
Snode
Geekulcha ITWeb Hackathon 2025
GEEKULCHA/>
iWeb SECURITY SUMMIT 2025

CTI (Cyber Threat Intelligence)

This is one of the most common uses in cybersecurity. CTI refers to the collection, analysis, and sharing of information about potential or existing cyber threats. It helps organizations anticipate and defend against cyberattacks.

Types of CTI:

- Strategic CTI – high-level info for decision-makers (e.g., threat actor motivations, geopolitical context).
- Tactical CTI – insights into tactics, techniques, and procedures (TTPs) used by attackers.
- Operational CTI – information about specific attacks, such as malware indicators.
- Technical CTI – raw data like IP addresses, URLs, file hashes.

DF (Digital Forensics)

Digital forensics is the process of identifying, preserving, analysing, and presenting digital evidence in a way that is legally admissible. It is a branch of forensic science that deals with investigating cybercrimes, data breaches, and other incidents involving digital systems.

Key Goals of Digital Forensics:

1. Identify what happened and how it happened.
2. Preserve evidence without altering or damaging it.
3. Analyse data to extract relevant information.
4. Present findings clearly, often in legal or organizational settings.

Network Traffic Analysis

Network Traffic Analysis (NTA) is the process of monitoring, capturing, and analysing data moving across a network. It's used to understand what's happening in the network — to spot performance issues, detect security threats, and ensure everything's running smoothly.

NTA helps answer questions like:

- Is someone trying to hack into the network?
- Why is the internet so slow?
- Is data being leaked from a device?
- Which devices are communicating, and with whom?

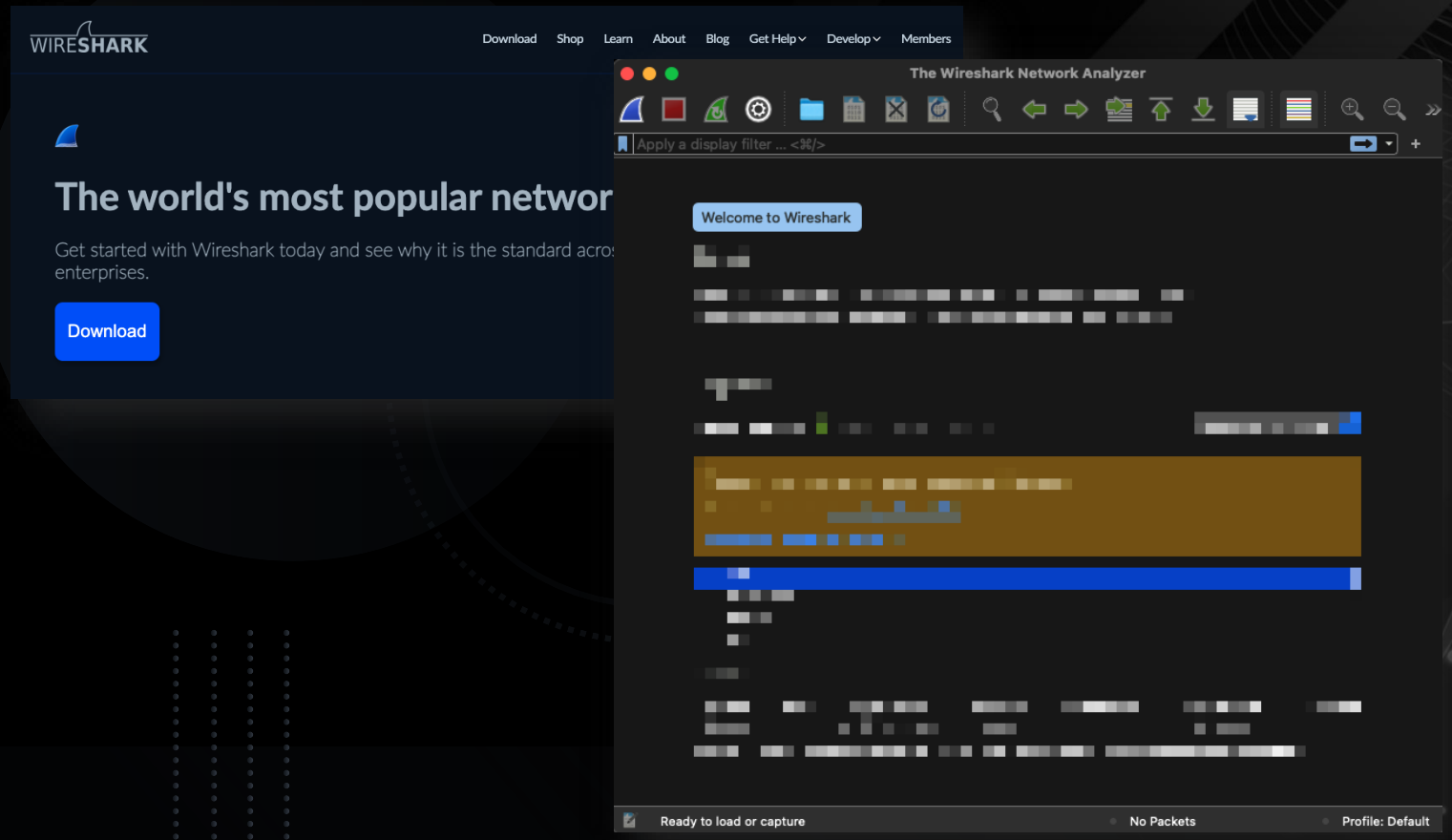
In Cybersecurity, It Helps You:

