DRAGOS

OSINT Analysis for Industrial Defenders

A Framework

Content

- OSINT Overview
- Targeting ICS
- Developing OSINT Assessment
- Taking Action

What is OSINT?

- The collection of publicly and semi-publicly available information that is used to inform multiple functions including intelligence gathering and reporting, business and policy analysis, and adversary attack development.

- Dragos focuses on OSINT from a cyber threat intelligence perspective, with applications from ICS asset owners, operators, and adversaries.

Key Terms

- **Personal/Personnel Information:**
  - Allows for identification of critical personnel, general personnel, or outside source personnel (e.g. contractors, third-party operators).
- **Criticality Information:**
  - Informs an adversary of the impact of an attack for a target's continued operations. A target's criticality is determined by if its compromise or destruction has a highly significant impact in the overall organization and by its ability to conduct business or operations.

Key Terms

- **Accessibility Information:**

- Informs the adversary of the ability or method to remotely/physically access or egress from a target.

- **Recoverability Information:**

- Gives an adversary insight into the ability of a target's process, system, or network infrastructure to recover from an attack or compromise.

Key Terms

- **Vulnerability Information:**

  - Informs an adversary of a vulnerability that exists in a target's infrastructure, processes, or response actions.

- **Effect Information:**

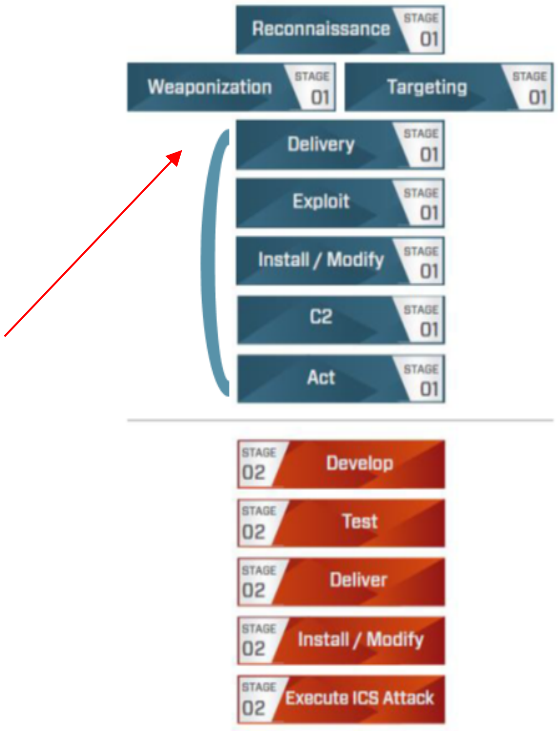
  - Information about the direct or indirect loss a target would have from an attack or compromise.

- **Recognizability Information:**

  - Assists adversaries in identifying targets for operational gain and the level of obscurity that the target has from internal and external sources.

Targeting ICS

- Attacks can be used to further political, economic, or national security goals.
- ICS attacks can be used for messaging purposes or retaliation with the potential impact extending to citizens of a target's community.
- Targeting ICS can provide monetary value to an adversary. ICS entities increasingly experience ransomware attacks that disrupt operations.

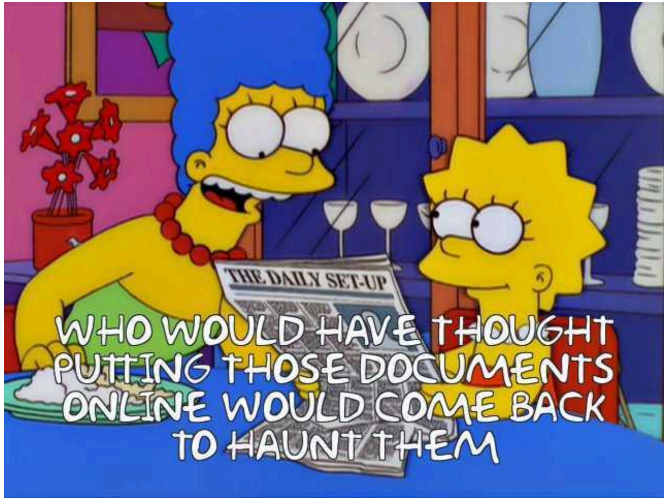


Developing an OSINT Assessment

By identifying and prioritizing data that could be used in OSINT collection, defenders can establish methods to reduce the availability of potentially high-risk OSINT and limit the information an adversary can identify and use in a potential attack.

