Mastering Cyber Defense:

Hands-On Training with Montimage Cyber Range

Session 1

Wissam Mallouli
Montimage, France

Montimage

Key information of the company :

Type: SME

Creation date : 2004

Location: Paris, France

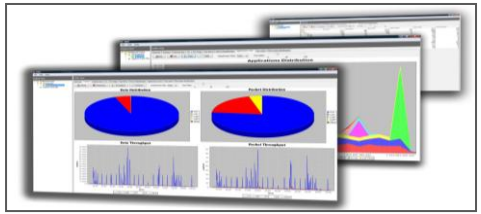
Employees : 15

Expertise

- Cybersecurity – Risk management
- Network Monitoring and analysis
  - Classification of network traffic, Statistics, QoS/QoE
  - Incidents/Anomaly detection: behaviour, security and performance
- Research and innovation in different fields related to cybersecurity in future networks, 5G and beyond, IoT, CPS, cloud computing etc.
- Flagship tool: MMT for Montimage Monitoring Tool

Activity :

Analysis of network traffic – supervision, detection, decision making, reactions



Montimage

AI4CYBER

PRECINCT

DYNABIC

DETERMINISTIC6G

Agenda

- Part 1: Introduction to Cyber Ranges
  1. Understanding Cyber Ranges
  2. Motivation and Need for Cyber Ranges
  3. State-of-the-Art Cyber Range Solutions
- Part 2: ADR Cyber Range
  1. Introduction to ADR CR
  2. Attack and Defense
  3. Monitoring and Detection with Montimage Monitoring Tool (MMT)
  4. Response and Mitigation Strategies
  5. Hands-On the ADR CR - Practical exercises
- Part 3: Anti-Phishing Cyber Range
  1. Introduction to Phishing attacks and Anti-Phishing CR
  2. Recognizing Phishing Indicators
  3. Classification and Response to Phishing Attacks
  4. Hands-On the Anti-Phishing Cyber Range – Pratical exercices
- Part 4: Closing and Wrap-Up
  1. Summary of key takeaways
  2. Open discussion for any remaining questions
  3. Feedback collection from participants

Introduction to Cyber Ranges

What is a cyber-range ?

- **European Defence Agency** in their Common Staff Target for Military Cooperation on Cyber Ranges in the European Union : https://www.eda.europa.eu/docs/default-source/procurement/annex-a---cyber-ranges-cst.pdf
- **NIST**: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf
- **Wikipedia :** Cyber ranges are virtual environments used for cyberwarfare training and cybertechnology development.
- **Technopedia:** A cyber range is a virtual environment that is used for cyberwarfare training and cybertechnology development. It provides tools that help strengthen the stability, security and performance of cyberinfrastructures and IT systems used by government and military agencies…

What is a cyber-range ?

- **European Defence Agency** in their Common Staff Target for Military

Cyber ranges are closed virtual environments used for training about Cybersecurity. It can emulate real environments and provide tools that help strengthen the stability, security and performance of cyber infrastructures and IT systems (used by government, military and companies etc.)

- **Technopedia:** A cyber range is a virtual environment that is used for cyberwarfare training and cybertechnology development. It provides tools that help strengthen the stability, security and performance of cyberinfrastructures and IT systems used by government and military agencies…

Importance of Cyber Ranges

Cyber ranges play a crucial role in developing **cyber resilience**. They allow organizations to simulate real-world attacks, assess their **defense mechanisms**, and identify weaknesses. This proactive approach helps in preparing teams for actual cyber incidents.

Types of Cyber ranges

There are various types of cyber ranges, including **private**, **public**, and **hybrid** ranges. Each type serves different purposes, from corporate training to academic research, enabling diverse stakeholders to enhance their **cybersecurity capabilities**.

Specificities of Cyber ranges

- Cyber ranges are equipped with essential features such as **realistic scenarios**, **customizable environments**, and **comprehensive analytics**.
- These features facilitate **effective training**, allowing participants to learn from their mistakes and improve their **incident response skills**.
- Organizations utilize cyber ranges for various purposes, such as employee training, incident response drills, and **research and development**.
- These use cases demonstrate the **versatility of cyber ranges** in addressing different aspects of cybersecurity.

