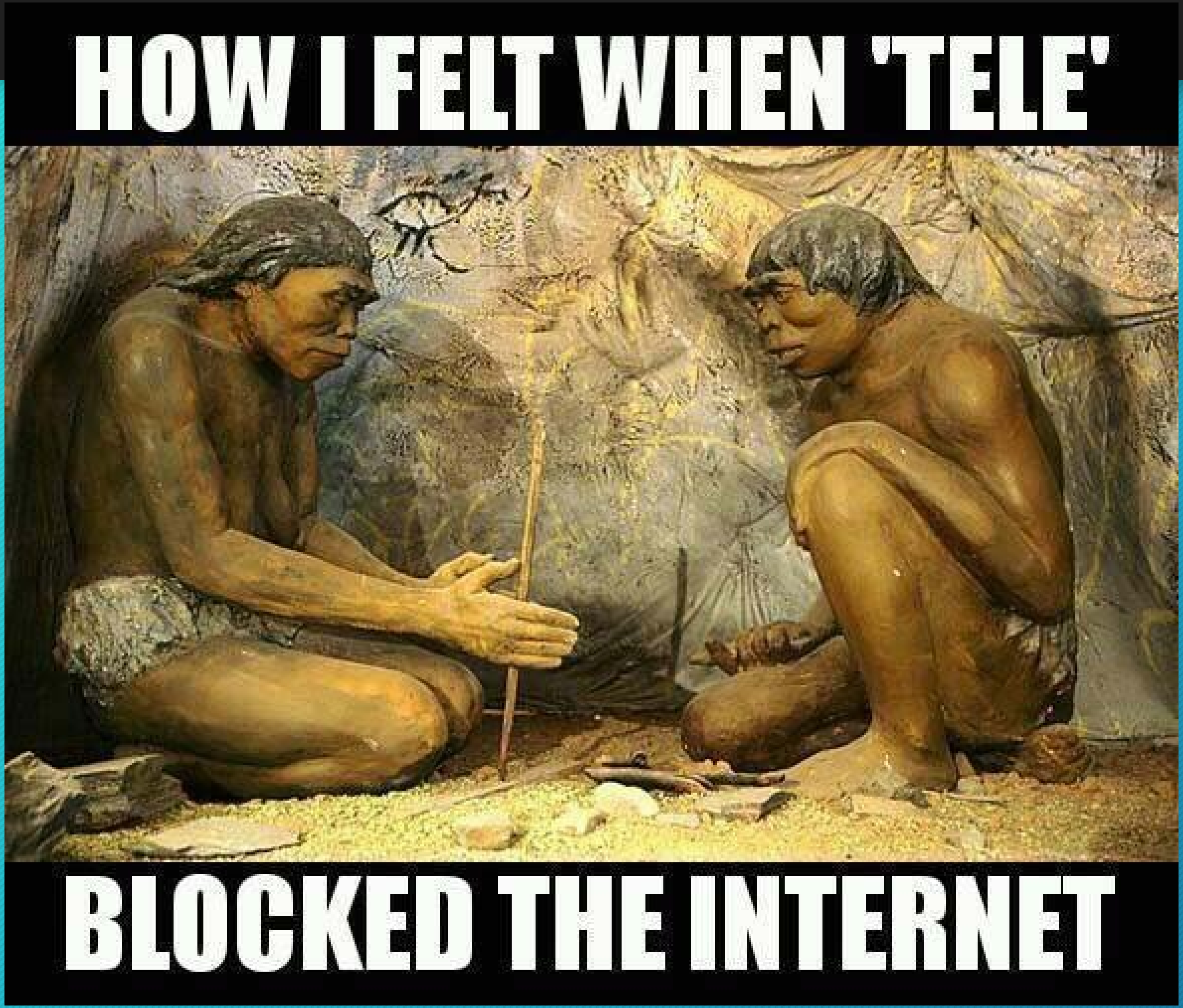
Enhancing Proactive Measures against Cyber Attacks in Oman's Telecommunications Sector through Situation Awareness

