OMSAR WORKSHOP ON CYBERSECURITY

April 30, 2025

WORLD BANK GROUP

Republic of Lebanon

OMSAR

Office of the Minister of State for Administrative Reform

DEVELOPING A CYBERSECURITY STRATEGY

GROUP DISCUSSION

Context

- Lebanon is preparing the roll-out of digital health service. Before launch, **a malware outbreak** hits multiple hospitals, compromising patient records and interrupting critical care. The malware could spread to other government systems if not contained swiftly. A **high-level task force** has been tasked to develop a **cybersecurity response.**

Your Task as a Table

- What should have been done to prevent this? And what should be done now?
- Assign a team member to facilitate and another to report to plenary.
- You have **10 minutes** to brainstorm, and each table has **1 minute** to report to plenary.

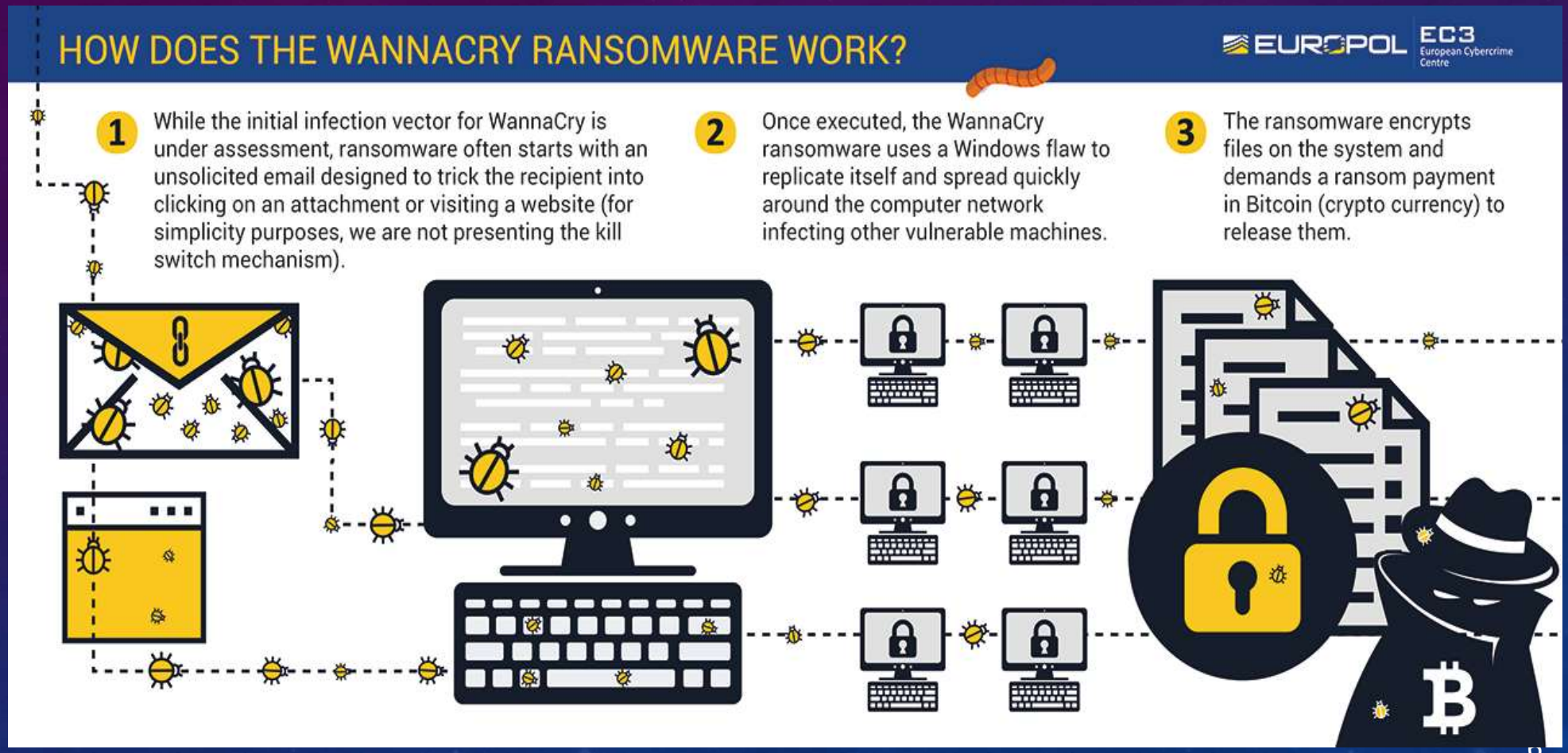
#

PRESENTATION OF GOOD PRACTICES AND INTERNATIONAL EXAMPLES

WHY INTERNATIONAL EXAMPLES?

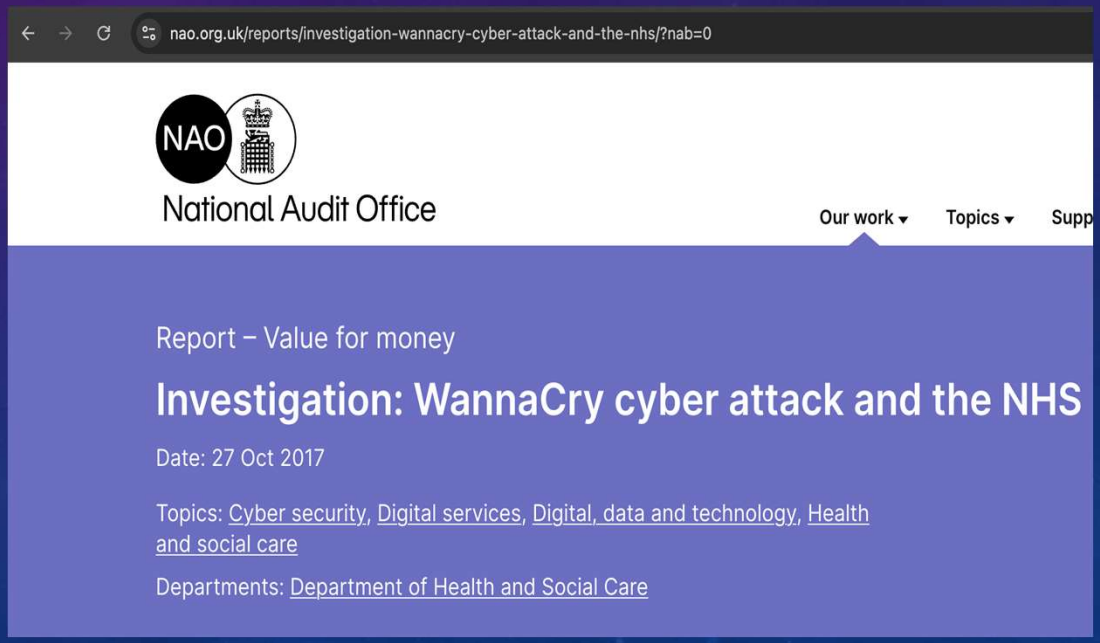
- Learn from proven security approaches
- Adapt frameworks to local contexts
- Strengthen cross-border cooperation
- Stay informed on emerging threats

CASE FOCUS: WANNACRY ATTACK



IMPACT OF WANNACRY ON THE UK

- NHS services severely disrupted
- Medical appointments cancelled
- Critical data access denied
- Public confidence shaken

