# Unit 2 Study Guide : Cyber Threat Intelligence and Malware

## 1.1 Key concepts of cyber threat intelligence

- **Definition**: Cyber threat intelligence is information about threats that helps organisations understand and prepare for cyber attacks.
- **Types of intelligence**:
  - **Strategic**: High level trends and risks for decision makers.
  - **Operational**: Timely information about ongoing campaigns and capabilities.
  - **Tactical**: Details on attacker tools, techniques, and procedures that security teams can act on.
  - **Technical**: Indicators of compromise such as malicious IPs, file hashes, and URLs.
- **Purpose**: Improve detection, response, and risk decisions by turning data into useful, actionable knowledge.

## 1.2 Terms related to cyber security

- **Threat actor**: Person or group behind an attack.
- **Indicator of Compromise (IOC)**: Evidence that a system was breached, for example an IP or file hash.
- **TTPs**: Tools, techniques, and procedures used by attackers.
- **Vulnerability**: Weakness in software or process that attackers can exploit.
- **Exploit**: Method or code that takes advantage of a vulnerability.
- **Phishing**: Social engineering technique using deceptive messages to trick victims.
- **Zero day**: Vulnerability that is unknown to the vendor and unpatched.

## 1.3 The threat intelligence lifecycle

- **Direction**: Define what intelligence is needed and who will use it.
- **Collection**: Gather data from logs, sensors, open sources, commercial feeds, and partners.
- **Processing**: Normalise, filter, and structure raw data.
- **Analysis**: Turn processed data into meaningful findings and context.
- **Dissemination**: Share intelligence with the right people in the right format.

- **Feedback**: Receive user feedback to refine requirements and improve future intelligence.

## 1.4 How to find out about emerging attack techniques and how to recognise them

- **Sources**: Vendor advisories, CERTs, security blogs, academic papers, threat feeds, and industry sharing groups.
- **Signals**: New IOCs, unusual outbound traffic, odd processes, or new file types.
- **Methods**: Set up automated monitoring of security feeds, subscribe to trusted alerts, and use threat hunting to proactively search for anomalies.
- **Recognition**: Map behaviours to MITRE ATT&CK techniques to identify attacker goals and likely next steps.

## 1.5 What could be included in open source intelligence

- **Examples**: News articles, social media, public code repositories, WHOIS and DNS records, job adverts, leaked documents, forums, and academic research.
- **Value**: Can reveal attacker claims, planned campaigns, exposed data, or misconfigurations.
- **Note**: Open sources are powerful but require validation and context.

## 1.6 Why it is important to use only reliable and valid sources of Open Source Intelligence information

- **Risk of false data**: Inaccurate or malicious information can lead to wrong responses.
- **Reputation and legal risk**: Acting on bad intelligence can harm operations or break laws.
- **Best practice**: Cross check multiple sources, use trusted feeds and established organisations, and document provenance.

## 1.7 The importance of using reliable sources of information in relation to cyber security threats

- **Decision quality**: Reliable sources lead to better risk assessments and prioritisation.
- **Operational safety**: Prevent unnecessary disruption by avoiding false positives.
- **Compliance**: Accurate reporting and audit trails support legal and regulatory requirements.
- **Recommendation**: Maintain a vetted list of sources and update it regularly.

## 1.8 Current threat status and making possible recommendations based on cyber threat intelligence information

- **Assess status**: Determine whether threats are active, emerging, or dormant. Use severity and confidence levels.
- **Prioritise**: Focus on threats that affect critical assets and have high impact likelihood.
- **Recommendations examples**:
  - Patch specific vulnerabilities immediately.
  - Block malicious IPs and domains at the perimeter.
  - Increase monitoring for certain TTPs.
  - Isolate or harden exposed services.
- **Report**: Provide clear, actionable recommendations and estimated effort or impact.

## 1.9 Relevant cyber threat intelligence information requirements for an organisation

- **Identify stakeholders**: Which teams need the intelligence, such as SOC, incident response, executive team, or legal.
- **Define scope**: Types of threats to monitor, critical assets, regulatory concerns, and geographic considerations.
- **Format and cadence**: How intelligence is delivered, with what granularity, and how often.
- **Success criteria**: How to measure usefulness, for example reduced mean time to detect or patching speed.