مركز الدفاع الإلكتروني
Cyber Defense Centre

Moath Abdullah Alzakwani



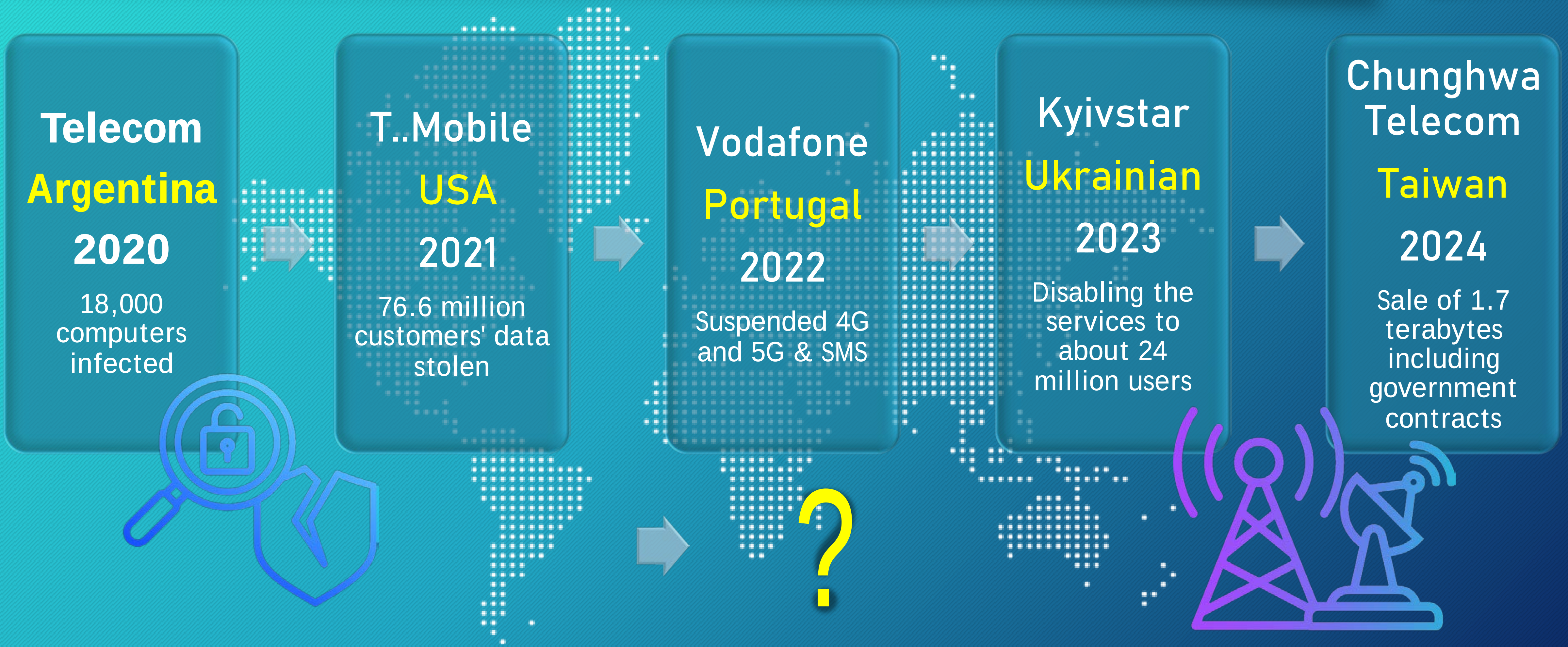
No Internet

Try:

- Turning off your device
- Going outside
- Talking to real people

Attacks to Telecommunication Sector

مركز الدفاع الإلكتروني
Cyber Defense Centre



Telecom
Argentina
2020
18,000 computers infected

T..Mobile
USA
2021
76.6 million customers' data stolen

Vodafone
Portugal
2022
Suspended 4G and 5G & SMS

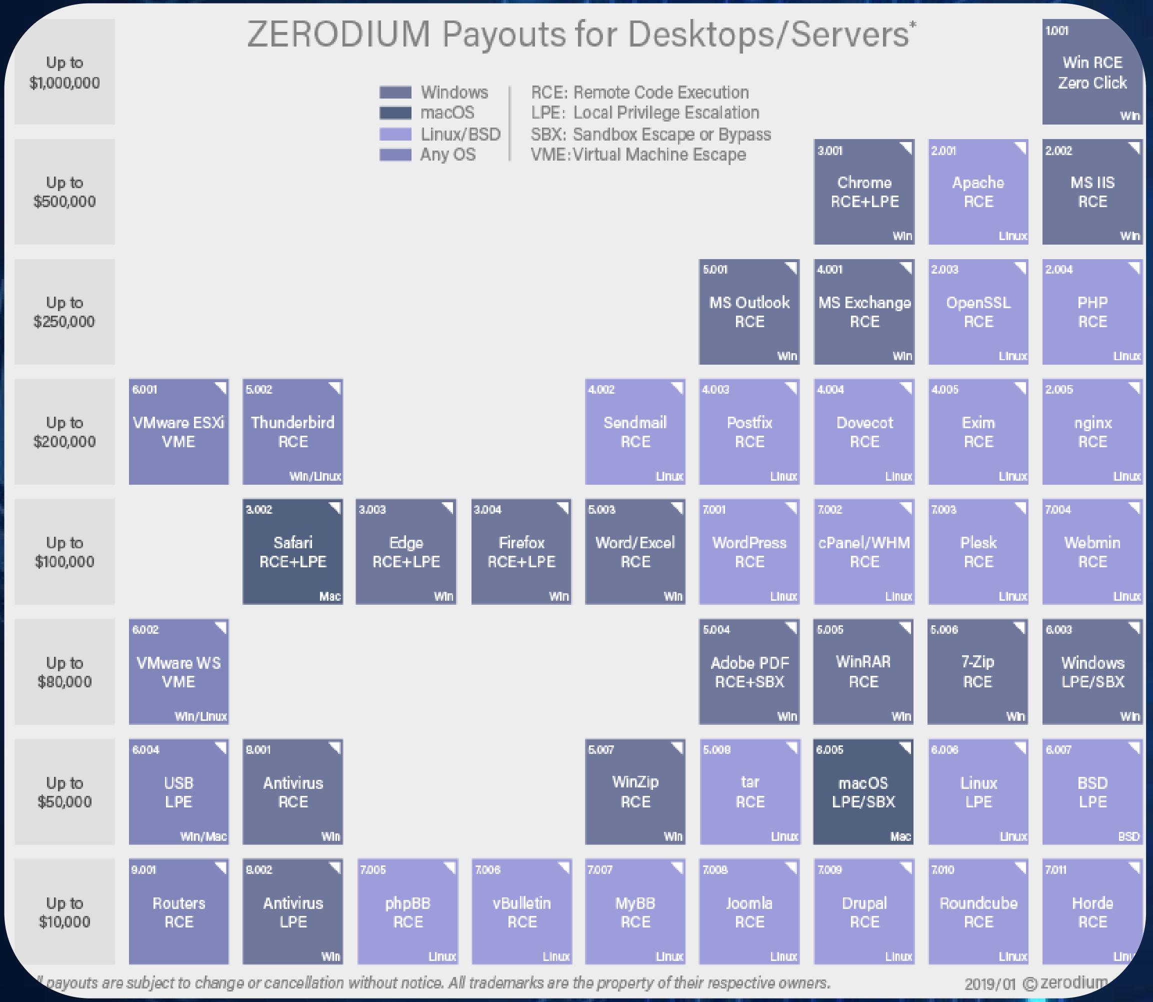
Kyivstar
Ukrainian
2023
Disabling the services to about 24 million users

Chunghwa Telecom
Taiwan
2024
Sale of 1.7 terabytes including government contracts

Human errors

Fresh Phish
CLICK HERE!
IT
Tim Rickard
... AND THIS CYBER SECURITY TOOL ELIMINATES THE HUMAN FACTOR!