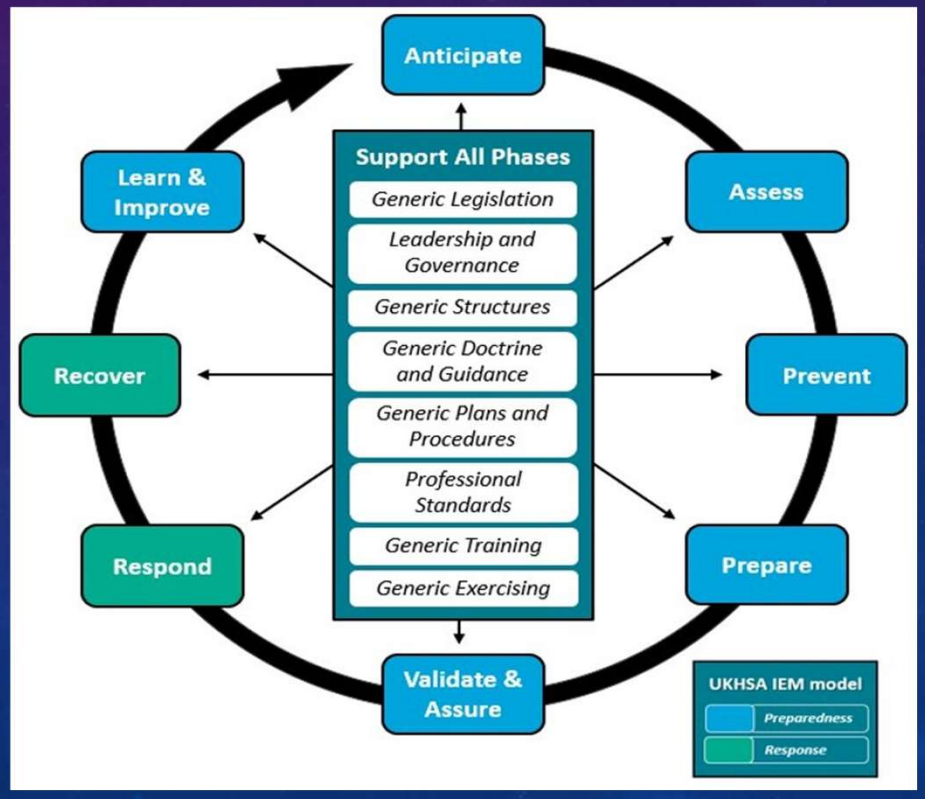


RAPID NATIONAL GUIDANCE

- Security patches issued promptly
- Mandatory vulnerability checks
- Emergency hotlines for institutions
- Crisis communication channels activated

COLLABORATION AMONG AGENCIES

- Coordinated threat intelligence sharing
- Engagement with private sector experts
- Joint operational task forces
- Unified incident command structure

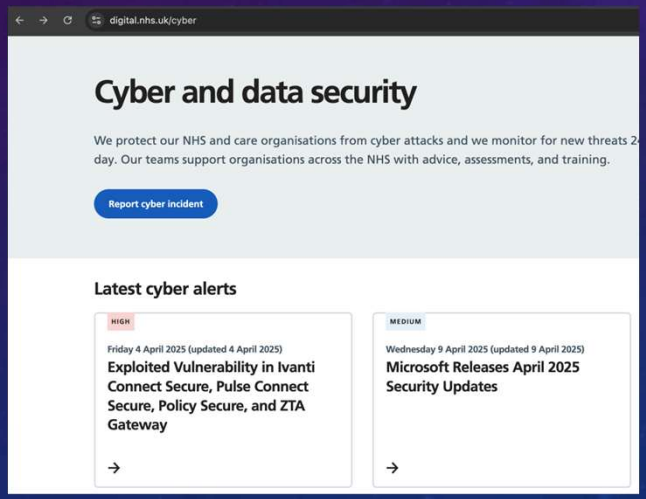


PUBLIC AWARENESS MEASURES

- Regular media updates
- Simple prevention tips
- Warning bulletins circulated
- 24/7 hotline support

LESSONS FOR STRATEGY

- Identify high-risk systems early
- Prioritize patch management
- Establish clear escalation paths
- Build trust through transparency



KEY ELEMENTS OF THE UK APPROACH

- Centralized cybersecurity authority (NCSC)
- Robust legal frameworks
- Ongoing public-private partnerships
- Nationwide security culture

www.gov.uk/government/organisations/national-cyber-security-centre

Documents

Services

Avoid and report internet scams and phishing

See all services

Guidance and regulation

Where to Report a Cyber Incident
13 May 2022 Guidance

Academic Centres of Excellence in Cyber Security Research
3 December 2020 Guidance

See all guidance and regulation

News and communications

Business leaders supported to bolster online defences to safeguard growth
7 April 2025 Press release

New cyber laws to safeguard UK economy and secure long-term growth
31 March 2025 Press release

See all news and communications

Policy papers and consultations

Cyber Governance Code of Practice
7 April 2025 Policy paper

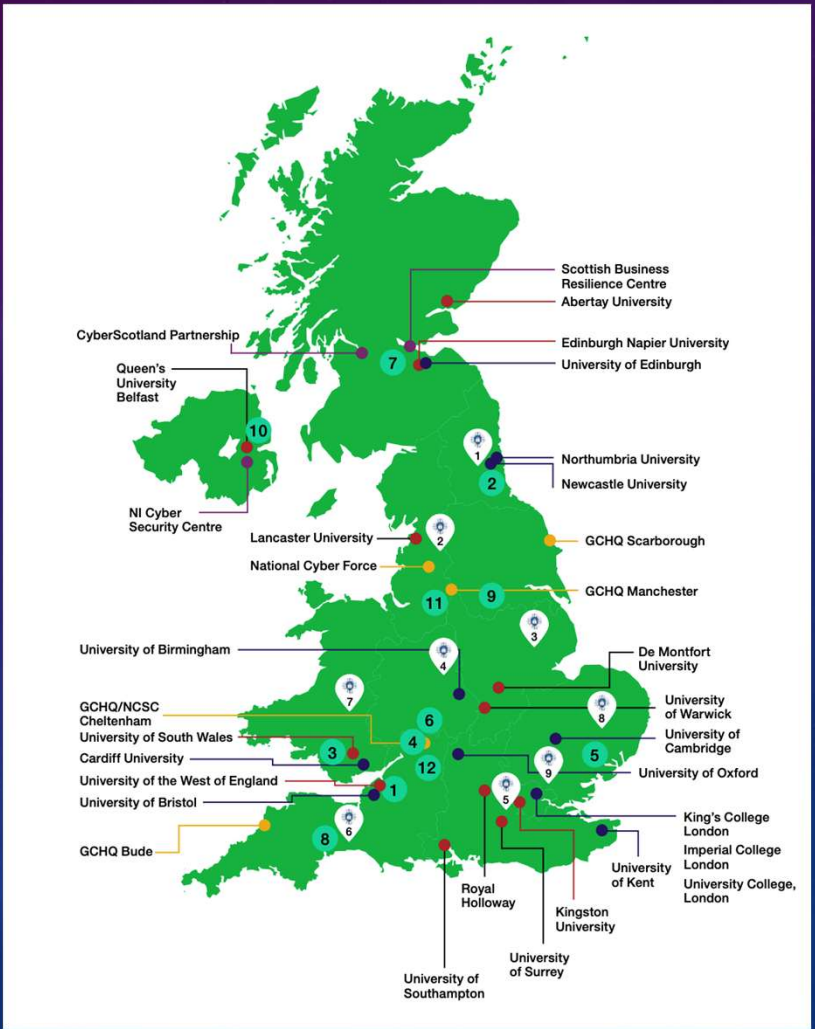
The second UK-Nigeria Security and Defence Partnership Dialogue Communique
14 February 2024 Policy paper