- Detect malware and intrusions.
- Spot suspicious behaviour (e.g., internal port scanning, data exfiltration).
- Investigate breaches.

Network Traffic Analysis = Visibility + Insight.
It's a foundational practice in both network management and cybersecurity defense.

Network Traffic Analysis Exercise

In this exercise you will be expected to analyse a PCAP (Packet Capture) file that was recorded from a host that is connected to the internet. You need to open the file in a network traffic analysis tool called Wireshark.



Network Traffic Analysis (Task 1)

The PCAP file will be provided, in the PCAP file there is 1 specific IP that is pointing to malicious activity.

Task:

1. Analyse the PCAP file using Wireshark.
2. Identify the malicious IP.
3. Provide intelligence on the IP address.
4. Analyse the IP address and link it back to any malicious activity, you will have to do a bit of research to get this type of intel.

VERY IMPORTANT: Please remember to take screenshots as evidence of your findings for your report!

Malicious File Analysis

Malicious file analysis is the process of examining files that are suspected of being harmful or malicious to understand their behavior, intent, and potential impact. This is a key component of cybersecurity and digital forensics, aimed at identifying, mitigating, and preventing threats such as viruses, worms, trojans, ransomware, spyware, and other types of malware.

Key Objectives of Malicious File Analysis:

1.Identify the type of malware.
2.Determine how it operates, including how it infects systems, spreads, and executes malicious actions.
3.Discover indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, and registry changes.
4.Assess the damage the file can or has caused.
5.Develop detection and mitigation strategies to prevent future infections.

Indicators of Compromise (IOC)

IOC stands for **Indicators of Compromise**. These are pieces of forensic data that can help detect and identify malicious activities on a network or system. They are essentially artifacts or traces left behind by cybercriminals during or after a cyberattack, which can be used to identify, track, and prevent further breaches.

IOCs can include various types of data, such as:

1.IP Addresses: Malicious or suspicious IPs that are known to be involved in cyberattacks.

2.Domain Names: Domains associated with phishing sites, command-and-control servers, or malware distribution.

3.File Hashes: Unique identifiers (e.g., MD5, SHA-1, SHA-256) of files that are known to be malicious.

4.URLs: Web addresses used to host malicious content or direct traffic to malware distribution sites.

5.Email Addresses: Associated with phishing or spam campaigns.

6.File Names: Specific filenames used by malware or attackers to identify malicious files or tools.

7.Registry Keys: In Windows environments, certain registry keys or modifications may indicate the presence of malicious software.

8.Network Traffic Patterns: Unusual or suspicious traffic patterns that might indicate malware communication with an external server (e.g., command-and-control communications).

9.Mutexes: Used by malware to ensure that only one instance of it is running at a time.

Malicious File Analysis (Task 2)

You will be given a virtual machine file that you will need to ingest into a hypervisor called Oracle Virtual Box. For this exercise you will be using the VM (Virtual Machine) to complete this task. You will be able to download Oracle Virtual Box from https://www.virtualbox.org/wiki/Downloads.

Objectives for Malicious File Analysis:

1. In the VM (Virtual-Machine) you will need to access https://analyze.intezer.com/ that will be a crucial tool to be able to complete this step. Please note that you will need to create an account on the Intezer website.
2. Identify the malware name.
3. Identify the key port and the main port connections are made on, and why this might be a risk.
4. Identify the registry activity that was created during the analysis, list all the registry activity observed.
5. Extract the IOC's.
6. After IOC extraction, list what type of IOC's was extracted. File base, Network based or Behavioural.

