RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: LAB2-T08

Bad Intelligence: Or How I Learned to Stop Buying and Love the Basics

Heather Gantt-Evans

Cyber Threat Management
Ernst & Young LLP

Brett Rogers

Cyber Threat Management
Ernst & Young LLP

Larry Lipsey

Cyber Threat Management
Ernst & Young LLP

Define Cyber Threat Intelligence (CTI)

IS	ISN’T	DOES
The collection, analysis and production of information about adversaries used to make a decision and/or take action	Crystal ball Magic 8 ball Oracle of Delphi Pretty dashboard	Strengthens network defense posture in timely, specific, measurable and impactful ways

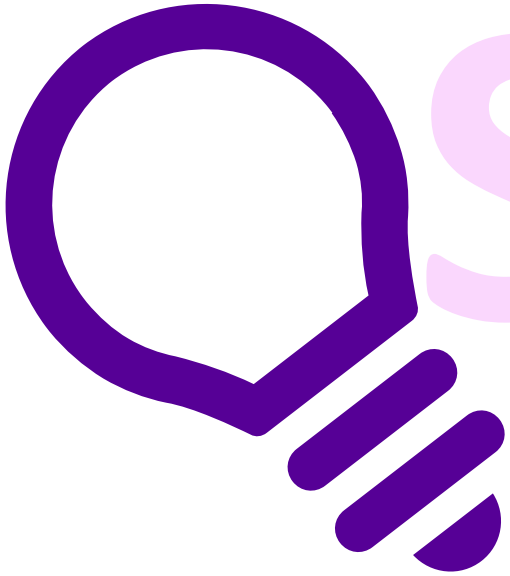
Bad intelligence

Where is the breakdown?

- Years-long training pipeline
- Many information silos
- Granular attribution
- Many highly specialized resources
- Thousands of offices
- Collect everything
- Support everyone

- Staffing struggles and turnover
- Lack “internal intelligence”
- Small return on effort
- Over-budget intelligence programs
- Integration failures
- Data overload / heavy vendor reliance
- Over-scoped mission

Story time



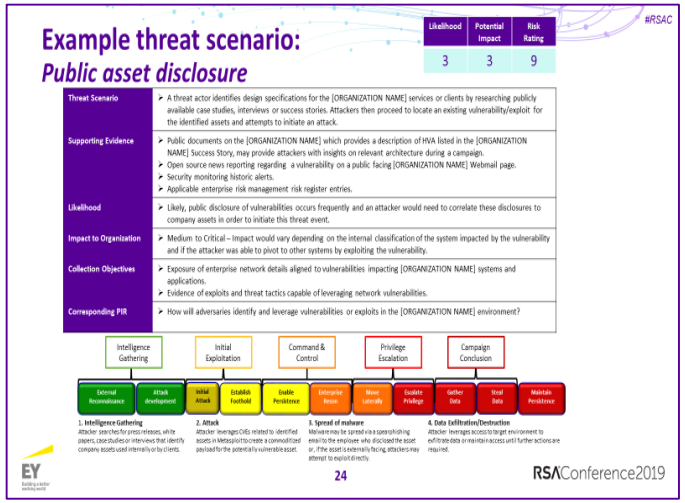
STARTUP
STORY

Key tenants

1 Threat priorities
2 Customer scope
3 Actionable integration and feedback
4 Manual minimal viable product (MVP)

Pics or it didn't happen

Threat Landscape Assessment → Collection Plan → Integration & Workflows → Reporting



Example threat scenario:
Public asset disclosure

Likelihood	Potential Impact	Risk Rating
3	3	9

Threat Scenario	➢ A threat actor identifies design specifications for the [ORGANIZATION NAME] services or clients by researching publicly available case studies, interviews or success stories. Attackers then proceed to locate an existing vulnerability/exploit for the identified assets and attempts to initiate an attack.
Supporting Evidence	➢ Public documents on the [ORGANIZATION NAME] which provides a description of HVA listed in the [ORGANIZATION NAME] Success Story, may provide attackers with insights on relevant architecture during a campaign. ➢ Open source news reporting regarding a vulnerability on a public facing [ORGANIZATION NAME] Webmail page. ➢ Security monitoring historic alerts. ➢ Applicable enterprise risk management risk register entries.
Likelihood	➢ Likely, public disclosure of vulnerabilities occurs frequently and an attacker would need to correlate these disclosures to company assets in order to initiate this threat event.
Impact to Organization	➢ Medium to Critical – Impact would vary depending on the internal classification of the system impacted by the vulnerability and if the attacker was able to pivot to other systems by exploiting the vulnerability.
Collection Objectives	➢ Exposure of enterprise network details aligned to vulnerabilities impacting [ORGANIZATION NAME] systems and applications. ➢ Evidence of exploits and threat tactics capable of leveraging network vulnerabilities.
Corresponding PIR	➢ How will adversaries identify and leverage vulnerabilities or exploits in the [ORGANIZATION NAME] environment?

Intelligence Gathering → Initial Exploitation → Command & Control → Privilege Escalation → Campaign Conclusion

External Reconnaissance → Attack development → Initial Attack → Establish Foothold → Enable Persistence → Enterprise Recon → Move Laterally → Escalate Privilege → Gather Data → Steal Data → Maintain Persistence

1. Intelligence Gathering Attacker searches for press releases, white papers, case studies or interviews that identify company assets used internally or by clients.

2. Attack Attacker leverages CVEs related to identified assets in Metasploit to create a commoditized payload for the potentially vulnerable asset.

