories - Delete file write events
Scheduled Tasks	Windows registry EDR, similar tools Security event logs	- Look for deleted tasks - Tasks created using unexpected user accounts - Executed from attacker staging directories
Powershell Execution	Powershell script block logs Powershell module logs EDR, similar tools	- Suspicious script blocks ("warning" level) - Suspicious script paths - Suspicious PowerShell command lines

Operational Drivers: CTI

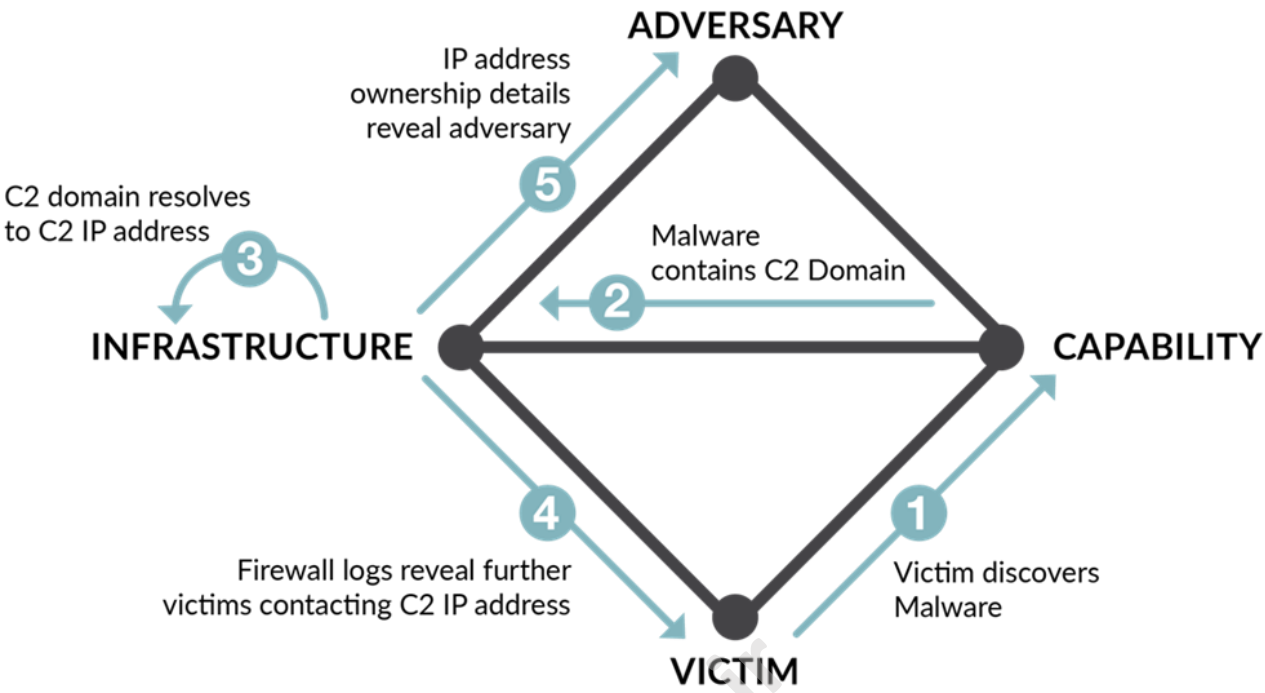
- Hunt teams should review CTI products that describe:
  - Adversaries targeting organization, industry, or sector
  - Relevant groups' motivations
  - Emerging TTPs
- Use CTI to stay informed of the threat landscape
- Uncovered adversarial activity resulting from hunt missions should inform CTI
- Understand the scope & intent of the intelligence
  - Comprehensive vs informative
  - Strategic, operational, or tactical
- Know when to leverage CTI
  - Pivoting
  - Validation & deep-dive analysis
  - Attribution
  - Communications