See all policy papers and consultations

Transparency and freedom of information releases

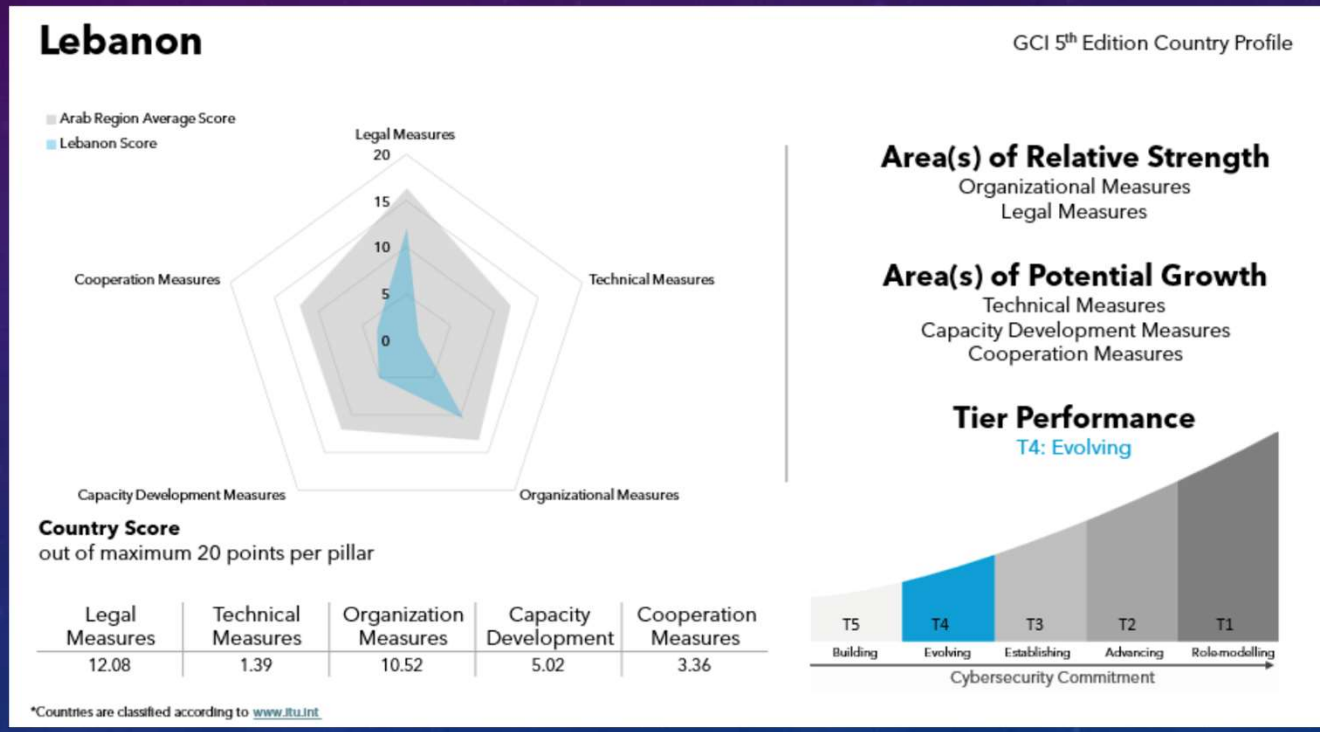
CONTINUOUS RESILIENCE EFFORTS

- Regular national drills
- Real-time threat monitoring
- Cyber hygiene campaigns
- Funding for research and innovation



ADAPTATION BY OTHER COUNTRIES

- Map existing vulnerabilities
- Clarify institutional mandates
- Engage local private sector
- Ensure resource allocation



ASPIRATIONAL PRACTICES

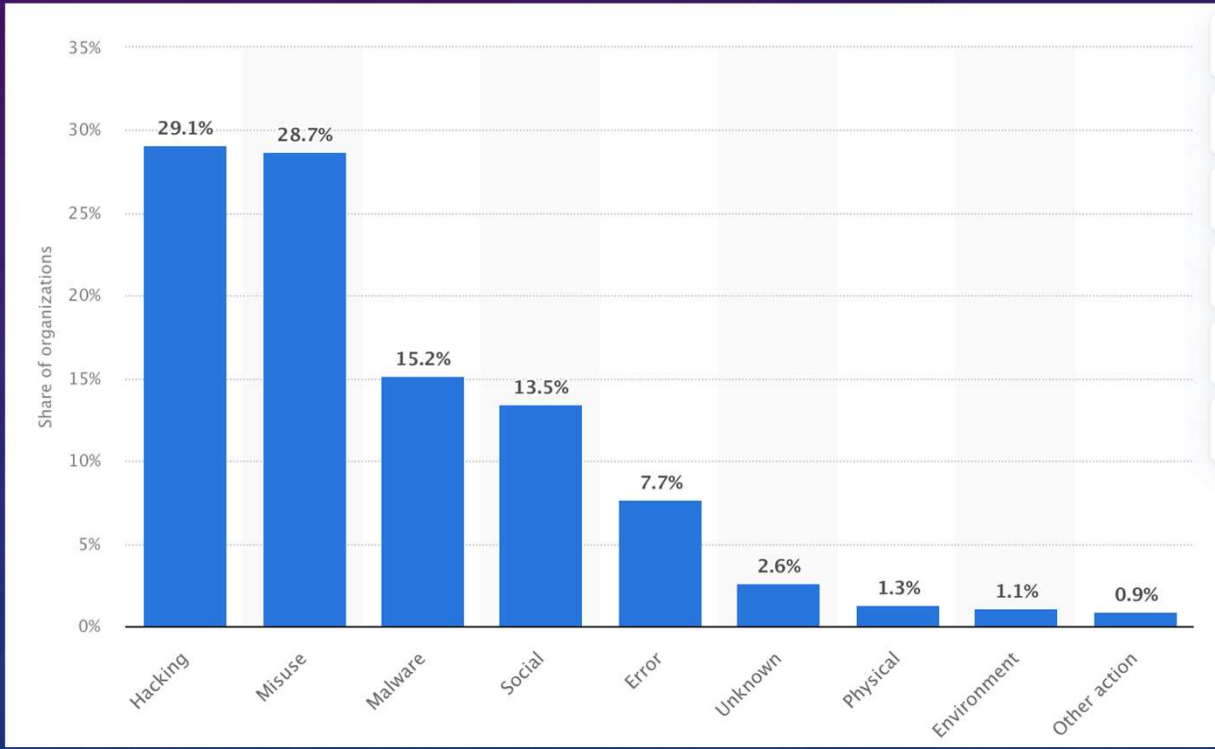
- Institutionalized cybersecurity training
- Multistakeholder governance models
- Timely threat intelligence sharing
- Cross-sectoral incident coordination

GLOBAL FRAMEWORK ALIGNMENT

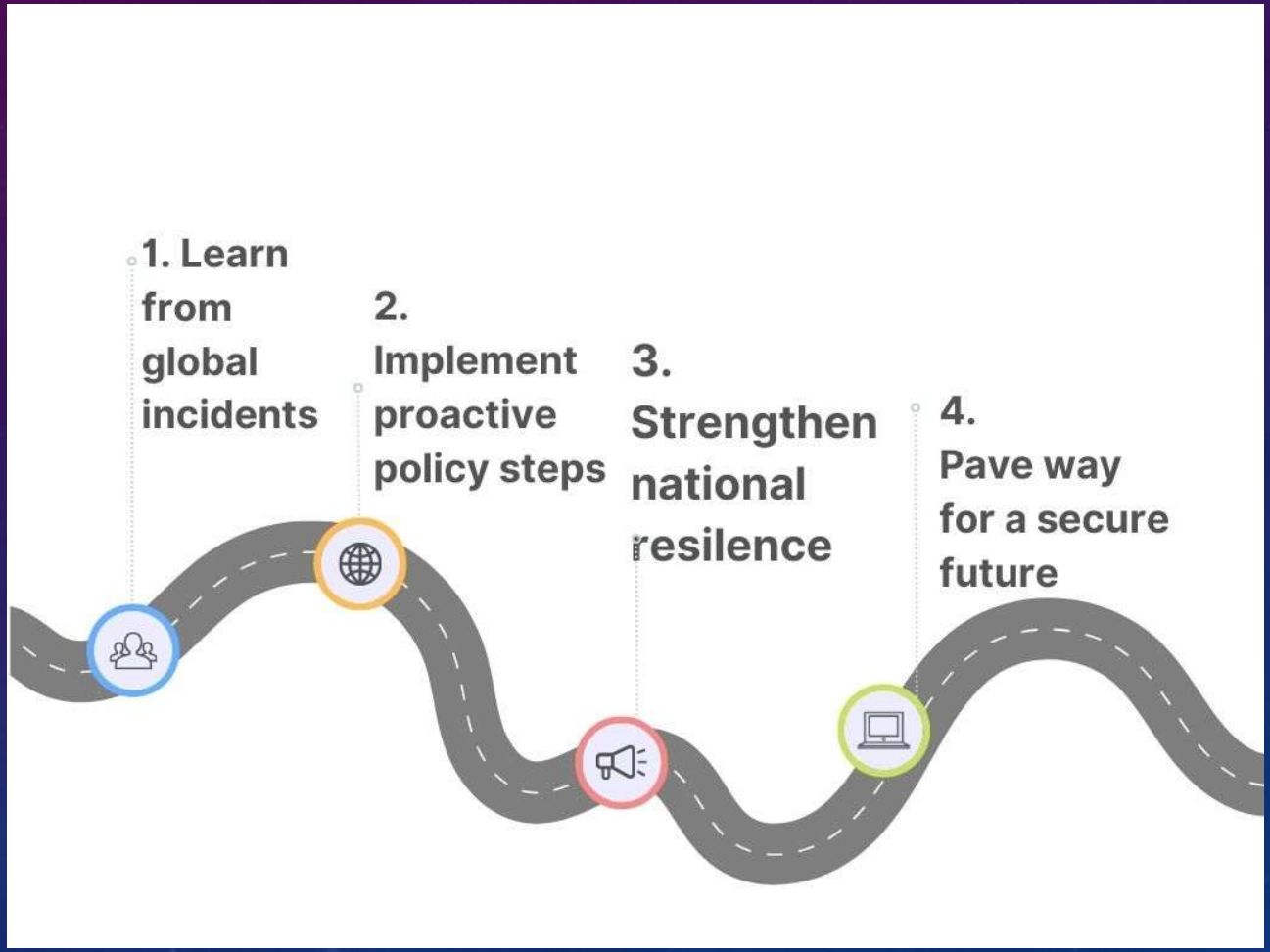
- Adopt ISO/IEC or NIST standards
- Leverage World Bank resources
- Participate in global cyber forums
- Benchmark with leading nations

