

Gov-X Innovation Challenge 2021

Cyber Security & Threat Landscape

Niel van Rooyen

Head: Information Security(CISO)





Niel van Rooyen

Cyber Security & Threat Landscape

Background:

With 15 years experience in ICT and Cyber Security space, within the private sector ranging from mining, retail, manufacturing and telecommunication industries, I believe better collaboration between all of these industries and governments specifically around Cyber Security, we will start gaining the required knowledge and have the necessary edge against the ever evolving requirements and threat actors in the "Cyberspace".





Cyber Security & Threat Landscape

- Threat Landscape
- Challenges for Incident Management



1.

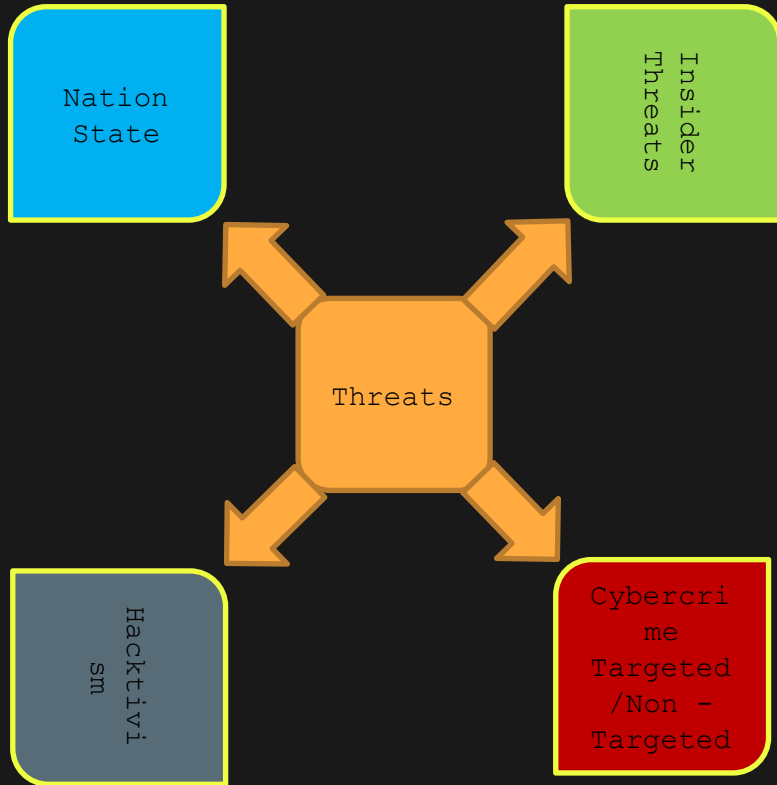
Threat Landscape

Explaining/Understanding Risks



Threat Types

Relevant for any industry



Cybercrime - Most common, main goal is monetization

Nation State - depending on company profile can be espionage, intellectual property theft, sabotage

Insider Threat - monetization, sabotage / revenge

Hacktivism - indirect target for a political / social statement



Advanced Threat Actors

Advanced persistent threat landscape in 2020

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

According to their data, in 2020 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:

- 1 Government
- 2 Banks
- 3 Financial Institutions
- 4 Diplomatic
- 5 Telecommunications
- 6 Educational
- 7 Defense
- 8 Energy
- 9 Military
- 10 IT companies

Top 12 targeted countries:

- Chile
- Mexico
- Brazil
- France
- UK
- Turkey
- India
- Russia
- China
- Japan

Top 10 significant threat actors:

- | | |
|--------------------|---------------------|
| 1 Lazarus | 6 StrongPity |
| 2 DeathStalker | 7 Sofacy |
| 3 CactusPete | 8 CoughingDown |
| 4 IAmTheKing | 9 MuddyWater |
| 5 TransparentTribe | 10 SixLittleMonkeys |



[apt.securelist.com](https://securelist.com)