مركز الدفاع الإلكتروني
Cyber Defense Centre



ZERODIUM Payouts for Desktops/Servers*

▨ Windows
▨ macOS
▨ Linux/BSD
▨ Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Lin

ll payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium

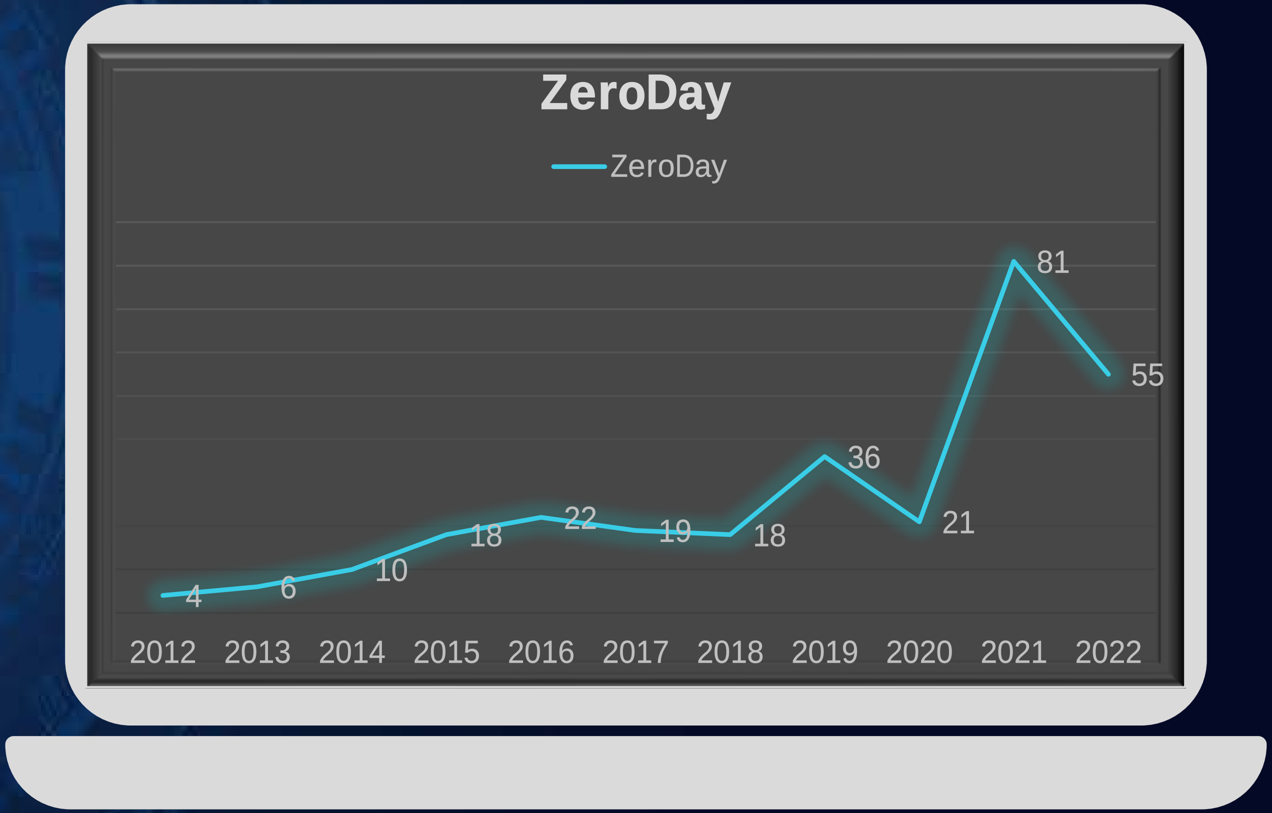
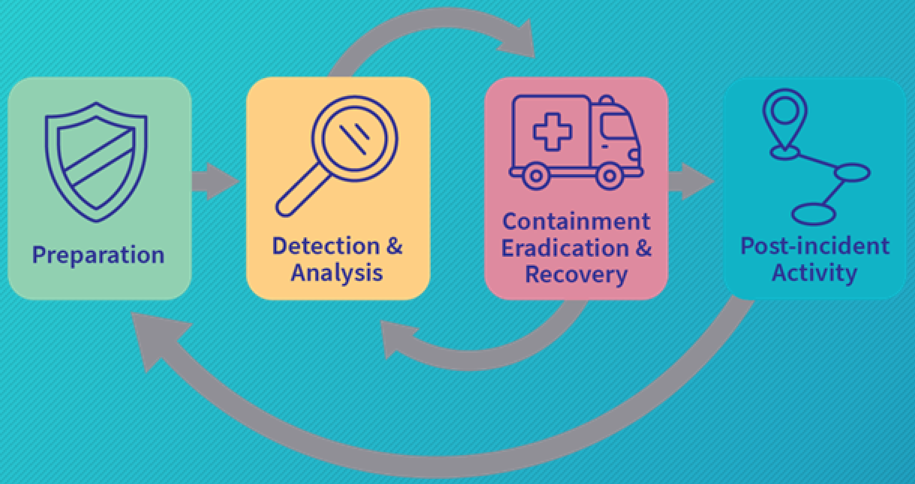


