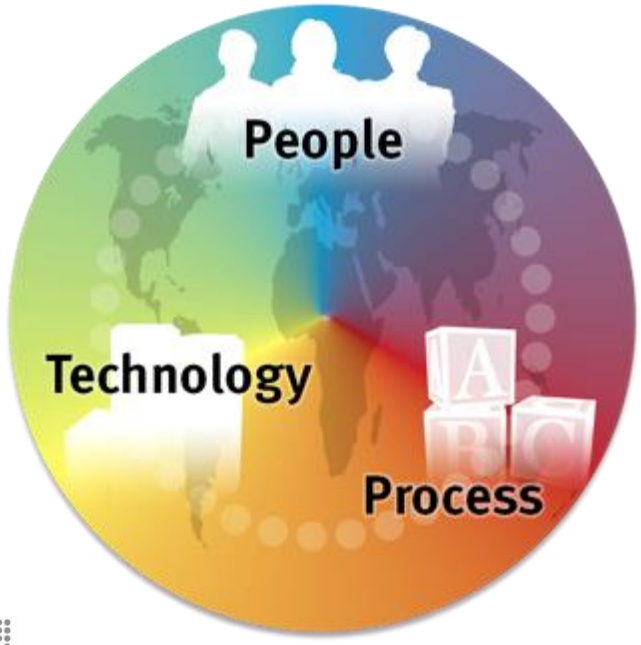
CYBER RESILIENCE IN FOURTH INDUSTRIAL REVOLUTION

Presented by:
Mohamad Firham Efendy Bin Md. Senan
Specialist,
Digital Forensics Department
CyberSecurity Malaysia
firham@cybersecurity.my

A HOLISTIC APPROACH TO CYBER SECURITY

Adoption of holistic approach that **identifies potential threats** and **impacts to the security & public well-being**
AND;
to develop the industry to become **cyber resilience** by having the **capability to safeguard the interests** of its **stakeholders, reputation, brand and value creation activities**



Cyber Resilience is the ability for an organization to resist, respond and recover from threats that will impact the information they require to do business.

People – Process – Technology

People

- Public Awareness
- High Competent People - Certified / Qualified Staff (Internal & External Resources)

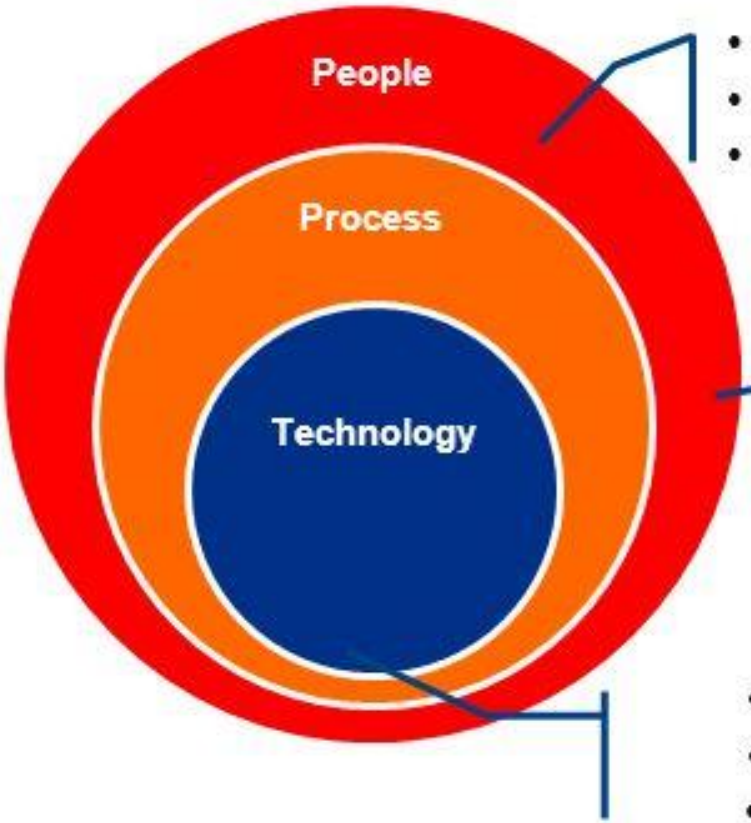
Process

- Policies, SOP and Guideline properly packaged and protected (ie. Intellectual Property such as copyright etc)

Technology

- Latest equipment/tools/software (ie. certified lab)