Operational Drivers: Tactics

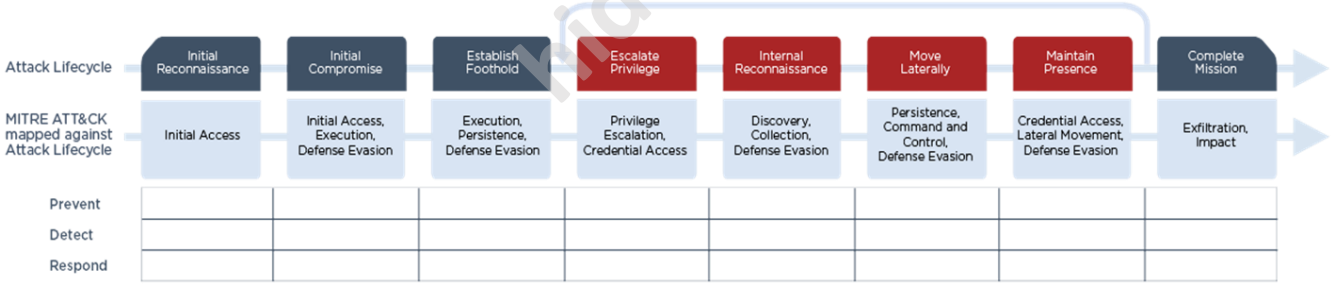
- Hunt missions often get stuck
  - Too much to disregard, not enough to advance
- "Pivoting" allows us to push through the stall points
- A diverse set of pivoting sources is crucial:
  - Previous hunts (Internal intelligence)
  - Other intelligence sources (Int. & Ext.)
  - Automated tools (Sandboxing)
  - Community sources (Blogs, COI)
  - Indicator investigation (Whois)



Diamond Model



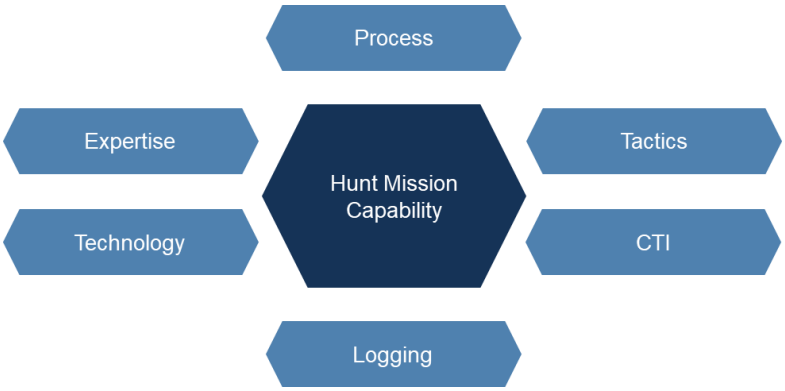
Mandiant Attack Lifecycle Mapped to MITRE Attack



- Hunt Use Case/Scenario Development
- Supports Analysis and Provides Context
- Assists in determining threat exposure and impact
- Examples:
  - Lockheed Kill Chain
  - Mandiant Threat Lifecycle
  - MITRE ATT&CK Framework

Operational Drivers: Gap Analysis

- Current Capabilities?
- Strengths?
- Weaknesses?
- Gaps?
- Planned End State?