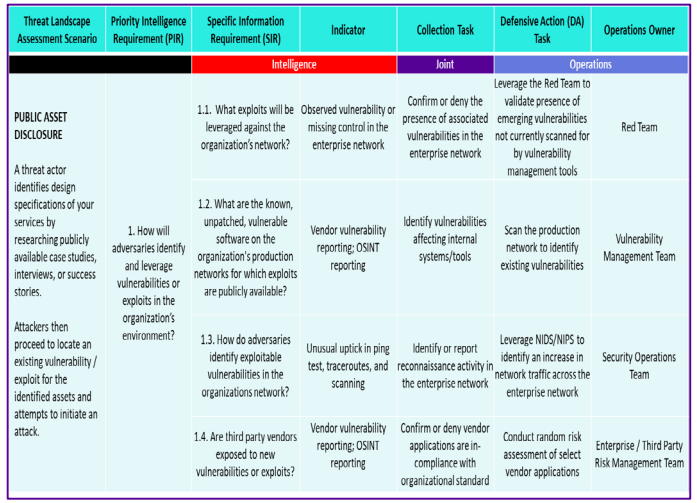
3. Spread of malware Malware may be spread via a spear phishing email to the employee who disclosed the asset or, if the asset is externally facing, attackers may attempt to exploit directly.

4. Data Exfiltration/Destruction Attacker leverages access to target environment to exfiltrate data or maintain access until further actions are required.