VERY IMPORTANT: Please remember to take screenshots as evidence of your findings for your report!

Mitre Att&ck Framework

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

The framework is widely used in the cybersecurity industry for threat intelligence, detection, and incident response. It is developed and maintained by MITRE, a nonprofit organization that works in partnership with government and private sector entities to improve security.

Key Elements of the MITRE ATT&CK Framework:

Tactics:

Tactics represent the high-level objectives or goals that adversaries aim to achieve during an attack. These are the "why" behind an adversary's actions.

Techniques:

Techniques describe the specific methods or procedures that adversaries use to achieve their objectives (tactics).

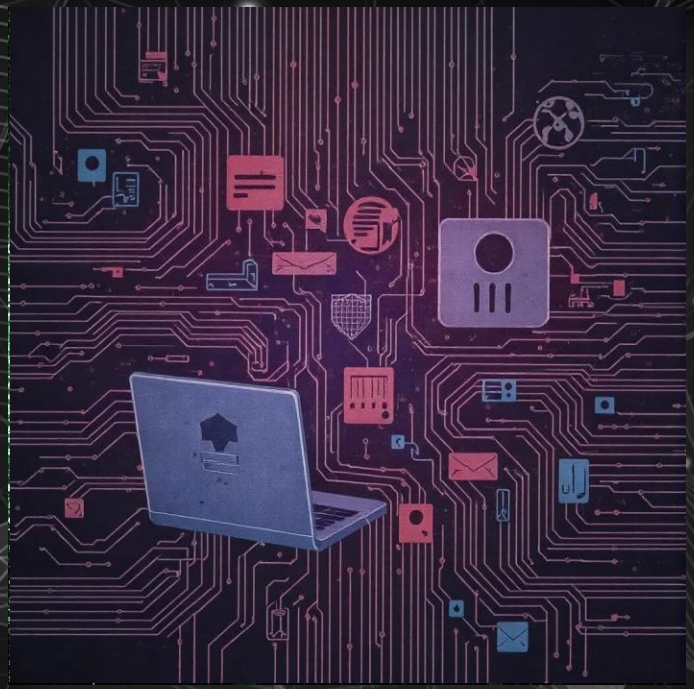
Procedures:

Procedures are the actual implementations of techniques and sub-techniques. These describe specific, real-world actions or tools that adversaries use. Procedures can vary widely between different threat actors but typically fall within the bounds of known techniques.

TTP (Tactics, Techniques, and Procedures)

Tactics, Techniques, and Procedures (TTPs) describe the behaviour and methods used by cyber attackers at each stage of an attack. Understanding TTPs helps security teams recognize and respond to threats even when specific tools or malware signatures change.

They are a key part of behavioural-based detection, as opposed to simply looking for known bad files or IPs (which can be easily changed by attackers).



Tactics:

Tactics represent the high-level objectives or goals that adversaries aim to achieve during an attack. These are the "why" behind an adversary's actions.

Techniques:

Techniques describe the specific methods or procedures that adversaries use to achieve their objectives (tactics).

Procedures:

Procedures are the actual implementations of techniques and sub-techniques. These describe specific, real-world actions or tools that adversaries use. Procedures can vary widely between different threat actors but typically fall within the bounds of known techniques.

Mitre Att&ck Mapping (Task 3)

In this task you will be taking the **MITRE ATT&CK®** framework and map it back to a certain threat actor group. It's important to understand TTPs to defend against threats, when mapping out the TTPs please map it out in a table that lists ID, Name, Use. This is mapping it correctly to the **MITRE ATT&CK®** framework.

Objectives for Mitre Att&ck Mapping:

1. Map all the TTPs for the threat actor, and what lead you to the conclusion that you think it's the identified threat actor. (Remember to map it into a table format).
2. Identify the threat actor and list the name/names.
3. List industries the threat actor targets.
4. List the motive/motives behind the threat actor.
5. Do a threat research write up on the threat actor.

VERY IMPORTANT: Please remember to take screenshots as evidence of your findings for your report!

Solutions #ChangeTheWorld #DefendTheFuture

In today’s hyperconnected world, every click, connection, and cloud sync introduces a new opportunity and a new risk. As organisations embrace digital transformation, cyber threats are evolving faster than ever, morphing into sophisticated, targeted campaigns designed to breach, disrupt, and exploit.