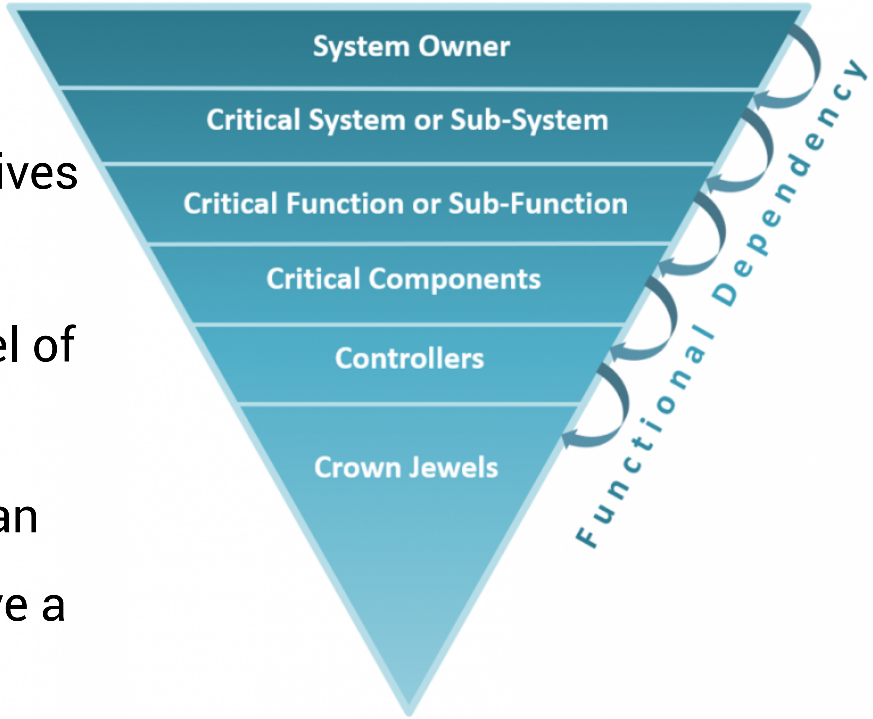
1. Scope the Scenarios

- Begin by scoping multiple scenarios and potential for attacks.
- These can be found from examples of known cyberattacks, results of tabletop exercises and red team activities, and scenarios developed by internal security teams.
- The goal of this step is to identify the type of attack that defenders try to prevent.


THE DAILY SET-UP
WHO WOULD HAVE THOUGHT PUTTING THOSE DOCUMENTS ONLINE WOULD COME BACK TO HAUNT THEM

1. Scope the Scenarios

- Leverage consequence-driven security assessments to identify attacker objectives and how to combat them.
- The Dragos Crown Jewel Analysis model of consequence-driven ICS cybersecurity scoping helps defenders visualize how an attacker may access a system to achieve a specific objective.