Ransomware

- MSP`s Reported downtime costs 94% higher than in 2019 & an astonishing 486% higher than 2018
- Nearly 20% of MSP`s reported SMB`s was forced to pay ransoms
- Consequences resulting from ransomware attacks:
 - 62% - loss of business productivity
 - 39% - business-threatening downtime
 - 28% - lost data and/or device
 - 24% - decreased customer profitability
 - 19% - clients paid the ransom and recovered data
 - 17% - damaged reputation
 - 13% - stolen data
 - 10% - hackers threatened to publicize data if ransom went unpaid
 - 6% - report ransomware remained on system and struck again
 - 6% - failure to meet SLA requirements
 - 4% - failure to achieve regulatory compliance
 - 4% - paid a ransom but data was never released
- Survey results show that MSPs understand that the damage associated with business downtime is far more costly than the actual ransom.

Ooops, your important files are encrypted.

If you see this text, then your files are no longer available. They have been encrypted. Perhaps you are busy looking for your files, but don't waste your time. Nobody can recover your files without a decryption service.

We guarantee that you can recover all your files safely. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

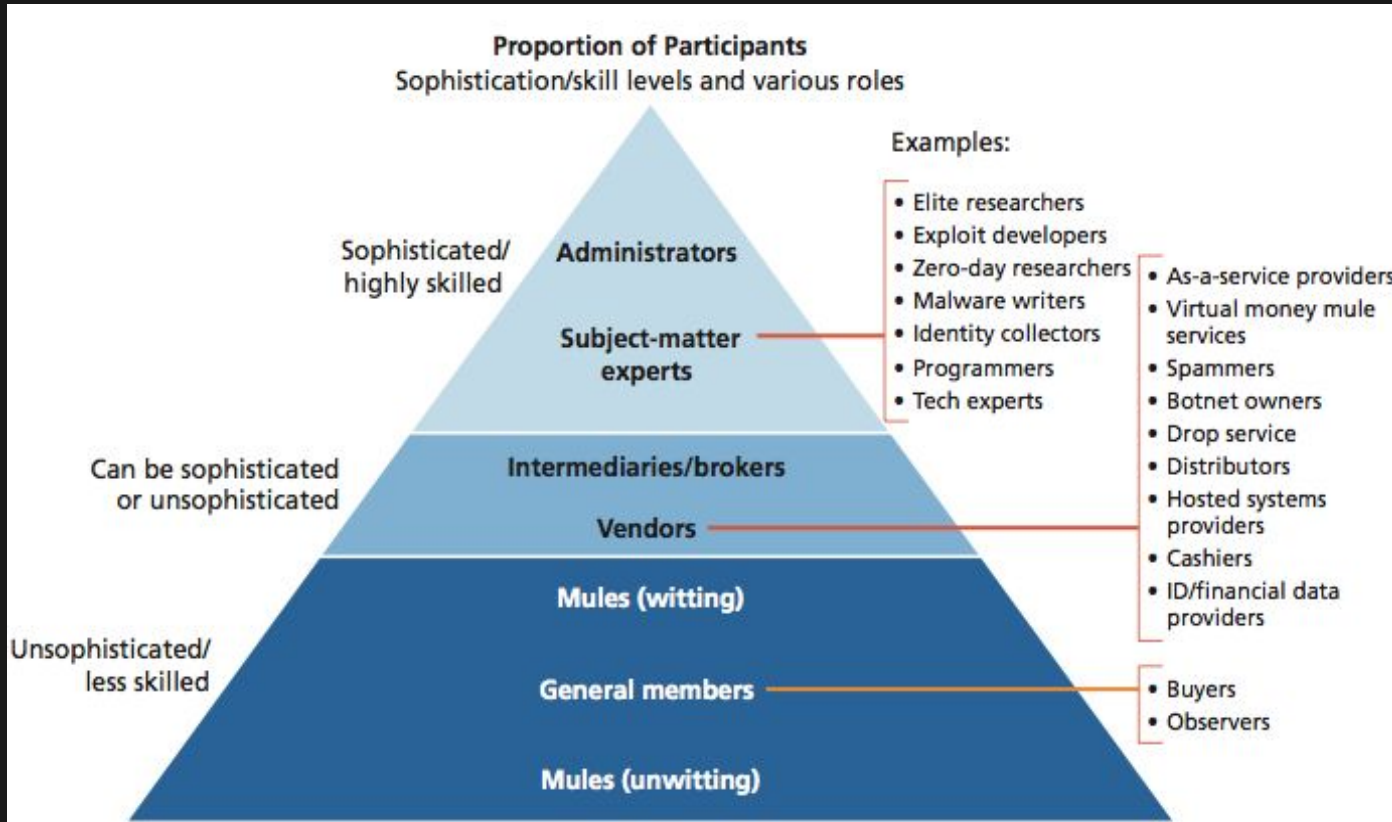
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to: howsmith123456@posteo.net. Your personal installation key is:

74f296-2Nx1Gm-yHQrWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kl

If you already purchased your key, please enter it below:
Key: _

CyberCrime

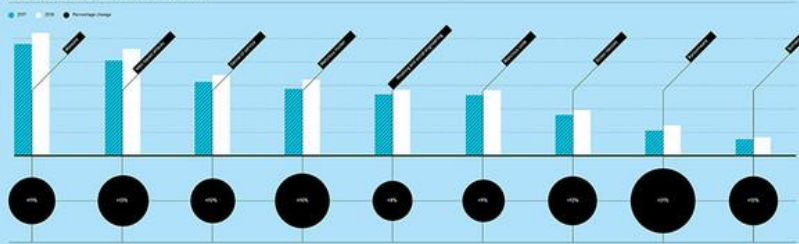


CyberCrime

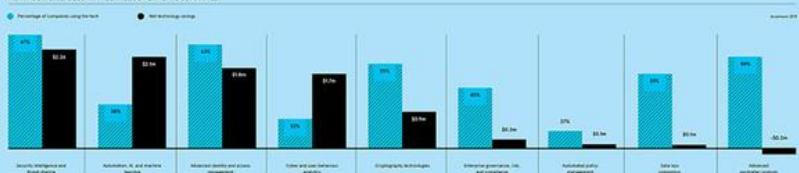
THE REAL COST OF CYBERCRIME

Cybercrime can impact an organisation's reputation, customer base and ability to function, but the cost of poor cybersecurity is never clearer than when looking at the money companies stand to lose

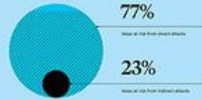
AVERAGE ANNUAL COST OF CYBERCRIME BY TYPE OF ATTACK