MEASURING SUCCESS

- Reduced ransomware incidents
- Improved national cyber ranking
- Robust crisis response capabilities
- Stronger public trust in systems



CONCLUSION


1. Learn from global incidents
2. Implement proactive policy steps
3. Strengthen national resilence
4. Pave way for a secure future

GROUP DISCUSSION: RESPONSIBLE INSTITUTIONS FOR ENFORCEMENT

SCENARIO

Context

- Lebanon is updating its **National Cybersecurity Compliance Directive** to unify public and private security standards. The directive outlines requirements for data protection, threat reporting, and incident response. Some ministries claim partial jurisdiction for overseeing compliance. Private service providers are confused over which entity holds final authority, leading to inconsistent enforcement and gaps in cybersecurity readiness.

- The Prime Minister is requesting guidance on which entity has final authority and which accountability mechanisms will ensure the public and private sectors will adhere to these robust security measures.

Task

- At your tables, propose one final Authority and justify your choice. What motivations or penalties will best drive consistent adherence to the directive? You have 10 minutes to brainstorm and 1 minute to present.

GROUP DISCUSSION: RETAINING CYBERSECURITY TALENT

SCENARIO

Lebanon faces a challenge **retaining cybersecurity talent**. Economic uncertainties, limited professional development, and attractive offers from abroad have contributed to brain drain. Lebanon's capacity to build robust cybersecurity systems is being severely compromised.

Task

As a team at your table:

1. Identify **practical strategies** to address short-term retention tactics and long-term solutions for nurturing Lebanon's next generation of cyber talent.
2. Which agency (ies) should lead this effort?

Ensure all team member participate. You have 10 minutes to brainstorm and 1 minute to present.

THREAT INTELLIGENCE ON A BUDGET

WHY THREAT INTELLIGENCE?

- Prevent costly incidents
  - WannaCry $4B, NHS £92M; NotPetya $10B – FedX, Mersk, Merck, TNT, Mondelez, Saint-Gobain.
- Stay ahead of attackers
  - Ryuk ransomware, 59 healthcare providers across 510 facilities
- Boost overall resilience
  - Estonia 2007-2017

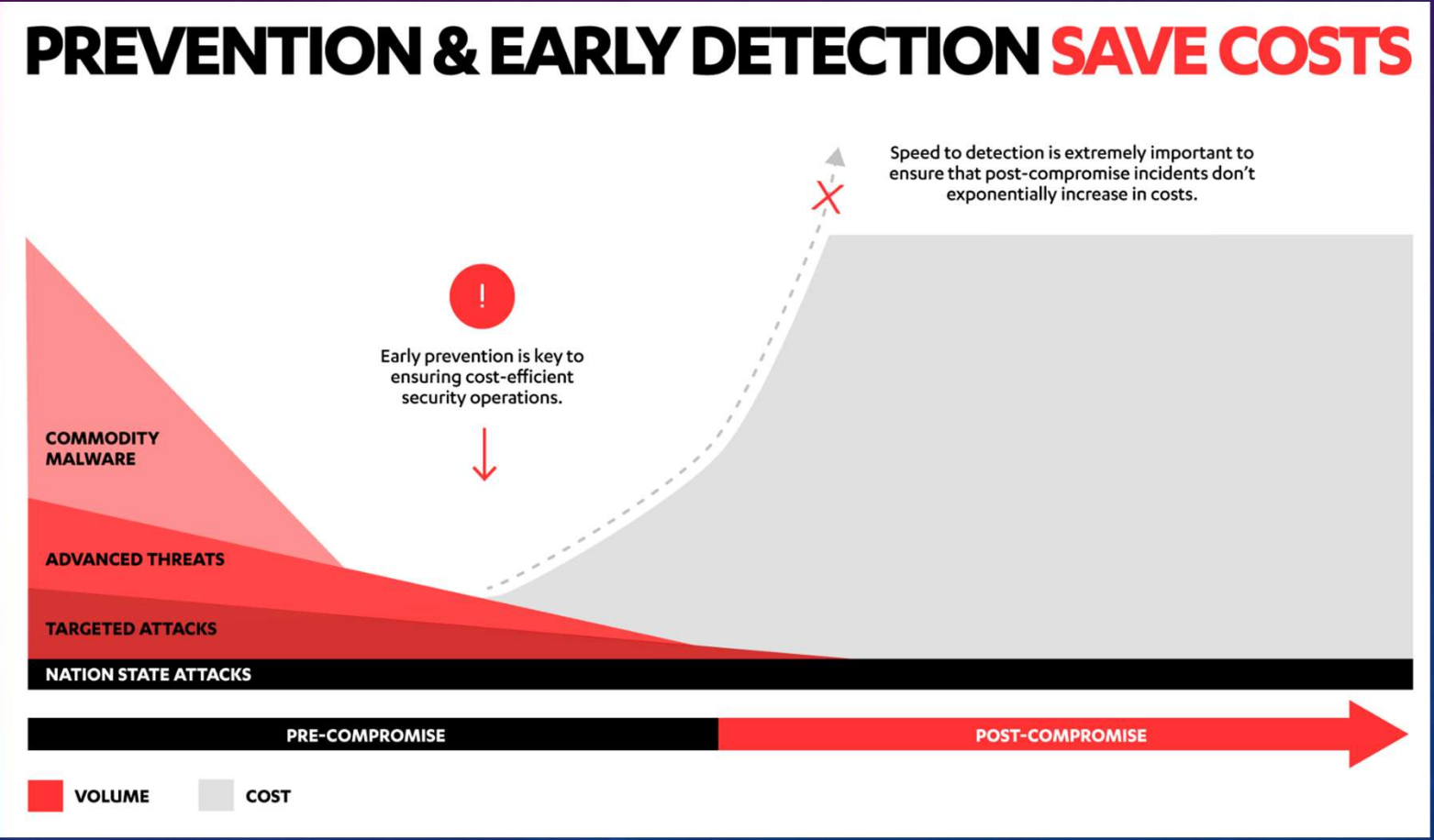
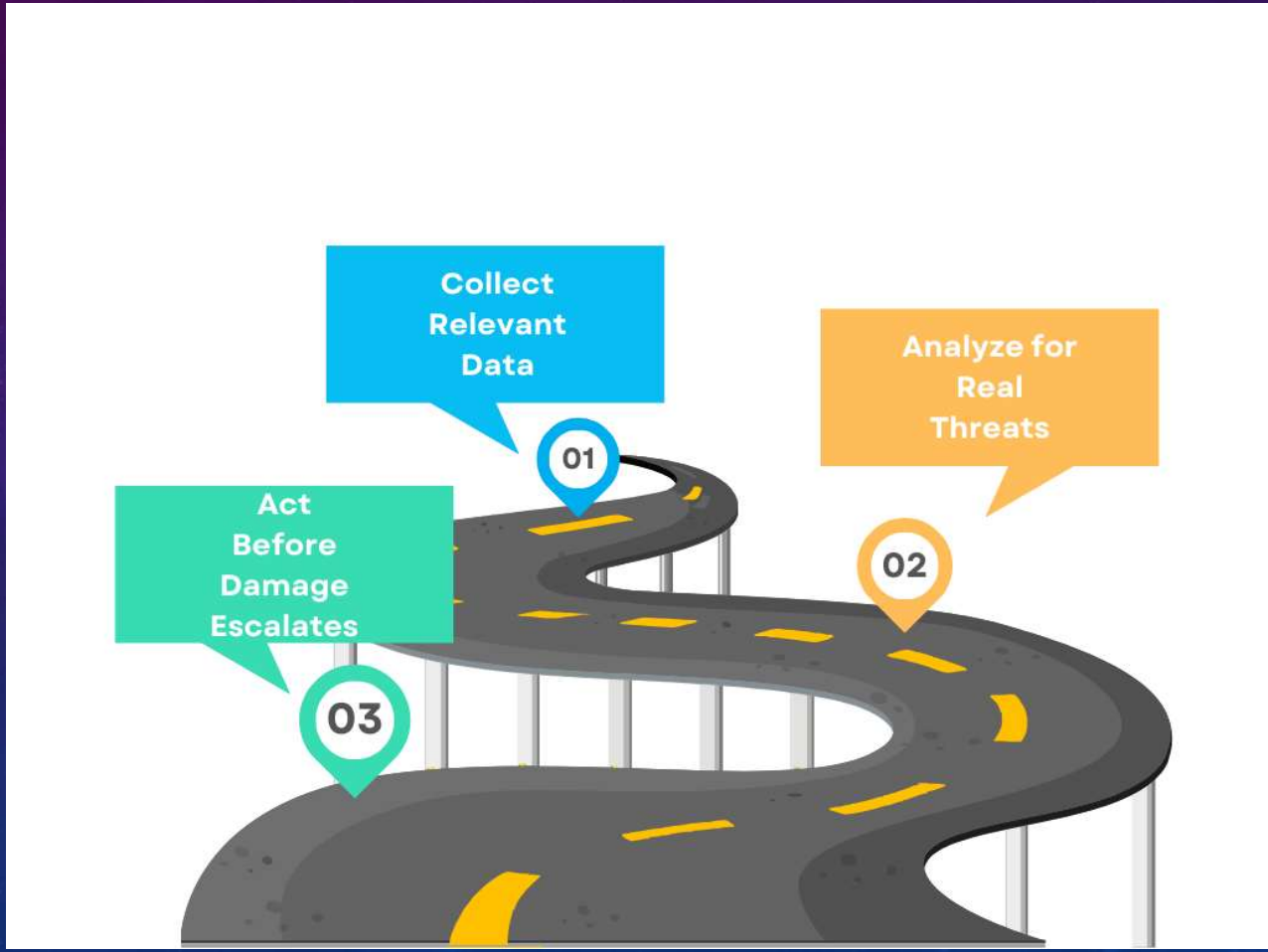