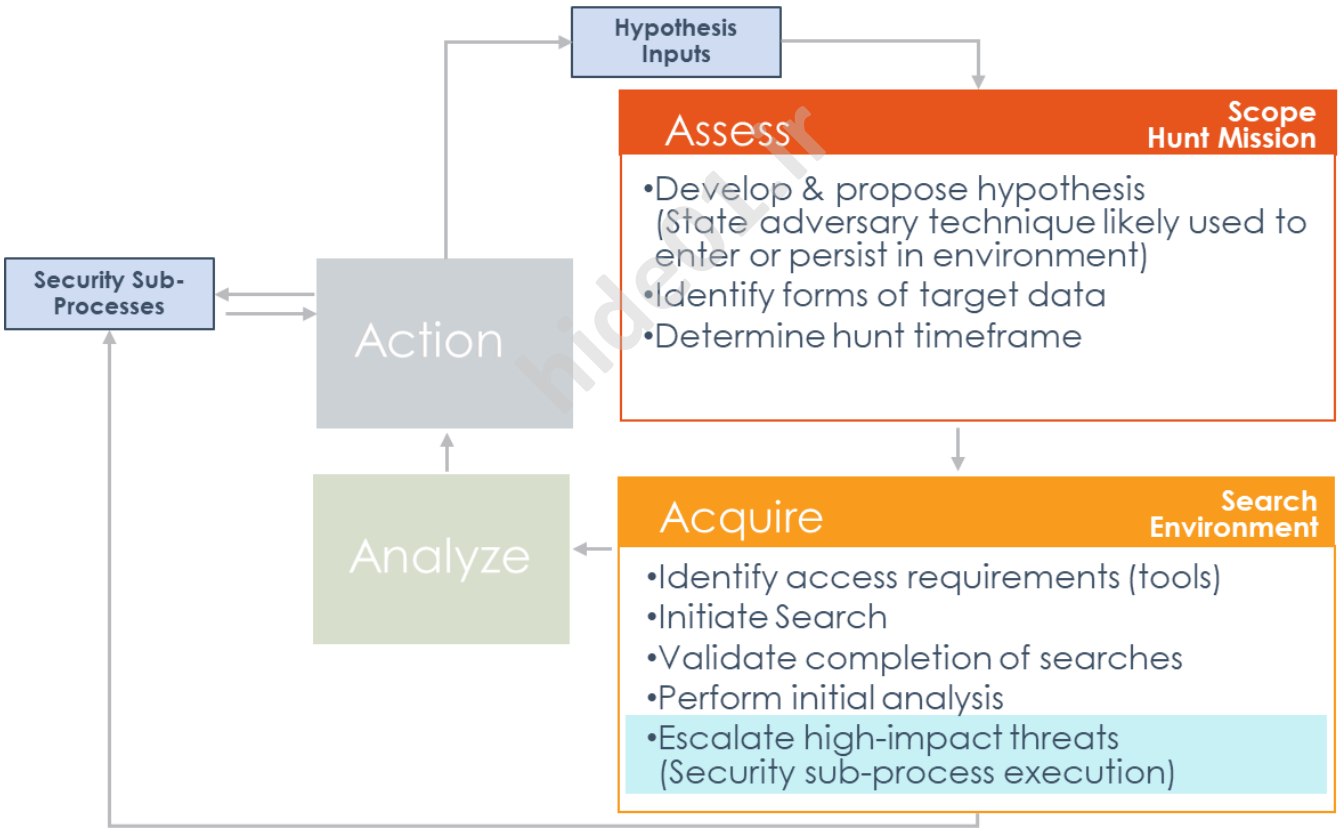


Module 2: Understanding Assess & Acquire

Objectives

- Process framework review (assess & acquire)
- Scoping the hunt mission (assess)
- Hypothesis development
- Threat modeling/learning objective
- Searching the environment (acquire)
- Security sub-processes

Process Framework



Define Target and Objectives

- What are we looking for?
- Where will we look?
- What do we expect to find/ not find?
- Why are we looking for it?
- What does its presence/ absence tell us?
- Who would be interested in our results?

Assess: Scope Hunt Mission

- Develop hypothesis
- Identify target criteria
- Estimate timeframe and expected duration
- Identify execution resources and constraints
- Establish expected outcomes
- Communicate intent and scope of effort

Assess: Develop Hypothesis

Hypothesis should answer a set of questions; it is not solely IOC based.

