Snode

Geekulcha Ideathon 2025

GEEKULCHA/>

iWeb SECURITY SUMMIT 2025

Welcome Introduction – ***Jason van Niekerk***

Jason van Niekerk is a skilled cybersecurity professional with over 10 years of experience in the ICT and Cyber Security sector. Specializing in Cyber Threat Intelligence (CTI), Jason has developed deep expertise in identifying, analysing, and mitigating cyber threats across complex digital environments. With a strong foundation in digital forensics and network security, he excels in investigating cyber incidents, conducting malware analysis, and reverse engineering to uncover hidden threats.

Jason also has a keen understanding of the dark web and its role in modern cyber threats, allowing him to proactively monitor and defend against illicit activities in this often-overlooked space.

- CTI (Cyber Threat Intelligence)
- Digital Forensics
- Network Security
- Malware Analysis and Reverse Engineering
- Cyber crime investigation
- Threat profiling & Tracking
- Dark Web

iWeb SECURITY SUMMIT 2025 GEEKULCHA/>

Discussion Points Covered In This Session:

- Ideathon & Hackathon
- Snode Technologies
- CTI (Cyber Threat Intelligence)
- Network Traffic Analysis
- Network Traffic Analysis Exercise
- IOC (Indicators of Compromise)
- IOC Analysis Exercise
- TTP (Tactics, Techniques & Procedures)
- TTP Correlation and Mapping Exercise

Ideathon & Hackathon

iWeb SECURITY SUMMIT 2025

GEEKULCHA/>

COUNTDOWN TO THE IDEATHON

12 April 2025, UNISA Muckleneuk Campus

gklink.co/ss25hack

economic development & tourism
Department: Economic Development & Tourism
NORTHERN CAPE PROVINCE
REPUBLIC OF SOUTH AFRICA
Snode
UNISA university of south africa
SOL PLAATJE UNIVERSITY
telspace AFRICA HACKERS FOR HIRE
CompTIA
IITPSA Institute of Information Technology Professionals South Africa
ISACA South Africa Chapter

HACKATHON

#SS25HACK

3 & 4 June 2025 Sandton Convention Centre

Snode GEEKULCHA/> iWeb SECURITY SUMMIT 2025

Snode Technologies

Snode Technologies is a locally founded cyber defence firm that protects local to global. Our technology is locally engineered and built. Snode secures around 5 million devices across six continents, working with everyone from intelligence agencies to large-scale uranium facilities. And the cyber security firm is also shattering misconceptions that a South African company couldn't possibly build technologies that compete with the rest of the world.

Snode

MDR MANAGED DETECTION & RESPONSE

CVA CONTINUOUS VULNERABILITY ASSESSMENT

CTI CYBER THREAT INTELLIGENCE

CAS CYBER ATTACK SIMULATION

BUILD LOCALLY DEFEND GLOBALLY

Global Defence Achievements:

- SA Innovation Summit 2020 Winner.
- One of only two vendors to be endorsed by our national state security.
- The first African company to be listed in the Top 100 deep-tech innovations.
- ML-based patent for M2M cyber threat detection within encrypted data stream.
- Securing key Namibian National Infrastructures
- Defending the largest Agri-Tech IoT plantation in the world.
- Defending the worlds first blockchain stock exchange.
- Defending the second largest online trading platform in the world.
- Defending one of the largest global mining environments in world.