Image Source: blogs.f-secure.com

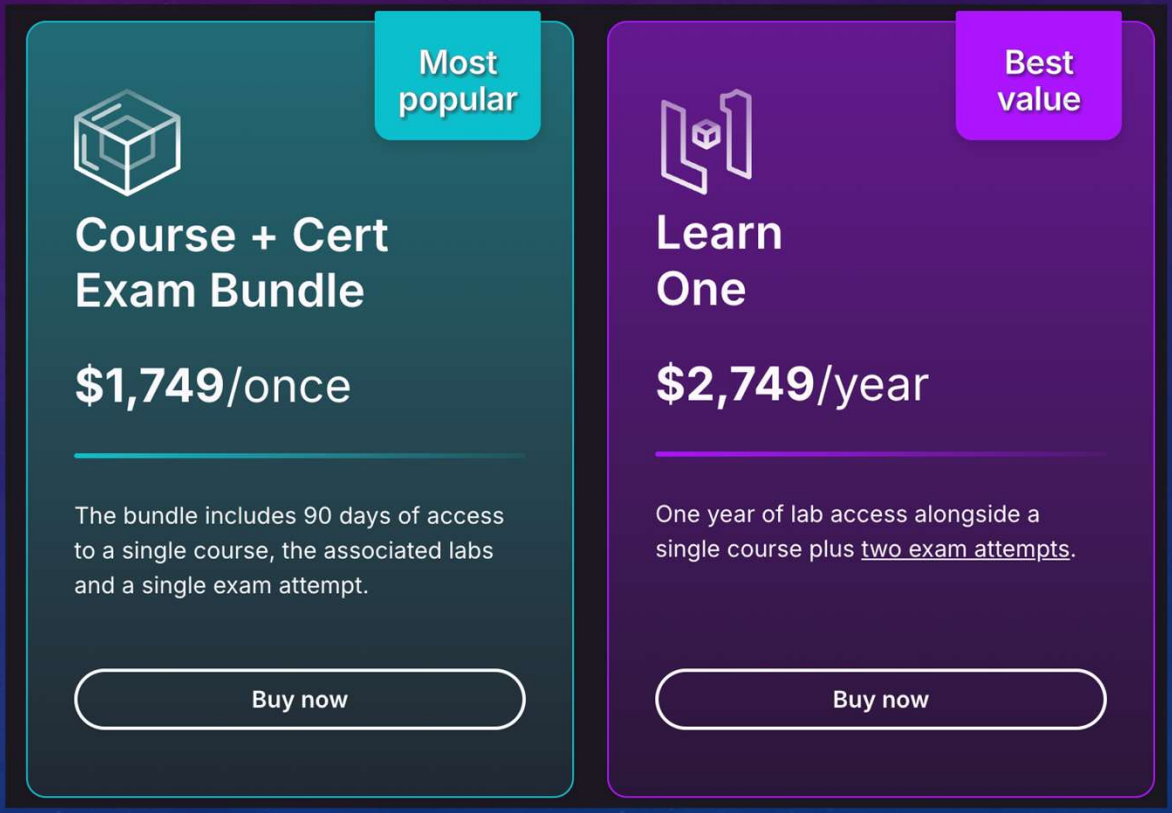
KEY PRINCIPLES

- Target 2013, 70M customer records, 40M card details
- Equifax 2017, 143M Americans' data, $1.2B for cleanup, Apache
- Log4j/Log4shell 2021, 93% cloud, RCE



COMMON BUDGETARY HURDLES

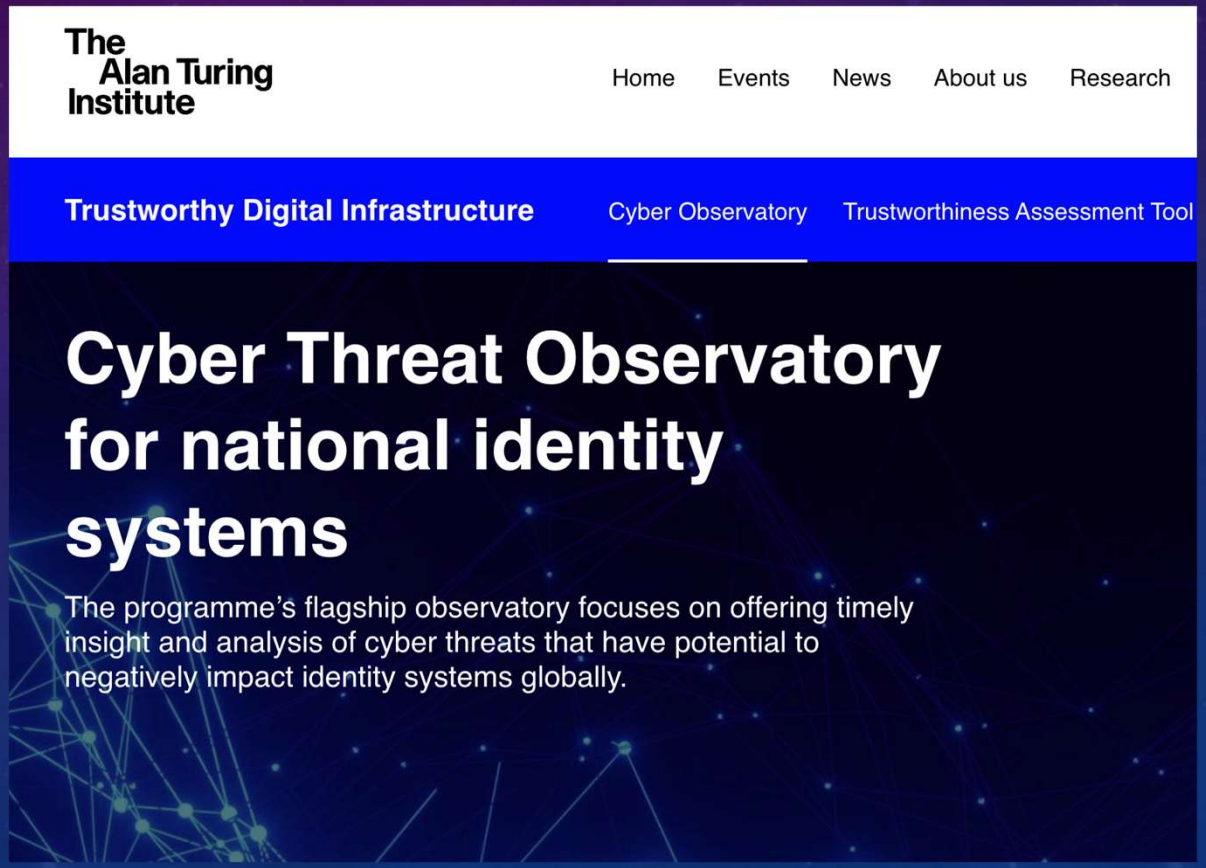
- Limited financial resources
  - Baltimore 2019, £76K ransomware, $18M
- Skills gaps and training costs
  - Bangladesh SWIFT 2016, $81M, $1B
- Aging digital infrastructure
  - WannaCry 2017