What's the threat?	Where will it occur?	Why do we care?
Malware Unusual pattern or behavior Malicious email campaign Unpatched vulnerability	Web traffic Email data Specific network segment (e.g., OT environment)	Specific threat groups Relevance to the organization

Assess: Hypothesis Inputs

Inputs to formulate a hypothesis:

- Past incident data
  - Blocked and Allowed events
- Cyber Threat Intelligence
  - Recent campaign reporting
  - Threat Profile
- Emerging Threat Trends and TTPs

- Attack frameworks
  - MITRE ATT&CK

Assess: Hypothesis Factors to Consider

- **Source confidence**
  Does the source have a history of proving high-confidence intelligence?
- **Expected ease of the search**
  Do you have the capability to search for the specific type of threat?
- **Target and searchable data of relevance**
  Is the threat associated with malicious activity targeting the organization, or the industry? Or is the threat related to technologies and applications currently deployed?
- **Existing infrastructure and visibility**
  Is there visibility or detection capability for the specific IOC?
- **Potential impact**
  If the actors were successful, does the activity lead to significant damage?

Assess: Hypothesis Examples

An example hypothesis structure:

<**Threat Actor**> verb <**capability**> preposition/verb <**infrastructure**> to achieve their <**objective**> against <**victim**>.

Example derived from CTI:

Suspected APTX threat actors are exercising social-engineering tactics via email involving spoofed domains to achieve access into mission-critical systems within your organization's industry/sector.

Example derived from previous events

An unknown threat actor is exercising social-engineering tactics over legitimate email infrastructure to achieve credential theft against the organization's executives.

Assess: Threat Modeling

- Expanded into sequence of steps
  - Not the actual query/rule syntax
- Defines the possible attack vectors
- Mapped to a phase in the attack lifecycle
- Vectors can be "white boarded" or sketched
- Broken down into specific TTPs for each phase and vector
- Continues until threat model has good coverage of attacker activity related to original hypothesis

Assess: Threat Modeling – Parsing Intelligence Data

UNC2053 Campaign Leverages Google and JetBrains Infrastructure to Distribute SPIKEDNOG

On Dec. 10, 2020, Mandiant Threat Intelligence observed a widespread phishing campaign that distributed SPIKEDNOG downloader payloads. This campaign used tactics, techniques, and procedures (TTPs) consistent with prior operations, including the use of Google Documents, payloads hosted on Google Drive and JetBrains, code-signed payloads, and similar lure themes. UNC2053 is a cluster of threat activity responsible for the distribution of multiple loader and backdoor combinations.

- Phishing emails from this campaign used several generic subjects and lure themes relating to terminations, debits, and office calls commonly seen in prior UNC2053 phishing campaigns.
- Observed emails included a link to a Google Documents PDF, which contained a link to a malicious payload hosted on Google Drive. The documents from this campaign used customer complaint, bonus report, and employee termination lure themes
- Upon clicking the link contained within the PDF, a SPIKEDNOG downloader payload hosted on the Google Drive was downloaded; we also observed evidence that this campaign used JetBrains for payload hosting
    - hxxps://www[.]google[.]com/url?q=hxxps://drive[.]google[.]com/uc?export%3Ddownload%26id%3D1wSbTEFw0i5NiOeC7YZ23ARLc9rejsSvA&sa=D&ust=1607624297614000&usg=AOvVaw3RxcJWkzJcihfNwtM5CNyq
- Payloads used in this campaign were signed using a certificate with the common name "OOO Inversum."

Produce Searchables and Obtain Matches

Definitions

- Searchables - How you find potential matches
- Matches - Result of running searchables

Acquire: Search the environment

- Access, Tools and Data
- Aggregate and Prepare Target Data
- Search Infrastructure and Data
- Validate Completion of Searches
- Document Finding and Update Case Status

Acquire: Develop Searchables

Searchables can be any of the following:

- **Atomic IOCs** – may have been set aside during the Assess phase
- **Related infrastructure** – results of initial pivoting across unique or exclusive infrastructure (WHOIS, pDNS)
- **Forensic artifacts** – known TTPs of attacker activity
- **Behavior and patterns** – what is the modus operandi of a specific phase of the threat lifecycle (e.g., compromise foreign embassy sites)
- **Target profile** – what is the expected set of assets or personnel likely to be affected

