CERT-MU

Computer Emergency Response Team of Mauritius

Cyber Drills: A tool to develop a proactive and robust security posture or the importance of security simulations

Dr. Kaleem Usmani
Head, CERT Mauritius

22 November 2023

Points to highlight for today's event

- Importance of cybersecurity preparedness and cyber incident response.
- Design and review of incident response plans.
- Design a cybersecurity simulation exercise and develop realistic scenarios.
- Execute exercises such as table-top, capture the flag, red team vs blue team or full-scale cyber attack simulation.

Cyber Threat Trends and Statistics 2023 (1) *Source: Forbes*

Cyber attack surface trend

- Metaverse (a new vector of exploitation)
- Artificial Intelligence and Machine Learning (i.e. ChatGPT), new tools for advanced attack
- Deep fakes are being deployed
- Bots are continuing to run rampant
- Critical infrastructures are one of the main focus of attack (DDOS, website defacement)
- Russia and Ukraine war is a live example of CII attacks.

Cyber Threat Trends and Statistics 2023 (2)

During the past 12 months, this is trend noticed:

- Accounting and financial data
- Sophisticated and malicious malware
- Ransomware
- Social engineering
- Payment through cryptocurrencies
- Growth of Internet of Things Industry

Targets

- Small Businesses, organisations and healthcare institutions

Cyber Threat Trends and Statistics 2023 (3)

According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.

- Open source vulnerabilities
- Phishing is one of the most preferred methods
- Business Email Compromise
- Fraud is trending digital especially identity theft

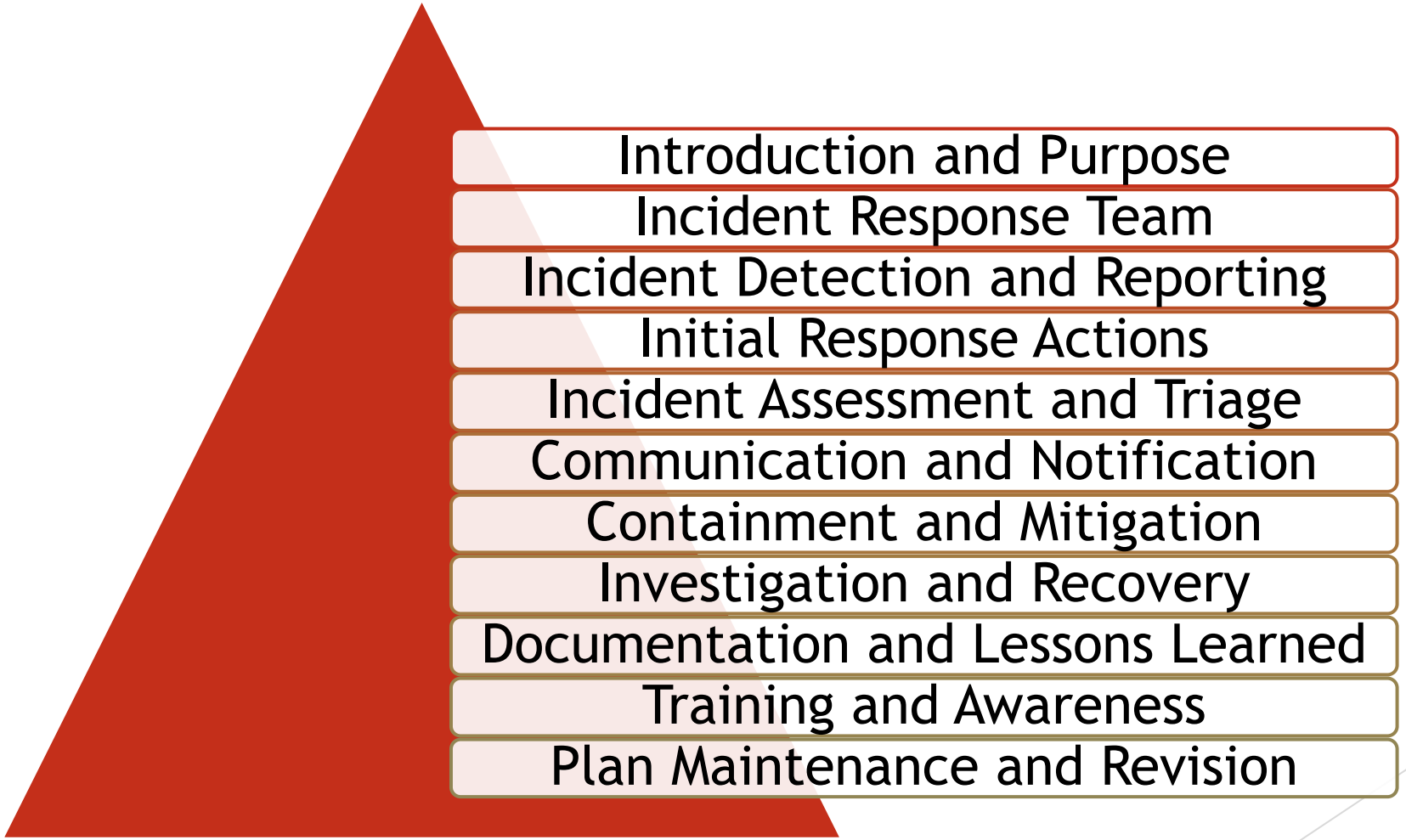
Cyber Threat Trends and Statistics 2023 (4)