Challenges in Cyber Range Implementation

Despite their benefits, implementing a cyber range can pose challenges such as **cost**, **technical complexity**, and the need for continuous updates. Organizations must navigate these hurdles to effectively leverage cyber ranges for **training and development**.

Cyber Range Solution	Open Source	Features	Limitations	Target Audience	Pricing Model
Cyberbit	No	- Comprehensive training modules - Realistic attack scenarios - Team-based exercises - Continuous monitoring	- High cost - Requires significant setup - Focuses on enterprise level	Large enterprises, government agencies	Subscription-based
RangeForce	No	- Gamified training - Scalable platform - Hands-on, interactive scenarios - Team collaboration features	- Limited advanced scenarios - Focus on beginner to intermediate levels	Corporations, cybersecurity teams	Subscription-based
Circadence Project Ares	No	- AI-powered simulations - Gamified learning environment - Real-time feedback - Emphasis on team collaboration	- Requires continuous internet connection - Learning curve for new users	Medium to large enterprises	Subscription-based
CybExer Technologies	No	- Cloud-based - Focus on critical infrastructure - Realistic environments - Customizable scenarios	- Limited to specific sectors - Higher cost for advanced scenarios	Government, critical infrastructure	Subscription-based
OpenStack Cyber Range	Yes	- Open-source - Flexible and customizable - Supports multiple hypervisors - Integration with other tools	- Requires technical expertise to set up - Limited pre-built scenarios	Educational institutions, small to medium enterprises	Free, with paid support
PICO CTF	Yes	- Open-source - Focus on Capture the Flag (CTF) challenges - Suitable for beginners - Community-driven	- Limited scope - Not suitable for advanced training - Less enterprise-focused	Educational institutions, hobbyists	Free
SANS NetWars	No	- Comprehensive training - Focus on gamified CTF challenges - Real-time scoring - Multiple difficulty levels	- Expensive - Limited to SANS curriculum participants	Security professionals, corporations	Subscription-based
NICE Challenge Project	Yes	- Open-source - Scenarios aligned with NICE Cybersecurity Workforce Framework - Focus on workforce development	- Limited to educational scenarios - Requires technical setup	Educational institutions, government	Free
Immersive Labs	No	- Continuous learning paths - Interactive, real-world scenarios - Focus on human factors in cybersecurity	- Limited in advanced attack simulations - Subscription can be costly	Corporations, cyber teams	Subscription-based
MetaCTF	Yes	- Open-source - Focus on CTF challenges - Suitable for large events - Web-based platform	- Limited scenario variety - Requires setup and hosting	Educational institutions, CTF events	Free, with paid support
Testbeds (Cyber Range)	Yes	- Open-source - Configurable for specific use cases - Integrated with real-world devices - Modular approach	- Requires technical expertise - Customization can be complex	Research institutions, advanced users	Free, with optional costs

Future of Cyber Ranges

- The future of cyber ranges looks promising with advancements in **AI and machine learning**.
- These technologies will enhance simulations, making them more **realistic and effective** in preparing teams for emerging cyber threats in a rapidly evolving landscape.