Cyber Security Defence in Depth



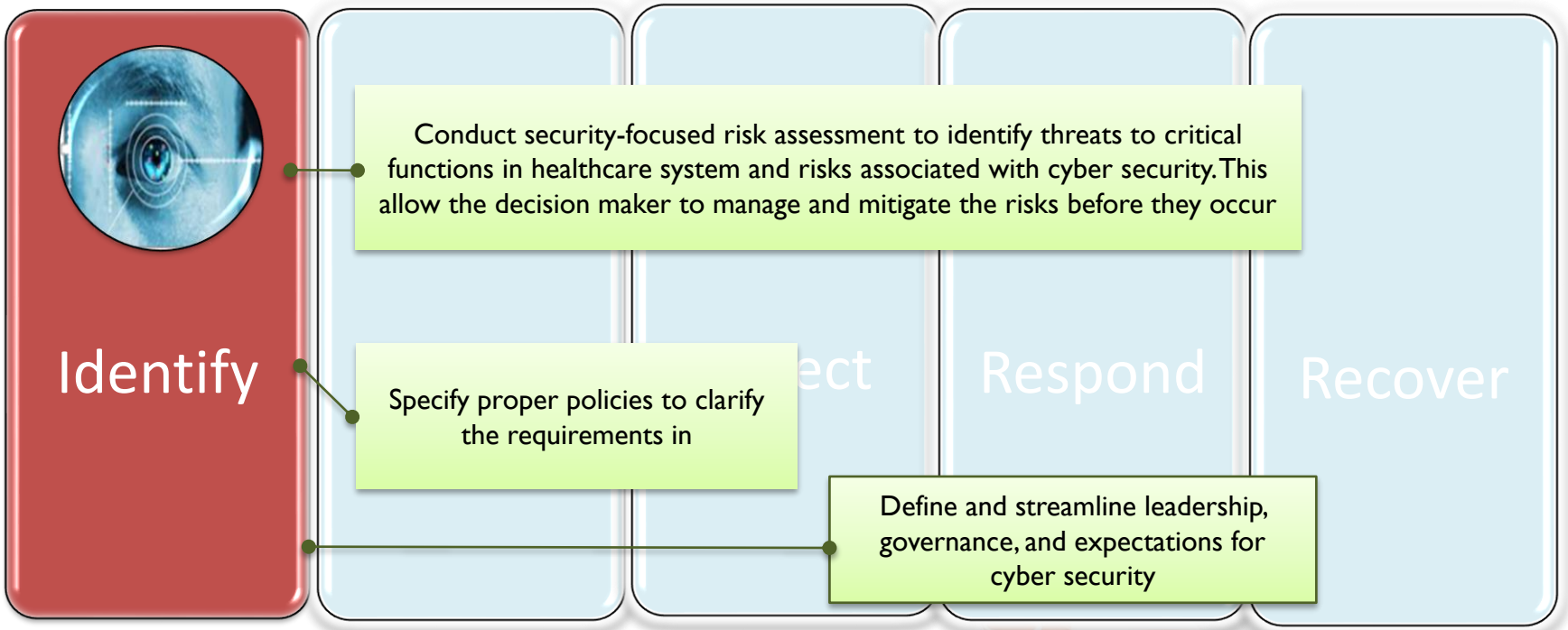
- *Education & Training*
- *Personal Responsibility*
- *Building a Security Culture*

- *Defined Security Policies*
- *Incident Management*
- *Access Control*

- *Network Technology*
- *Patching*
- *Encryption*

Best Practices in Industry 4.0

Best Practices in Industry 4.0 - Identify



Cooperation of both public and private stakeholders working together to enhance cyber security

Best Practices in Industry 4.0 - Protect

Based on the risk assessment results, the decision maker will determine and implement relevant information security controls including establishing relevant policies and installing preventive tools

Employ physical security access controls and protection measures

Protect

Develop secure and private communication networks

People is the weakest link in cyber security chain

- Based on the risk assessment results, appropriate trainings for employees' competency and capability to manage information security are needed
- Raise awareness on cyber threats to all levels of staff including management to address threats from unintentional damage, accidental errors/malfunctions/ failures, disruptions/outages and insider threat
- Engaging in regional or national information-sharing organizations to learn more about the cyber security risks faced by Healthcare services

Cooperation of both public and private stakeholders working together to enhance cyber security

ISO/IEC 27001:2013 Info Security Controls

Requirements	Information security controls	
Clause 4 Context of the organisation	A.5 Information Security Policies	A.13 Communications Security
Clause 5 Leadership	A.6 Organization Of Information Security	A.14 System Acquisition, Development and Maintenance
Clause 6 Planning	A.7 Human Resources Security	A.15 Supplier Relationships
Clause 7 Support	A.8 Asset Management	A.16 Information Security Incident Management
Clause 8 Operation	A.9 Access Control	A.17 Information Security Aspects of Business Continuity Management
Clause 9 Performance evaluation	A.10 Cryptography	A.18 Compliance
Clause 10 Improvement	A.11 Physical and Environmental Security	
	A.12 Operations Security	