Acquire: Pyramid of Pain

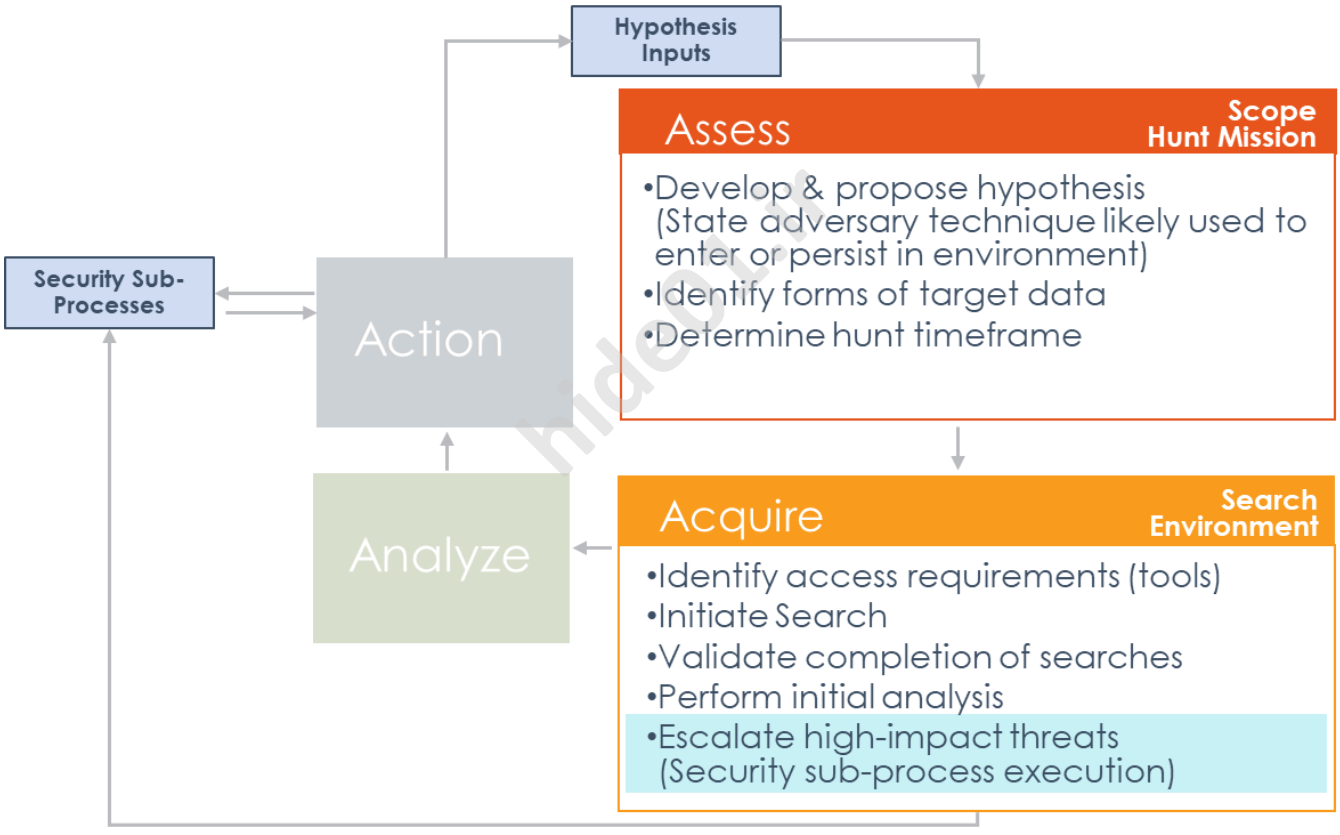
Acquire: Building the Search

- Start small and simple – test queries and syntax against small data sets to ensure execution success
- Document gaps/failures – record any gaps in data availability, parsing, performance errors and failures
- Validate outputs – (if yielded results) verify the output matches expectations in terms of data points and query logic
- Refine and build-out – as output is validated and tools/system performance is realized, tune and expand accordingly the query(ies)