ADR Cyber Range

Montimage Cyber-Range Target public

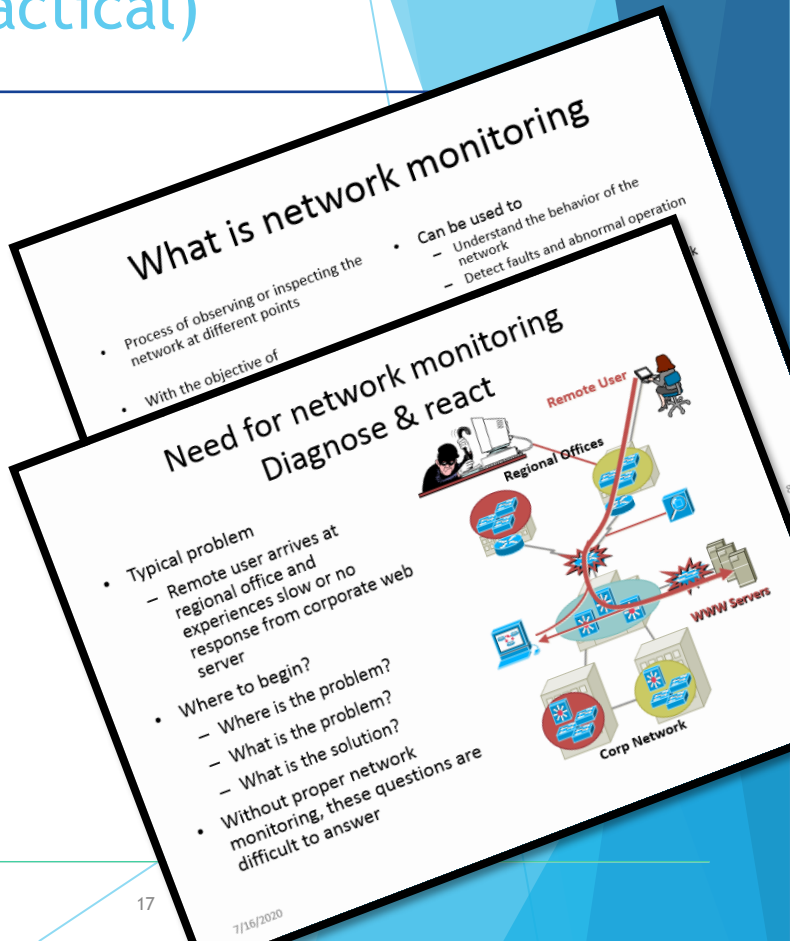
- Any employee of a company concerned by the development of good practices in terms of cyber security including
  - ~~Category 1: Non-ICT experts~~
  - Category 2: ICT experts
  - Category 3: Security experts

Montimage Cyber-Range - Functionnalities

- Traffic generation
- Attacks detection and reporting
- Reaction to attacks

Training program (Theoretical + Practical)

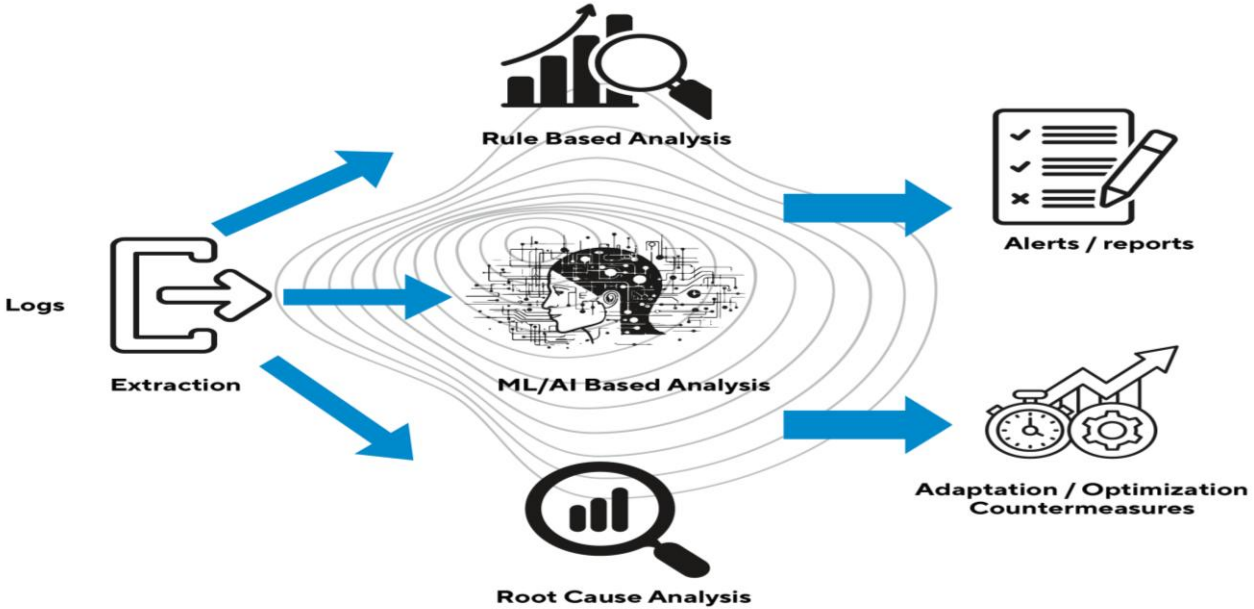
- Theoretical training
  - Slides-based training
    - Understand the terminologies used in Cyber-Security (vulnerability, risk, attack, countermeasure etc.)
    - Understand the need of network monitoring
    - Concepts related to Deep Packet Inspection
    - Concepts related to IDS and IPS
    - Different detection techniques
    - Different algorithms and tools
    - Examples