Source: OffSec

CASE SPOTLIGHT

Alan Turing Institute's Cyber Threat Observatory



TURING OBSERVATORY FOCUS

- Twitter/X's threat monitoring
  - SandBoxEscaper
- Software/Hardware BOM tracking
  - Log4j
- Heat maps for system risk

afcea.org/signal-media/cyber-edge/us-army-signs-software-bill-materials

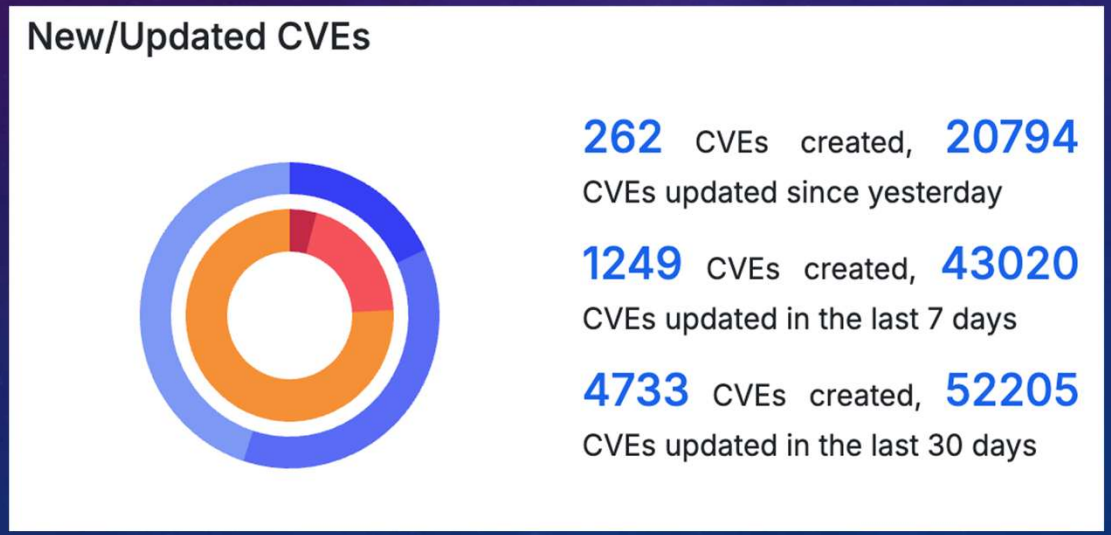
The U.S. Army Signs Software Bill of Materials

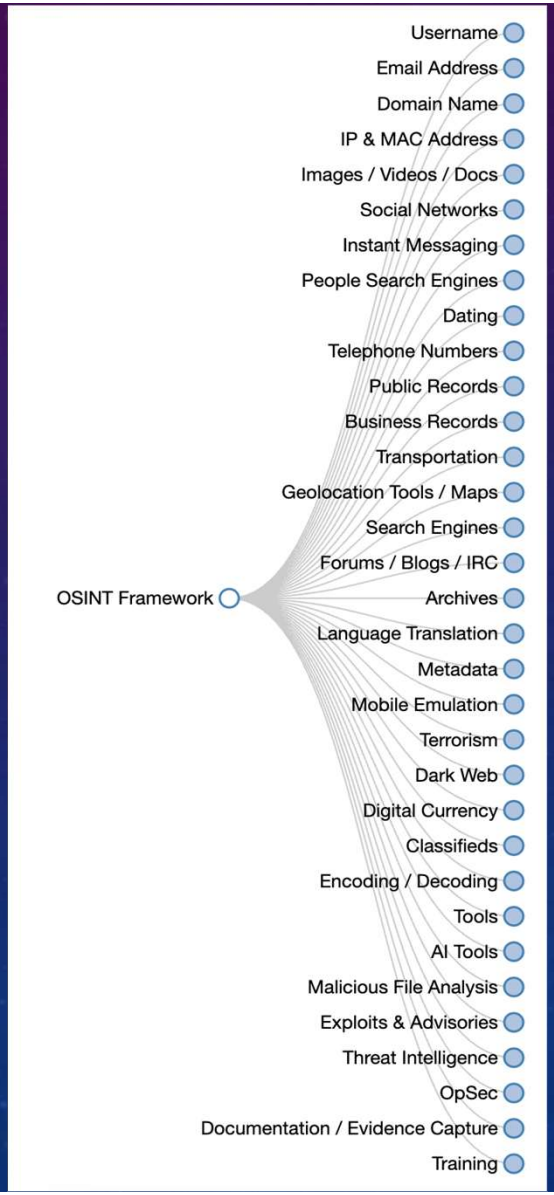
The policy provides a framework for transparency of software products.

LOW-COST INTEL SOURCES

- Open-source data (OSINT)
- Public vulnerability databases
- Sector collaboration groups

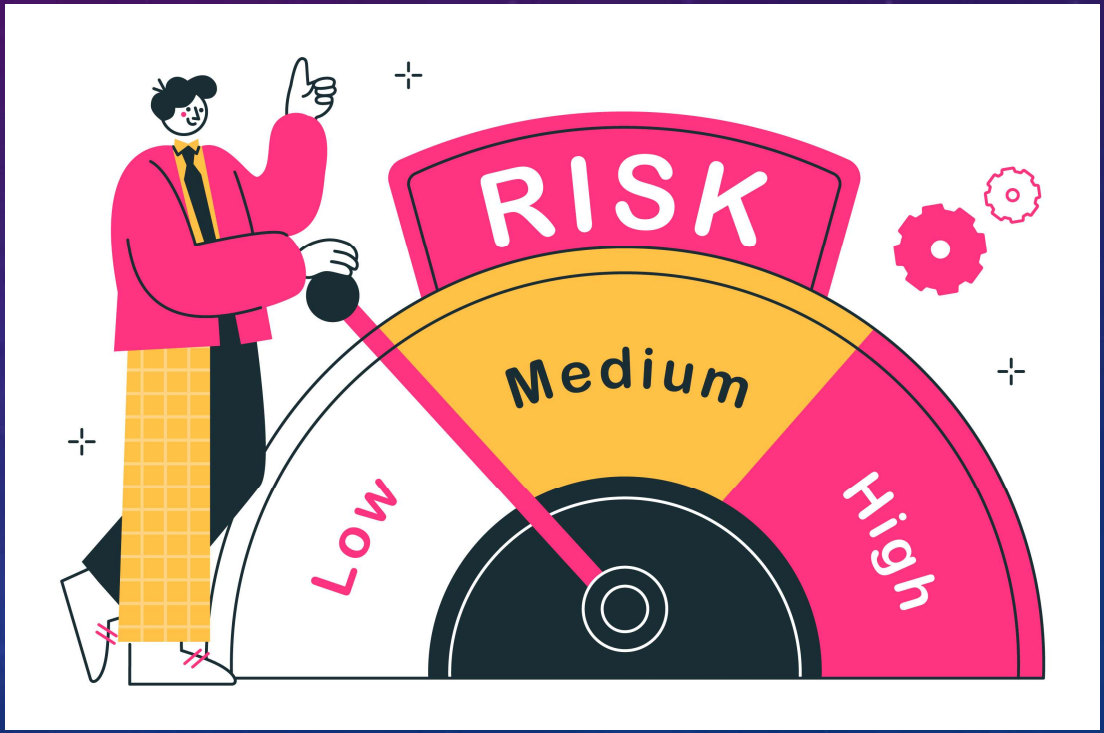
Information Sharing and Analysis Center





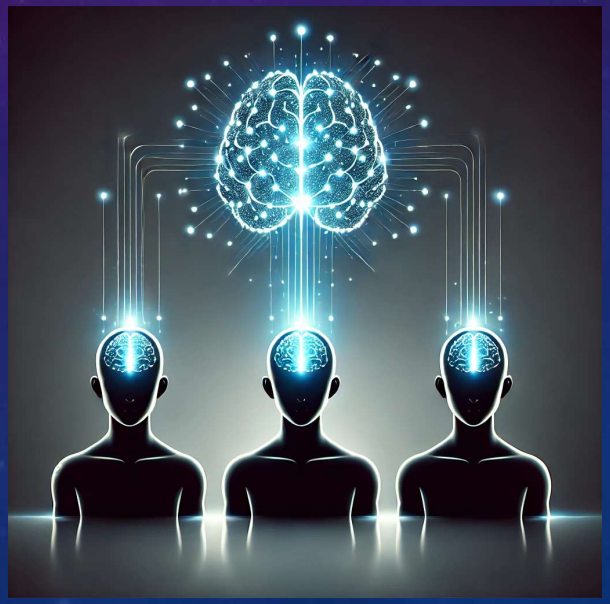
FOCUS ON CRITICAL COMPONENTS

- Identify high-impact assets
  - Aramco 2012 Shamoon; 30,000 computers wiped
- Prioritize potential failures
- Allocate scarce resources wisely



