Chapter 1: Intro to CTI

What is Intelligence? Humit, Geoint, Masint, Sigint, Osint (focus)	Intelligence lifecycle: Operational environment -> Data collected -> Data will be processed and exploited to obtain information -> Information will be analysed and utilised -> Intelligence	Analysis: 1. Requires analysts to immerse themselves into ambiguous situations. Data/Info may not be useful, so need to generate hypothesis to determine possible answers. Hypothesis is then tested against evidence. 2. Analytical judgements should have process searching for, sorting, structuring and evaluating data/info. Even if not enough time or data, decision should still be made.	Forensic process: systematic investigation used to uncover what happened during an incident (like a cyberattack) by examining the evidence. The goal is to gather facts that are defensible, repeatable, and understandable.
Defensibility: Your conclusions must be backed by evidence.	Repeatability: Another investigator should be able to follow your process and reach the same conclusion.	Understandability : Your findings must be clear and easy to explain to others, including non-technical people (like executives or law enforcement).	Everyone views issues in different ways. Perception should be active instead of passive one (dont passively accept data, actively interpret it)
Dont let your views cloud your analysis since critical situations are ambiguous situations.	WannaCry: Ransomware worm that exploit a vulnerability in windows os. Infected 300k machines. Adversary from north korea.	Adversary intent one of the hardest questions to crack in cyber security. Understanding actor intent helps structure defenses.	What is CTI? Gathering, processing, analysing information about potential & active cyber threats. Goal is to help organisations make better security decisions by staying ahead of criminals.
Info vs Intel: 1. Info: Raw, unfiltered feed, non actionable. 2. Intel: Processed, sorted information, actionable	Why use CTI? Prevent, mitigate, solve threats. Make correct decisions to: 1. Prevent significant losses 2. Keep ourselves safe. 3. Protect sovereignty of our society.	Assets: Anything valuable that needs protection	Vulnerability: Weakness that can be exploited.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Chapter 1: Intro to CTI (cont)

Threat: Something that can exploit a vulnerability to harm an asset.	Risk: Likelihood & impact of a threat exploiting a vulnerability.	Threat actors: 1. Nation states: big 4 (russia, china, north korea, iran) 2. Hacktivists: Individuals or group with political motivations. 3. Cyber criminals: Attackers seeking financial gain.	Zero day vulnerability: Vulnerability that hasnt been discussed or patched yet.
Advantage of Intelligence led security: 1. Mitigate risk, 2. Help make better decisions. 3. Prioritise resources, 4. Ensure value of operations. 5. Sync between intel and core business	Understand true risk -> Inform business and develop risk mitigation -> Build proactive and reactive strategies -> Demand right budgets + drive right investments.	Types of CTI: 1. Strategic, 2. Operational, 3. Tactical	Strategic intelligence: Focused on high level trends and adversarial motives, leverage this understanding to engage in strategic security and business decision making. Stakeholders: C suite, Executive board, Strategic intel. (who/why questions)
Tactical intelligence: Focused on performing malware analysis and take in behavioural threat indicators into defensive cybersecurity systems. Stakeholders: SOC analyst, SIEM, firewall, IDS. (What questions)	Operational intelligence: Focused on understanding adversarial capabilities, infrastructure, TTPs and leverage that understanding to conduct more targeted and prioritised cybersecurity operations. Stakeholders: 1. Threat hunter, 2. SOC analyst, 3. Incident response, 4. Vulnerability management. (How/Where questions)	TTP: Tactics: Describe what an adversary is trying to accomplish. Aka tactical objective. 2. Technique: Represents how the threat actor achieves tactical objective. 3. Procedures: Analysis of procedures used by adversary can help understand what the adversary is looking for within target infrastructure.	Models to convey cyber activity: 1. Mandiant Attack Lifecycle (to be covered in detail) 2. Mitre attack: Framework that maps out tactics & techniques used by attackers. 3. Diamond model of Intrusion, 4. Pyramid of Pain

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Chapter 1: Intro to CTI (cont)

Diamond Model of Intrusion Analysis: Framework used in cybersecurity to help analysts understand cyberattacks by identifying the key components of an intrusion and the relationships between them. 1. Adversary – The attacker (e.g., hacker group). 2. Victim – The target (e.g., company, person, or system). 3. Capability – The tools or methods the attacker used (e.g., malware, phishing). 4. Infrastructure – The resources used to carry out the attack (e.g., IP addresses, domains).

