COS30015 IT Security

Week 8

Presented by Dr Rory Coulter

25 September 2024

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Data, Information, and Intelligence
Intelligence & Sources
Cyber Intelligence
Espionage
TLP
Classification
Assignment 2

SWINBURNE UNIVERSITY OF TECHNOLOGY

Data, Information, and Intelligence

SWINBURNE UNIVERSITY OF TECHNOLOGY

Data, Information, Intelligence

Multiple definitions, what are the building blocks for a common and general understanding

Data: Representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means

Information: Meaningful interpretation or expression of data

Intelligence: Intelligence products and/or organisations and activities that incorporate all sources of information, most frequently human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence

SOURCE: Data https://csrc.nist.gov/glossary/term/data (NIST SP 800-160v1r1)

Information: https://csrc.nist.gov/glossary/term/information (NIST SP 800-88 Rev. 1 under Information)

Intelligence: :https://csrc.nist.gov/glossary/term/intelligence (CNSSI 4009-2015 under all-source intelligence from DoD JP 1-02 - Adapted)

Data, Information, Intelligence

Beyond a definition, but everyday terms

Data

- Example: distance, temperature, name, age
- Is: fact(s), raw, measurement, statistics
- Not: opinion, the result of analysis, may not be actionable

Information

- Example: today is sunny, test this week
- Is: processed , arranged fact(s), structured facts, multi-sourced, contextualised
- Not: evaluated, actionable, relevant

Intelligence

- Example:
- Is: actionable, selective, processed, accurate*, timely*, and complete*, collected and analysed information needed for decisi on
- Not: complete (as possible)

* as possible

Data, Information, Intelligence

In cyber terms

Data

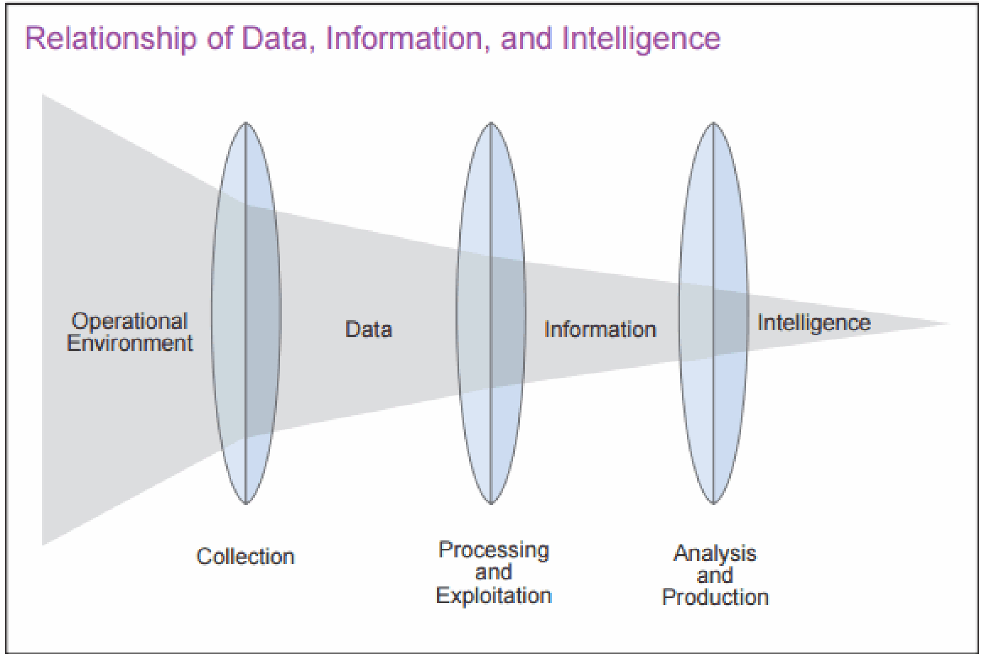
- Easy observed as indicators of compromise (IoC)
- IP, domain name, adversary group, time, hash

Information

- Contextualising and arranging data
- TTPs, Threat, incident type, adversary

Intelligence

- Interpreting objectives, aims or intentions, trends of cyber threat, adversaries
- Enables the facilitation of strategic and effective measures, decision making
- Political, business, social, environmental, health, espionage, terrorism, etc.