COLLABORATION IS KEY

- Public-private partnerships
- Shared intelligence across sectors
- Stronger collective defense



FELEG
FIVE EYES LAW ENFORCEMENT GROUP

AUTOMATED TOOLS

- Free threat intel platforms
- Community-driven research
- Basic monitoring solutions

INTERNAL BEST PRACTICES

- Set clear reporting lines
- Train staff on cyber hygiene
- Patch vulnerabilities quickly

LEVERAGE INTERNATIONAL SUPPORT

- Partner with global institutions
- Seek grants and guidance
- Adopt recognized standards

LOCAL PARTNERSHIPS

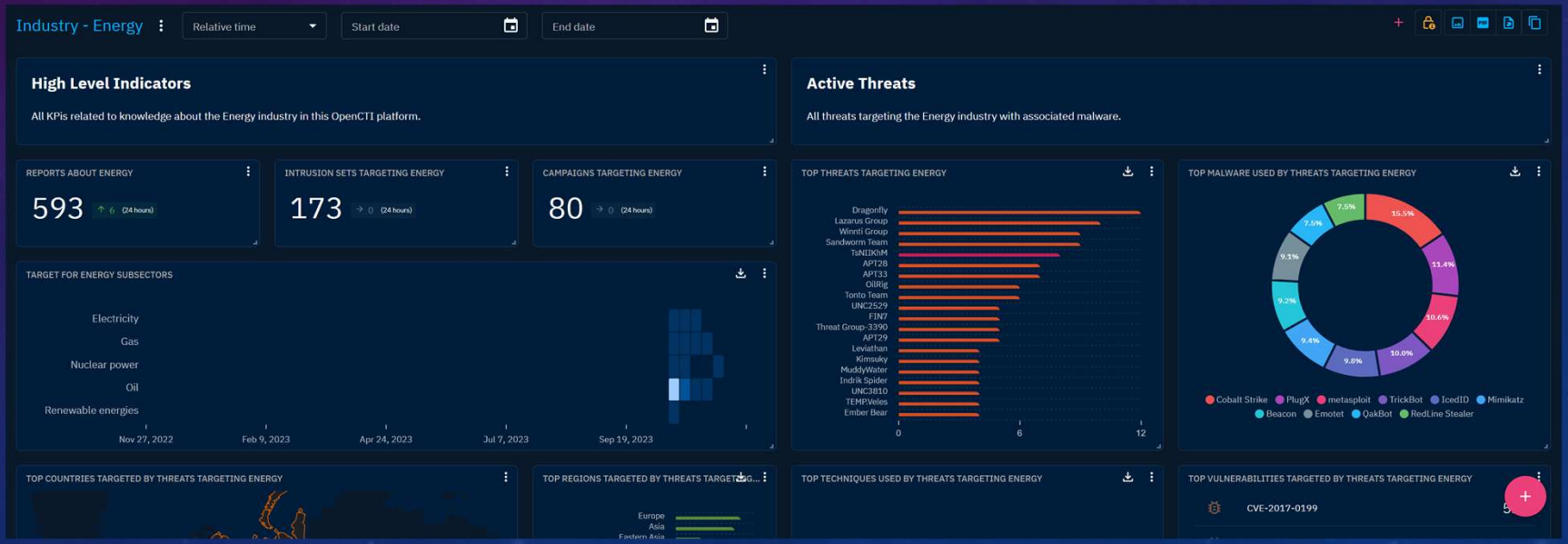
- Universities for research
- Telecom operators for threat data
- NGOs for community outreach

INCIDENT RESPONSE FRAMEWORK

- Clearly defined roles
- Updated contact lists
- Regular tabletop exercises

COST-EFFECTIVE TECHNOLOGY STACK

- Free/open-source solutions
- Low-cost cloud services
- Tailored intel feeds



SUCCESS METRICS

- Fewer serious breaches
- Faster detection times
- Stronger public trust

ROADMAP FOR LEBANON

- **Short term**: quick wins identify CI, basic cyber hygiene, setup OpenSource TI
- **Medium term**: formal intelligence unit, war gaming, inter departmental collaboration
- **Long term**: sustainable synergy, regional collaboration, advanced metrics

First Analysis of Cyber Attacks on Lebanon - 2,500,000 attacks within 21 days

Sunday, 17 April, 2022 Lebanon CERT

Reading time: 3 min | Study

Key element within the set of tools in cyber defense is an early warning system as of Honeypots. Honeypots simulate vulnerable systems or services and trap threat actors, which help estimate their behavior to strengthen the deployed defensive strategy. In this study, we deploy honeypot sensors in Beirut to understand the cyber-attacks that roam around the Lebanese perimeter. Here, the main goal is to detect automated attacks where threat actors apply large scans to identify vulnerabilities and exploit these. The analytics showed that more than 2,500,000 attacks had been performed within 21 days.

Read More

CYBERSECURITY

Final thoughts and Conclusion

03 Secure a Resilient Future

02 Adopt Global Good Practices

01 Align with National Needs

#

EMERGING TECHNOLOGIES

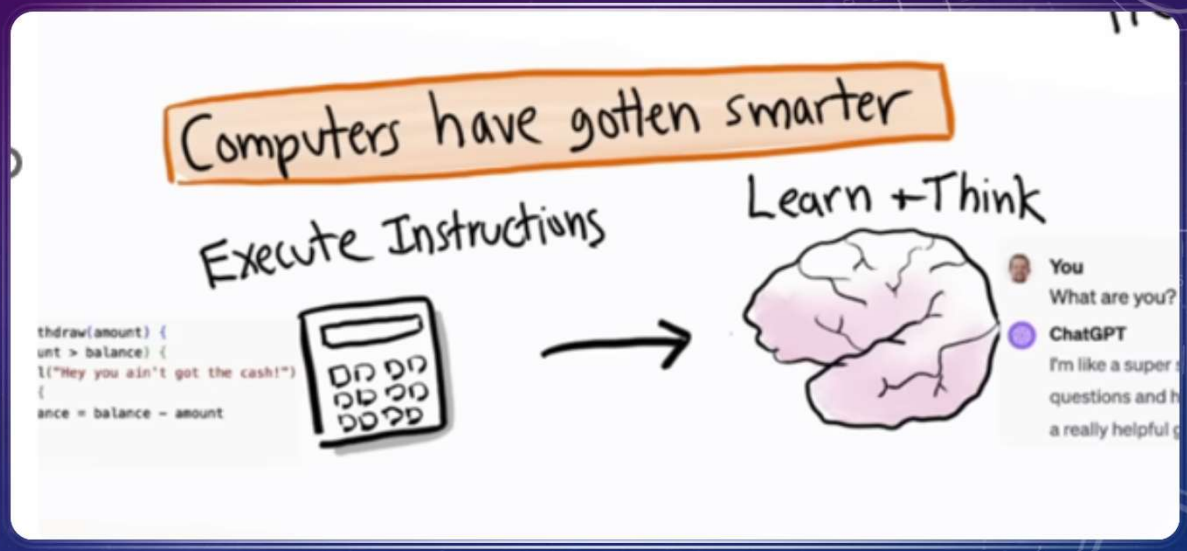
ARTIFICIAL INTELLIGENCE & QUANTUM COMPUTING