CIS - CRITICAL SECURITY CONTROLS

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

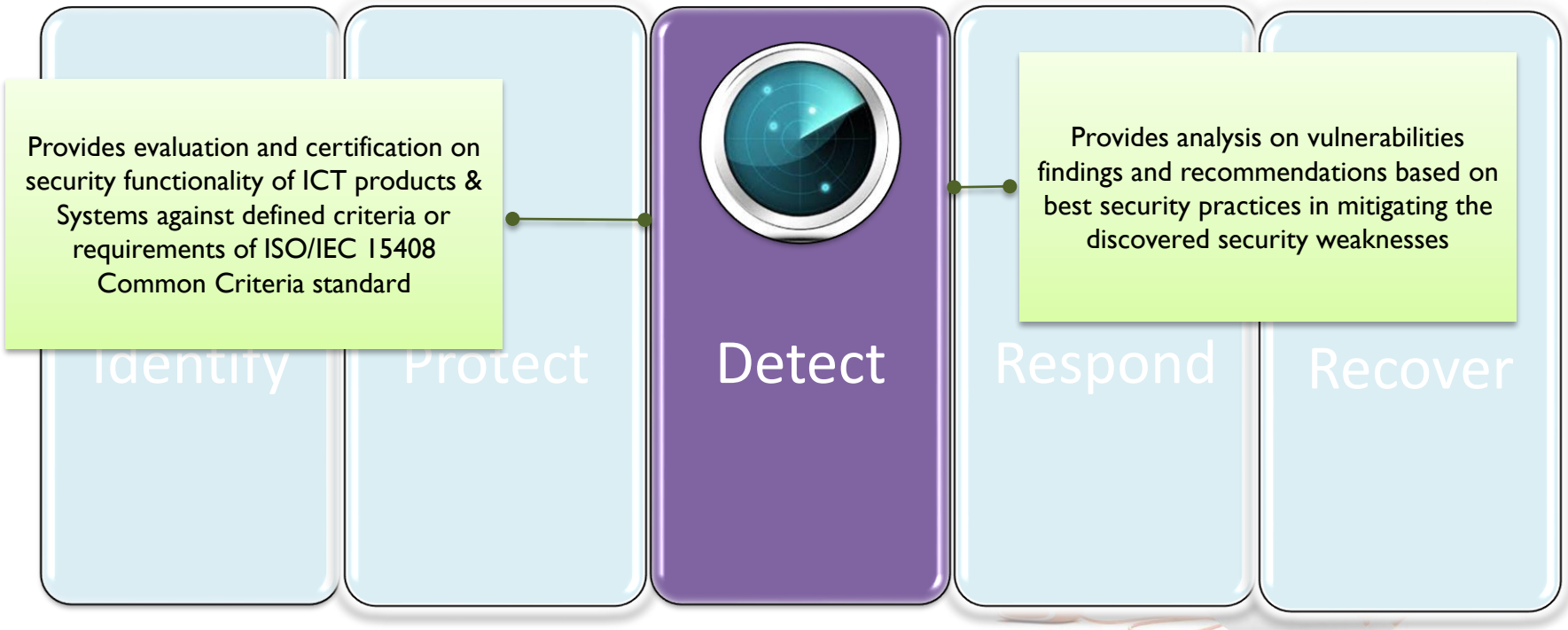
Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Best Practices in Industry 4.0 - Detect



Cooperation of both public and private stakeholders working together to enhance cyber security

CYBER THREAT INTELLIGENCE

ANALYTICS

115+ MILLION
node graph-based analytics engine

340 MILLION
correlation relationships defined

OVER 600 TERABYTES
of analytics storage

212 PETABYTES
sensor traffic analyzed each month

45 BILLION URLS
analyzed each month

DATA SOURCES

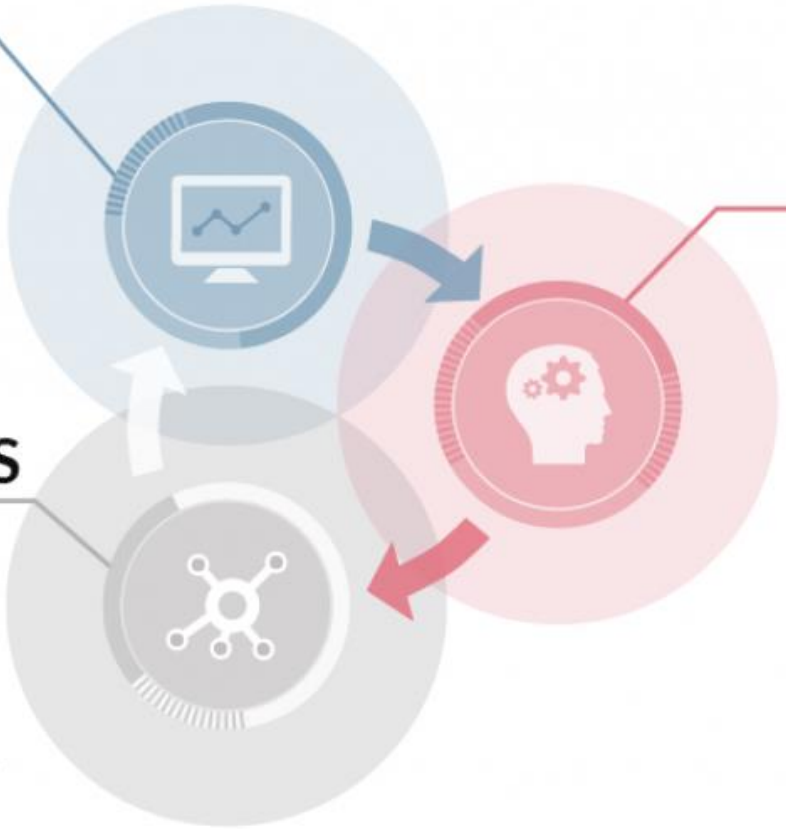
Incident Response
Over 100,000 incident response hours/year

Hundreds of subject matter experts across 16 countries

SENSORS
11 million sensors around the world deployed across 60 countries

24x7x365 visibility through 6 worldwide SOCs

THREAT ANALYTICS
Billions of events processed each day



INTELLIGENCE

DETECTION
Identify threats that other solutions miss
7 million attacks detected each month

Discovered 19 out of 36 zero days

PROACTIVE
Stay a step ahead of the attacker by understanding motivations and techniques

delivered across 40 technology partners

40+ targeted industry profiles

RESPONSE
Answer key questions and prioritize threats based on attacker context

30+ advanced threat actors tracked

300+ advanced malware families tracked

10+ nation-state threat sponsor profiles

Ref: VPN Reviews

ALERT LOGIC®

DOMAINTOOLS

IBM Security

Infocyte®

Raytheon

sqrrl

STEALTHbits TECHNOLOGIES

KEY SECURITY CHALLENGES

The survey results reveal that cybersecurity professionals prioritize detection of advanced threats (55 percent) as the top challenge for their SOC. Lack of expert security staff to mitigate such threats (43 percent) rose to second place.