Password attacks	34,740 per minute[1]	SQL injection attacks	1 every 2 minutes[5]
IoT-based attacks	1,902 per minute[2]	New threat infrastructure detections	1 every 35 minutes[6]
DDoS attacks	1,095 per minute[3]	Supply chain attacks	1 every 44 minutes[7]
Phishing attacks	7 per minute[4]	Ransomware attacks	1 every 195 minutes[8]

Source: Microsoft, 2022

Need for a cyber incident response plan

Basic structure of a cyber incident response plan



Why a cyber simulation exercise?

- It plays a crucial role in improving readiness and resilience in the face of cyber threats by providing a controlled environment to practice and refine cybersecurity strategies and incident response plans.

- It usually involves various stakeholders, such as government agencies, critical sectors, cybersecurity professionals and others, who come together to test their preparedness, response capabilities, and coordination in dealing with cyber threats (large-scale).

Benefits of simulation exercises

- Test the effectiveness of incident response plans
- Identify weaknesses in an org's cybersecurity posture
- Provide training opportunities for employees
- Foster collaboration and comm. between teams
- Enhance overall cybersecurity readiness

Types of exercises

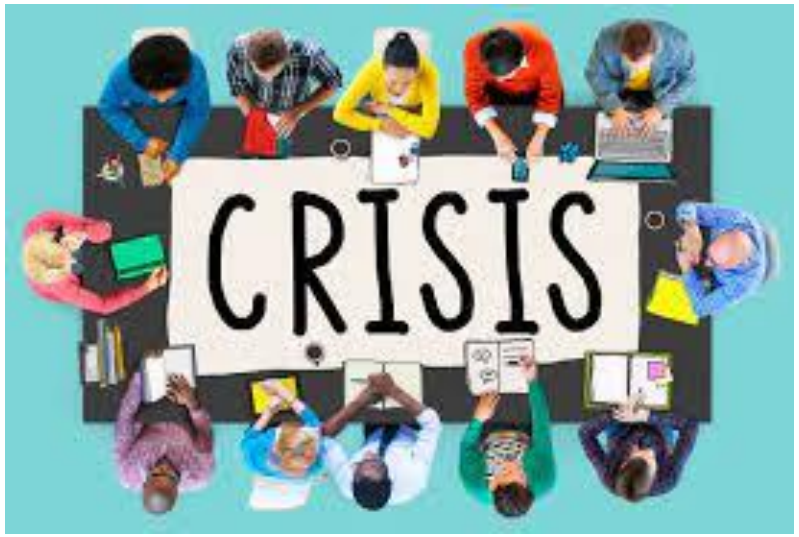
- Table-top exercises
- Capture the flag (CTF) competitions
- Red team vs blue team exercises
- Full-scale cyber attack simulations