Figure 2: The number of zero-day vulnerabilities uncovered in recent years, adopted from: (SADOWSKI & CHARRIER, 2023)

Incident Response

مركز الدفاع الإلكتروني
Cyber Defense Centre

Cyber Incident Response Cycle



In addressing security concerns, the organization forms an Incident Response (IR) team whose sole purpose is to effectively manage and resolve incidents. Their primary objective is to protect digital assets while ensuring a swift recovery of IT services. (Ahmad at el., 2020).

Minimizing Damage

Reducing Downtime

Predicting the future

Situation awareness as a solution

Situation awareness enables organizations to quickly detect and respond to incidents, make informed decisions, and prevent future incidents. (Husák et al., 2022).

Endsley's definition as her definition is widely adopted in the literature and serves as a base ground for further research in CSA. (Husák et al., 2022).

The widely applicable situational awareness definition given by Endsley. (Franke & Brynielsson, 2014).

Dr. Mica R. Endsley

Situation Awareness Model

The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. (Endsley, 1995).

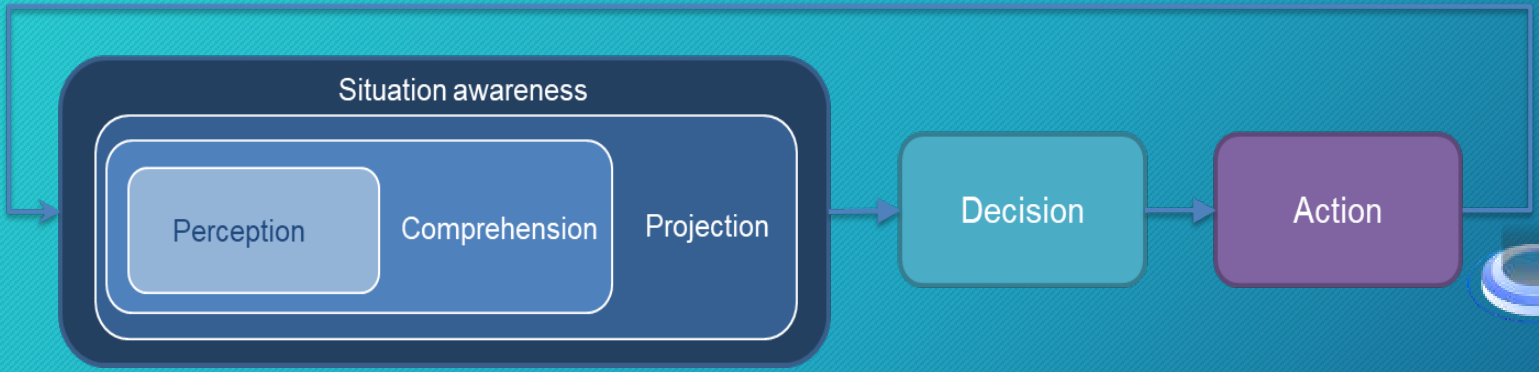
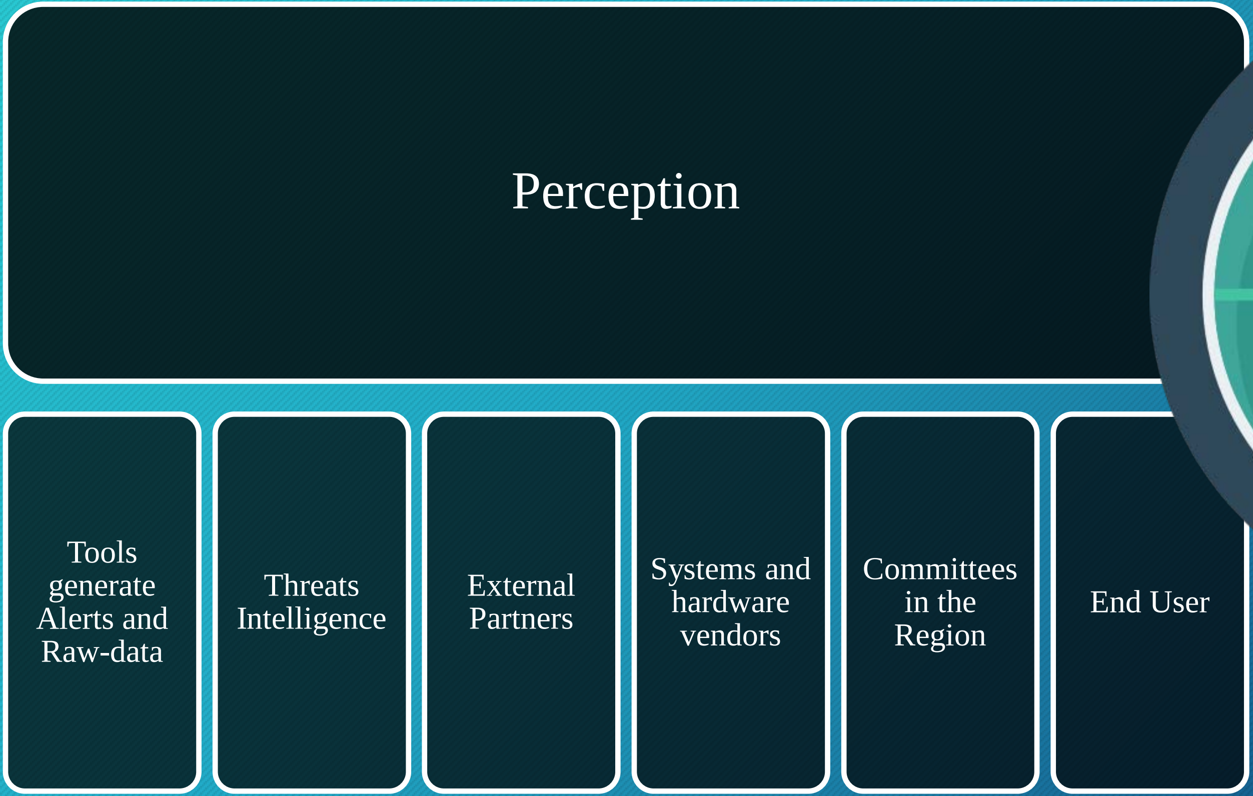


Figure 2: SA process Model – Source: (Endsley, 1995).