Notably, lack of confidence in automation tools catching all threats (36 percent), jumped from fifth place in last year's survey to third today.

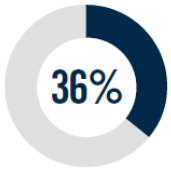
Which of the following do you consider to be top challenges facing your SOC?

55%

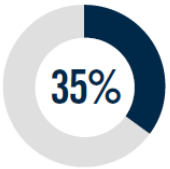
Detection of advanced threats (hidden, unknown, and emerging)

43%

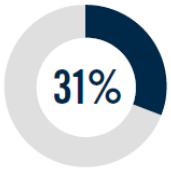
The lack of expert security staff to assist with threat mitigation



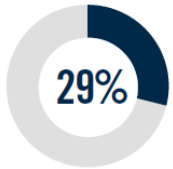
Lack of confidence in automation tools catching all threats



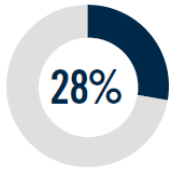
Too much time wasted on false positive alerts



Slow response time to find or detect advanced threats



Working with outdated SIEM tools and SOC infrastructure



Lack of proper reporting tools

Other 7%

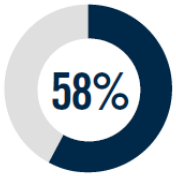
THREAT INDICATORS

Understanding Indicators of Compromise (IOCs) allows organizations to develop effective defense methodologies that help with rapid detection, containment, and denial of future exploits. Knowing what IOCs to look for aids cybersecurity professionals in threat triage and remediation.

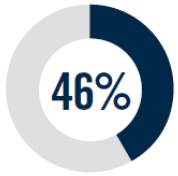
Our research reveals that hunt teams most frequently investigate behavioral anomalies (67 percent), followed by IP addresses (58 percent), and tied for third are both domain names and denied/flagged connections at 46 percent.

What kinds of indicators are most frequently investigated by your hunt team?

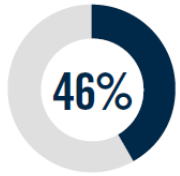
67% Behavioral anomalies (unauthorized access attempts, etc.)



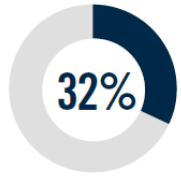
IP addresses



Domain names



Denied/flagged connections



File names

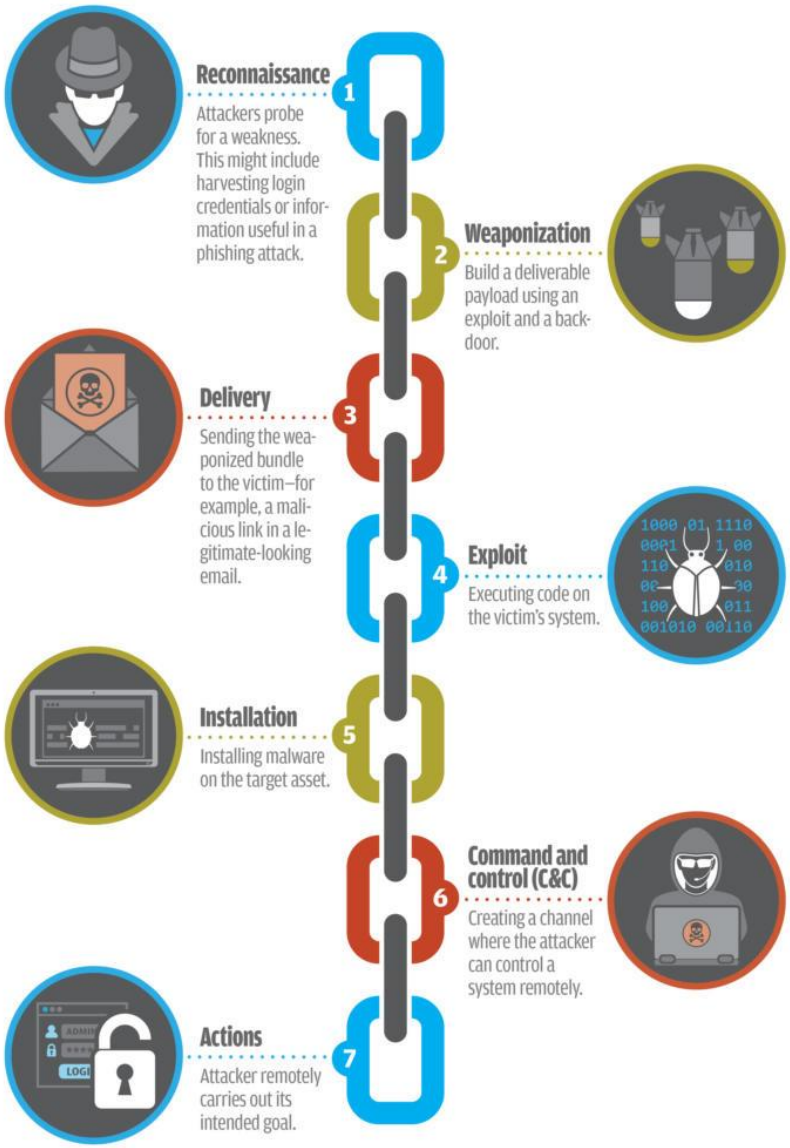
Not sure/Other 24%

A New Paradigm For Cyber Threat Hunting

Monday, June 11, 2018 Mohit Kumar

What is the CYBER KILL CHAIN?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.