Acquire: Security Sub-Processes

- Derivative tasks from hunt mission
- Critical findings should be escalated
- Escalate these high-fidelity, critical findings to the appropriate teams
    - Examples may include DDoS attacks, high-risk host exposures, malware command and control
- Some hunts will have higher-fidelity matches that don't require additional analysis to determine as positive
    - These are most typical with endpoint-based hunts

Review

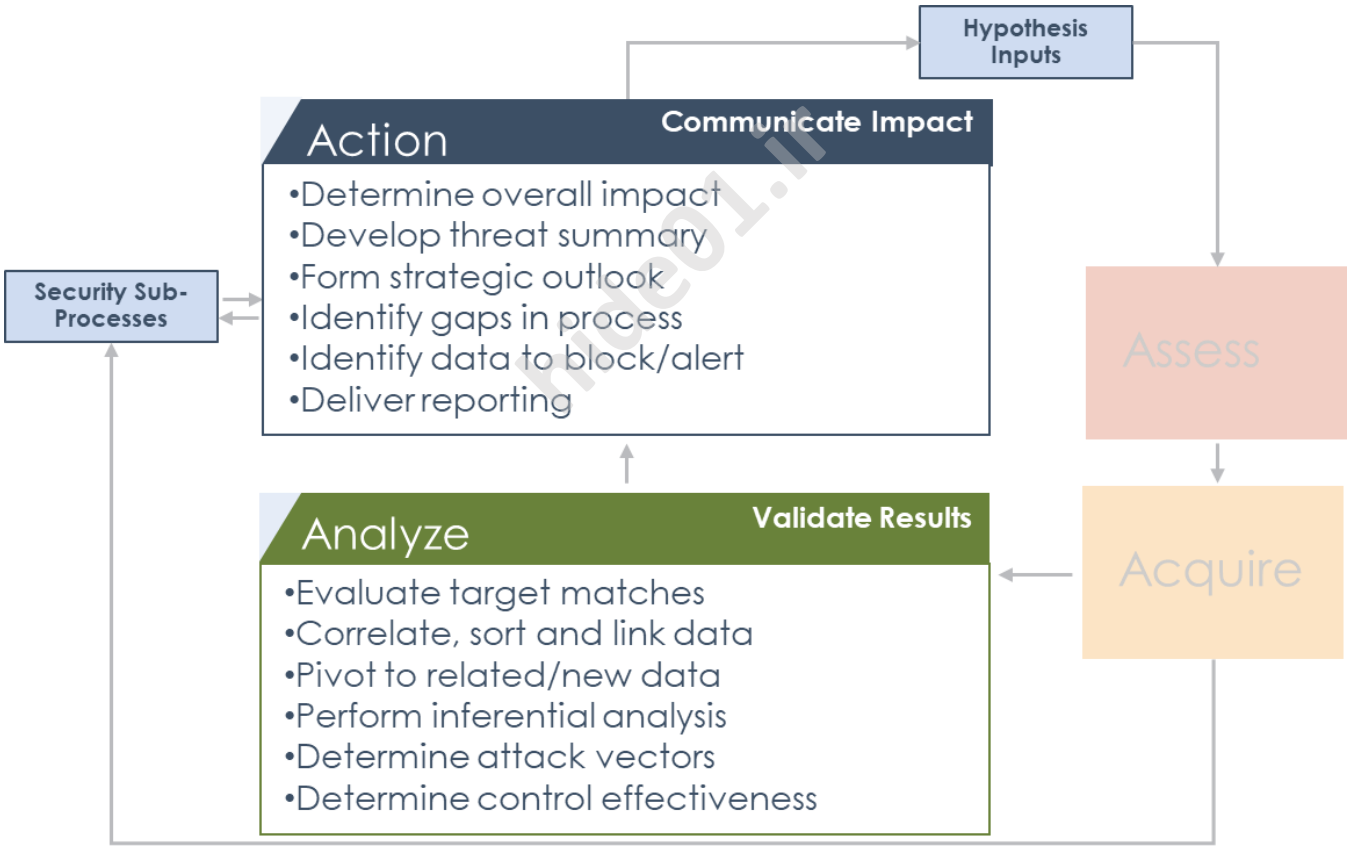


Module 3: Understand Analyze & Action

Objectives

- Process framework review (analyze & action)
- Validate results & draw conclusions (analyze)
- Developing judgments/learning objective
- Impact future tasking, create CTI (action)
- Threat summary development
- A4 review/inputs & outputs

Process Framework



Determine Exposure and Likely Impact

- Make determinations
- Make assessments
- Leverage operational intel

Analyze: Validate results and draw conclusion

- Modify and re-execute searches, if needed
- Sort, link, and prioritize data
- Identify additional indicators and activity
- Initiate secondary hunt cycle
- Perform in-depth analysis, judgements, and address security controls
- Determine vectors and related TTPs

Analyze: Determinations

- Fact-based
  - Validating matches
  - False positive vs. true positive vs. something else (i.e. unrelated to the hunt, but may be “bad”)
- Often the result of technical analysis
  - Task other functional teams if necessary (e.g., malware analysis team)
  - Leverage other sources to minimize redundant tasks
  - Applied scripts or tradecraft to process the output
- A hard science – no confidence ratings necessary
  - What occurred and how did it happen

Analyze: Facts vs. Judgments

The *threat analysis* part of the Analyze phase

- Draw conclusions from facts and determinations
- Clearly differentiate **facts** from **judgements and inferences**
  - Facts generally answer: what, when, where, and how

Example: On <when>, a GET request was made to <what> from <where> as a result of <how>