Choosing a method for an exercise

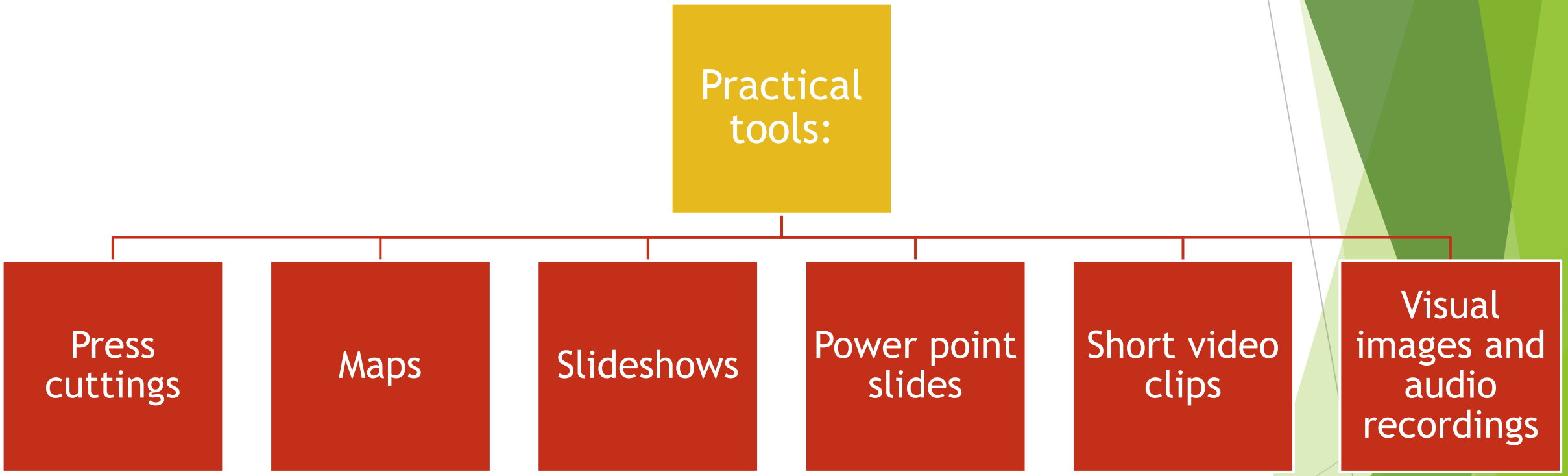
- How many people will be involved in the exercise simultaneously and in what function(s)?
- How long will it take to plan, carry out, evaluate and do a follow-up of the exercise?
- What financial resources have been allocated?
- How much experience has the organisation had with exercises?

Format 1: Table-top exercise

- Discussion-based simulation that tests an organisation's response plan in a simulated environment.
- **Benefits:** Provides an opportunity for teams to review their plan and identify gaps in their response capabilities.



Format 1: Table-top exercise



When to conduct a table-top exercise?

- A table-top exercise is a good exercise form for groups that allows organisations to theoretically analyse problems and discuss potential solutions with less pressure and stress.
- It can be used to
  - highlight and develop roles, areas of responsibilities, working methods, priorities, cooperation, support functions, practical or technical needs
  - analyse a particular risk or vulnerability
  - evaluate a plan
  - investigate and analyse potential problems in cooperation

Format 2: Capture the flag (CTF)

- Capture the Flag (CTF) competitions are cybersecurity events where participants engage in a hands-on challenge to find and exploit vulnerabilities in computer systems and networks.
- The goal is to “capture the flag,” which is typically a specific piece of information or a digital artifact hidden within the system.
- They serve as a platform for participants to hone their cybersecurity skills, gain practical experience, and stay updated on the latest threats and vulnerabilities.

Format 2: Capture the flag (CTF)

Team formation	Competition infrastructure	Challenges	Scoring system
Time limit	Collaboration and learning	Ethical conduct	Post-competition analysis