RECONNAISSANCE

WEAPONIZATION

DELIVERY

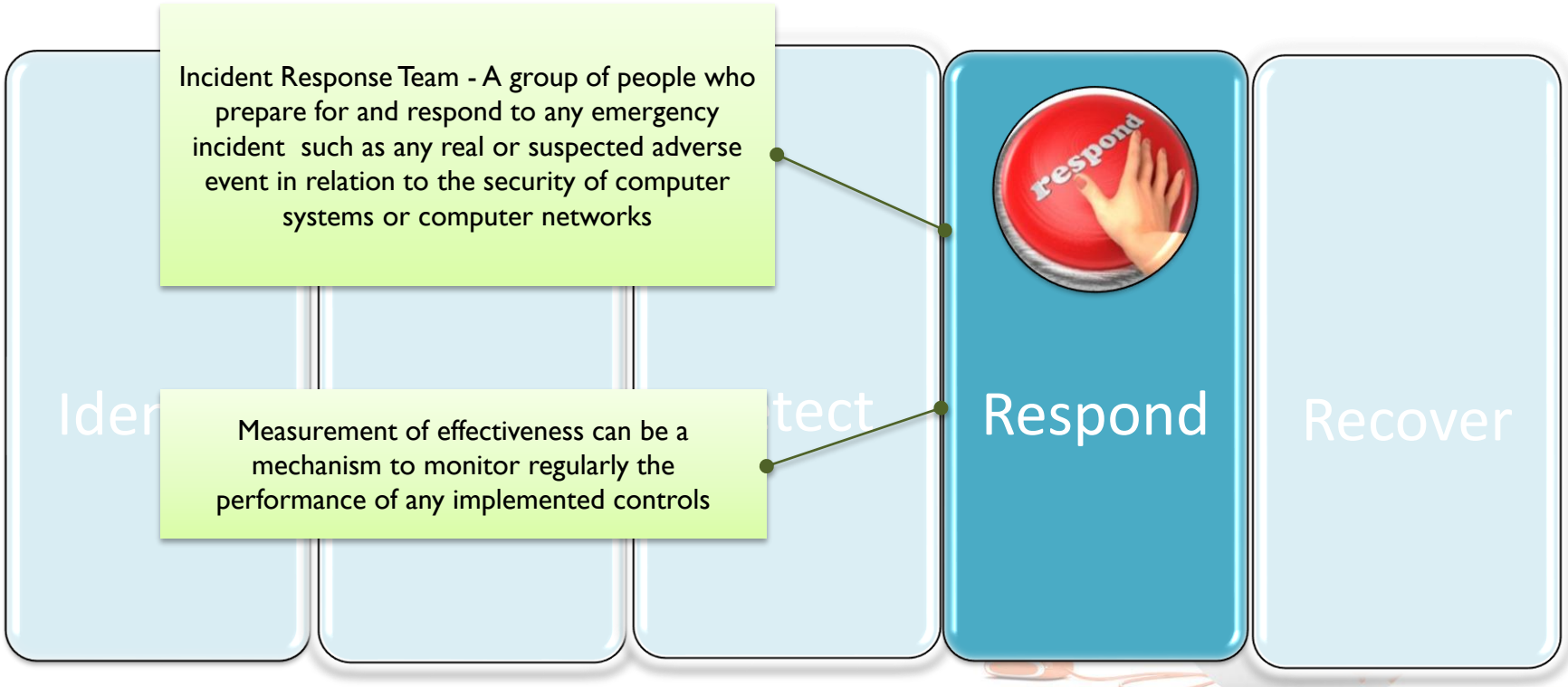
EXPLOIT

INSTALLATION

COMMAND AND CONTRO (C&C)

ACTIONS

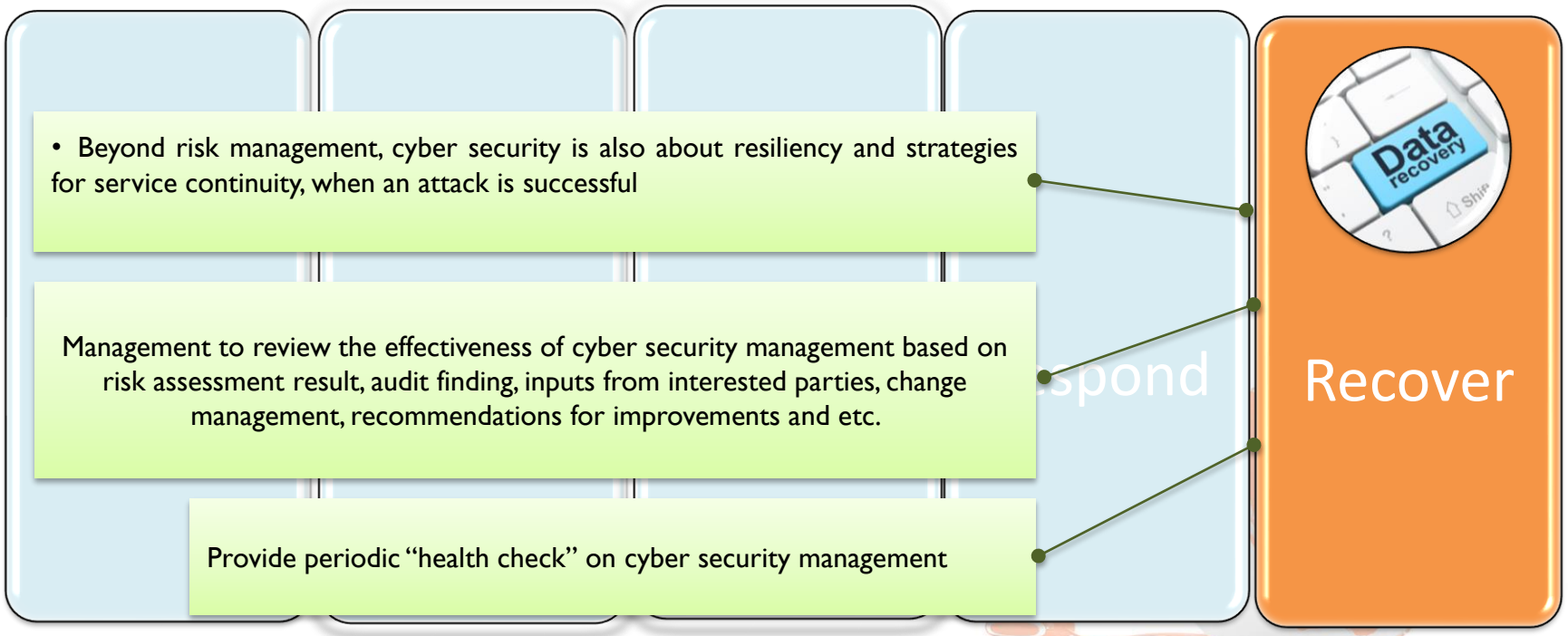
Best Practices in Industry 4.0 - Respond



