KRAVEN SECURITY

CYBER THREAT INTELLIGENCE

CTI Report Template

Company Name

Report Title

Report ID	
Date	
Priority	
Source and Information Reliability	
Sensitivty	

1. Executive Summary

A brief summary of the report. It should explain the report's significance, create a simple, easy-to-follow narrative of its key findings, and support a single decision. The reader should be able to make an informed decision based entirely on this summary.

Aim to answer the following questions concisely:

- *What intelligence requirement(s) has this report fulfilled?*
- *Why is this report relevant to the organization?*
- *What is the biggest takeaway?*
- *What new intelligence has been provided?*
- *Does this report support or contradict existing assumptions, security initiatives, or objectives?*

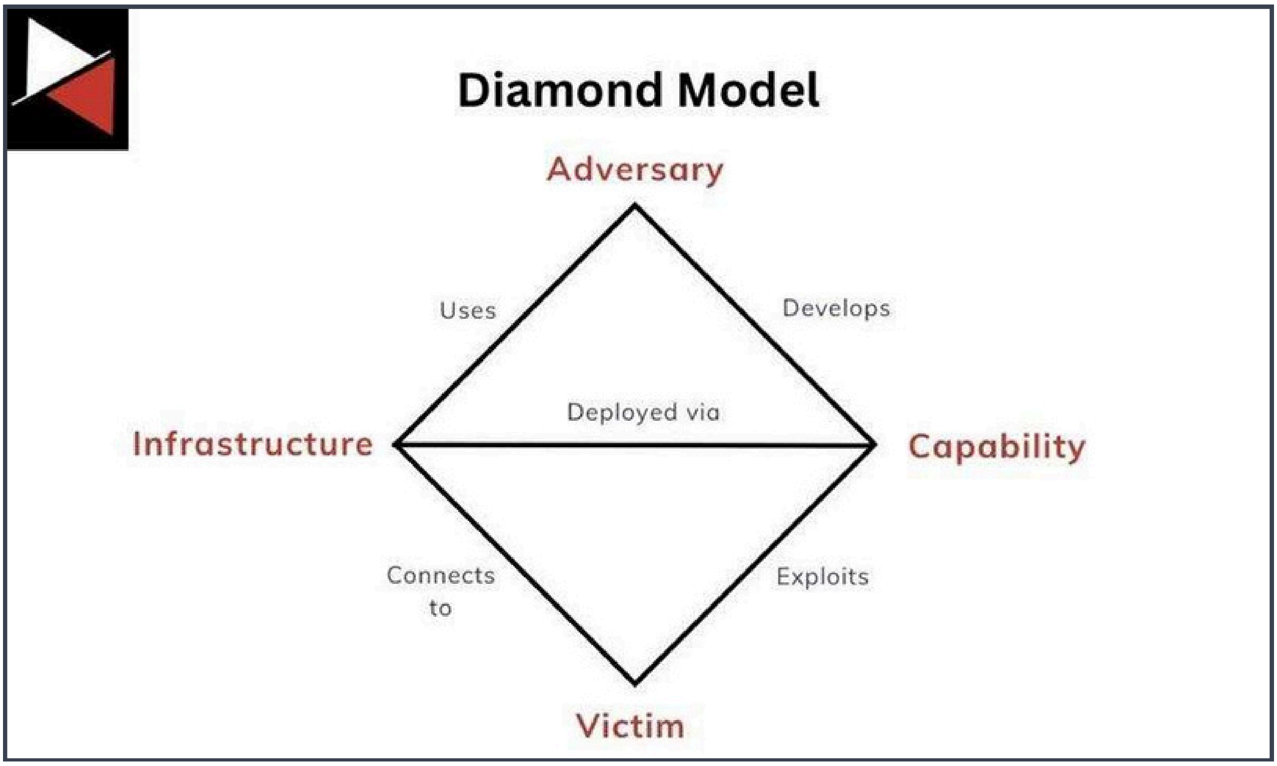
2. Key Takeaways

A bulleted list of the key findings from this report. Aim to answer the following questions:

- *Who is this report for?*
- *Where was the data collected (source)?*
- *Who was the attacker?*
- *Who was the victim?*
- *Why does this report matter to the target audience?*
- *What is the main takeaway from this report?*

This bulleted list is followed by a table summarizing key intelligence and a general analysis of the threat the report discusses using the Diamond Model. This allows key intelligence metrics to be easily identified and visualized.