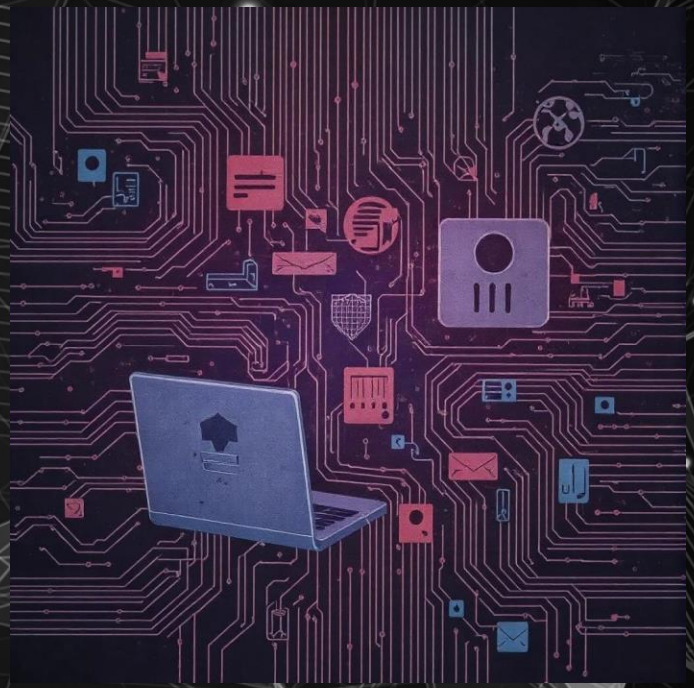
From ransomware that can paralyze an entire enterprise to stealthy nation-state actors lurking in networks for months, the threat landscape no longer plays by the old rules and neither can our defenses.

Enter the need for a comprehensive security solution one that doesn’t just react, but anticipates. A solution that’s not only built to detect known threats but smart enough to adapt to the unknown. One that turns fragmented defenses into a unified shield.

In a world where cyber threats evolve by the hour, innovation isn't optional it's essential. From zero-day exploits to social engineering attacks, organisations and individuals alike face a digital battleground where only the most adaptive survive.

That's why we’re here not just to code, but to create, collaborate, and conquer some of the toughest challenges in cybersecurity.

At this hackathon, we’re not just building another app we’re building defenses for tomorrow. Whether it’s detecting threats in real time, defending against phishing attacks, visualizing vulnerabilities, or rethinking digital identity every keystroke is a strike back against cybercrime.



iWeb SECURITY SUMMIT 2025

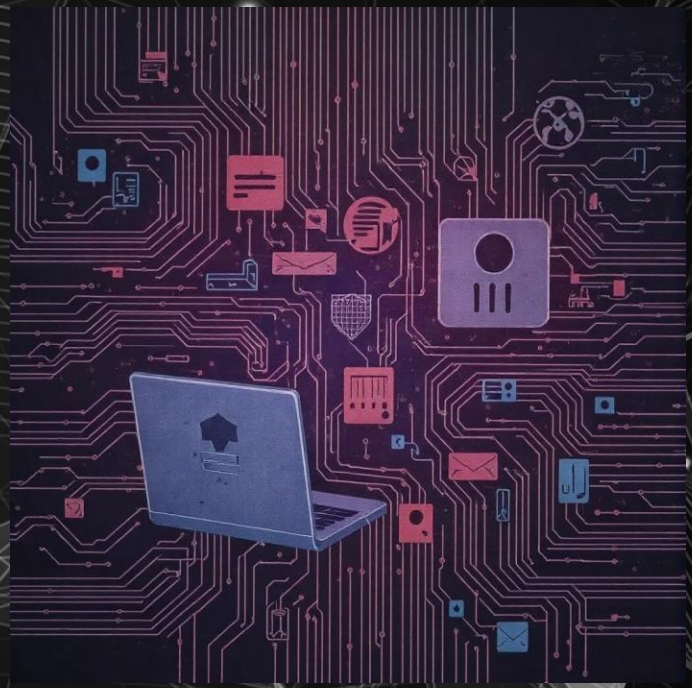
GEEKULCHA/>

Build a Solution (Task 4)

In this last Task you will be expected to build a solution that can be used to protect against the identified threats you have identified from the previous Tasks:

1. You are required to build a SIEM (Security, Incident and Event Management) solution that can monitor for anomalies and the ability to ingest IOCs for detections. You will be able to use Wazuh SIEM https://wazuh.com/.
2. You are required to build Yara rules that will be able to detect the malware from the previous tasks that will be used in your SIEM solution.
3. Provide a marketing proposal to market your solution.

VERY IMPORTANT: Please remember to take screenshots as evidence of your findings for your report!




Snode