Cooperation of both public and private stakeholders working together to enhance cyber security

RESPONSE: SYSTEMS WILL BECOME MORE INTELLIGENT AND INTEGRATED – THE RISE OF "EXPERT SYSTEMS"

Best Practices in Industry 4.0 - Recover

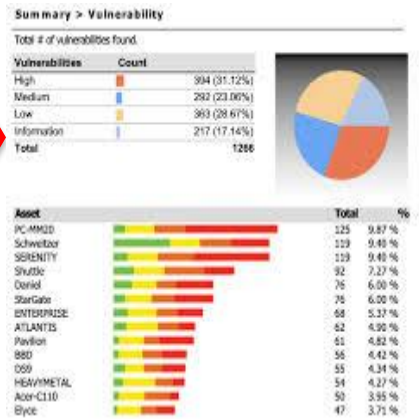


Cooperation of both public and private stakeholders working together to enhance cyber security

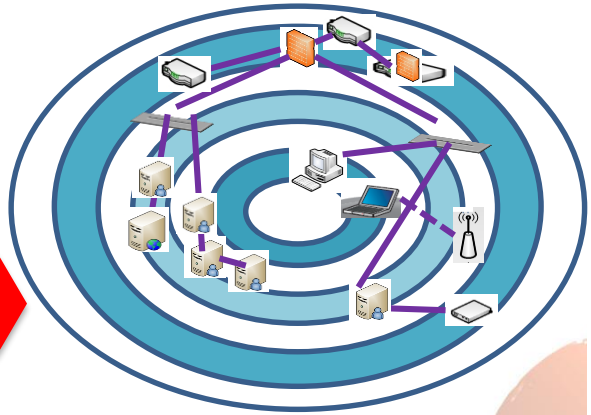
Process Assurance - Vulnerability Assessment & Penetration Testing (VAPT)

VAPT provides in-depth analysis of vulnerabilities and recommendations based on best security practices in mitigating the discovered security weaknesses

(1) Detect known vulnerabilities and potential exploits/ security flaws



(2) Provide vulnerability impacts level to assist organisation for corrective action plan



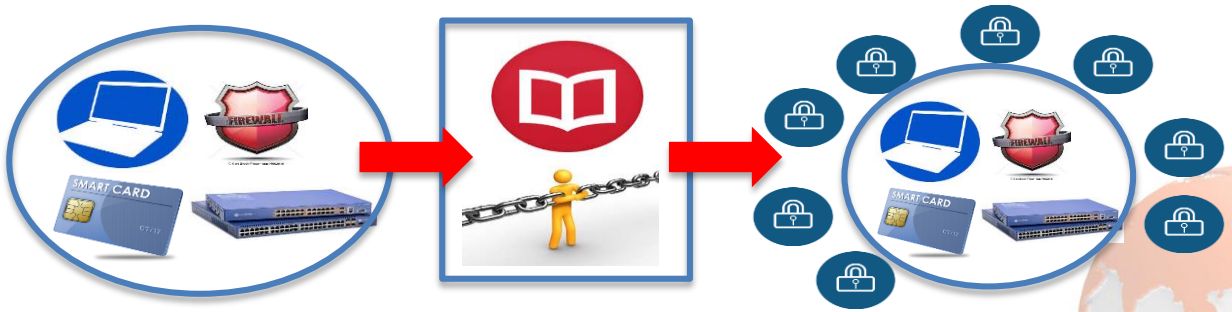
(3) Provide specific remediation to eliminate the attack vectors

(4) Evaluate effectiveness of security controls and procedures to meet the minimum ICT infrastructure security baselines

ICT Products & Systems Assurance

MySEF lab is MS ISO/IEC 17025 accredited.