HOW MUCH CYBERSECURITY TECHNOLOGY CAN SAVE COMPANIES



GLOBAL VALUE AT RISK FROM DIRECT AND INDIRECT CYBERATTACKS, CUMULATIVE 2019 TO 2023



CYBERCRIME COSTS AROUND THE WORLD

Average annual cost of cybercrime by region in billions of dollars

\$27.4m

\$13.6m

\$13.1m

\$11.5m

\$9.7m

\$9.3m

\$9.3m

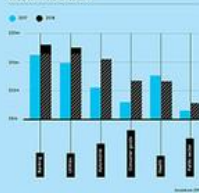
\$8.1m

\$8m

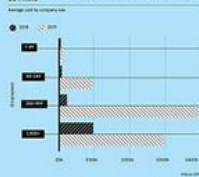
\$7.2m

\$6.8m

AVERAGE ANNUAL COST OF CYBERCRIME BY INDUSTRY



COST OF LARGEST SINGLE CYBERATTACK TO EUROPEAN AND US FIRMS



TIME SPENT INVESTIGATING FRAUD CAN COST MORE THAN THE FRAUD ITSELF

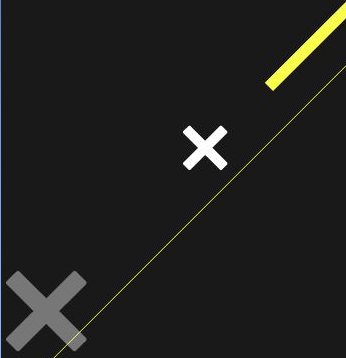
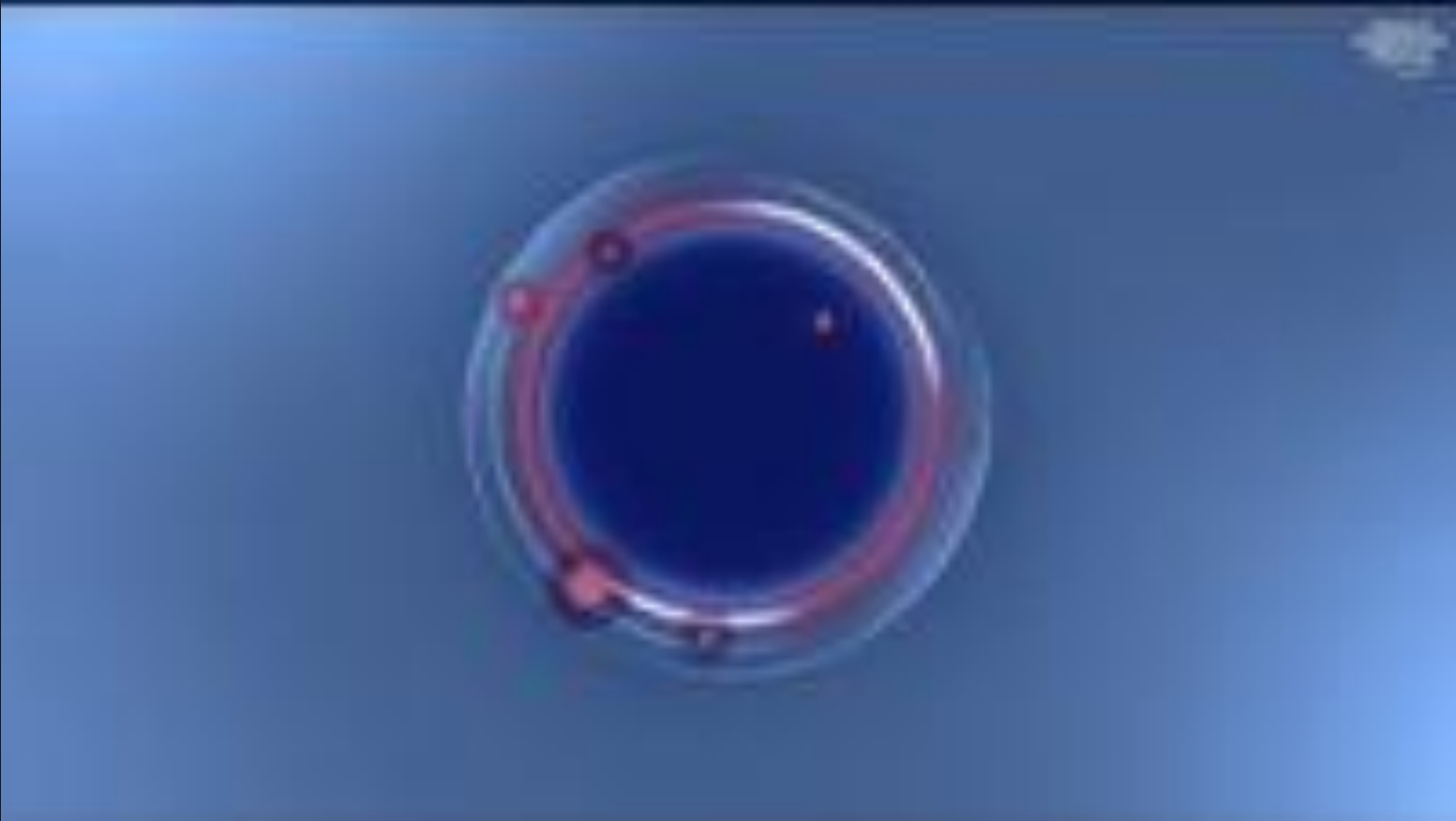