Intelligence Requirements Addressed	
Data Sources	
Threat Actor	
Victim Location	
Sectors	
Actor Motivation	



Capabilities	Adversary	Infrastructure	Victim

3. Intelligence Assessment

This section should include:

- *A call to action, recommendation, or judgment: This threat (e.g., activity, threat actor, malware, etc.) demonstrates X and could potentially impact us. Therefore, we should do Y.*
- *Any new information: This threat has a new tool, capability, TTP, etc.*
- *Key evidence: The threat has the following characteristics that uniquely distinguish it.*
- *Estimative language (see Probability Matrix): "I assess with a <low/medium/high> level of certainty that < judgment> will impact us <impact>."*
- *Background information: Any relevant background information about the threat actor, malware, TTP, etc., to give context to this new assessment.*
- *Relations to your organization: How does this threat relate to your organization? Does it target your country or sector? Does it target vulnerabilities in the systems or technologies you use? Does it relate to any previous security incidents or detections?*

This section should include a kill chain analysis technique like Lockheed Martin's Cyber Kill Chain. List the IOCs or TTPs found at each stage of the attack to create an attack narrative for the reader. The security operations team can then use this to identify possible mitigations or gaps.

Cyber Kill Chain	
S1: Reconnaissance	
S2: Weaponization	
S3: Delivery	
S4: Exploitation	
S5: Installation	
S6: Command & Control (C2)	
S7: Actions on Objective	

4. Key Intelligence Gaps

A bulleted list that summarizes additional information the CTI team needs to complete their analysis and raise the confidence of the assessment. You should highlight gaps affecting the assessment, such as if new information is discovered or existing information is proven wrong.

These gaps should be tracked externally from the report using a project/task management system.

5. Indicators of Compromise (IOCs)

This section consists of IOCs found on endpoint devices (workstations, servers, mobile devices), in network logs, related malware, and any vulnerabilities relevant to the threat being discussed.

Endpoint Artifacts

A list of any unique artifacts associated with the threat that can be found on endpoint devices through intrusion analysis. This includes process names, filenames, DLLs, registry keys, scheduled tasks, command lines, services, etc. Use the MITRE ATT&CK tactic for the Tactic column.

Endpoint Artifact	**Type**	**Description**	**Tactic**

Network Artifacts

A list of any unique artifacts associated with the threat that can be found in network logs. This includes IP addresses, domain names, email addresses, URLs, etc. Use Recon, Delivery, C2, AoO – Exfiltration, etc. for the Kill Chain Stage column.

Network Artifact	**Type**	**Description**	**Kill Chain Stage**

Malware

A list of any malware or hacking tools associated with the threat. The Malware Analysis Report could be a link to an internal report or an external hyperlink. The Kill Chain Stage includes Recon, Delivery, Exploitation, Installation, C2, AoO – Exfiltration, AoO – Ransomware, etc.

Malware	Hash Type	File Hash	Description	Malware Analysis Report	Kill Chain Stage

Common Vulnerabilities and Exposures (CVEs)

A list of CVEs associated with the threat. Completing this section may require help from other teams (e.g., vulnerability management).

CVE #	CVSS Score	Patch Avaliable (Y or N)	Remediation	Description	Date Reported	Patch Applied (Y or N or N/A)

6. MITRE ATT&CK Techniques

This section lists the MITRE ATT&CK techniques relevant to the threat broken into tactics, techniques, and procedures (TTPs). It also contains the MITRE D3FEND countermeasure that can be used to defend against said technique and/or the security control used by the organization.

Tactic	Technique	Procedure	D3FEND	Security Control

7. Detection Opportunities

This section includes opportunities to detect using vendor-specific detection rules, threat hunting queries, Sigma rules, or YARA rules that correspond with the threat. Reference can be a link to an internal detection rule/query or an external hyperlink.

Rule / Query Name	Type	Description	Reference

8. Appendices

Probability Matrix

You should use estimative language to describe your confidence in intelligence assessments or related judgments. The following table describes the certainty the language you use in the report conveys to the reader to provide additional context.

Almost Impossible	Highly Unlikely	Unlikely	Possible	Likely	Highly Likely	Almost Certain
0 - 5%	5 - 25%	25 - 45%	45 - 55%	55 - 75%	75 - 85%	95 - 100%

Priority Matrix

You should assign each report a priority based on its impact on your organization. The following table describes four general priority levels you can assign to a report.

Low	The threat needs to be monitored closely and addressed.
Moderate	The threat needs to be monitored closely and addressed.
High	The threat needs to be addressed quickly and monitored.
Critical	Immediate action is required.