## 2.1 Some different threat models

- **Adversary-focused**: Based on known attacker profiles and motivations.
- **Asset-focused**: Start from critical assets and model threats against them.
- **Use-case or scenario-based**: Simulate specific attacks or incidents.
- **Risk-based**: Combine likelihood and impact to prioritise threats.
- **Hybrid**: Mix of the above tailored to organisational needs.

## 2.2 The steps within a threat model

- **Define assets and scope**: What you are protecting and the boundaries.
- **Identify threats and actors**: Who might attack and why.

- **Identify vulnerabilities and controls**: What weaknesses exist and what mitigations are in place.

- **Assess likelihood and impact**: Rate how likely an attack is and what the consequences would be.

- **Prioritise and plan**: Decide on mitigations and monitoring based on risk.

## 2.3 Evaluate a threat model

- **Completeness**: Does the model cover key assets and likely attackers?

- **Accuracy**: Are threat probabilities and impacts realistic and evidence based?

- **Actionability**: Does the model lead to clear controls and measurable outcomes?

- **Maintainability**: Can the model be updated when threats or business assets change?

- **Testing**: Validate with tabletop exercises, red teaming, or threat simulations.

## 3.1 Types of malicious software

- **Virus**: Code that attaches to files and spreads when those files are shared.

- **Worm**: Self-replicating malware that spreads across networks without user action.

- **Trojan**: Malware disguised as legitimate software, used to gain access.

- **Ransomware**: Encrypts files and demands payment to restore access.

- **Spyware**: Collects data from the victim without their knowledge.

- **Backdoor / Remote Access Trojan (RAT)**: Gives attackers persistent remote control.

- **Botnet malware**: Compromised machines used for distributed attacks or spam.

- **Adware**: Displays unwanted adverts, sometimes with privacy implications.

## 3.2 The effects of different types of malicious software on an infected system

- **Data loss or corruption**: Ransomware or destructive malware can make data unavailable.

- **Performance degradation**: Worms and bots can consume CPU, memory, or bandwidth.

- **Unauthorized access**: Trojans and RATs allow attackers to steal information and credentials.

- **Privacy breach**: Spyware can exfiltrate personal or business data.

- **Reputational and financial damage**: Business disruption, recovery costs, and lost trust.

## 3.3 The motives for using specific malicious software attacks

- **Financial gain**: Ransomware, banking trojans, and fraud-focused malware.
- **Espionage**: RATs and spyware used to collect sensitive business or state secrets.
- **Political or ideological goals**: Hacktivist or nation state operations.
- **Vandalism**: Destructive malware intended to cause disruption.
- **Testing or proving skills**: Some attackers act to demonstrate capability.

## 3.4 Specific malicious software attacks can be made more effective due to human factors

- **Social engineering**: Phishing and impersonation increase success rates by tricking users.
- **Poor patching and weak passwords**: Make exploitation simple.
- **Insider risk**: Disgruntled or careless staff may enable attacks.
- **Lack of awareness**: Users who do not recognise suspicious behaviour are more likely to run malware.

## 4.1 The term social engineering

- **Definition**: Social engineering is the art of manipulating people to give up confidential information or perform actions that compromise security.
- **Common forms**: Phishing emails, vishing phone calls, pretexting, baiting, and tailgating.

## 4.2 How open source intelligence can be used in social engineering

- **Reconnaissance**: Public data can provide names, roles, company structure, and technical details.
- **Personalisation**: Attackers craft convincing messages using publicly available personal or corporate information.
- **Examples**: Using LinkedIn to find finance staff or company press releases to time an attack.

## 4.3 Ways a social engineering attack could take place

- **Email phishing**: Fake messages that ask for credentials or contain malicious attachments.
- **Spear phishing**: Highly targeted phishing using personal details.

- **Phone based attacks**: Attackers impersonate IT or vendors to get passwords.
- **In-person attacks**: Physical access gained by tailgating or impersonation.
- **Watering hole**: Compromise a site frequented by the target group to infect visitors.