CTI

Assignment - 1

Date 22/02/25 Page No.

Topic:

1) What is Cyber threat Intelligence (CTI) ~~refers to it~~ and how does it contribute to enhance Cyber Security.

→ CTI refers to the process of collecting, analyzing and sharing information about potential or existing cyber threats that could harm an organization's information systems, data, and operations.

→ This Intelligence typically includes information on tactics, techniques, and procedures (TTPs) used by Cybercriminals or adversaries, as well as malicious IP addresses, file hashes, or domains.

→ How CTI Enhances Cyber Security :-

(1) Proactive Threat Detection :-

→ By analyzing patterns of known Cyber threats, CTI helps organizations anticipate identify potential risks before they cause harm.

(2) Better Risk Management:-

→ CTI provides insights into the most relevant threats based on the organization's specific environment, helping prioritize security efforts and allocate resources more effectively.

(3) Enhanced Defense Mechanisms:-

→ The knowledge gained from CTI enables organizations to strengthen their security posture by implementing specific defense measures against identified attack techniques or known vulnerabilities.

2) What are the key frameworks used in Cyber threat intelligence in detail explanation

→ The frameworks help organizations to better understand and respond to cyber threats.

Date: _____ Page No.

Topic: _____

→ Key Frameworks :-

(1) MITRE ATT&CK :-

→ This Framework is one of the most widely used Frameworks for Understanding Cyber threat. It is comprehensive knowledge base of adversary tactics and techniques based on real world observations.

→ Components :- Tactics, techniques, Mitigation and Detection.

(2) Cyber Kill chain :-

→ This framework developed by Lockheed martin that outlines the stages of a Cyber attack, from initial reconnaissance to Exfiltration. It provides a step-by-step model for Understanding and preventing Cyberattacks by breaking them into phases that can be detected and Mitigated.

→ Stages of the Kill chain :-

MFG BY : GANESH ENTERPRISE, 99251 13335, 98795 28526

AGL®

(1) Reconnaissance
(2) Weaponization.
(3) Delivery.
(4) Exploitation
(5) Installation.
(6) Command and Control (C2)
(7) Actions on Objectives.

(3) Diamond Model of intrusion Analysis:-

→ This Framework for Understanding and analyzing cyber intrusions. It Emphasizes the relationships between four key components that define an intrusion: Adversary, Capability, Infrastructure, Victim.

→ Components:- Adversary, Capability, Infrastructure, Victim.

Date: _____ Page No.

Topic: _____

3) What are the main phases of intelligence Cycle in cti.

→

(1) Planning and Direction:-

→ Define the intelligence requirements and prioritize the areas of focus based on the organization's needs and the threat landscape.

(2) Collection:-

→ Gather raw data from various Sources that will help in identifying, understanding, and tracking potential Cyber threats.

(3) Processing:-

→ Convert the raw collected data into a structured, usable format for analysis.

4) Analysis:-

→ Analyze the processed data to derive

Asian Granito India Ltd AGL®

Topic:

derive actionable insights and understand the implications of the gathered intelligence.

(5) Dissemination:-

→ Share the analyzed intelligence with the appropriate stakeholders in a timely and clear manner.

4. Who are the common threat Actor in cyber security and what are their typical Modules?

→ Hactivists:-

→ Hactivists are individuals or groups that use hacking as a form of protest or to further a political or social agenda. Their goal is typically to draw attention to a cause or to disrupt the operations of entities they oppose.

Date: _____ Page No.

Topic: _____

→ Typical Modules :-

(1) DoS (Denial of Service) :-

→ Overloading Target Servers or websites with traffic to make them Unavailable.

(2) Website Defacement :-

→ Modifying the Content of Websites to send a political or Social Message.

(3) Data leaks :-

→ Exposing Sensitive information, like emails or documents, to the public as a form of protest.

(4) Social Media Manipulation :-

→ Using Social Media platforms to spread propaganda or destabilize public opinion.

Topic:

5) What are the primary sources of threat intelligence and what are methods are used to collect this data.

→ Primary Sources :-

(1) OSINT :-

→ OSINT refers to publicly available information that can be collected from open sources such as websites, blogs, forums, social media, and other publicly accessible platforms.

→ Methods

(1) Web Scrapping
(2) Social Media Monitoring.
(3) public Data Aggregators.

(2) Human Intelligence (HUMINT) :-

→ HUMINT involves gathering intelligence through interpersonal interactions.

Asian Granito India Ltd
AGL

Date: _____ Page No.

Topic: _____

→ Methods:-

(1) Interviews and informants.
(2) Conferences and Meetings.
(3) Undercover operations.

(3) Dark web and Deep web Intelligence:-

→ Intelligence from the deep and dark web, which includes forums, Marketplaces, and Networks that are not indexed by traditional Search engines and often requires Specific tools to access. (e.g., Tor, I2P).

→ Methods:-

(1) Dark web Monitoring.
(2) Web Crawling with Tor.
(3) Threat Actor profiling.

Asian Granito India Ltd.
AGL®
Tiles · Marble · Quartz · Bathware