

---

# Cyber Threats

## How do we Handle them ?

---

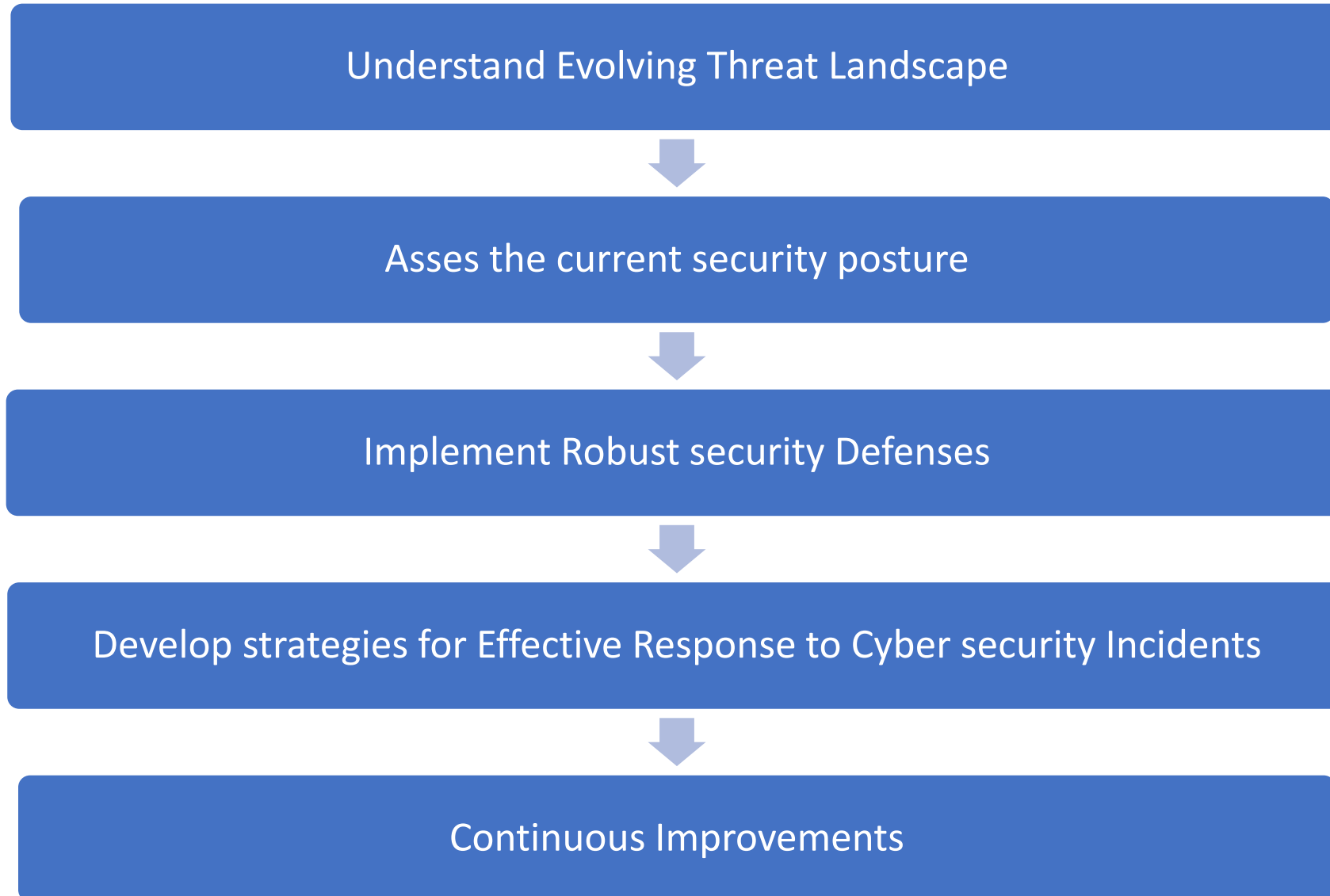
APTLD 86 – Da Nang - Vietnam

Ruwan Maldeniya  
LK Domain Registry – Sri Lanka

- 



# Our Approach for Building Cyber Resiliency



# Modern-Day Cyber Threats

## Insider Threat

Authorized individuals use their knowledge to harm the organization, either intentionally or unintentionally.