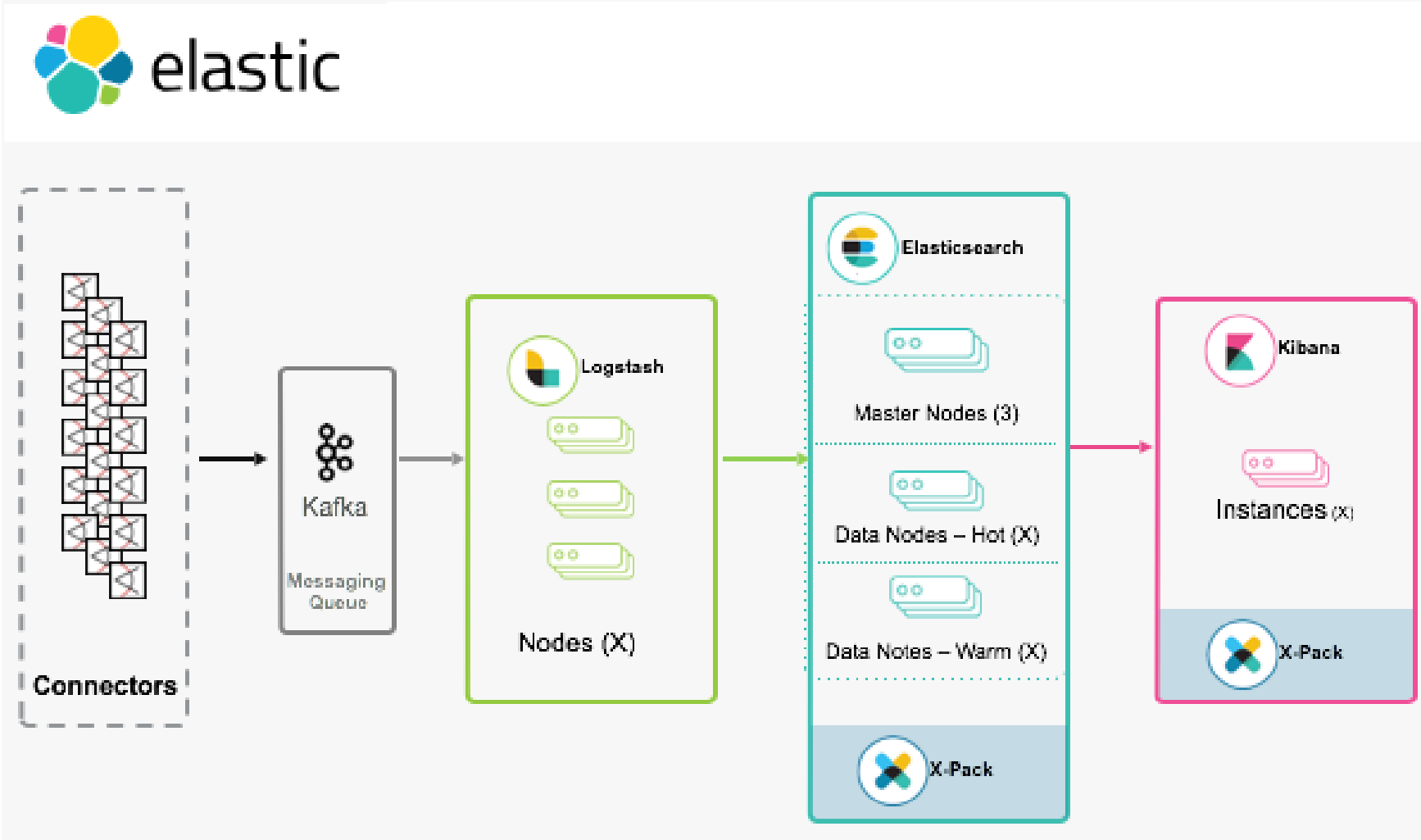
Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme provides a systematic process for evaluating and certifying the security functionality of ICT products & systems against defined criteria or requirements of ISO/IEC 15408 Common Criteria standard



