

Presentation

Ransomware



By: Thabo Sebola

What is Ransomware

- ❖ Cybercrime has transformed in both sophistication and scale, with ransomware standing out as one of the most devastating digital threats. The aims to create awareness about ransomware's methods, its financial and operational consequences, and its specific risks to South African government systems and infrastructure.
- ❖ The concept of ransomware dates back to the 1989 AIDS Trojan, distributed via floppy disks. In the past decade, ransomware incidents have increased exponentially with major strains like CryptoLocker, WannaCry, Ryuk, and DarkSide targeting healthcare systems, municipalities, and government agencies worldwide
- ❖ WannaCry (2017): Affected over 200,000 systems globally, including public hospitals.
- Colonial Pipeline (2021): Led to a fuel supply disruption in the US.
- ❖ **RANSOMWARE** is another type of malware which is design to encrypt files or even the entire disk and making them inaccessible.

encryption is to convert information or data into code.

For the victim to get his/her data back a payment/ransom is demanded by the attacker, that is why it is called "Ransomware" –you have to pay a ransom hence it is called a Ransomware

How Ransomware Works

- ❖ Ransomware typically spreads through:
 - Malicious email attachments and links (phishing).
 - Exploitation of remote desktop services (RDP).
 - Drive-by downloads from compromised websites.
- Once active, it encrypts files or locks systems and demands payment for data restoration.

How would you see that you have been attacked

- ❖ Once your computer is infected with ransomware, you will not have access to your data.
- ❖ Your screen will be left with such message and a link re-directing you to payment of the ransom:



Impact of Ransomware Attacks

- ❖ Financial losses through ransom payments and operational disruptions.
 - Downtime in essential services like healthcare, municipal operations, and public safety systems.
 - Loss of sensitive citizen and government data.
 - Reputational damage and public mistrust.
 - Non-compliance penalties under laws like South Africa's POPIA.

Rise in cyber-attacks in South Africa

South Africa has seen an increase in ransomware incidents due to growing digital adoption, limited cybersecurity budgets, and inadequate public awareness. Government organizations and municipalities remain high-value targets given the sensitive data they hold and the essential services they provide.

VICTIM	DATE OF INCIDENT	NATURE OF INCIDENT
Transnet	Jul-21	Ransomware attack
Department of Justice and Constitutional Development (DoJ & CD)	Sep-21	Ransomware attack
Department of Defence (DOD)	Starting in 2022	Data breach with extortion threat
Companies and Intellectual Property Commission (CIPC)	Starting from 2021	Data breach with extortion threat
International Trade Administration Commission of South Africa (ITAC)	Jan-24	Ransomware attack
Government Pensions Administration Agency (GPAA)	Feb-24	Data breach with extortion threat
National Health Laboratory Service (NHLS)	Jun-24	Data breach with extortion threat
South African Weather Service (SAWS)	Jan-25	Ransomware attack

These incidents paint a worrying picture of how vulnerable South Africa is to cyber criminals

Hanno Labuschagne (3 February 2025), South Africa under attack, <https://mybroadband.co.za/news/security/580762-south-africa-under-attack.html>

Prevention Best Practices

User Awareness

- ❖ Train staff to recognize phishing and social engineering attacks.
- ❖ Run simulated phishing tests regularly.
- ❖ Never use unknown USB stick/storage devices
- ❖ Be careful with public Wi-Fi

What to do when you have been attacked?

Should You Pay the Ransom?

No, paying is not recommended because there's no guarantee you'll get your data back.

It funds cybercrime and encourages further attacks.

You may be targeted again. Instead, invest in prevention, response planning, and tested backups.

Prevention Best Practices

Technical Controls

- ❖ Install Anti-Virus solution and keep it updated.
- ❖ Regularly update and patch systems.
- ❖ Use strong, unique passwords and enforce MFA.
- ❖ Limit user privileges and network segmentation.
- ❖ Deploy endpoint protection and anti-ransomware tools.
- ❖ Disable RDP if not needed or secure it with MFA and IP whitelisting.