## Social Engineering

Manipulating human Trust & Emotions, non technically, to gain access, information or valuables through persuasion.

## Malware Attack

Malicious software sneaks into a computer, system or a network to potentially harm or interrupt the system.

## Ransomware

A malicious software which encrypts data/information or the entire system & hold them as hostage for a ransom payment.

## Mobile device compromise

Malicious code or unauthorized access turns your trusted mobile device into a data-stealing spy

## AI-powered Cyber Threats

Use analytical & adaptive capabilities of AI to craft cyberattacks that bypass traditional defences.

## Zero-Day Exploits

A cyber attack which target an unknown vulnerability of a software or a system to gain access / harm the system.

# Implementing Robust Security Defenses

## ❑ Defense In Depth / Layered security

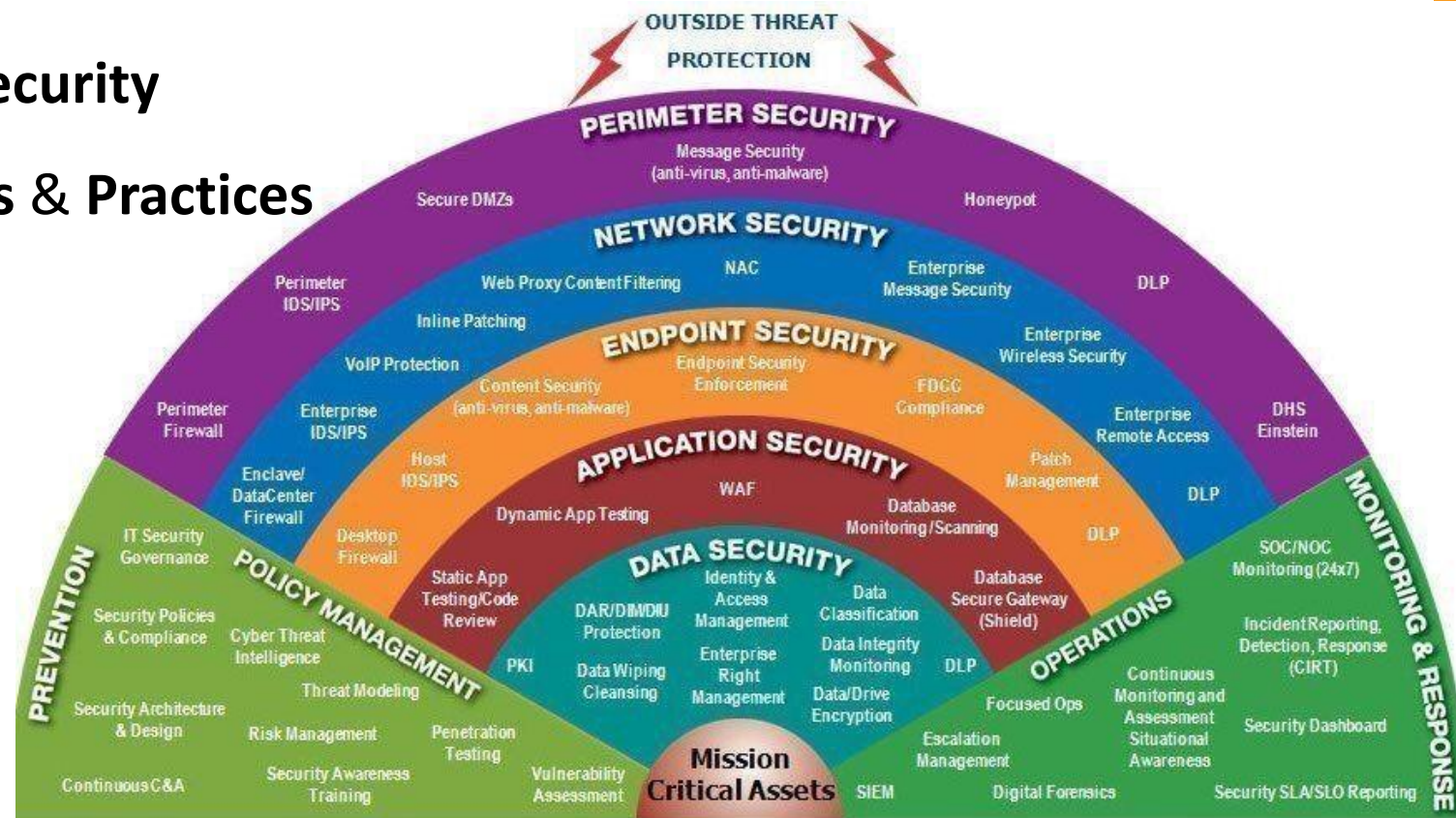
### ➤ Multiple Security Products & Practices