Let's revisit intelligence as we progress

SOURCE: https://www.recordedfuture.com/blog/threat-intelligence-data

Intelligence & Sources

SWINBURNE UNIVERSITY OF TECHNOLOGY

Intelligence

We've established that intelligence grants context and enables decision making, how is intelligence fulfilled?

As a process

- Means by which certain type of information is required/requested, analysed and disseminated (think process with steps)
- Consider in fulfilling answering an objective, it sets a process in which to do so

As a product

- Product from process (output of analysis and operations)
- Consider it as an output of a process

As an organisation

- Carries out a range of function for intelligence
- Consider it carrying out its functions

SOURCE: Lowenthal, M. M. (2000). Intelligence: from secrets to policy. Washington, DC, CQ Press.

Intelligence Lifecycle

Direction:

- Setting the requirements for which intelligence will contribute
- Decision maker's objectives
- Sources and priority

Collection:

- Data collected from a range of sources (next slide)

Processing and exploitation

- Data is exploited, or made us of, processed and transformed into the required format
- Data to information

Analysis

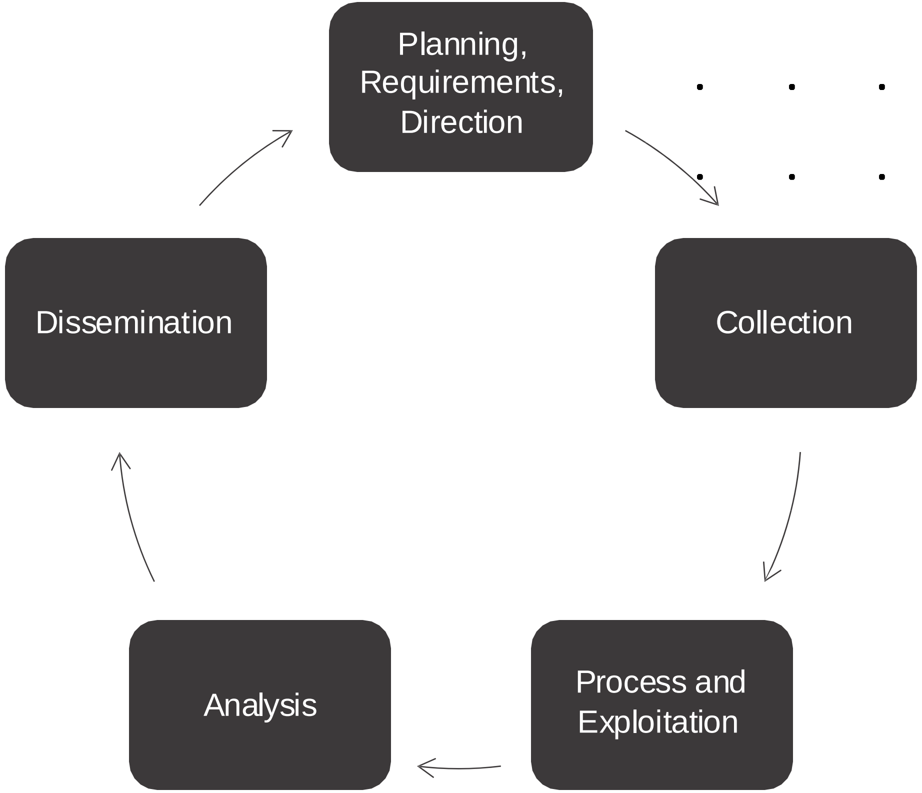
- Refinement of information
- Objective, timely, accurate, and actionable
- Apply induction, deduction, abduction and the scientific method