CYBERSECURITY AND AI

IDENTIFYING, PRIORITIZING AND MITIGATING AI THREATS

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

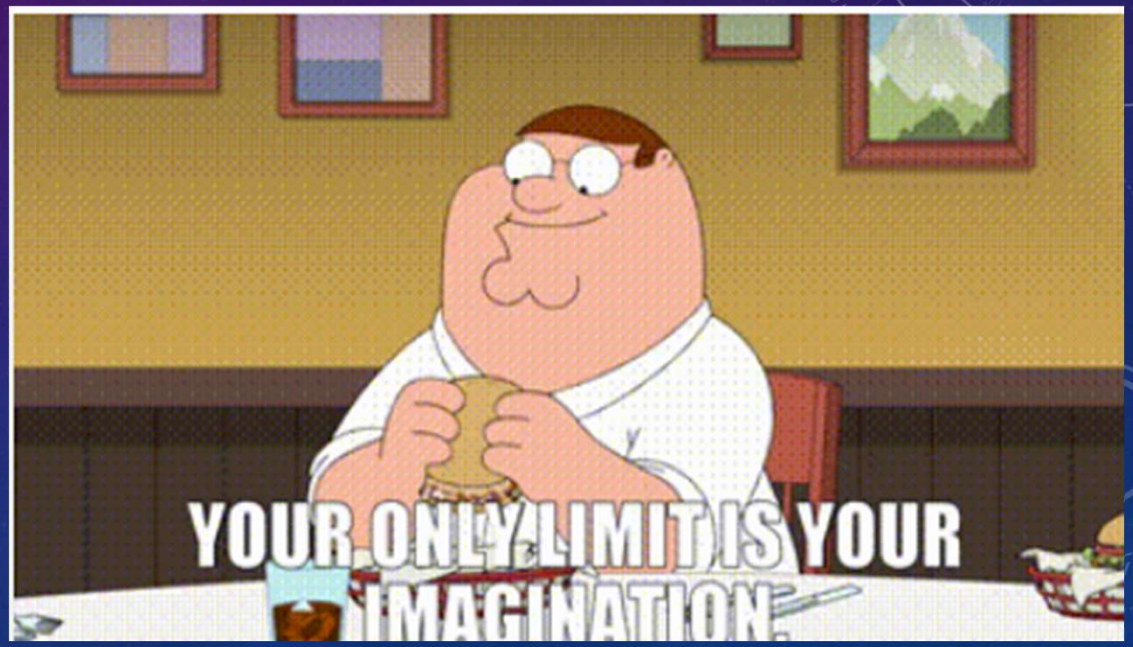
- Prominence of AI
- Predictive AI
- Generative AI
  - Large language models
  - Generative pretrained transformers
- Agentic AI



CYBERSECURITY IMPLICATIONS OF THE USE AND MISUSE OF AI

Like you, threat agents are using AI in their works.

- Identify AI cybersecurity threats
- Governance - strategy and policy
- Security controls



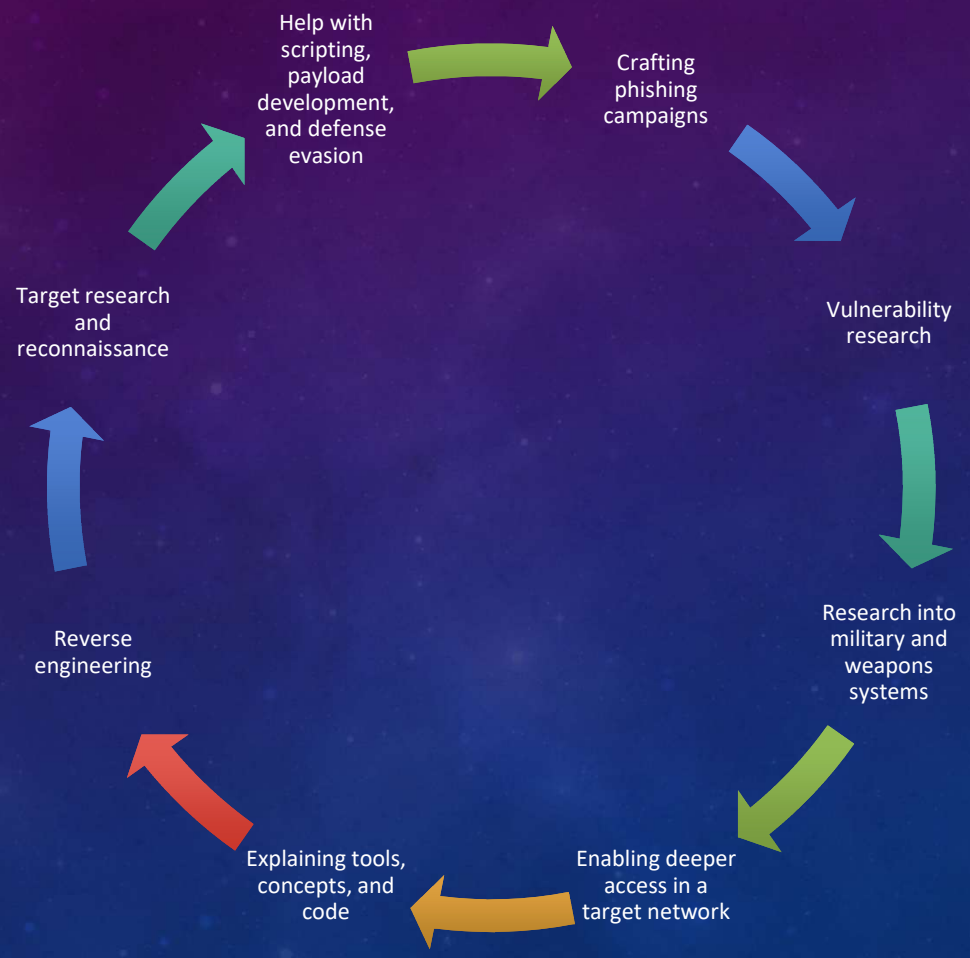
ADVERSARIAL IMPACT OF AI

- **Adversarial impact**: criminals are and will continue to leverage AI in an adversarial manner:
  - Code generation to craft exploit
  - Finding vulnerabilities
- **Defense impact**: the need to defend AI itself from abuse and takeover
- **AI Tooling impact**
  - Firewalls
  - Intrusion Detection Systems (IDS)
  - Intrusion Prevention Systems (IPS)
  - Endpoint Detection and Response (EDR)
  - Network Detection and Response (NDR)
  - Security Information and Event Management (SIEM)
  - Security Orchestration Automation and Response (SOAR)

ADVANCED PERSISTENT THREAT (APT) ATTACKS

- Highly leveraged threat actors
  - Highly resourced criminals
  - State-backed threat actors
- APT threat actors and their use of AI
  - Making creative and advanced use of GenAI in several areas
- Attacks leveraging AI systems
- Attacks against AI systems

TYPICAL USE OF AI BY THREAT AGENTS



AI SECURITY INCIDENTS

Attacks

- Backdoors
- Data poisoning
- Model extraction

Failures

- Data drift
- Discrimination
- Opaqueness

Intentional Abuse

- Ethnic profiling
- AI-enhanced cybercrime
- Killer autonomous bots

Unintentional **Abuse**

MITIGATING THREATS WITH AI

- AI-powered IDS and IPS
- AI for endpoint security
- Behavioral analysis and anomaly detection
- AI-driven threat hunting
- Automated incident response and remediation
- AI against phishing and social engineering attacks

AI USAGE IN CYBERSECURITY DEFENSE

- Threat Detection and Response for Security Orchestration Automation and Response (SOAR)
- Security Policy Optimization
- Code Generation with Static Application Security Testing (SAST) Remediation

AI CYBERSECURITY STRATEGY

AI cybersecurity risk cannot be ignored

Each country must identify the risk associated with AI

Each country must determine and define approach to AI

AI can be useful in AI risk identification, prioritization and mitigation

CYBERSECURITY AND QUANTUM COMPUTING

QUANTUM COMPUTING

Quantum computing - development of computers based on the principles of quantum theory

Using unique behaviors of quantum physics to solve problems that are too complex for classical computing

QUANTUM COMPUTING THREATS

1. Breaking Current Encryption
2. "Harvest Now, Decrypt Later" Attacks
3. Vulnerability of Critical Systems

QUANTUM COMPUTING OPPORTUNITIES

- Post-Quantum Cryptography (PQC)
- Quantum-Resistant Technologies
- Quantum-Enhanced Security

KEY ACTIONS NEEDED

1. Proactive Approach
2. Education and Awareness
3. Continuous Monitoring
4. Quantum-Resistant Technologies
5. Balancing Act