Backup Strategy

- ❖ Implement 3-2-1 backup rule (3 copies, 2 media types, 1 off-site).
- ❖ Ensure backups are immutable or offline to prevent ransomware from encrypting them.
- ✓ Active monitoring and incident response protocols. (where SITA offers SOC services)

The SOC Portfolio and Catalogue

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

IMPROVE

The SOC Platform

- Methodology
- Cyber and Threat Intelligence
- Cyber security analysis
- Threat Hunting
- Merging

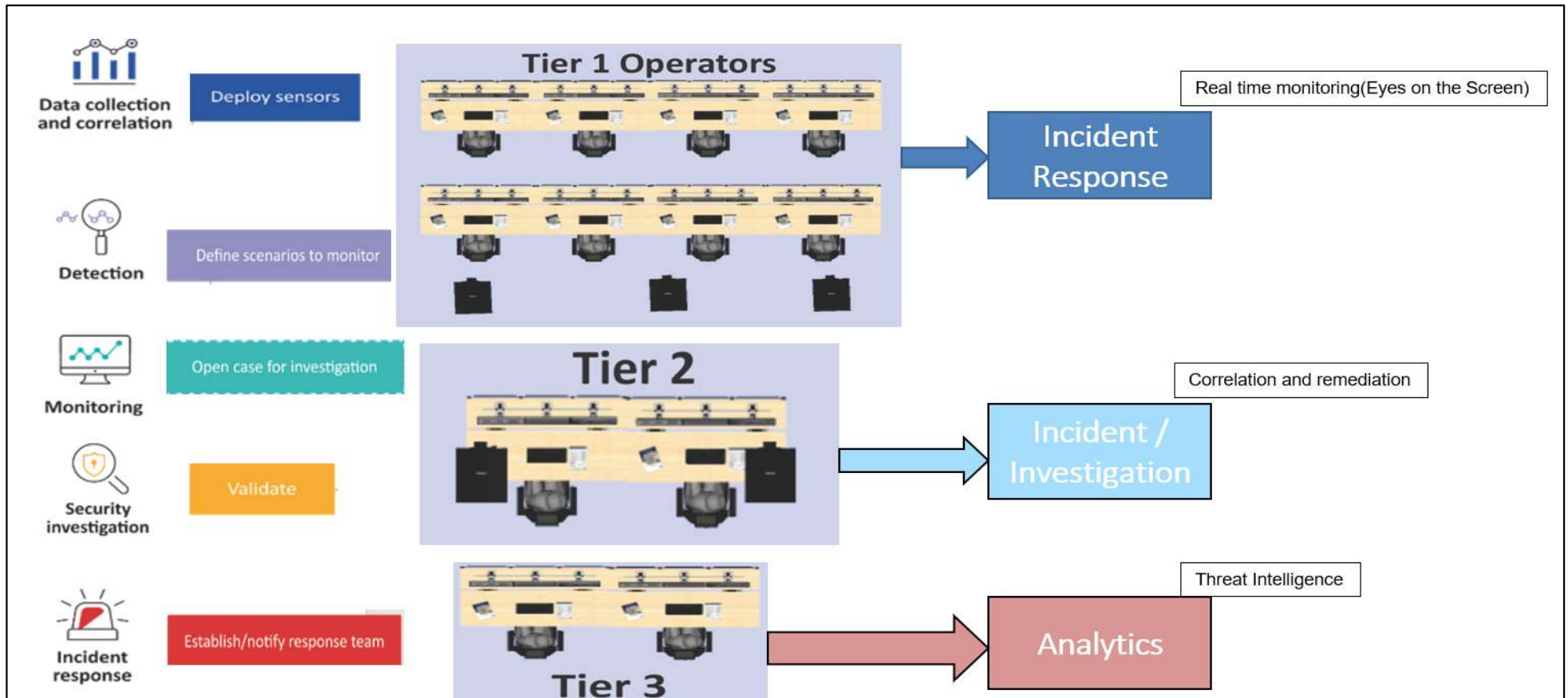
Managed Detection and Response

- Security Incident monitoring and response
- Security Investigation and Escalation
- Security Incident Mitigation
- Security Incident Remediation
- Recovery and Improvement