APPSAFRICA Innovation Award 2017 FINALIST

STARTUP World Cup 2019 FINALIST

MEST Africa Challenge 2019 WINNER

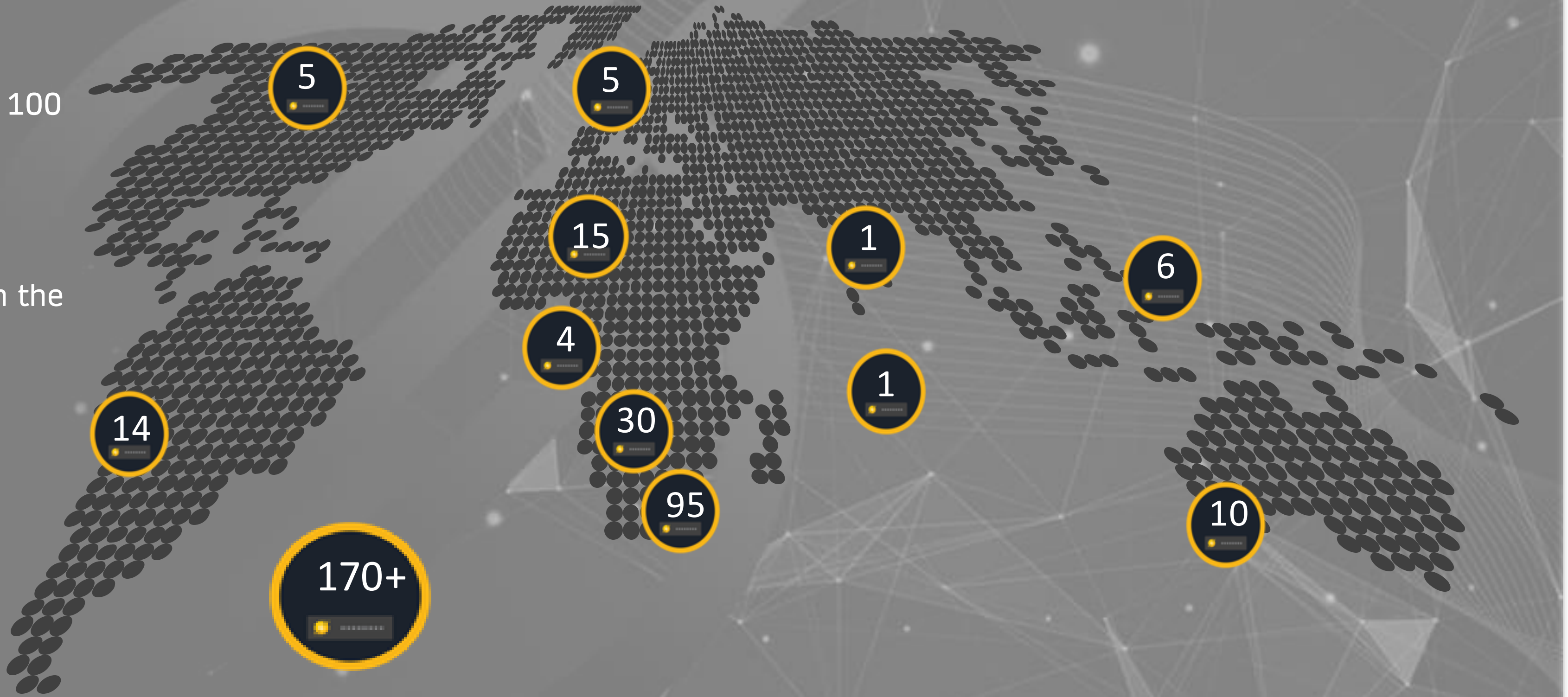
SLINGSHOT 2020 Global TOP 100

SA Innovation Summit 2020 WINNER

AfricArena 2021 Emerging Entrepreneur of the Year

DTIC 2024 – Black Industrialist Award (Innovation)

Defending **5 million** devices across **6 continents**



Total Client Points of Presence

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.

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:

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?