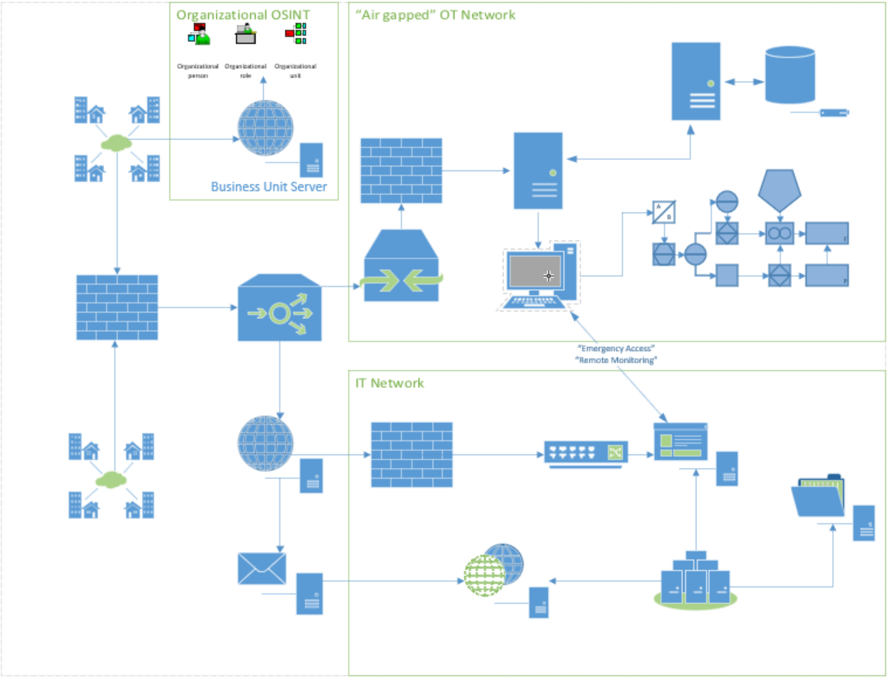
2. Collaborate Across the Company

- Consult security operators and network technicians from IT, incident response and forensics, security operations and engineering, and physical security specialists.

- These professionals can provide insight on the value of information from an adversary perspective and how OSINT can enable potential attack scenarios.

3. Detail the System and Network

- A detailed map of the network should be developed and maintained to visually describe where information is hosted, stored, and maintained through system diagrams, flow charts, and network maps.



3. Detail the System and Network

- **Example:** If an individual evaluates a domain hosting contractor information and third-party network access, the system being evaluated is technical and contextual. This means the content of the information hosted should be detailed to the technical specifications of the actual hosting server.

4. Identify Sources and Collect Information

- Sources vary for individual companies.
- Consider information exposed by third-party entities that could be used in reconnaissance operations.

-Search engines
-Social media websites
-Job listings
-News websites
-Company websites
-Vendor websites and documentation including installation documentation containing default passwords
-Financial and legal resources such as 10-K filings or indictments
-Reconnaissance tools such as Shodan or Censys
-Online scanning engines such as VirusTotal
-Business solicitation portals
-Usernames and passwords in public repositories dumped by adversaries or stored in GitHub