MMT Tool Description

- MMT stands for Montimage Monitoring Tool
  - It is a software tool that allows to analyze application, system and/or network traces offline or at runtime
  - It provides statistics at different levels and detects functional/performance/security incidents
  - It relies on rule-based and ML/AI-based analysis engines to detect attacks and anomalies
  - It allows to determine the root cause of incidents and propose recommendations
  - MMT has an open source version available https://github.com/Montimage/mmt-probe/
  - It can also proposed as containerized solution

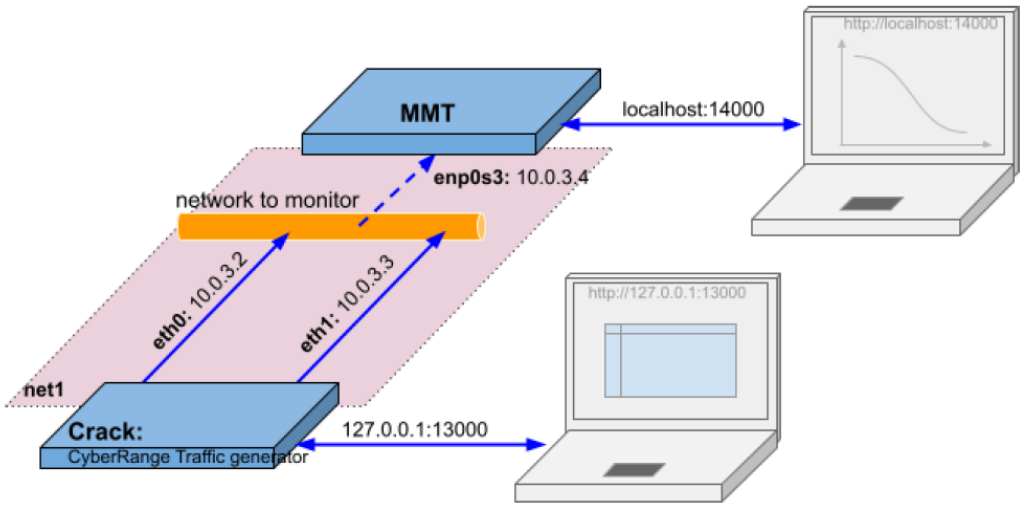
MMT Tool architecture and subcomponents



Training program (Theoretical + Practical)

- Practical training
  - Using Montimage Cyber-Range Platform
  - 4/12 exercises
    - Generate legitimate traffic
    - Generate different kinds of attacks
    - Report network characteristics using MMT
    - Detect attacks using MMT
    - ~~Trigger countermeasures~~
    - ~~Generate a new attack~~
    - ~~Extend MMT-IDS with a new protocol~~
    - ~~Extend MMT-IDS with a new rule~~
    - ~~Extend MMT-IDS with a new reaction~~
    - ~~Use the platform in an IoT context~~
    - ~~Use the platform in a 4G/5G context~~
    - ~~Use the platform for high-bandwidth networks~~

Montimage Cyber-Range - Architecture



- 2 or 3 virtual machines
  - Traffic generator (legitimate or malicious)
  - Network probe : MMT-IDS

  and MMT-Operator

- Deployed on a classical desktop PC (trainee device) or in the cloud (ongoing)

ORACLE VM VirtualBox

links

- https://github.com/Montimage/mmt-operator/tree/main/www/data/attack
- https://github.com/Montimage/mmt-probe

Video

Discovering the Cyber-range

- Traffic generator : Possibility to generate network traffic
  - Legitimate / malicious
  - Based on python scripts or by replaying pcap files
  - Read some python scripts (try to understand)
  - Read some pcap files using Wireshark (in the host machine)
- Probe:
  - Capture the trafic and analyse it
  - See the configuration file and understand it
  - See the rules (XML rules)
- Operator
  - Understand the operator dashboard

List of threats

- Ransomware
- Identity theft
- DoS/DDoS
- Web attack
- Phishing mail attack
- Scanning
- Evasion (optional)

Steps:
1- Understand the threat
2- Undertand the specific attack
3- Launch it on the cyber-range
4- See the detection result (on the dashboard)
5- See the reaction (if any)
6- Understand why
7- Write a small report

Threat : Ransomware – Attack: WannaCry

- WannaCry ?
  - https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
  - https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

- When, What was the impact ?
- How is it working ?
- How to protect against it ?

What contains the pcap file ?
How the probe is able to detect the ransomware ?

- Fact : WannaCry tries to connect to non-existent URLs. If the URL exists, the ransomware propagation stops..

Threat : Identity theft – Attack : SSH brute force attack

- What is a brute force attack ?
- What is an ssh brute force attack ?

- When, What was the impact of such an attack ?
- How is it working ?
- How to protect against it ?

What contains the pcap file ?
How the probe is able to detect the ssh brute force attack ?

Threat DDoS – Attack: Small IP fragments

- What is a distributed deny of service attack ?
  - https://en.wikipedia.org/wiki/Denial-of-service_attack

- How to detect this attack ?
- How to differenciate legitimate requests from malicious ones ?

- What is the impact ?
- What are the possible mitigations ?

What contains the pcap file ?
How the probe is able to detect the ssh brute force attack ?

Web attack – Phishing email – Attack : malicious URI

- What is a malicious URI ?
- How to list these URI ?
  - From experience
  - Honeypots and darknets
  - CTI
- Where we can find these URIs ?
  - In phishing emails
  - In social media
  - In malicious websites
- What is the impact ?

What contains the pcap file ?
How the probe is able to detect the ssh brute force attack ?

Threat: Scan – Attack Scanning using Nikto

- Techniques ?
  - Net scan (Nikto, Nmap ...)
  - Web scan (ZAP)
  - Pentesting
- What is the purposes ?
  - Gathering sensitive information
  - Discover the weakness

What contains the pcap file ?
How the probe is able to detect the network scans ?

Threat: Evasion (optional)

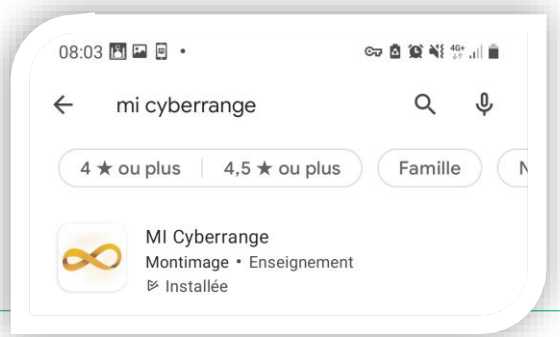
- What is the purposes ?
  - Confusing the IDS/IPS:
    - Invalid IP version
    - Invalid GRE version
  - Hide information
    - (e.g., communication between bots)
  - Evasion:
    - The IDS and the endpoint (e.g, browsers) treat the non-standard things differently.

What contains the pcap file ?
How the probe is able to detect the non-standard activities ?

Anti-Phishing Cyber Range

Phishing threat cyberrange

- Is a mobile application available in a beta version on play store and apple store
  - Under testing
  - Thank you for accepting to test this mobile application



Montimage Cyber-Range Objectives

- Raise awareness about cyber-threats and their impact on organisations
  - Specific target “phishing email threat”
- Understand the necessity of identifying phishing emails
  - That can contain malicious URLs
  - That can contain malicious attachments

What is a phishing email

Phishing is a type of **social engineering** where an attacker sends a **fraudulent** (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a human victim into **revealing sensitive information** to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

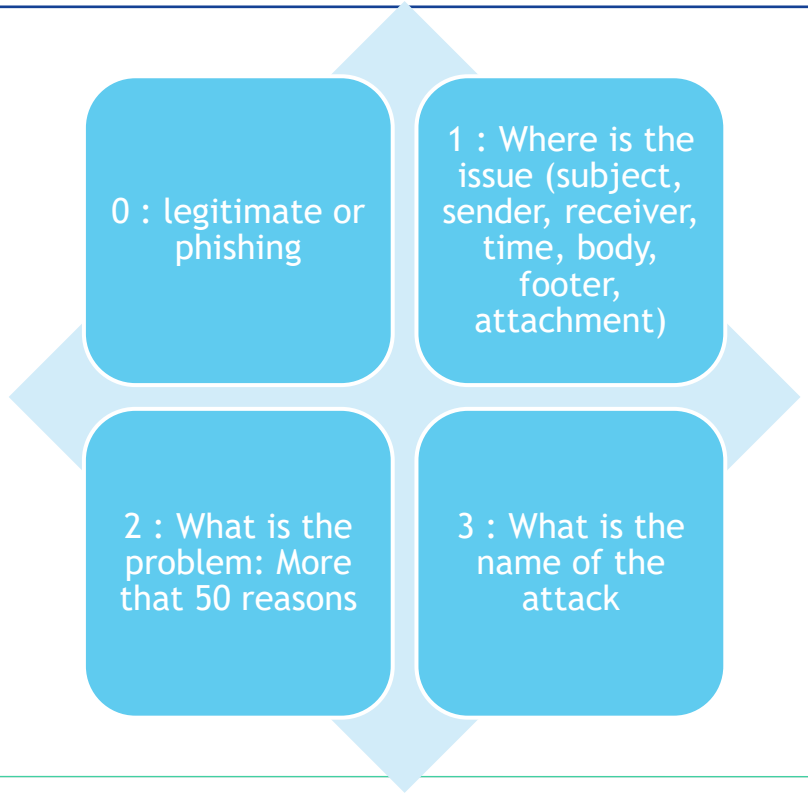
Montimage Cyber-Range Target public

- Any employee of a company concerned by the development of good practices in terms of cyber security including
  - Category 1: Non-ICT experts
  - Category 2: ICT experts
  - Category 3: Security experts

Montimage Cyber-Range - Functionnalities

- Receive email
- Classify it (legimate / phishing) and say why
- Score and Ranking
- Training

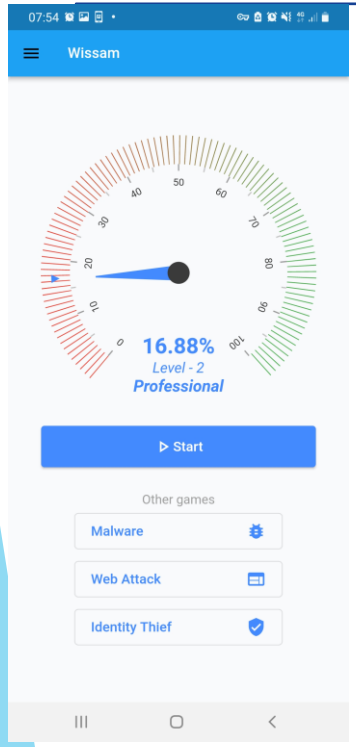
Anti-Phishing CR Levels



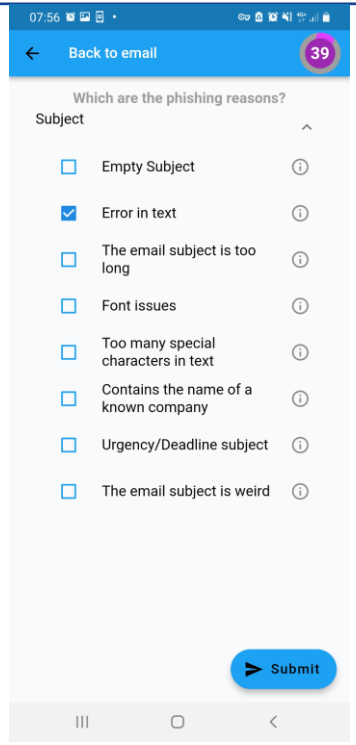
Privacy

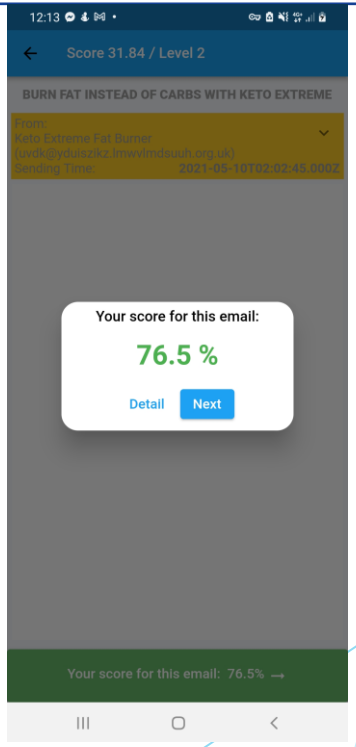
- We care about your privacy
- Either you don’t consent to share any information and all your information will stay locally in your phone
- Either you consent to share your score with
  - Geiger cloud (Geiger can use your score anonymously)
  - Your company (ranking between employees from the same company)
  - The community (ranking between the cybergame users)