Perception (L1)

مركز الدفاع الإلكتروني
Cyber Defense Centre



Perception

Tools generate Alerts and Raw-data

Threats Intelligence

External Partners

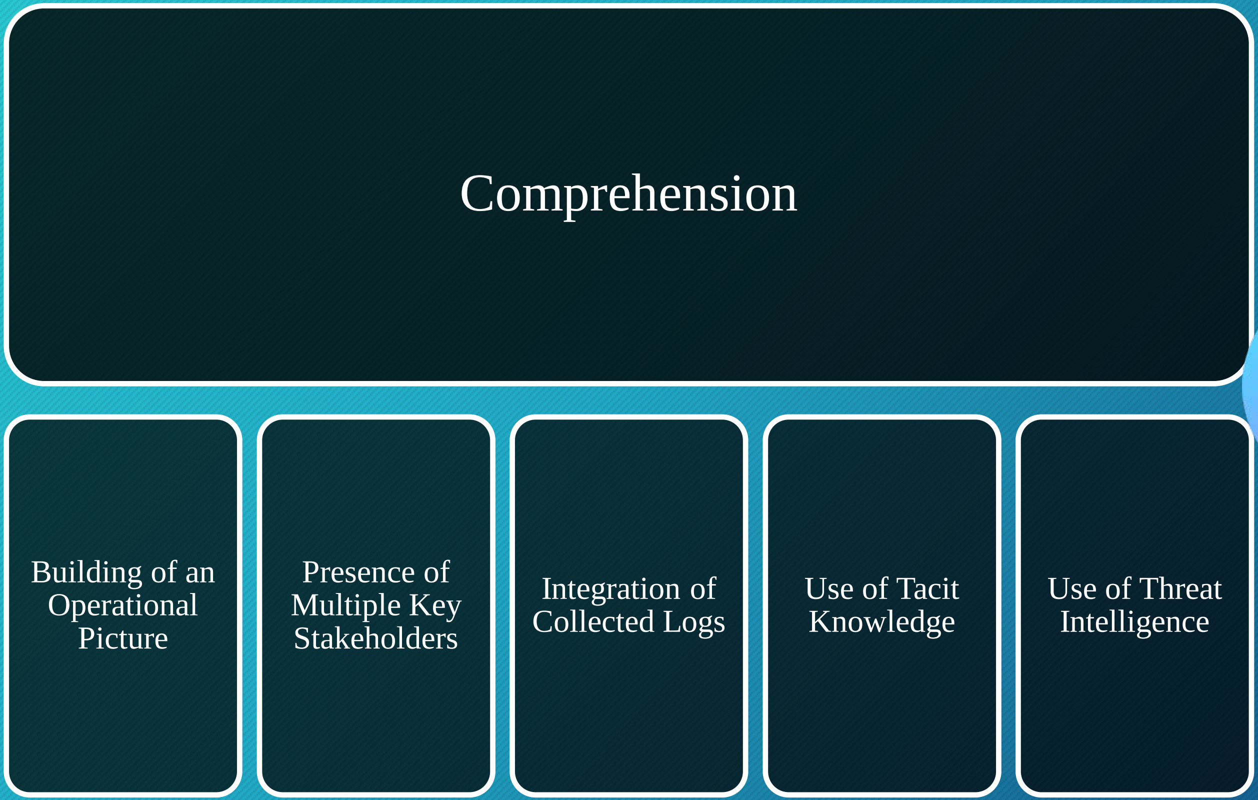
Systems and hardware vendors

Committees in the Region

End User

Comprehension (L2)