4. Identify Sources and Collect Information

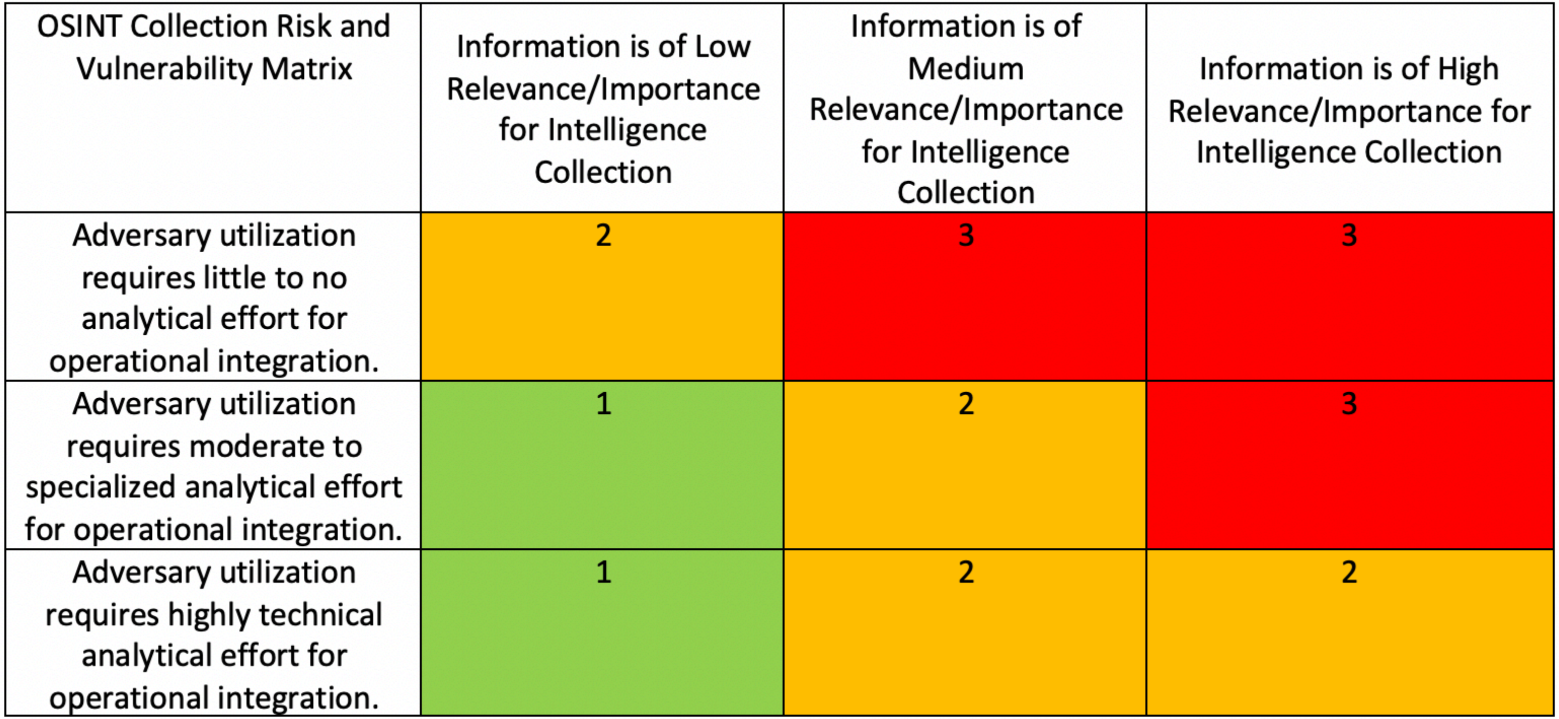
- Focus on publicly available information that could be used to facilitate reconnaissance or attack development.

- Security teams should also identify gaps in security architecture, such as remote login portals, that lack strong passwords and multi-factor authentication including RDP and VPN services.

5. Conduct Analysis and Risk Assessment

- Determine how an adversary might operationalize data to achieve objectives outlined in potential attack scenarios.
- Data should be assigned severity scores to facilitate prioritization.

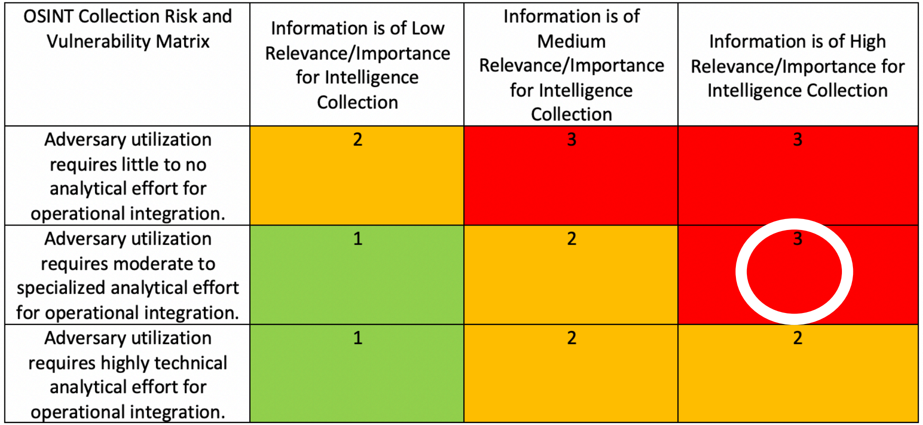
OSINT Collection and Risk Scoring Matrix