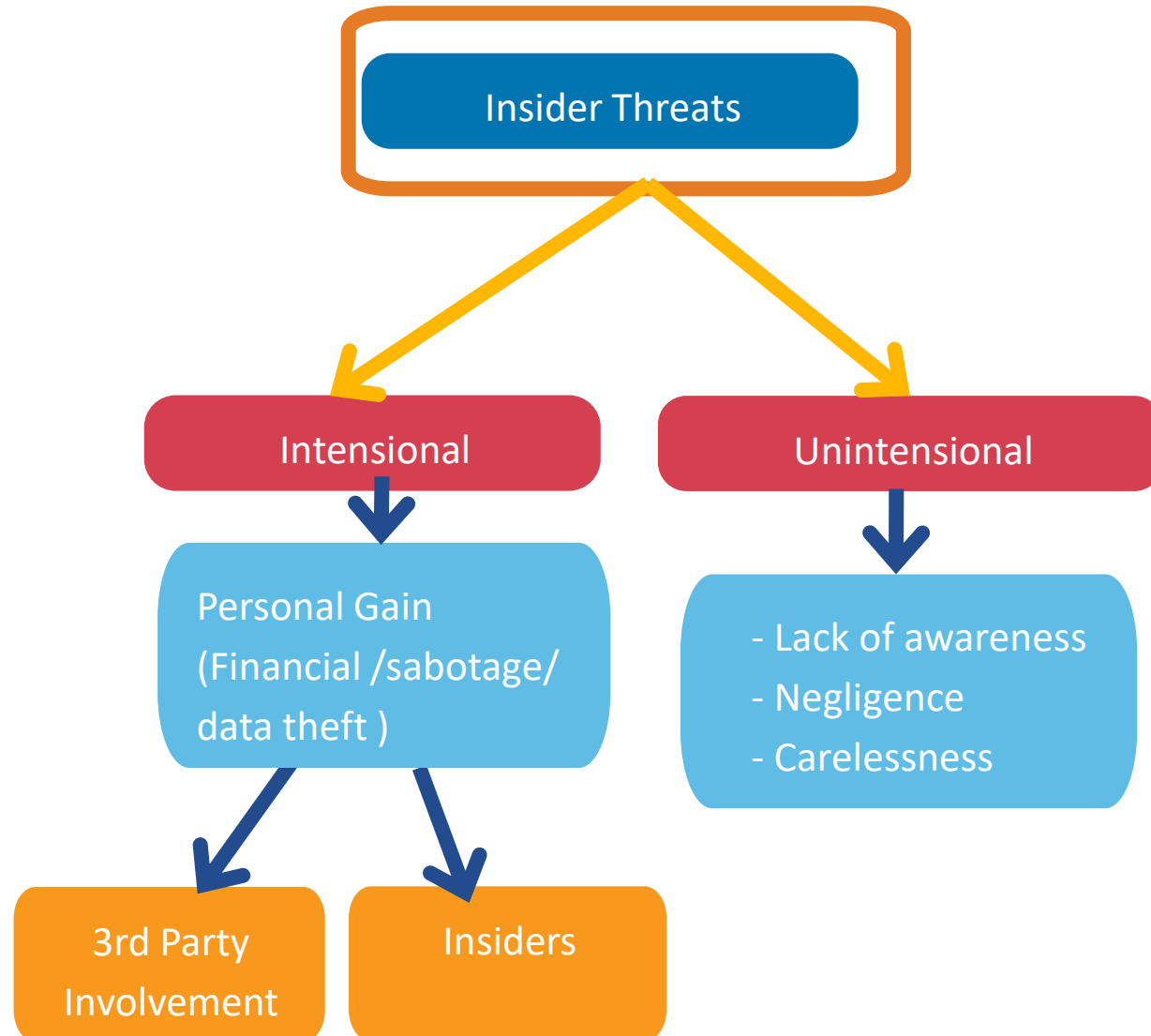
#### Products

- Perimeter Firewalls / Data centre Firewall
- Web Application Firewalls (WAF)
- Intrusion Detection/Prevention (IDS/IPS)
- DDOS Protection
- EDR

#### Practices

- Network Segmentation
- Multifactor Authentication (customers , employees)