RACONTEUR

- Malware
Major consequence: Information Loss
Average cost: \$1.4M (54% of total losses)
- Web-based attacks
Major consequence: Information Loss
Average cost: \$1.4M (61% of total losses)
- Denial-of-Service (DOS)
Major consequence: Business Disruption
Average cost: \$1.1M (65% of total losses)
- Malicious insiders
Major consequences: Business Disruption and Information Loss
Average cost: \$1.2M (\$0.6M each, 75% of total losses)



CyberCrime Impact Explained: Covid-Like Characteristics



**// If you spend more on coffee than on
IT Security, you will be hacked.
What`s more, you deserve to be
hacked //**

- Richard Clarke



2.

Challenges for Incident Management



The Real Impact of Incidents

Source: Beneath the surface of a Cyber Attack

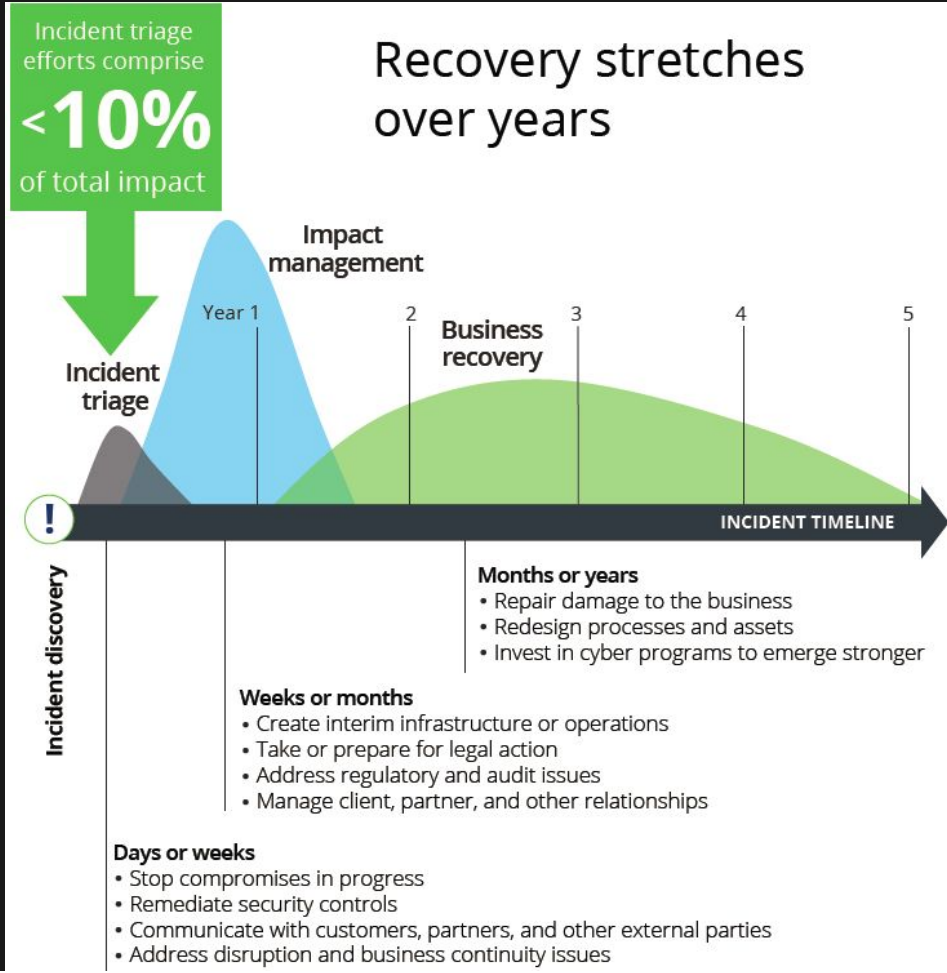
Cyberattack impact factors:

- **Technical** investigation
- **Customer breach** notification
- **Regulatory** compliance
- **Attorney** fees and litigation
- **Post-breach** customer protection
- **Public relations**
- **Cybersecurity** improvements

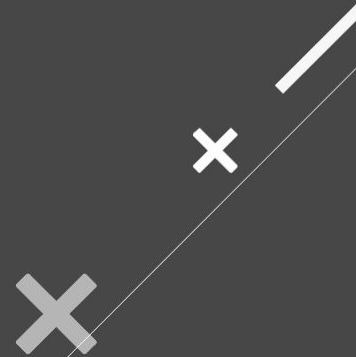
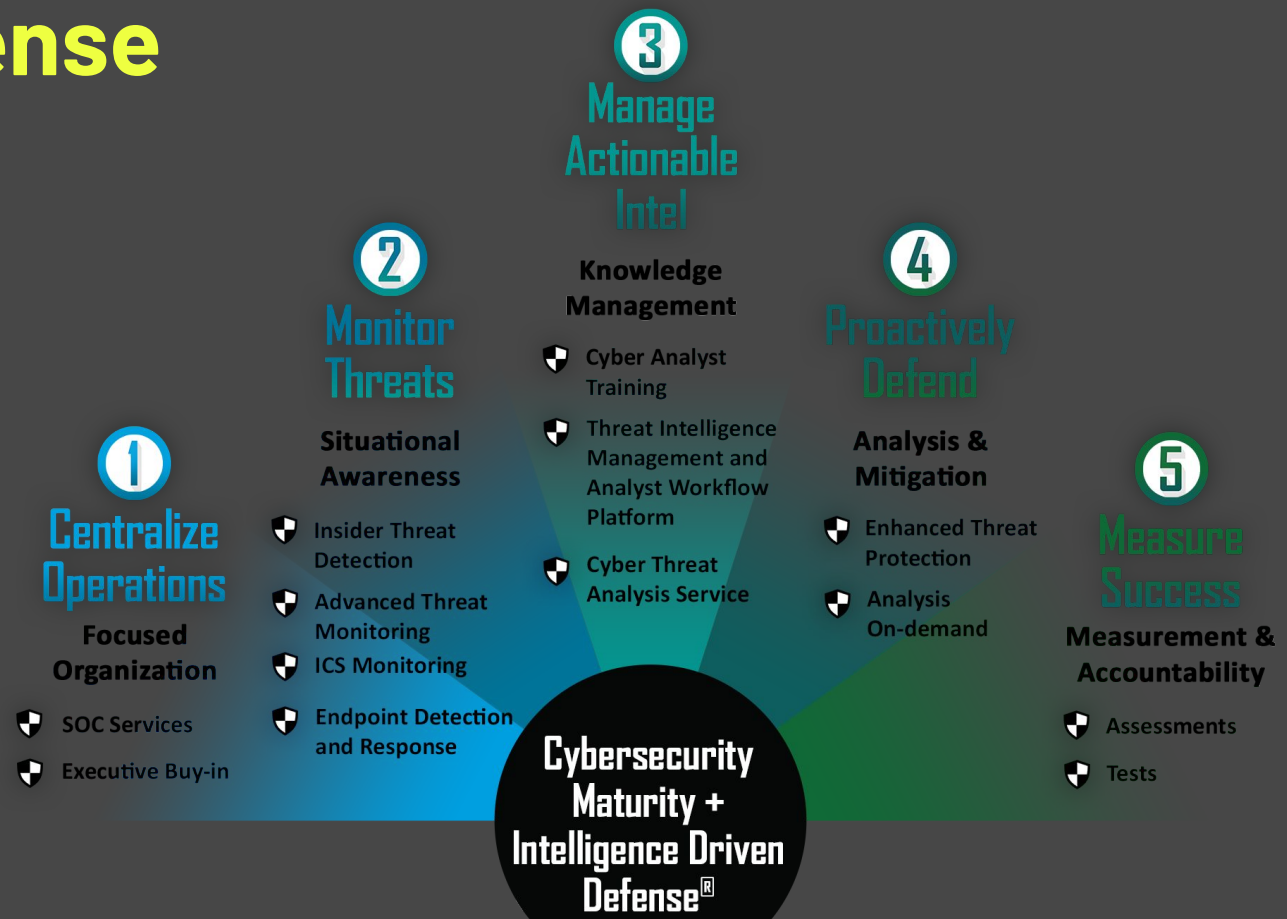
But also:

95
%

- **Insurance** premium increases
- **Increased costs** to raise debt
- **Impact** of operational disruption
- Value of **lost contract revenue**
- **Devaluation** of trade name
- Loss of **intellectual property**
- Lost **value of customer** relationship

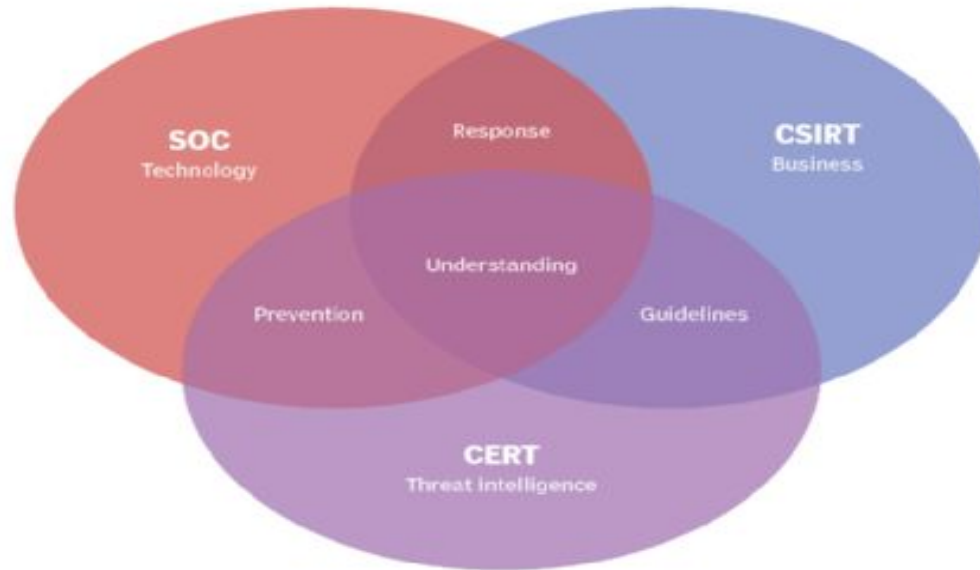


Maturity & Intelligence Driven Defense



CERT/CIRT – Computer Incident/Emergency Response Team

Comparing CSIRT, CERT and SOC



Defence Fundamentals

Secure
Your
Organization

First 5 CIS Controls

Eliminate the vast majority of your organization's vulnerabilities

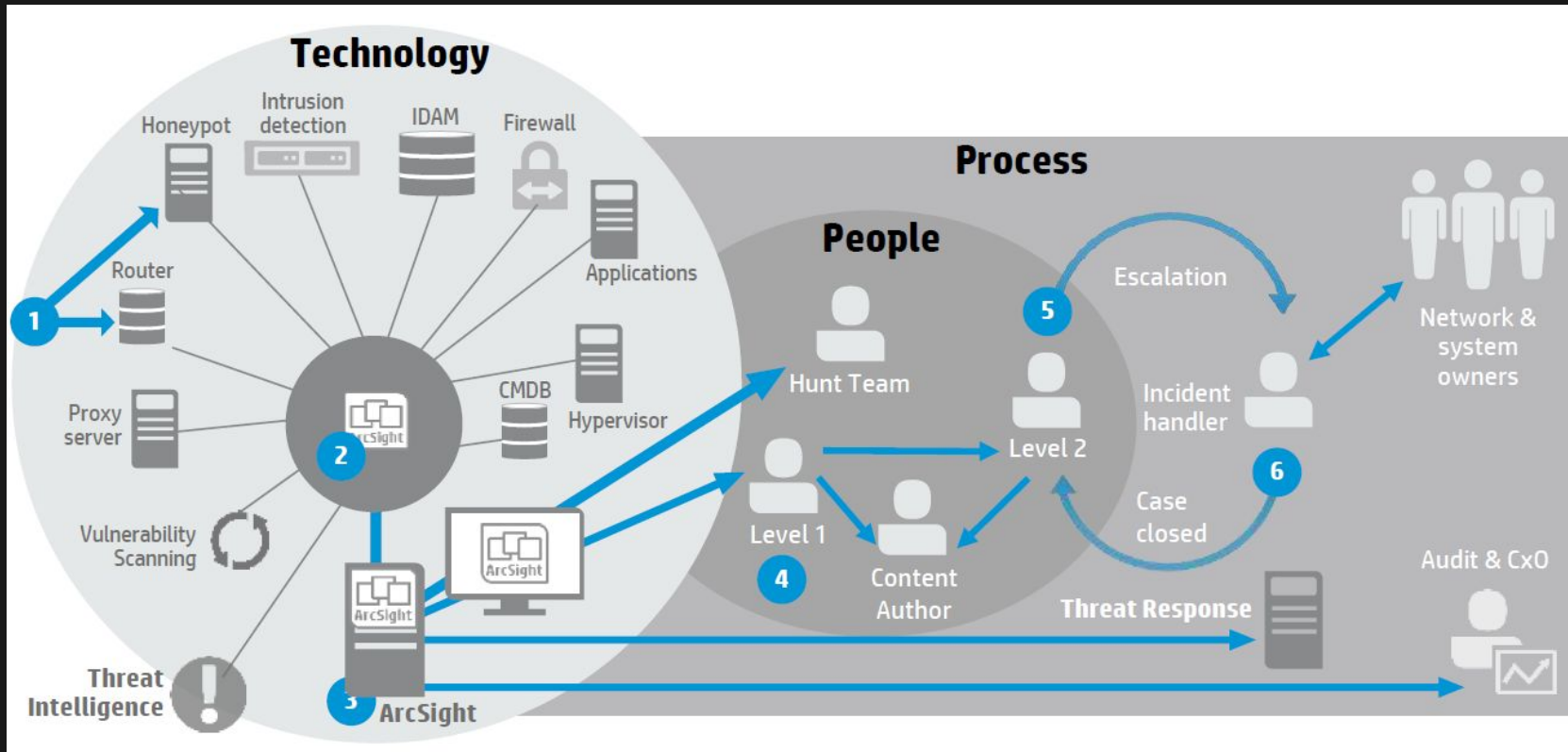
- 1: **Inventory of Authorized and Unauthorized Devices** →
- 2: **Inventory of Authorized and Unauthorized Software** →
- 3: **Secure Configurations for Hardware and Software** →
- 4: **Continuous Vulnerability Assessment and Remediation** →
- 5: **Controlled Use of Administrative Privileges** →

All 20 CIS Controls

Secure your entire organization against today's most pervasive threats

- 6: **Maintenance, Monitoring, and Analysis of Audit Logs** →
- 7: **Email and Web Browser Protections** →
- 8: **Malware Defenses** →
- 9: **Limitation and Control of Network Ports** →
- 10: **Data Recovery Capability** →
- 11: **Secure Configurations for Network Devices** →
- 12: **Boundary Defense** →
- 13: **Data Protection** →
- 14: **Controlled Access Based on the Need to Know** →
- 15: **Wireless Access Control** →
- 16: **Account Monitoring and Control** →
- 17: **Security Skills Assessment and Appropriate Training to Fill Gaps** →
- 18: **Application Software Security** →
- 19: **Incident Response and Management** →
- 20: **Penetration Tests and Red Team Exercises** →

Continues Monitoring





"If you know your enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" - Sun Tzu, The Art of War



THANK YOU!

Any questions?

You can find me at

niel.vanrooyen@voxtelecom.co.za