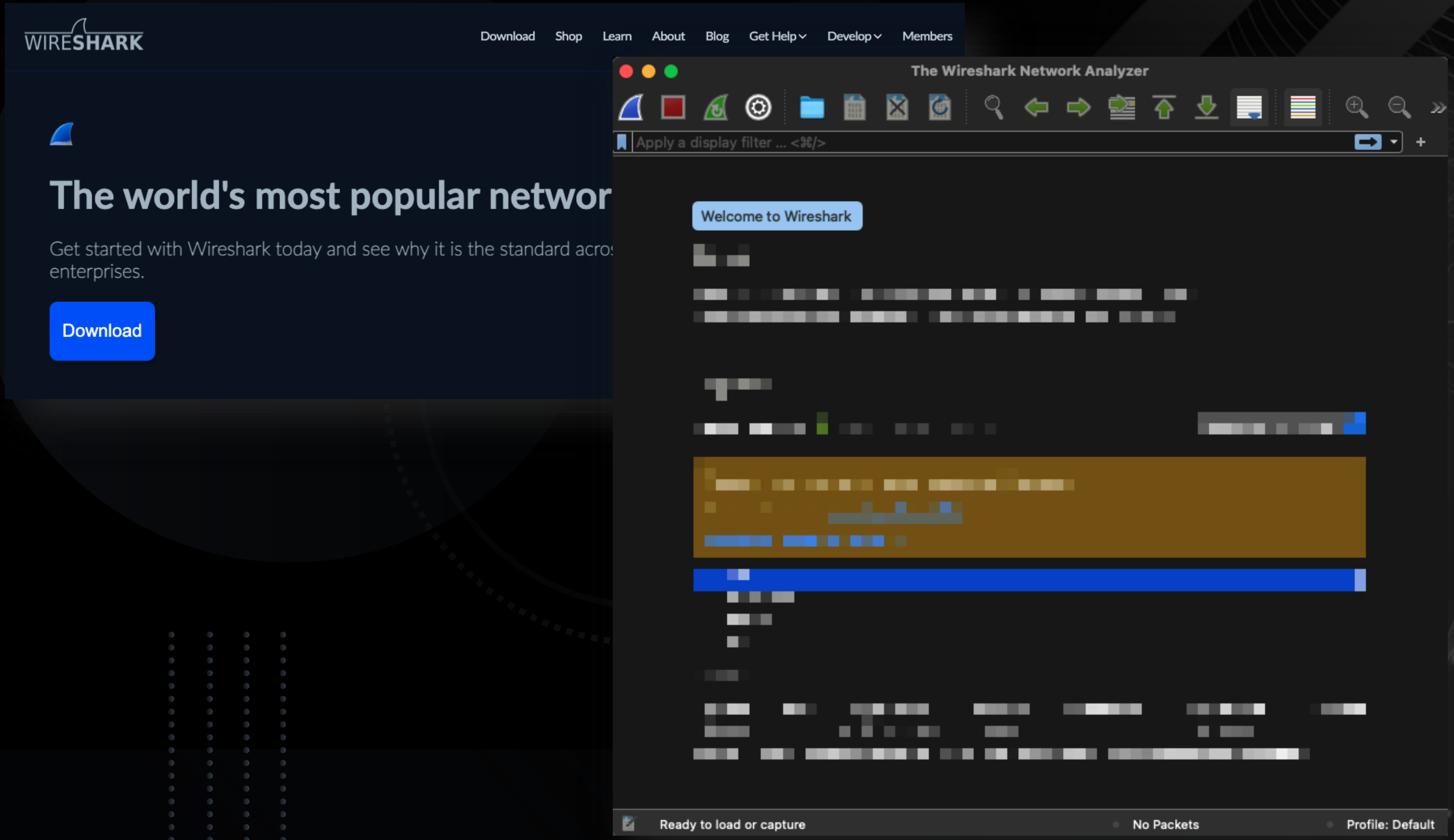
In Cybersecurity, It Helps You:

- Detect malware and intrusions.
- Spot suspicious behavior (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 analyse tool called Wireshark.



The world's most popular networ

Get started with Wireshark today and see why it is the standard acros enterprises.

Network Traffic Analysis Exercise

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 can check this by using Virustotal. https://www.virustotal.com/gui/home/upload

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

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.

IOC Correlation & Analysis

In this next exercise you will be expected to analyse a specific IOC (Indicator of Compromise) that will be provided to you and link it back to a specific type of threat.

Task:

1. The IOC that we will provide to you is 453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb. You can check this by using Virustotal. https://www.virustotal.com/gui/home/upload
2. Identify what type of malware this might possibly be connected to.
3. What type of hash is this?
4. List the risk/risks that might be associated with it.
5. Do a writeup on the malware and include in your report.
6. List at least 5 things you can do to protect yourself and an organization from this type of threat. And also include how you can use an IOC to enhance security, please also list at least 5 things.