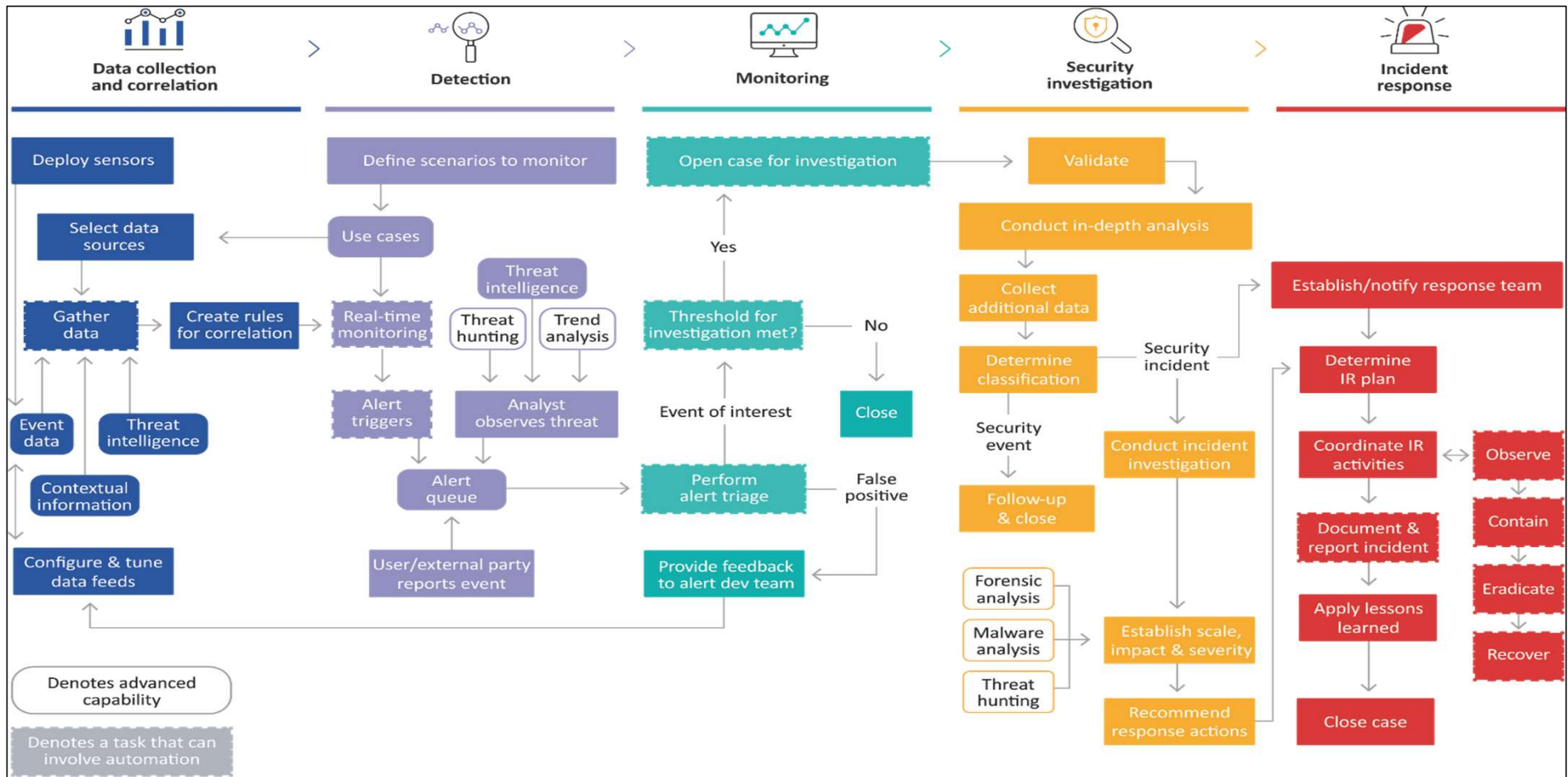
Secure Operations

- Vulnerability Management
- PENTESTING
- Awareness
- Training
- Ethical Hacking

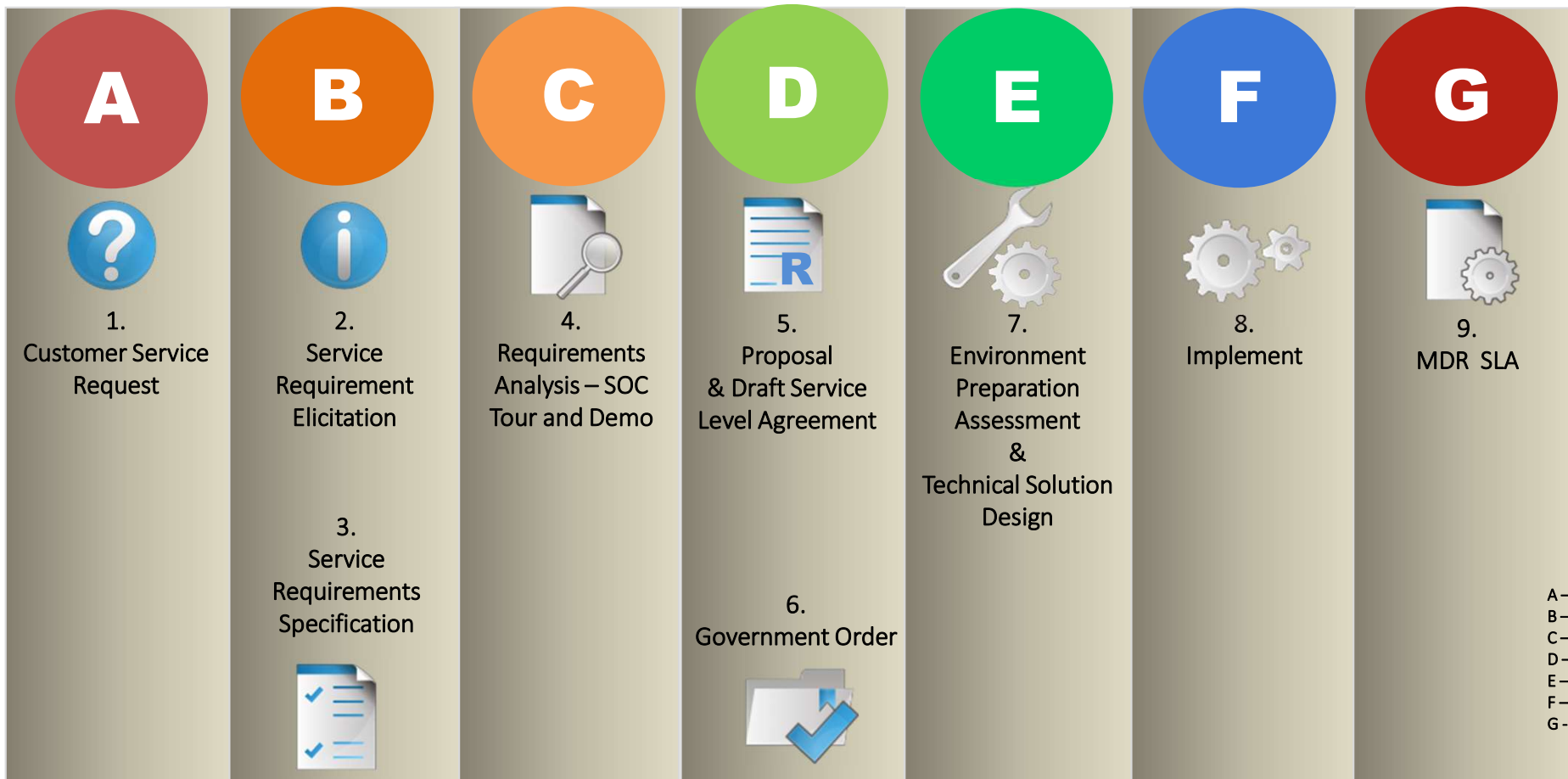
The SOC People



The SOC Process



Business Engagement Process - Managed Detection and Response



Who is responsible for information security?

The answer is simple:
Information Security is the
responsibility of **ALL** employees.



THANK YOU