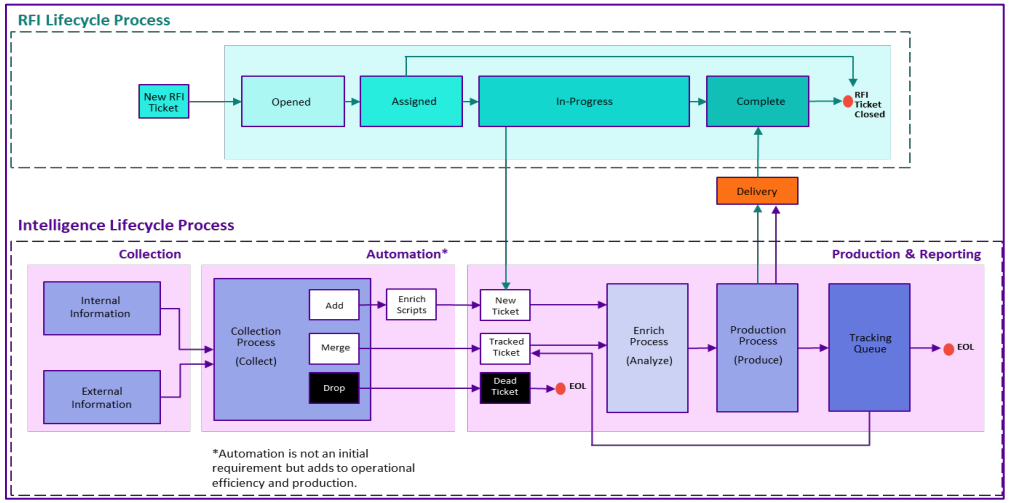
EY Building a better working world

24

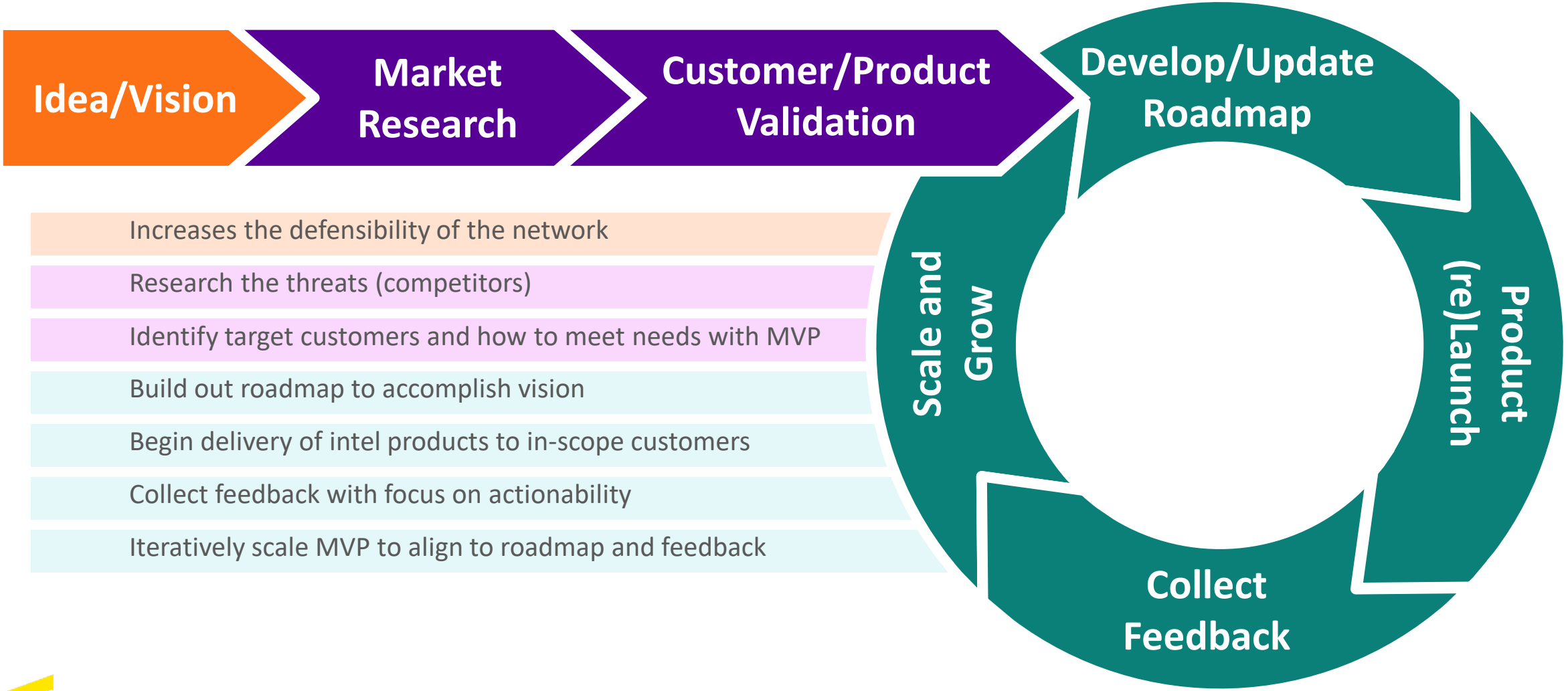
RSAConference2019



Threat Landscape Assessment Scenario	Priority Intelligence Requirement (PIR)	Specific Information Requirement (SIR)	Indicator	Collection Task	Defensive Action (DA) Task	Operations Owner
		Intelligence		Joint	Operations	
PUBLIC ASSET DISCLOSURE A threat actor identifies design specifications of your services by researching publicly available case studies, interviews, or success stories. Attackers then proceed to locate an existing vulnerability / exploit for the identified assets and attempts to initiate an attack.	1. How will adversaries identify and leverage vulnerabilities or exploits in the organization's environment?	1.1. What exploits will be leveraged against the organization's network?	Observed vulnerability or missing control in the enterprise network	Confirm or deny the presence of associated vulnerabilities in the enterprise network	Leverage the Red Team to validate presence of emerging vulnerabilities not currently scanned for by vulnerability management tools	Red Team
		1.2. What are the known, unpatched, vulnerable software on the organization's production networks for which exploits are publicly available?	Vendor vulnerability reporting; OSINT reporting	Identify vulnerabilities affecting internal systems/tools	Scan the production network to identify existing vulnerabilities	Vulnerability Management Team
		1.3. How do adversaries identify exploitable vulnerabilities in the organizations network?	Unusual uptick in ping test, traceroutes, and scanning	Identify or report reconnaissance activity in the enterprise network	Leverage NIDS/NIPS to identify an increase in network traffic across the enterprise network	Security Operations Team
		1.4. Are third party vendors exposed to new vulnerabilities or exploits?	Vendor vulnerability reporting; OSINT reporting	Confirm or deny vendor applications are in-compliance with organizational standard	Conduct random risk assessment of select vendor applications	Enterprise / Third Party Risk Management Team



How do we start?



- Increases the defensibility of the network
- Research the threats (competitors)
- Identify target customers and how to meet needs with MVP
- Build out roadmap to accomplish vision
- Begin delivery of intel products to in-scope customers
- Collect feedback with focus on actionability
- Iteratively scale MVP to align to roadmap and feedback

Agenda

✓ Introduction	25 mins
Group exercise 1: Market Research	25 mins
Group exercise 2: Customer/Product Validation part 1	25 mins
Group exercise 3: Customer/Product Validation part 2	25 mins
Next Steps and Apply	10 mins
Q & A	10 mins

Group exercise 1

Time: 12 minutes table prep, 8 minute debrief to the room

Instructions:

At each table, group together and leverage the following artifacts from *President Business' Worldwide Conglomerate (PBWC)* to populate the provided risk register with ratings and determine PBWC's highest risk threat scenario.

1. Business background and high value asset list
2. List of threat scenarios produced from a recent threat landscape assessment
3. Risk rating criteria

Group exercise 2

Time: 12 minutes table prep, 8 minute debrief to the room

Instructions:

Within “Group Exercise 2” handout, discuss and try to fill in the blanks across the three columns. Examples are provided. Afterwards, please select one Primary and Secondary intelligence customer. Be prepared to present your team’s decision and logic.

Tip: Consider customers’ ability to impact network defense.

Group exercise 2 answers

Group	CTI Provided Support	Enabled Defensive Capabilities
Physical/Supply Chain	Analysis regarding cyber threats to facilities or distribution channels	Use of ad-hoc actions to protect facilities and distribution channels
Security Operations	All-source analysis to drive continuous network monitoring, response, defense and threat hunting	Use of ad-hoc actions to protect the network through: blocking, alerting, investigating, temporarily restricting and monitoring items of interest
Red Team	Collaborative effort to create realistic threat scenarios for testing	Ability to simulate the tactics, techniques and procedures of relevant threat actors and identify associated vulnerabilities
Vulnerability Management	Analysis used to validate and prioritize vulnerability risk	Prioritized out-of-cycle/emergency patching
Architecture/IT	Analysis regarding emerging threats to infrastructure	Prioritized implementation of controls and architecture designs to improve the long-term defensibility of the network
Executive Board	Trends and metrics analysis highlighting cyber threats with impacts to revenue	Prioritized security investments aligned to cyber risk reduction
Business Information Security Officers	Trends and metrics analysis highlighting cyber threats with impacts to business operations	Business Information Security Officers can prioritize controls to protect business operations
Enterprise/Third Party Risk Management	Analysis regarding current cyber threats to the enterprise and vendors/external partners	Ability to update risk assessment frameworks, refine enterprise security standards, policies and procedures, and more thoroughly assess/control risks posed by vendors
Data Protection	Analysis of adversary intent/capabilities to target high value data	Better targeted controls and policy designed to protect sensitive data

Primary Customer
(daily/weekly cycle)

Security Operations

Second Customer
(monthly/quarterly cycle)

Vulnerability Management

Group exercise 3

Time: 12 minutes table prep, 8 minute debrief to the room

Instructions:

At each table, group together and leverage the threat landscape assessment (TLA) and customer validation matrix to develop a collection plan.

Tip: Consider your organization's ability to collect given people and technology constraints.