مركز الدفاع الإلكتروني
Cyber Defense Centre



Comprehension

Building of an Operational Picture

Presence of Multiple Key Stakeholders

Integration of Collected Logs

Use of Tacit Knowledge

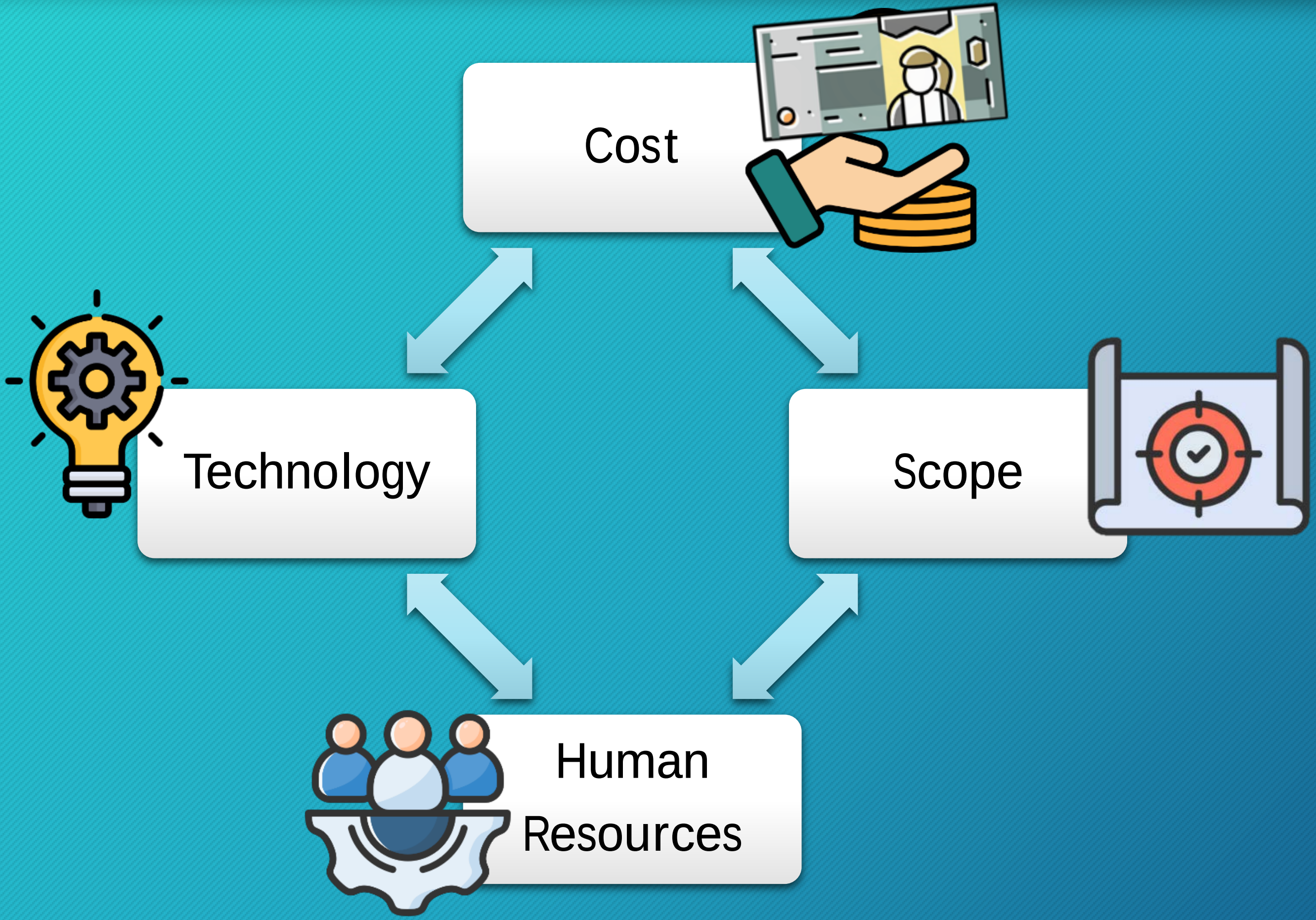
Use of Threat Intelligence

Projection (L3)

Projection

- Generation of Alternative Scenarios
- Senior Security Leadership Prediction
- Inputs from Scenarios
- Adversaries Next Step

Things to consider



Cost

Scope

Human Resources

Technology

SA Importance

Importance of SA

- □ Improve proactivity
- □ Improve visibility
- □ Enhance Incident Response

References

- Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1–147.
- He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. International Journal of Information Management, 62, 102435.
- Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., & Komárková, J. (2022). CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. *Computers & Security*, *115*, 102609.
- Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, *46*, 18–31.
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32–64.

مركـز الدفـاع الإلكتـروني
Cyber Defense Centre

Moath.alzakwani@cdc.gov.om