- Least privilege Access
- Backup strategy (off-line/off-site backup )
- 24X7 SOC/NOC monitoring





## *Caused by;*

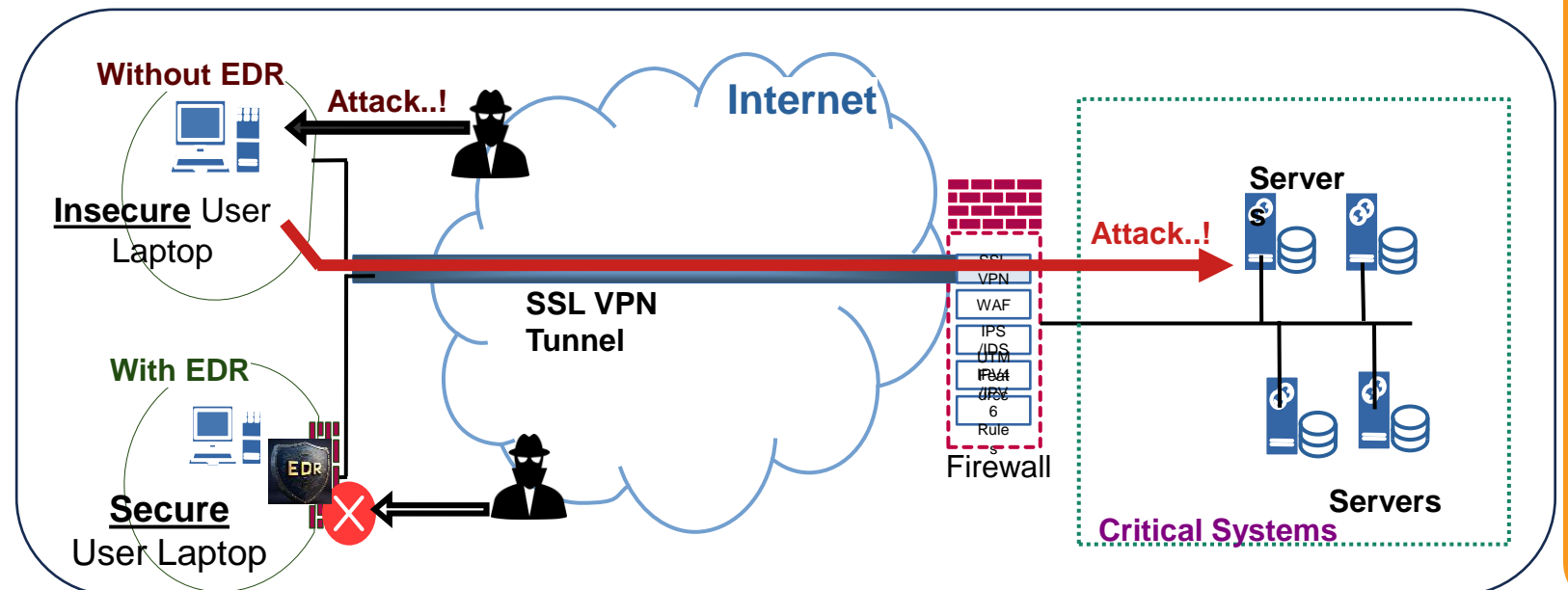
- Malicious intent
- Third-party involvement (e.g., contractors or vendors with access).
- Negligence