  - Judgements may address: who and why (that is, motivation)

Example: Based on the TTPs, we suspect with <confidence level> that <who> actors were attempting to <why>

- Don't represent an assumption or inference as fact

Analyze: Confidence Levels

- Consider confidence levels. Leverage other log sources, intelligence, or CTI team to discern confidence levels
- Judgements can become closer to fact as intelligence data deepens

Confidence Level	Judgments
Complete (100%)	We know… We are certain… We are positive…
High (80-95%)	We judge… We expect… It is highly probable…
Moderate (50-79%)	We believe… We think… We anticipate…
Low (11-49%)	We consider… We suggest… We have some indication…

Analyze: Developing Judgments

Threat Hunt Outcome:

- On Tuesday of the previous week, five (5) employees who work in the billing department received a suspicious email with characteristics that resemble APT33 TTPs.

Data:

- **Fact:** Last Tuesday, 5 employees in the billing department received a malicious email from [sender address] with subject line [subject] and containing an attachment [attachment name].
- **Fact:** If successfully executed, the attachment drops [malware name] and calls out to [network indicator].
- **Intel:** The 'industry threat sharing community' sent out a tipper about a suspected APT33 email campaign occurring on the same date involving the same sender address with similar subject theme and attachment.
- **Intel:** FireEye reported on an unattributed campaign with the same phishing characteristics as reported by the 'industry threat sharing community'

Possible Judgements

a) APT33 actors targeted our organization with a malicious email last Tuesday.

b) APT33 actors are targeting billing employees at our organization.

c) Suspected APT33 actors recently targeted multiple organizations, including ours, through a malicious email campaign.

d) We believe with medium confidence that APT33 actors recently targeted our organization, among other organizations.

Judgments A and B are less qualified judgments. Why?