Format 3: Red team vs. blue team exercise

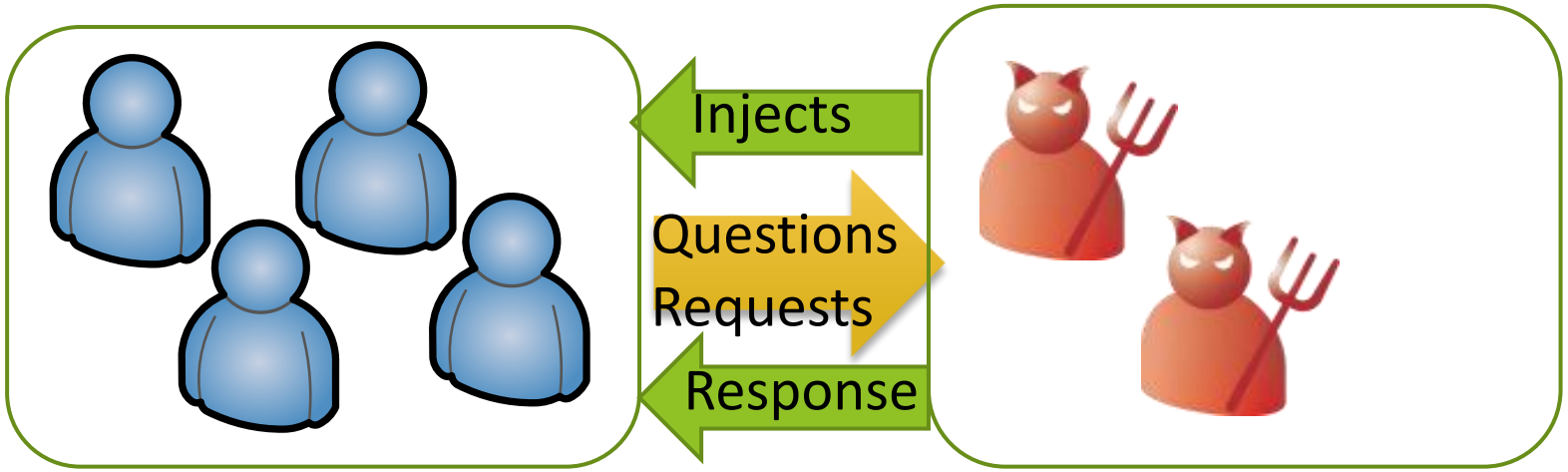
- A red team vs. blue team exercise involves a simulated attack scenario where a red team (attackers) tries to breach an organisation's defences, while a blue team (defenders) works to prevent the attack and respond to it if it is successful.
- Conducted in a constructed, fictional game environment, where the infrastructure is set up separately.
- **Benefits:** Provides a realistic environment to test an organisation's incident response plan and identify gaps in their security defences.

Roles and objectives of a red team vs. blue team exercise

- Blue-team mission: Identify the cause of incident as soon as possible and prevent the spread of secondary damage

Blue team = CSIRT

Red team = attacker, SOC, users, police, the media, others



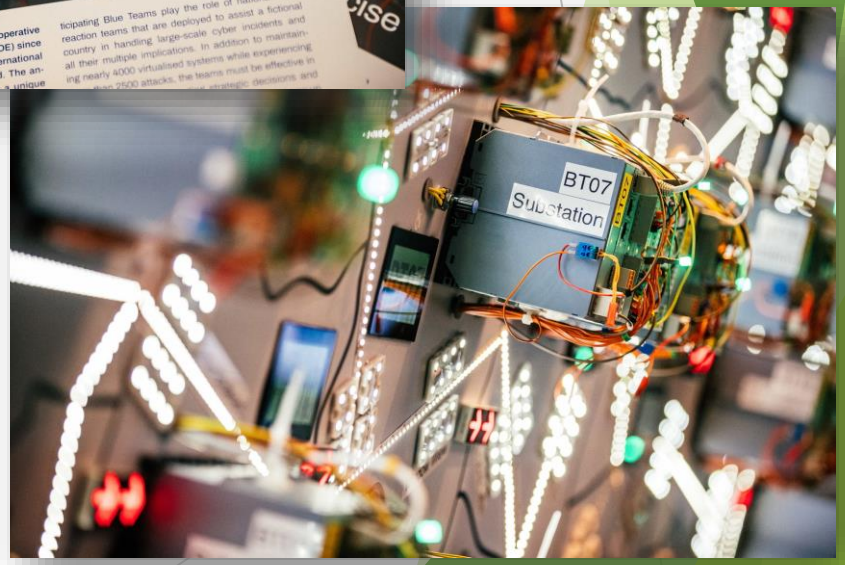
Format 4: Full-scale cyber attack simulation

- A full-scale cyber attack simulation involves simulating a real-world cyber attack on an organisation's systems and networks.
- These exercises are often conducted over an extended period and involve a wide range of participants.
- **Benefits:** Provides a comprehensive evaluation of an organisation's cybersecurity readiness and identifies areas for improvement in response plans, processes and technologies.

When to conduct a full-scale cyber attack simulation exercise?

- A full-scale cyber attack simulation exercise should be used with caution so that it does not interfere with regular activities.
- It is used to test an organisation's existing systems and procedures as well as identifying vulnerabilities and weaknesses within them.
- It requires very good planning and careful preparation so that it does not put the organisation in a compromising situation.

Full-scale cyber attack simulation example: Locked Shields/NATO



CERT-MU

Thank You

Computer Emergency Response Team of Mauritius (CERT-MU)

CONTACT US

Tel: 460 2600| Hotline: 800 2378

General Enquiry: contact@cert.govmu.org
Subscribe to Mail List: subscribe@cert.govmu.org

Incident Reporting: incident@cert.govmu.org

MAUCORS: https://maucors.govmu.org
Website: www.cert-mu.govmu.org