Group exercise 3 answers

Threat Landscape Assessment Scenario	Priority Intelligence Requirement (PIR)	Specific Information Requirement (SIR)	Indicator	Collection Task	Defensive Action (DA) Task	Operations Owner
		Intelligence		Joint	Operations	
PUBLIC ASSET DISCLOSURE A threat actor identifies design specifications of your services by researching publicly available case studies, interviews, or success stories. Attackers then proceed to locate an existing vulnerability/ exploit for the identified assets and attempts to initiate an attack.	1. How will adversaries identify and leverage vulnerabilities or exploits in the organization's environment?	1.1. What exploits/tactics will be leveraged against the organization's network?	Observed vulnerability or missing control in the enterprise network	Confirm or deny the presence of associated vulnerabilities in the enterprise network	Leverage the Red Team to validate presence of emerging vulnerabilities not currently scanned for by vulnerability management tools	Red Team
		1.2. What are the known, unpatched, vulnerable software on the organization's production networks for which exploits are publicly available?	Vendor vulnerability reporting; OSINT reporting	Identify vulnerabilities affecting internal systems/tools	Scan the production network to identify existing vulnerabilities	Vulnerability Management Team
		1.3. How do adversaries identify exploitable vulnerabilities in the organization's network?	Unusual uptick in ping test, traceroutes and scanning	Identify or report reconnaissance activity in the enterprise network	Leverage NIDS/NIPS to identify an increase in network traffic across the enterprise network	Security Operations Team
		1.4. Are third party vendors exposed to new vulnerabilities or exploits?	Vendor vulnerability reporting; OSINT reporting	Confirm or deny vendor applications are in compliance with organizational standard	Conduct random risk assessment of select vendor applications	Enterprise/Third Party Risk Management Team

Note: Additional collection plan inputs for consideration include measures of effectives, frequency of collection and collection tool/source.