Pyramid of Pain: How hard it is to change attack indicators. Bottom is hash values since tiny changes in file can produce completely different hash output. Top is TTPs since attackers core methods are difficult to change quickly.

Estimate language to convey uncertainty: 1. High confidence level (100%): Certain (75%), highly likely, likely, 2. Medium confidence level (50%): Even/May, 3. Low Confidence level (25%): Unlikely, Highly unlikely, Impossible.

Chapter 2: CTI Ops

Cyber espionage: Means to gather sensitive or classified data, trade secrets or other forms of intellectual property that can be used by threat actor for an advantage.

Financial crime: Illegal activties whose primary goal is to make money.

Hacktivism: Individual or group who utilises hacking techniques to promote a political or social agenda.

Information operations: Coordinated actions taken to influence, disrupt or exploit an adversary decision making process.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Chapter 2: CTI Ops (cont)

Analyst Tradecraft: 1. Intelligence Analysis: Like detectives piecing together clues, CTI analysts use reasoning to figure out what happened and why. 2. Technology Expertise: Analysts need to understand hardware and software engineering, systems integration, networks and protocols, exploits and vulnerabilities to spot issues.

Challenge of attribution and response: When attempting to find out who is behind an attack, Incident responders typically assess both indicators of compromise (IoCs) and attack tactics, techniques and procedures (TTPs) that had been observed during an attack. IoCs are good place to start but an attacker infrastructure like IP address, domains can be easily spoofed or generated which will obfuscate their real identity.

2 types of thinking (System 1 - intuition, fast, permits quick judgement. How we perceived the world around us System 2 - analytical, slow, deliberate, slow thinking process. Activated when we do something that does not come naturally and requires some thinking through.)

Cognitive bias in CTI: Cognitive biases are mental shortcuts that sometimes lead us astray. Think of them as illusions for the brain.

5 most common analytical traps: 1. Failing to consider multiple hypotheses or explanations. 2. Ignoring inconsistencies. 3. Reject evidence that does not support the hypothesis. 4. Insufficient resources to capture key evidence. 5. Improperly projecting past experience.

Failure to consider visibility: Form of failing to consider multiple hypotheses or explanations. Different organisations have different views of threat landscape. Your environment, your country, your industry. Example: Suspicious email with unknown backdoor sent to CFO, must be targeted. But this activity is hitting customers of european based banks, must be a regionally focused cyber crime.

Mixing facts with assessments: Result in failure to cope with evidence of uncertain accuracy. Example: Team wombat domain news.myworldnews.com resolved to same IP address as mail.mediacorp.com. (fact) Possible misinterpretation as mail.mediacorp.com is attributable to team wombat (assessment).

Failing to properly vet sources: threat intelligence lives and dies on the quality of inputs, garbage in and garbage out. However, many organisations start their threat intelligence program by signing up for a series of open source threat feeds without a proper vetting process in place. Can result in a flood of alerts that are difficult to trust or differentiate.

Sponsored by Readable.com
Measure your website readability!
https://readable.com

Chapter 2: CTI Ops (cont)