OSINT Collection Risk and Vulnerability Matrix	Information is of Low Relevance/Importance for Intelligence Collection	Information is of Medium Relevance/Importance for Intelligence Collection	Information is of High Relevance/Importance for Intelligence Collection
Adversary utilization requires little to no analytical effort for operational integration.	2	3	3
Adversary utilization requires moderate to specialized analytical effort for operational integration.	1	2	3
Adversary utilization requires highly technical analytical effort for operational integration.	1	2	2

OSINT Collection and Risk Scoring Matrix

Example: An OSINT assessment identified a document containing engineering diagrams of an oil production facility. The document included device type and implementation information, including safety systems and integration of ERP software. This document was a public vendor RFP.



OSINT Collection Risk and Vulnerability Matrix	Information is of Low Relevance/Importance for Intelligence Collection	Information is of Medium Relevance/Importance for Intelligence Collection	Information is of High Relevance/Importance for Intelligence Collection
Adversary utilization requires little to no analytical effort for operational integration.	2	3	3
Adversary utilization requires moderate to specialized analytical effort for operational integration.	1	2	[✓ 3]
Adversary utilization requires highly technical analytical effort for operational integration.	1	2	2

Priorities of Defense and Mitigation

- As information is assessed and assigned scores, users can leverage the Priorities of Defense and Mitigation (PODAM) table to visualize:
  - How collected data that could be operationalized
  - What is the value of the information
  - What protections and mitigations are in place to address the potential risk

Priorities of Defense and Mitigation

		ADVERSARY OSINT COLLECTION PODAM																												
		Target Identification			Exploitation			Infrastructure Development					Delivery						Capabilities Development								Actions on the Objective			
Information Collected ID	Utilization	Personnel	Technology	Organizational	Vulnerability	Social Engineering	Supply Chain	Domain Spoof	Legitimate Compromise	Vendor Supply Chain	Establishment	Staging	Phishing	Watering Hole	Downloader/Dropper	Credential Capture	Legitimate Access	Authentication Bypass	Research & Development	Automation	Evasion	Obfuscation	Installation	Environment Awareness	Weaponization	Interactive Operations	Command and Control	Persistence	Manuver	Cyber Key Terrain
Geographic Locations of Entities	Targeting	🟦	🟧	🟧 $	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩 x	🟩
Names and Emails of Engineers	Targeting, Exploitation	🟥 $	🟥	🟥	🟦	🟥	🟥 o	🟧	🟧	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟥 \ o	🟧 \	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟧	🟧	🟧	🟧 x	🟧
Vendor Names and Contracts	Targeting, Infrastructure Development, Exploitation	🟧 $	🟧 $	🟧 $	🟦	🟧	🟥 o	🟧	🟥	🟥 o	🟥	🟥	🟥	🟥	🟥	🟥	🟥 \ o	🟥 \	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟧	🟦	🟦	🟦	🟧

Legend

🟥	High Target Importance	X	Defense Capability Gap	*	Intelligence Data
🟧	Medium Target Importance	O	Missing Dependencies	$	Policy Issue
🟩	Low Target Importance	\	Requires Implementation		
🟦	N/A				

Priorities of Defense and Mitigation

- Remove sensitive information from public sources where applicable.

- Conduct an assessment of third-party and vendor integrations within the operations environment.

- Ensure third-party connections are properly secure with access restrictions, multi-factor authentication, segmentation, and defense in depth measures.

- Work with vendors and contractors to identify and acknowledge maintenance and related operations in advance to determine schedules and baseline legitimate activity.

Taking Action

- Implement remediation plans that focus on the most critical to least critical information for adversary operationalization.

- Plans should be documented and include realistic timelines required to address issues and include the entity responsible for addressing, removing, or correcting information and vulnerabilities identified.

- Once an assessment is completed, the results should be shared across teams.

Taking Action

- Implement communication plans to coordinate findings, investigation results, and determine information releases to and from different business units.
- Implement training and/or awareness of cybersecurity risks of publicly disseminated information.
- Incorporate OSINT assessments into regularly scheduled cybersecurity reviews, including red team activity.

THANK YOU