RSAConference2019

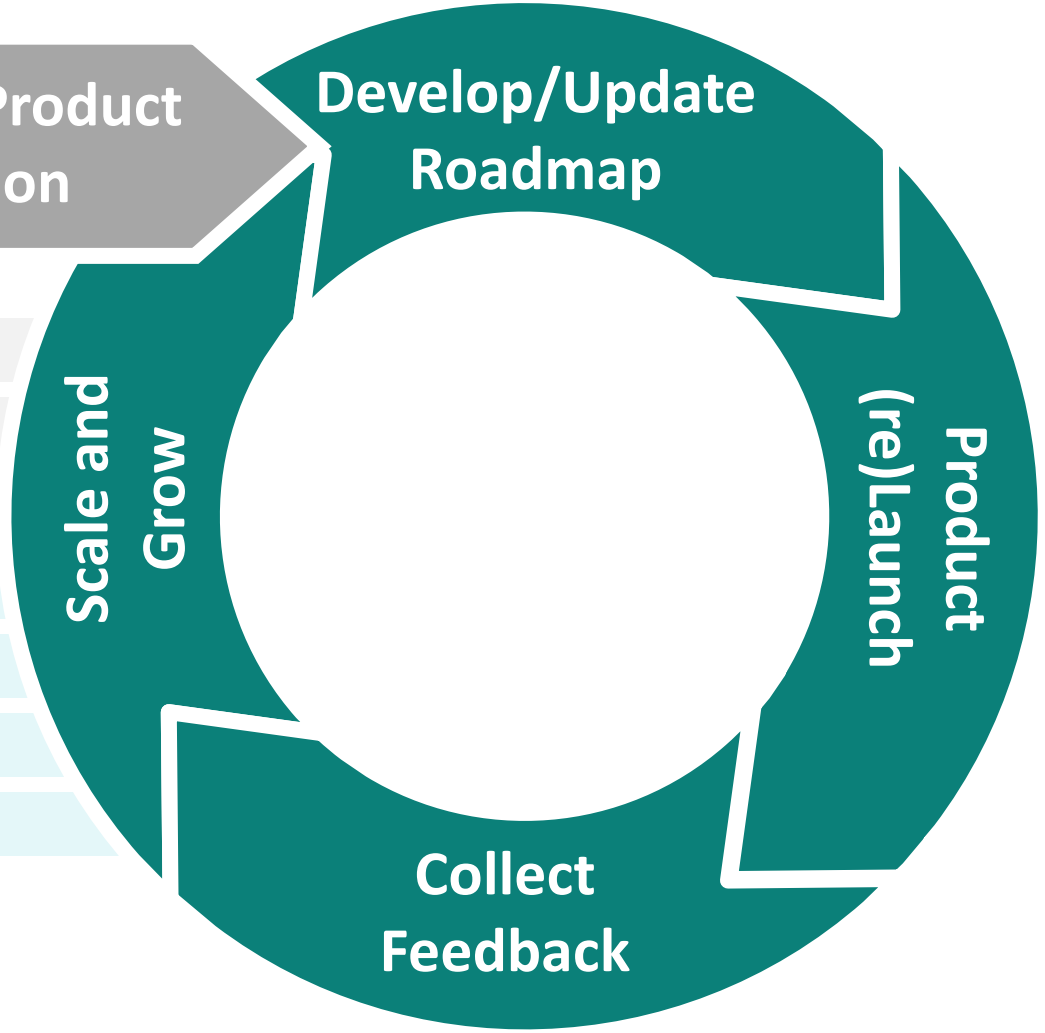
Next Steps and Apply

Applying what we learned

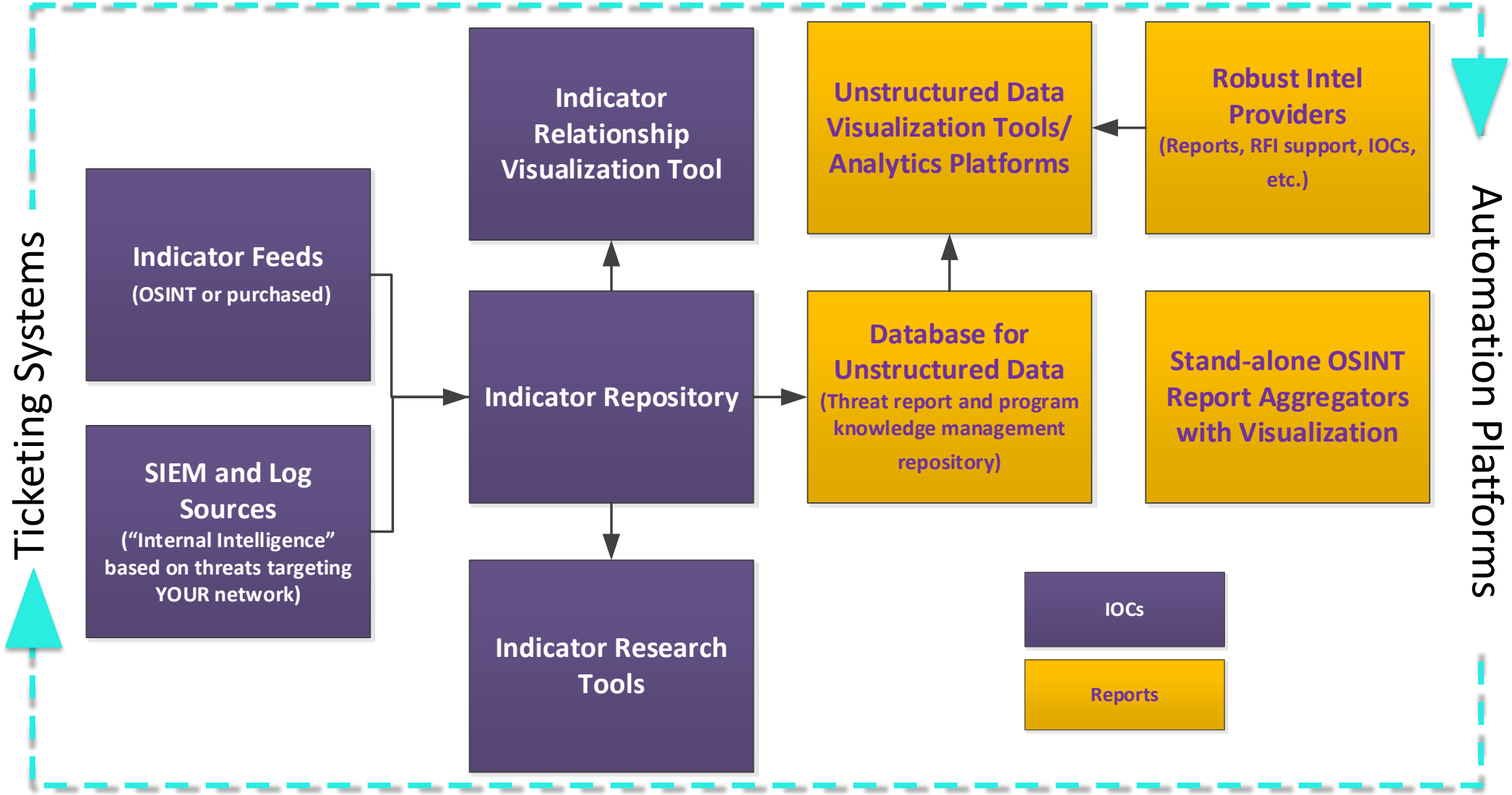
What comes next?

Idea/Vision → Market Research → Customer/Product Validation

- Increases the defensibility of the network
- Research the threats (competitors)
- Identify target customers and how to meet needs with MVP
- Build out roadmap to accomplish vision
- Begin delivery of intel products to in-scope customers
- Collect feedback with focus on actionability
- Iteratively scale MVP to align to roadmap and feedback

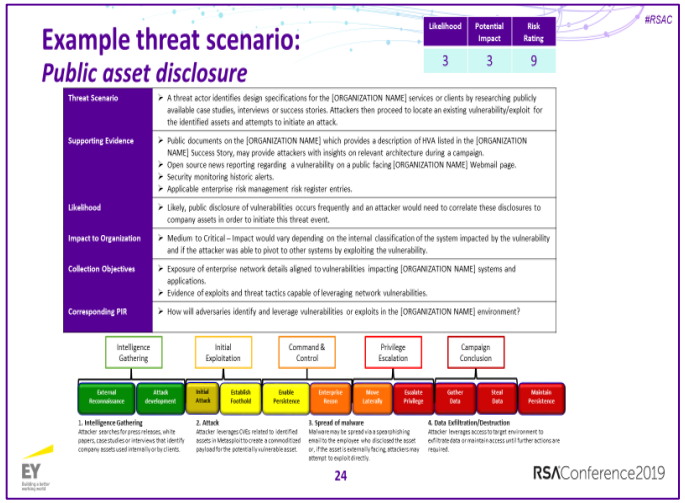


But can't a TIP do all of this for me?



Apply and artifact handout

Threat Landscape Assessment → Collection Plan → Integration & Workflows → Reporting



Example threat scenario:
Public asset disclosure

Likelihood	Potential Impact	Risk Rating
3	3	9

Threat Scenario	➢ A threat actor identifies design specifications for the [ORGANIZATION NAME] services or clients by researching publicly available case studies, interviews or success stories. Attackers then proceed to locate an existing vulnerability/exploit for the identified assets and attempts to initiate an attack.
Supporting Evidence	➢ Public documents on the [ORGANIZATION NAME] which provides a description of HVA listed in the [ORGANIZATION NAME] Success Story, may provide attackers with insights on relevant architecture during a campaign. ➢ Open source news reporting regarding a vulnerability on a public facing [ORGANIZATION NAME] Webmail page. ➢ Security monitoring historic alerts. ➢ Applicable enterprise risk management risk register entries.
Likelihood	➢ Likely, public disclosure of vulnerabilities occurs frequently and an attacker would need to correlate these disclosures to company assets in order to initiate this threat event.
Impact to Organization	➢ Medium to Critical – Impact would vary depending on the internal classification of the system impacted by the vulnerability and if the attacker was able to pivot to other systems by exploiting the vulnerability.
Collection Objectives	➢ Exposure of enterprise network details aligned to vulnerabilities impacting [ORGANIZATION NAME] systems and applications. ➢ Evidence of exploits and threat tactics capable of leveraging network vulnerabilities.
Corresponding PIR	➢ How will adversaries identify and leverage vulnerabilities or exploits in the [ORGANIZATION NAME] environment?

Intelligence Gathering → Initial Exploitation → Command & Control → Privilege Escalation → Campaign Conclusion

External Reconnaissance → Attack development → Initial Attack → Establish Foothold → Enable Persistence → Enterprise Recon → Move Laterally → Escalate Privilege → Gather Data → Steal Data → Maintain Persistence

1. Intelligence Gathering Attacker searches for press releases, white papers, case studies or interviews that identify company assets used internally or by clients.

2. Attack Attacker leverages CVEs related to identified assets in Metasploit to create a commoditized payload for the potentially vulnerable asset.

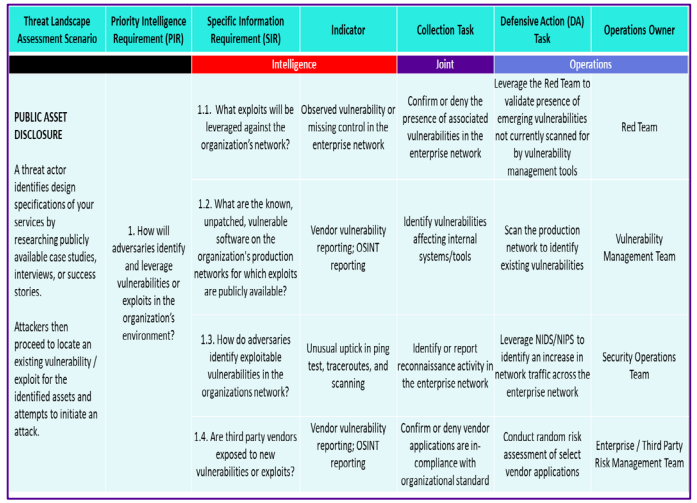
3. Spread of malware Malware may be spread via a spear phishing email to the employee who disclosed the asset or, if the asset is externally facing, attackers may attempt to exploit directly.

4. Data Exfiltration/Destruction Attacker leverages access to target environment to exfiltrate data or maintain access until further actions are required.

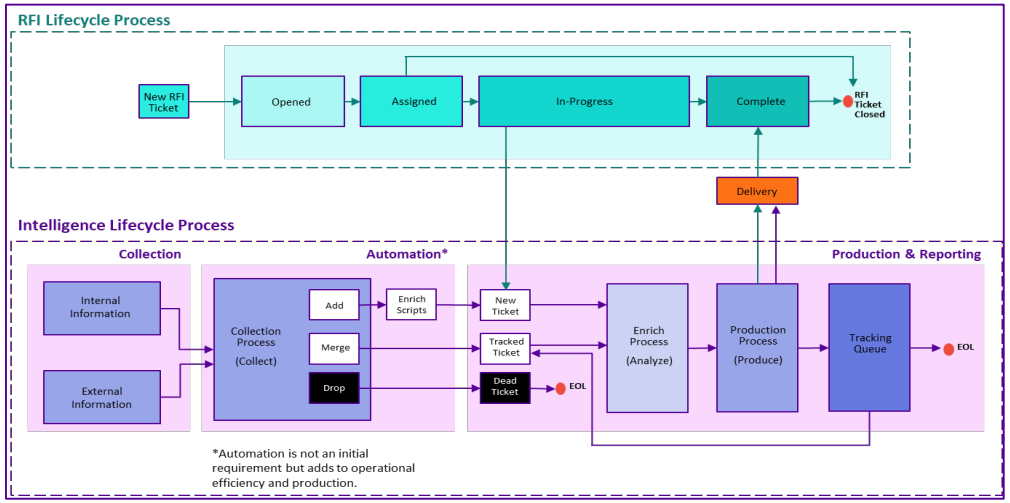
EY Building a better working world

24

RSAConference2019



Threat Landscape Assessment Scenario	Priority Intelligence Requirement (PIR)	Specific Information Requirement (SIR)	Indicator	Collection Task	Defensive Action (DA) Task	Operations Owner
		Intelligence		Joint	Operations	
PUBLIC ASSET DISCLOSURE A threat actor identifies design specifications of your services by researching publicly available case studies, interviews, or success stories. Attackers then proceed to locate an existing vulnerability / exploit for the identified assets and attempts to initiate an attack.	1. How will adversaries identify and leverage vulnerabilities or exploits in the organization's environment?	1.1. What exploits will be leveraged against the organization's network?	Observed vulnerability or missing control in the enterprise network	Confirm or deny the presence of associated vulnerabilities in the enterprise network	Leverage the Red Team to validate presence of emerging vulnerabilities not currently scanned for by vulnerability management tools	Red Team
		1.2. What are the known, unpatched, vulnerable software on the organization's production networks for which exploits are publicly available?	Vendor vulnerability reporting; OSINT reporting	Identify vulnerabilities affecting internal systems/tools	Scan the production network to identify existing vulnerabilities	Vulnerability Management Team
		1.3. How do adversaries identify exploitable vulnerabilities in the organizations network?	Unusual uptick in ping test, traceroutes, and scanning	Identify or report reconnaissance activity in the enterprise network	Leverage NIDS/NIPS to identify an increase in network traffic across the enterprise network	Security Operations Team
		1.4. Are third party vendors exposed to new vulnerabilities or exploits?	Vendor vulnerability reporting; OSINT reporting	Confirm or deny vendor applications are in-compliance with organizational standard	Conduct random risk assessment of select vendor applications	Enterprise / Third Party Risk Management Team



Summary

- Discovered an **end to end framework** developed for cost-effective, custom integration of intelligence.
- Learned how to implement **custom workflows** for the most valuable threat intelligence integration.
- Walking away with real **analytical artifacts** and become confident in application to your business.

Q & A

- Burning questions now, tomorrow, next month or next year?

Email us anytime at:

Heather Gantt-Evans
heather.gantt@ey.com

Brett Rogers
brett.rogers@ey.com

Larry Lipsey
larry.lipsey@ey.com

RSAConference2019

Appendix: Handout artifacts

Taking it back to the business

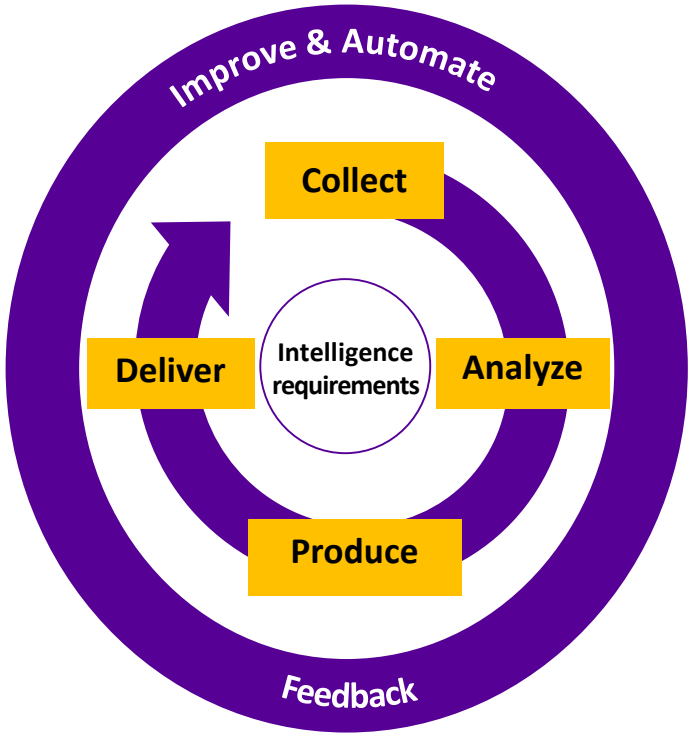
CTI operating model

DATA

Example Sources

- Threat intelligence feeds
- Technical logs
- Social media
- Open source news
- Asset Inventory

PROCESS*



PRODUCT

Recommended Actions delivered via:

- CTI Alerts
- CTI Reports
- Requests for Information (RFI) Responses

Intelligence

Cyber Threat Intelligence = the collection, analysis and production of information about adversaries used to make a decision and/or take action that strengthens defense posture

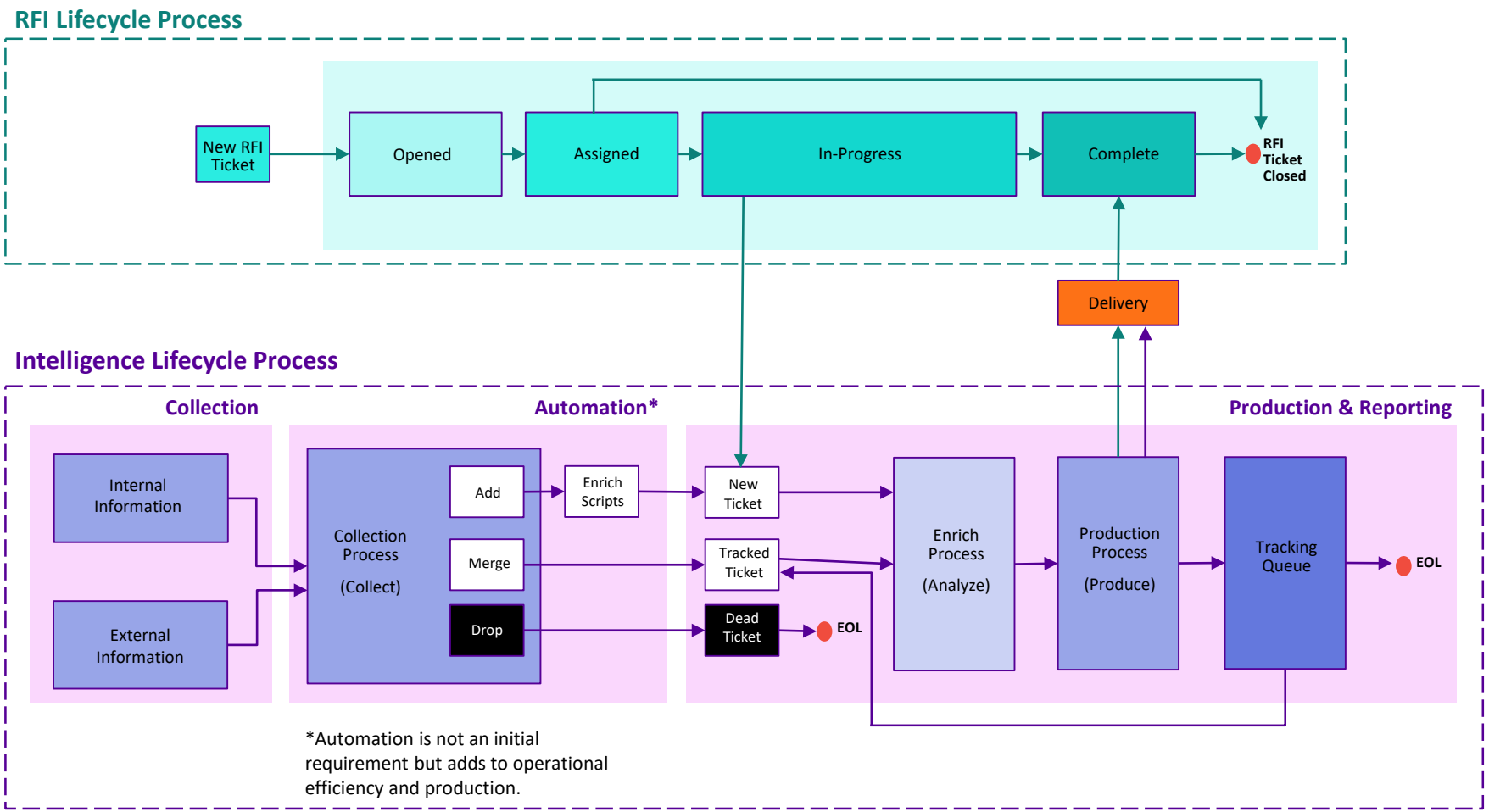
CONSUMER

Primary
(Daily/Weekly)