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:

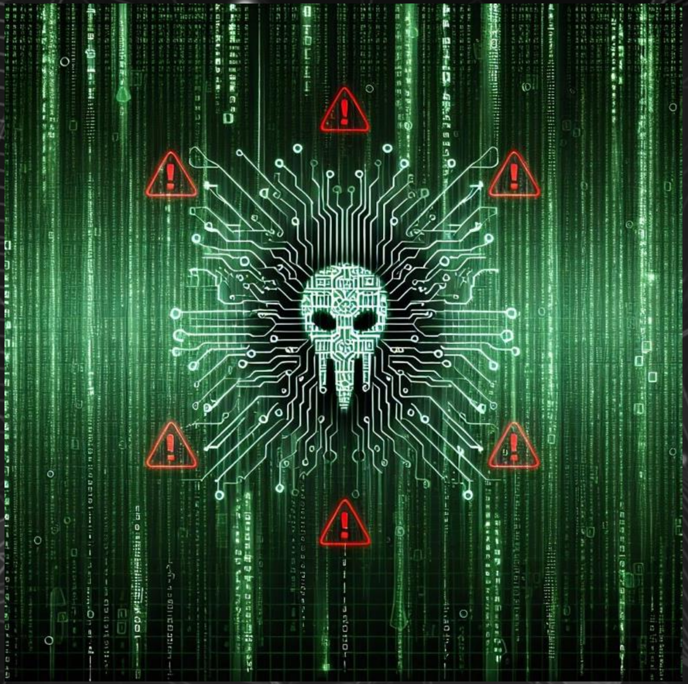
Tactics represent the high-level objectives or goals that adversaries aim to achieve during an attack. These are the "why" behind an adversary's actions.

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.



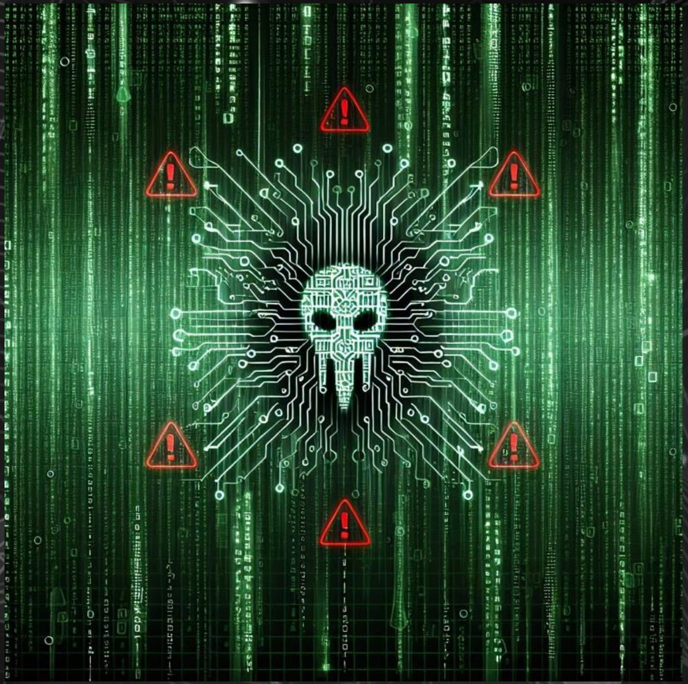
TTP (Tactics, Techniques, and Procedures) Exercise

In this third and final exercise you will be expected to map back certain TTPs of a threat actor to the Mitre Att&ck framework. Hint in this exercise is "Play". It's very important to specify via a table ID, Name, Use.

Task:

1. What would the techniques be for **initial access**?
2. What would the techniques be for **discovery**?
3. What would the techniques be for **defence evasion**?
4. What would the techniques be for **Credential access**?
5. What would the techniques be for **Lateral movement**?
6. What would the techniques be for **Command and Control**?
7. What would the techniques be for **Collection**?
8. What would the techniques be for **Exfiltration**?
9. What would the techniques be for **Impact**?

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



Snode