## Impact

- Data Theft / Leak
- Sabotage
- Reputational Damage
- Spying (espionage )
- Resource Misuse

# Mitigating Insider Threats

- ❖ Create user awareness
- ❖ Security training for staff
- ❖ End point Detection and Response systems implementation



## ***Focus:***

- **Evaluate effectiveness of security measures**
- **Identify vulnerabilities & Weaknesses**



**Informed decisions to enhance overall Security Posture**

- Conducting a security assessment once is often insufficient.
- Regular security assessments should be conducted as appropriate based on the threat profile.
  - *Quarterly / Bi-annually / Annually as appropriate*
- Use scanner tools for automated assessments

## **Different Types of Assessments**

- Automated & Manual Assessments
- Blackbox, Greybox, and Whitebox Assessments
- Internal and External Teams

## **Regular Assessments performed**

- ❖ External/Internal Vulnerability Assessments
- ❖ Web application Assessments
- ❖ Penetration Tests



## ❑ ISO27001 Information Security Management System implementation

- Policies

- Procedures

*eg: User Access Control , Quarterly Access review Audit*

- Risk Register

## ❑ Provide Framework for implementing security controls

## ❑ Worth engaging with implementation even with no intention ISO certification

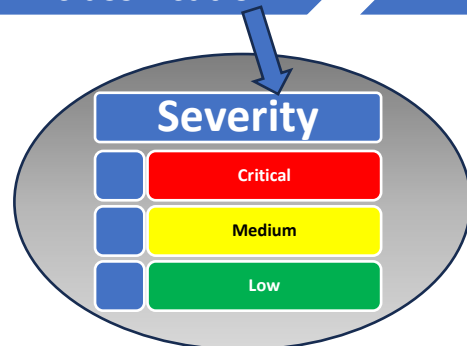
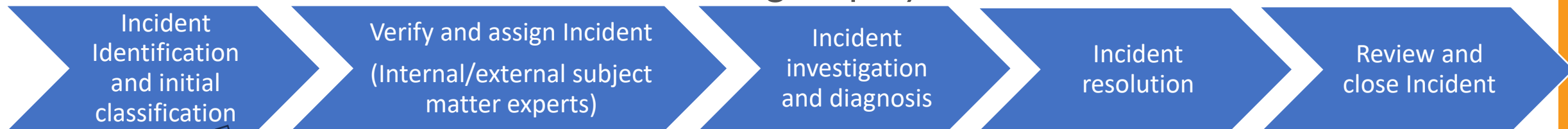
# Incident Response

**Incident :** adverse event/occurrence that poses risk to confidentiality, integrity, or availability of information systems, networks, or data.

Eg: Unauthorized Access/ Malware Infections / Phishing Attacks /Denial-of-Service (DoS) Attacks /Data Breaches,..etc.

## Incident Response

- Established Process in-line with ISO27001
- Conduct drills to create awareness among employees



- ✓ Build a Robust defense system using combination of various **Tools ,Practices, and Proactive measures.**
- ✓ Consider Defense in Depth Strategies
- ✓ 24X7 SOC (Security Operation Centre ) for monitoring is essential
- ✓ Establish Policies / Procedure / Practices based on Frameworks such as ISO27001
- ✓ Consider Insider Threats
- ✓ Be prepared to **Respond** promptly & effectively to Cyber **Security Incidents**
- ✓ Create User awareness – Regular training of staff on cyber security

# THANK YOU!