Secondary
(Monthly/ Quarterly)

***People Requirements:** 2-4 dedicated analysts depending on organizational size and intelligence mission scope

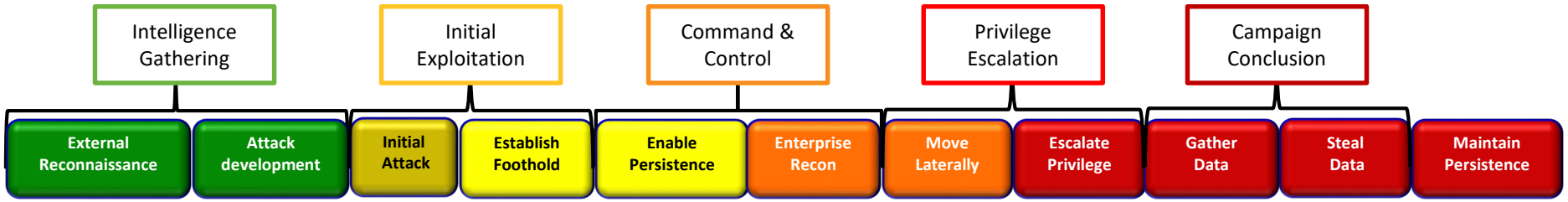
Example CTI workflow



Example threat scenario:
Public asset disclosure

Likelihood	Potential Impact	Risk Rating
3	3	9

Threat Scenario	➢ A threat actor identifies design specifications for the [ORGANIZATION NAME] services or clients by researching publicly available case studies, interviews or success stories. Attackers then proceed to locate an existing vulnerability/exploit for the identified assets and attempts to initiate an attack.
Supporting Evidence	➢ Public documents on the [ORGANIZATION NAME] which provides a description of HVA listed in the [ORGANIZATION NAME] Success Story, may provide attackers with insights on relevant architecture during a campaign. ➢ Open source news reporting regarding a vulnerability on a public facing [ORGANIZATION NAME] Webmail page. ➢ Security monitoring historic alerts. ➢ Applicable enterprise risk management risk register entries.
Likelihood	➢ Likely, public disclosure of vulnerabilities occurs frequently and an attacker would need to correlate these disclosures to company assets in order to initiate this threat event.
Impact to Organization	➢ Medium to Critical – Impact would vary depending on the internal classification of the system impacted by the vulnerability and if the attacker was able to pivot to other systems by exploiting the vulnerability.
Collection Objectives	➢ Exposure of enterprise network details aligned to vulnerabilities impacting [ORGANIZATION NAME] systems and applications. ➢ Evidence of exploits and threat tactics capable of leveraging network vulnerabilities.
Corresponding PIR	➢ How will adversaries identify and leverage vulnerabilities or exploits in the [ORGANIZATION NAME] environment?



1. Intelligence Gathering
Attacker searches for press releases, white papers, case studies or interviews that identify company assets used internally or by clients.

2. Attack
Attacker leverages CVEs related to identified assets in Metasploit to create a commoditized payload for the potentially vulnerable asset.

3. Spread of malware
Malware may be spread via a spearphishing email to the employee who disclosed the asset or, if the asset is externally facing, attackers may attempt to exploit directly.

4. Data Exfiltration/Destruction
Attacker leverages access to target environment to exfiltrate data or maintain access until further actions are required.

Example collection plan

TLA Scenario	Priority Intelligence Requirement (PIR)	Specific Information Requirement (SIR)	Indicator	Collection Task	Ops Owner	Collection Tool(s)	Collection Frequency	Measure of Effectiveness (MOE)
		Intelligence			Operations			Joint
ENTERPRISE NETWORK AS A VECTOR Attackers determine your organization stores critical PCI, PII, or data related to intellectual property in a cloud environment. The attackers then attempt to compromise your enterprise through any means necessary and pivot through assets.	1. What indications and warnings suggest adversaries are targeting PCI/PII information hosted in the enterprise environment?	1.1. Are there instances of an adversary searching for data strings similar to a date of birth (DOB) or SSN?	ID string character searches matching SSN/Credit Card/Visa number sequences; Observed account files and directory discovery activity	ID unique character string searches (SSN, CC, DOB, ACCT #'s, etc.)	Security Monitoring	IDS/IPS	Weekly	Anomalous behavior detection increased by 30%
				ID string search gaps to PII systems	Threat Hunting	IDS/IPS		
				Confirm ACL's	IAM	IAM platform		
		1.2. What internal teams or sysadmins will adversary target due to placement & access to PCI/PII ?	High volume of phishing against a particular team or sysadmin	ID new sysadmins by department and maintain an accurate personnel inventory	GRC	CRM platform	Quarterly	Phishing attempts to sysadmins decreased by 15%
				Confirm/Deny vulnerabilities for systems in sysadmins scope of responsibility	Vulnerability Management	Vulnerability Scanner		
				ID tactics for targeting internal PCI/PII teams/sysadmins	Threat Intelligence	Open source or vendor reporting		
		1.3. Is there an unusual amount of system login failure attempts?	Modified timestamps log files	Confirm/Deny pattern on system login failures	Active Defense	IDS/IPS, SIEM analytics	Weekly	Anomalous login activity detection increased by 20%
				ID system login failures	Security Monitoring	AD, NAC, VPN, Wireless		

Note: "Defensive Action (DA) Task" column omitted to allow room for additional columns that can be leveraged in a collection plan. Defensive Actions are not required to be in the collection plan but should be incorporated in all RFI responses, CTI alerts and CTI reports.