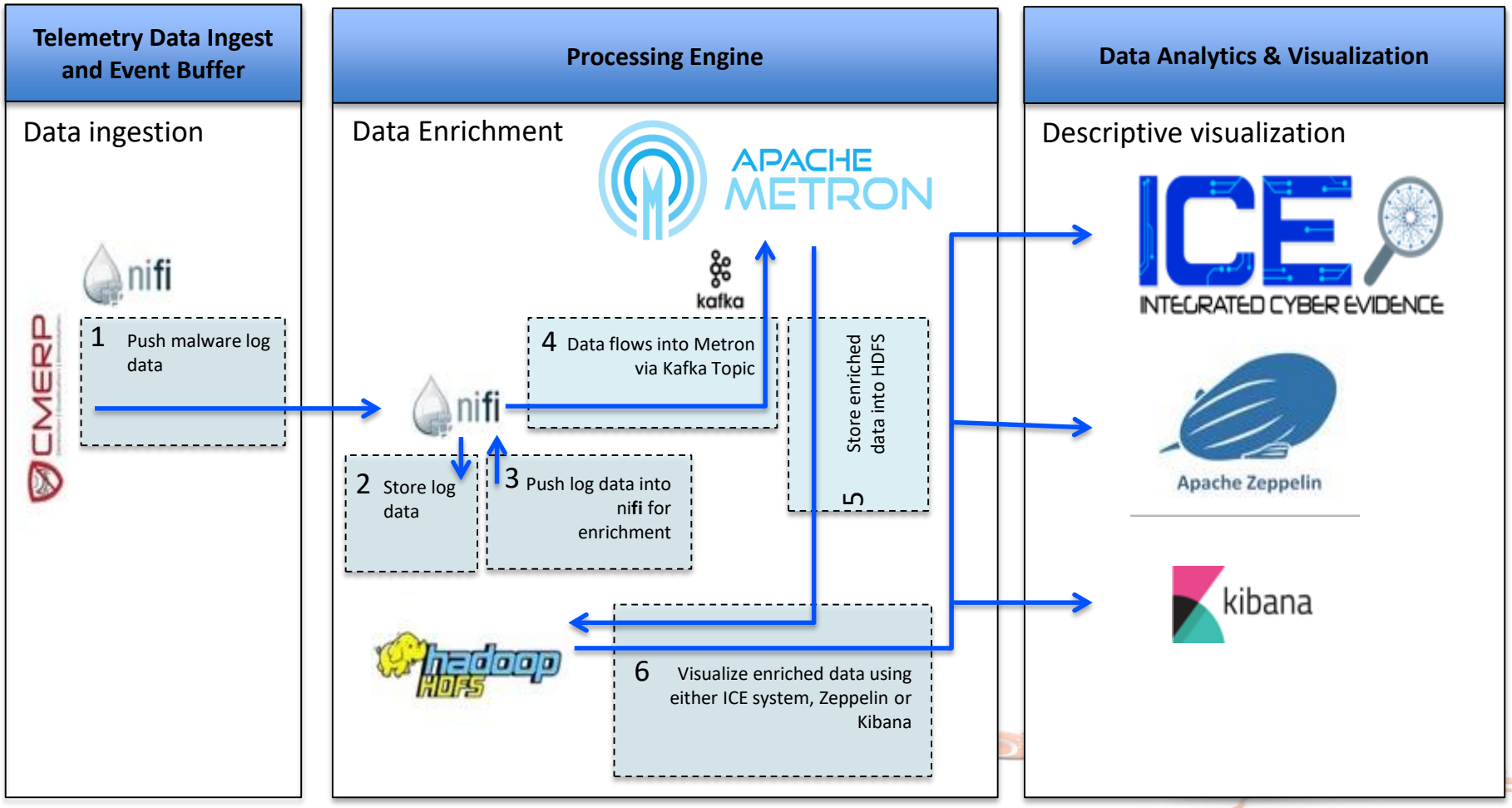
Detection and eradication of security flaws discovered on product, system or life cycle development during evaluation

Improvement during evaluation in terms of development and maintenance activities can avoid creating vulnerability to the product or system

SIEM With ELK Stack

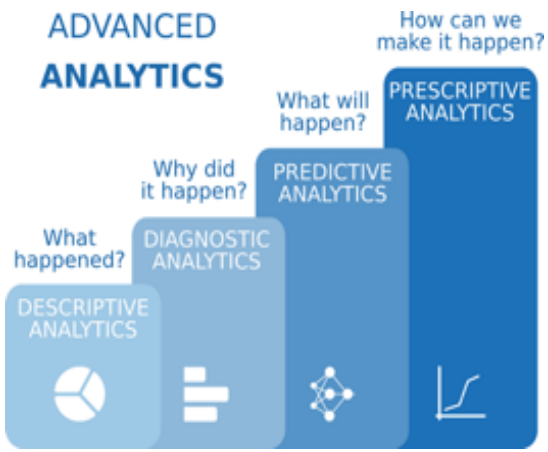


ICE - Integrated Cyber Evidence



Cyber I3 - Intelligence + Incident + Investigation

CyberI3
Hunt The Hunter



SERVICES	Cyber Security (Threat and Physical)
	Intelligence / Incident / Investigation
FACILITIES	Information Security Operating Center
	xForensik : Evidence Preservation Tool
POLICIES & GUIDELINES	Standard Operating Procedure
	Best Practices
	Standard and accreditation
POLARIZATION	Certification
	Learning
	Awareness
	Assessment
	Consultation

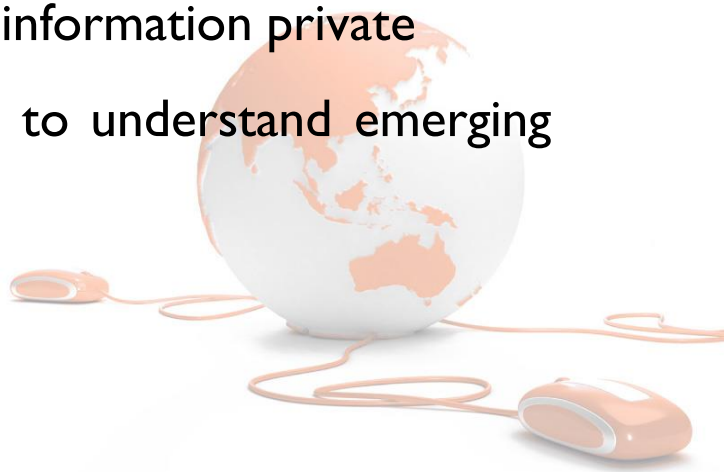
The Last Mile Of Security

AI and automation to perform an integrated expert security system:

- Device vulnerabilities
- Device misconfiguration
- Automatically rank devices

Take a Way Key Points

- Adopt more evolutionary & innovative cyber security measures through identify, protect, detect, respond and recover approaches
- Human factor is a key to good cyber security thus, it has to be managed well
- Embed resilience in systems and infrastructures
  - Process assurance i.e. CTI, Threat Hunting, ISMS, VAPT
  - ICT products evaluation and certification i.e. Common Criteria
- Everyone in the Industry 4.0 ecosystem must constantly remain vigilant about protecting data and keeping confidential information private
- Keep abreast new and advanced technologies to understand emerging threats



Thank you

Corporate Office
CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888
F : +603 8992 6841
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

www.facebook.com/CyberSecurityMalaysia
twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy