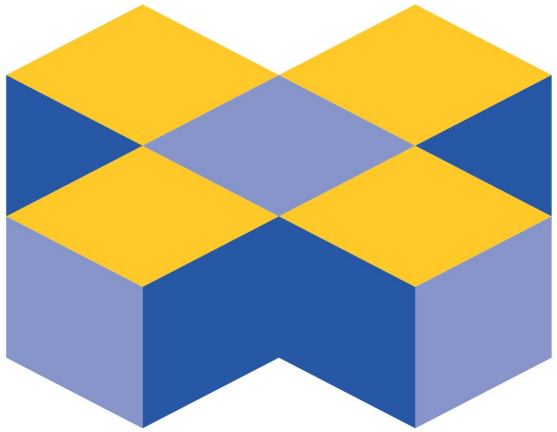


PUZZLE

Montimage Cyber-Range

Attack – Detect – React

Vinh Hoa La

vinh_hoa.la@montimage.com

UBITECH ubiquitous solutions · Mellanox TECHNOLOGIES · netcompany intrasoft · montimage · AEGIS IT RESEARCH · uni.systems · FOGUS INNOVATIONS & SERVICES · Suite5 We Deliver Intelligence · ETHZ ICCS · FORTH · European DIGITAL SME Alliance · VOJVODINA ICT CLUSTER

PUZZLE

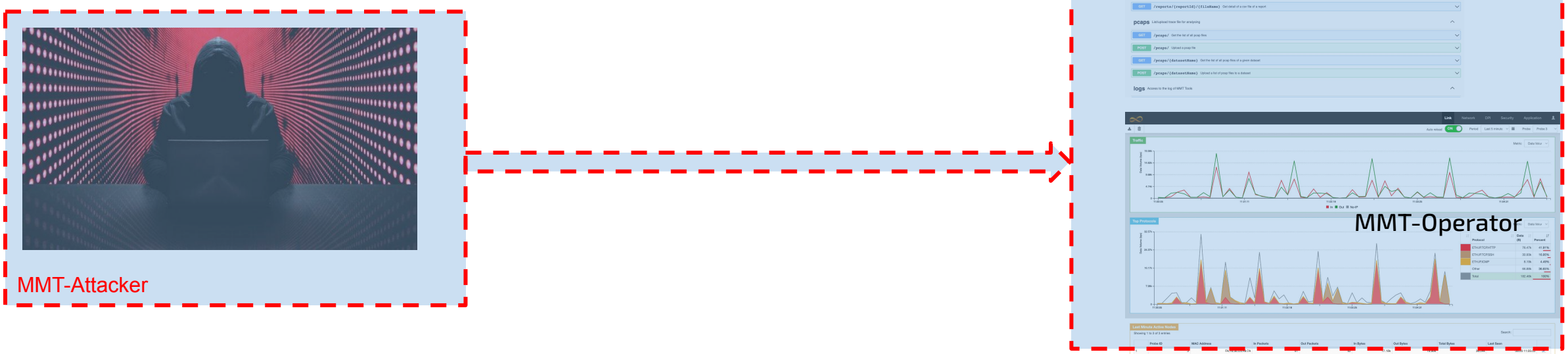
Objectives

- Raise **awareness** about **cyber-threats and their impact on organisations**
- Understand the **necessity of a serious monitoring** of the enterprise network for:
  - Drawing operation baselines
  - Producing reports
  - Notifying on abnormal operations
  - Providing input to network management

Components

- ACAS (Advanced Cybersecurity Analytics Service): http://acas.montimage.com:31057/
- MMT-Operator: http://acas.montimage.com:8080/
- MMT-Attacker: https://github.com/Montimage/mmt-attacker

*MMT: Montimage Monitoring Tool



PUZZLE

Exercise 1: Offline traffic analysis

- ACAS: Upload a pcap file
- ACAS: Get the list of all available pcap files
- ACAS: Start analysing an offline pcap file
- ACAS: Download the report
- Tutorial video

PUZZLE

Exercise 2: Online traffic analysis (1)

- ACAS: Start analysing real-time online traffic (net interface **ens3**)
- MMT-Operator: View technical dashboards
- MMT-Attacker: SSH brute force attack
- MMT-Operator: View security dashboard
- Tutorial video

PUZZLE

Exercise 3: Online traffic analysis (2)

- MMT-Attacker: Slowloris DoS attack
- MMT-Operator: View security dashboard
- Tutorial video

https://www.linkedin.com/showcase/h2020-puzzle

https://twitter.com/H2020Puzzle

https://www.facebook.com/H2020Puzzle

https://puzzle-h2020.com/

https://www.instagram.com/h2020puzzle/

https://www.youtube.com/channel/UCKYqEMdsaorfpEuVwdtISQQ

Thank you for your attention

Vinh Hoa La

vinh_hoa.la@montimage.com