Analyze: Assessments

Fusion of technical and threat analysis

- Leverage operational intelligence – Not as tactical as "what happened?", and not as strategic as "What will happen in the long-term?"
  - Operational Intelligence addresses…
    - Actor motivation and sophistication
    - Organizational targeting and impact
  - May rely on CTI team, but hunt teams can be self-serving to an extent
  - Access to TIP, intel portals, and threat profiles
- Compare and contrast intelligence sources - Challenge intelligence and before agreeing at face value
  - Consider weight of individual factual attributes
    Example: What attributes are used to form attribution?
  - Leverage CTI team to help clarify judgements or interpretations

Analyze: Other Analysis Tasks

- Modify and re-execute searches
  - Identify new target activity
  - Pivot from leads discovered
  - Contextualize events
  - Search other IOCs obtained
- "Table" future hunt needs
- Understand security controls effectiveness
  - Record control bypasses
  - Document potential recommendation/improvement

Communicate Exposure & Likely Impact

- Provide outlook and recommendations
- Tell a story; the reader must understand the message

Action: Impact, future tasking, create CTI

- Finalize overall business impact and form Threat Summary
- Form strategic outlook and recommendations.
- Identify gaps in Intelligence, collections; form new IRs
- Identify data for future detection
- Develop new use cases and base hunts
- Update intel lifecycle and gain feedback on input

Action: Threat Summary

- Formal summation derived from the Analyze phase
  - Technical assessment
  - Attribution judgements and basis
  - Understanding of affected users
  - Other target profiles addressed (geographic, role-based)
  - Impact analysis
- Create or enrich existing "Hunt Findings" template (refer to Exercise 1)
- Strong combined effort of hunt team and CTI Team at this phase
  - Ensure facts and judgements are sound – include PEER REVIEW process
- What additional hunting or other tasks should be formulated?

Hunt Results:

Five employees in the billing department received a malicious email that we suspect was attributed to APT33 actors. The attachment contained malicious code that would attempt to exploit CVE-2018-11882. Our organization's security controls blocked the email and there was no apparent infection or compromise that resulted. All related indicators were added to our block list.

Threat Summary:

The recipients of this malicious email all work in the billing department. As reported by multiple intelligence sources, other organizations across the industry received similar waves of emails that are suspected to be APT33. And while the specific motivation for this campaign is unclear, APT33 has a nexus to Iran and has previously targeted organizations in our industry; among a few select others. This most recent wave of activity suggests that future attempts by these actors against our industry are likely, which may include our organization as an intended target. The hunt team plans to… The CTI team plans to… The VAPT team plans to…

Action: Drive New Outputs

- Identify missing intelligence and collections
  - Actor profiles
  - Malware profiles
- Develop or modify related intelligence requirement(s)
- Explore opportunities to automate future hunts
- Create new use cases or base hunts
- Action indicators, rules, signatures across appropriate controls and systems
  - Ingest data into TIP
  - Deploy malicious indicators across SIEM watch lists
- Notify stakeholders, users, and so on, for threat awareness
- Update or create new threat models and mapping for Assess phase
- Solicit and incorporate feedback on any distributed information

Hunting Process Framework Reviewed

Inputs	Element	Outputs
Intelligence & Intel requirements	**Assess**	Mission target and objectives
Intel extracts; environment specifics Matches & context from all sources	**Acquire**	Potential matches Search results and initial analysis
Confirmed targets & intel (all sources) All pertinent facts around targets	**Analyze**	Logical conclusions from findings Analytic judgment of facts
Determinations, assessments, and intelligence requirements	**Action**	Outlook, recommendations, and intel products

Course Glossary

Term	Meaning
C2	Command and Control
CTI	Cyber Threat Intelligence
IR	Incident Response
IOC	Indicators of Compromise
OT	Operational Technology
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques, and Procedures
Threat Hunting	The methodical, use case driven, proactive identification of cyber threats within a computing environment or infrastructure.
Threat Profile	A matrix that compares priority threat concerns against possible threat actors to determine the likelihood that an attacker will use a given threat vector.

THANK YOU!

MANDIANT