Failure to account for human action: In the landscape of computer operations, we deal with data but it is easy to forget that there is a person behind the keyboard. Our minds naturally want to sort and categorise information, make sense of the environment but not always comfortable with grey areas.	Common Biases: 1. Confirmation Bias: Seeing what you expect to see, like ignoring evidence against your belief. 2. Ambiguity Effect: Avoiding decisions because of incomplete information. 3. Bandwagon Effect: Believing something just because everyone else does.	Impact on Cybersecurity: Bias can cause analysts to misjudge situations, like assuming an attack on multiple targets must be highly organized without verifying the evidence.	Bias is inherent and even awareness of biases not enough to neutralise them, what to do? Heuer says that when presented with an outcome, we ask ourselves the following questions: 1. If the opposite outcome had occurred, would I be surprised? 2. If this report had told me the opposite, would I believe it? 3. If the opposite outcome had occurred, would it have been predictable given the information that was available.
Structured Analytical Techniques: Frameworks to ensure logical and unbiased analysis. Pros: 1. Promote collaboration and clarity. 2. Show the reasoning process for conclusions, making them more transparent.	Intelligence lifecycle: 1. Planning and requirements, 2. Collection, 3. Analysis, 4. Production, 5. Dissemination and feedback	Planning and requirements: stakeholders defined, business needs and information concerns.	Collection: From information sources, raw internal and external data, open source, commercial and sensitive.
Analysis: Collation and aggregation via threat intel platform or analyst best practices.	Production: Estimative language, challenge analysis	Dissemination and feedback: Role based intelligence reporting, feedback loop firmly established.	Refer to case study for my details

Sponsored by Readable.com
Measure your website readability!
https://readable.com

Chapter 2: CTI Ops (cont)

Diamond Model : Connects the dots between attackers, victims, tools, and infrastructure. Four Elements: 1. Adversary: The attacker or group. 2. Infrastructure: Tools and assets like servers used in the attack. 3. Capability: The methods or techniques used (e.g., malware). 4. Victim: The target.

Considerations for the diamond model: 1. Timestamp: Date and time intrusion event occurred. 2. Result: Outcome of intrusion, succeed or failure or unknown. 3. Direction: How event moved through network or host (e.g victim to infrastructure, adversary to infrastructure, bidirectional) 4. Methodology: Category of event (portscan, spear phishing) 5. Resources: elements required for intrusion (e.g particular software, knowledge, funds, facilities, access rights) 6. Socio-political: Relationship between adversary and victim. 7. Technology: Tech involved in adversary capabilities and use of infrastructure.

Example: LAPSUS$ used social engineering to breach companies like Okta and Microsoft, demonstrating how attackers exploit human and technical weaknesses. Refer to case study for more details.

Cyber Kill Chain (7 stages): 1. Reconnaissance: Spying on the target to find weaknesses. 2. Weaponization: Creating tools like malicious emails or files. 3. Delivery: Sending the malicious tool to the target. 4. Exploitation: Activating the tool to break in. 5. Installation: Planting backdoors for ongoing access. 6. Command and Control (C2): Controlling infected machines remotely. 7. Actions on Objectives: Achieving the attacker's goal, like stealing data or causing disruption.

Cahpter 3: Analytical Skills

Cyber Assets Definition: These are resources that need protection from cyber threats. They include hardware (Physical devices like servers, computers, mobile phones, network equipment), Software (Programs and applications such as messaging apps, operating systems), Data (Information stored digitally, including databases, documents, usernames, passwords), People (Users who operate technology within a business), Physical infrastructure (Buildings, data centers, storage units)

Objectives of Analysts: To gather information that fills gaps in knowledge about threats or operational environments. Ask one question at a time, focus on specific facts/-events/activities to support decision--making.

TTP (Tactics, Techniques, and Procedures): 1. Tactics : High-level approaches attackers use to achieve their goals, 2. Techniques : More specific methods used to carry out tactics, 3. Procedures : Detailed steps taken by attackers.

Indicator = Data + Context. An indicator is forensic data (like unusual network traffic or changes in system files) that can point to malicious activity. E.gs: Unusual Outbound Network Traffic, Log-in Red flags, Mobile Device profile changes.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Cahpter 3: Analytical Skills (cont)

Indicator Lifespan: All intelligence has a useful lifespan; it should be retired when false positives arise. Adversaries determine how long an indicator remains useful.	Pyramid of Pain: Refer to notion case study	ACH: Refer to notion case study

By **csthrowaway**

cheatography.com/csthrowaway/

Not published yet.
Last updated 28th January, 2025.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com