Source and Information Reliability

Each report should include an evaluation of source reliability. An industry standard is the Admiralty Scale, developed by NATO. This scale scores source reliability on a scale of A-F and information credibility on a scale of 1-6. Attaching an appendix that describes this to the reader provides clarity.

Source Reliability (A-F)	
A (Completely reliable)	The source has a history of consistently providing accurate information.
B (Usually reliable)	Most of the time, the source provides accurate information.
C (Fairly reliable)	The source has provided accurate information on occasion.
D (Not usually reliable)	The source has provided accurate information infrequently.
E (Unreliable)	The source has rarely or never provided accurate information.
F (Reliability cannot be judged)	The source's reliability is unknown or untested.

Information Credability (1-6)	
1 (Confirmed)	Other independent sources have confirmed the information.
2 (Probably true)	The information is likely true but has not been confirmed.
3 (Possibly true)	The information might be true, but it is unconfirmed.
4 (Doubtful)	The information is unlikely to be true.
5 (Improbable)	The information is very unlikely to be true.
6 (Cannot be judged)	The credibility of the information cannot be assessed.

Sensitivity Matrix

Each report should attach a sensitivity level as defined by your organization's data protection policy. This ensures data is handled appropriately and only shared with appropriate personnel. Attaching an appendix that describes this to the reader provides clarity.

TLP:CLEAR	TLP:GREEN	TLP:AMBER	TLP:AMBER+ STRICT	TLP:RED
There are no sharing restrictions. The information can be publicly shared.	Information can be shared within a community or sector to raise awareness of a threat.	Sensitive information that can be shared on a need-to-know basis within an organization or community	The information is restricted to the organization and should not be shared with its clients or trusted partners.	Highly sensitive information that should only be shared with a limited number of authorized people

Feedback Contacts

Provide a point of contact where the intelligence consumer can direct their feedback once the intelligence report has been published. This will help the CTI team improve future reports, ensure intelligence requirements are being met, and maintain communication channels.

Role	Name	Title	Phone	Email
Head of CTI				
CTI Manager				
CTI Lead				
CTI Analyst (author)				

Definitions and Acronyms

A list of key terms and acronyms used throughout the report. This lets the reader understand how the CTI team defines a particular technical term.

Key Term	**Definition**
Actions on Objections (AoO)	The final stage of a cyber attack is where a threat actor achieves their goals. This may include exfiltrating sensitive data, deploying ransomware, or performing espionage.
Admiralty Scale	A method used to evaluate the reliability of sources and the credibility of information in intelligence gathering. Reliability is scored from A to F, and credibility from 1 to 6.
Command and Control (C2)	The communication channel attackers aim to establish between compromised systems and their command infrastructure.
Common Vulnerabilities and Exposures (CVE)	A system and standardized naming convention used to identify and catalog publicly known cybersecurity vulnerabilities and exposures.
Cyber Kill Chain	A structured framework for understanding the different stages a cyber attack must complete to be successful.
Cyber Threat Intelligence (CTI)	The process of gathering, analyzing, and disseminating information about current or potential threats to an organization's digital infrastructure
Diamond Model	A simple framework for analyzing and understanding cyber threats. Defenders use it to organize and structure their intrusion analysis.
Estimative Language	Carefully chosen words that convey the confidence, certainty, or likelihood of an intelligence assessment’s conclusion or judgment.
Indicator of Compromise (IOC)	A piece of data or evidence that indicates a malicious activity has occurred within a network or on a computer system.
Intelligence Requirement (IR)	Specific information needs to guide the collection, analysis, and dissemination of cyber threat intelligence within an organization.

Malware	A term used to define any malicious software designed to harm, exploit, or otherwise compromise a computer system, network, or device (e.g., ransomware).
MITRE ATT&CK	A framework that provides a detailed and organized catalog of common tactics, techniques, and procedures (TTPs) threat actors use.
MITRE D3FEND	A framework that provides a detailed catalog of defensive security controls and mitigations against attack techniques.
Sigma Rules	A standardized format for writing and sharing detection rules for identifying suspicious or malicious activity within log data.
Tactic, Technique, Procedure (TTP)	A way to describe and categorize the behavior of adversaries to help organizations anticipate, detect, and respond to cyber threats.
Traffic Light Protocol (TLP)	A classification framework for securely sharing and handling sensitive information in the cyber security community.
YARA Rules	A standardized format for identifying and classifying malware, detecting threats, and analyzing files based on patterns and signatures.