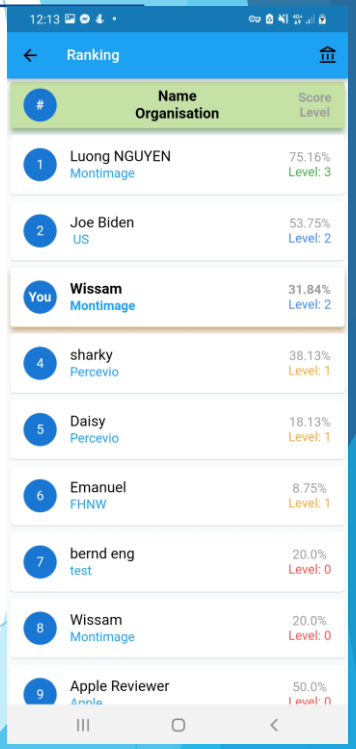
Dashboards


Wissam
16.88%
Level - 2
Professional
Start
Other games
Malware
Web Attack
Identity Thief


Score 16.88 / Level 2
47
Attention
From:Bank (kakinoaya@docomonet.jp)
Sending Time: 2021-04-14T11:35:23.000Z
Attention:
I have contacted my secretary to confirm if you have received the compensation DRAFT CHECK of US$8.5 Million United State Dollars which I issued in your name, but he told me that he could not send it to you because of the courier charges. Now I have called my bank to cancel any payment regards to the DRAFT CHECK and then authorized them to transfer the payment into ATM card in your name which they did. As of now be informed that I paid all the charges except the DELIVERY FEE of the ATM card, but to reactivate the ATM card you have to forward your current information as requested below to the bank then they will activate your ATM card and sent it to you immediately.
Here are the information you have to forward to the bank:
1. YOUR FULL NAMES:_____
2. Postal ADDRESS:_____
3. PHONE NUMBER:_____
4. EMAIL ADDRESS:____
6. SEX & AGE____
7. OCCUPATION:_____
8. COPY OD YOUR ID CARD _____
Contact them with below information,
Director, ATM Foreign Operation Dept.
Bank Name: UBA BANK Plc
Is this a phishing email?
Phishing
Legitimate


Back to email
39
Which are the phishing reasons?
Subject
Empty Subject
Error in text
The email subject is too long
Font issues
Too many special characters in text
Contains the name of a known company
Urgency/Deadline subject
The email subject is weird
Submit


Score 31.84 / Level 2
BURN FAT INSTEAD OF CARBS WITH KETO EXTREME
Your score for this email:
76.5 %
Detail
Next
Your score for this email: 76.5%


Ranking
Name Organisation Score Level
1 Luong NGUYEN Montimage 75.16% Level: 3
2 Joe Biden US 53.75% Level: 2
You Wissam Montimage 31.84% Level: 2
4 sharky Percevio 38.13% Level: 1
5 Daisy Percevio 18.13% Level: 1
6 Emanuel FHNW 8.75% Level: 1
7 bernd eng test 20.0% Level: 0
8 Wissam Montimage 20.0% Level: 0
9 Apple Reviewer 50.0%

URL

- https://anti-phishing.montimage.com/#/

Demo

Closing and Wrap-Up

Takeaways

- **Exploration of ADR Cyber Range:**
  - Implementing attacks is not trivial
  - LLM-based attack generation is under investigation
  - The more « classical way » to react to an attacker is to block its IP source
  - Next : Cyberrange as a service

Takeaways

- **Anti-Phishing Cyber Range Insights:**
  - Recognized 41 phishing indicators and categorized 14 types of phishing attacks.
  - Next: Web application

Post-training evaluation questionnaire

Profile

https://forms.gle/VN22UYAZFnkiuB6h6

Pseudo starts by ADR2……

Post-training evaluation questionnaire

https://forms.gle/JsA2nksf1LkuaH3Q6

- Use the same pseudo
- Select training : [DAY 1] Mastering Cyber Defense: Hands-On Training with Montimage Cyber Range (Session 1) by Wissam Mallouli (MI)