Dissemination:

- Advisory, report, makes it way to the intended recipient

Feedback:

- Not lsited but included in various alternatives
- Whether it meets the objective



Information Sources

Information of value can be collected from a range of sources

Human Intelligence (HUMINT)

Signals Intelligence (SIGINT)

Imagery Intelligence (IMINT)

Measurement and Signatures Intelligence (MASINT)

Open-Source Intelligence (OSINT)

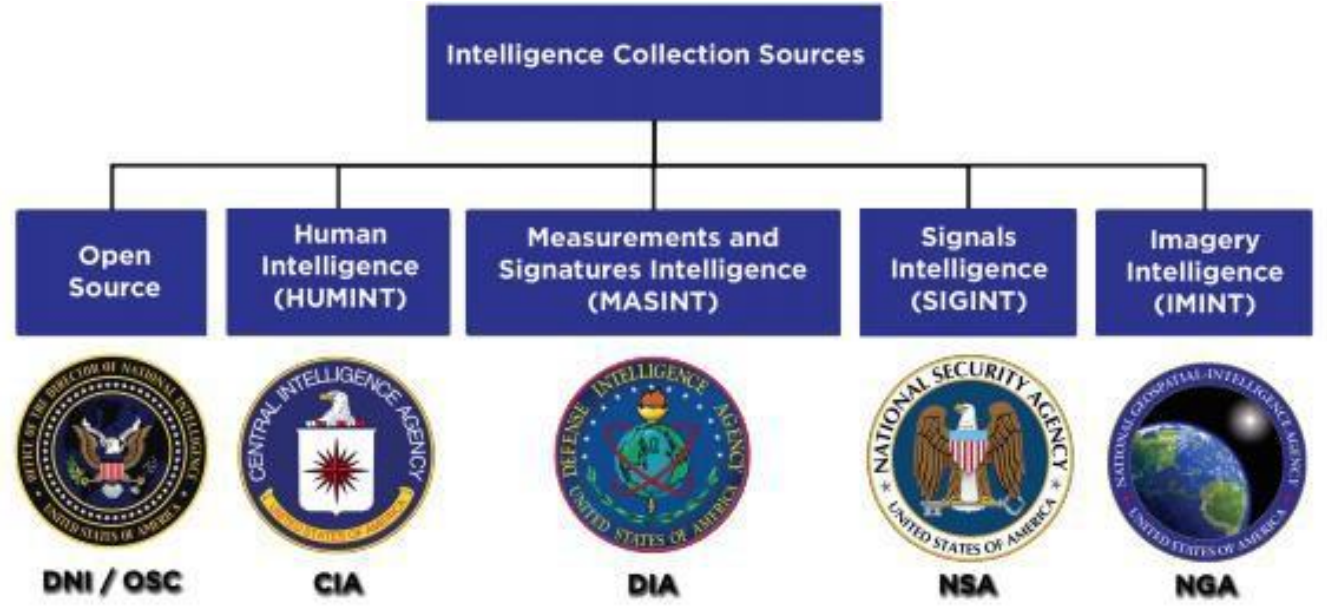

Intelligence Collection Sources
Open Source
Human Intelligence (HUMINT)
Measurements and Signatures Intelligence (MASINT)
Signals Intelligence (SIGINT)
Imagery Intelligence (IMINT)
DNI / OSC
CIA
DIA
NSA
NGA

IMAGE SOURCE:
https://usnwc.libguides.com/c.php?g=494120&p=3381426

Cyber Intelligence

SWINBURNE UNIVERSITY OF TECHNOLOGY

Detecting and Understanding Threats

There is a constant evolution of threats, adversaries and challenges

How do we:

- Keep up to date with different attackers, threats?
- Stay aware of actor and threat TTPs? (Mitre ATT&CK)
- Manage to detect malware, network attacks, scams, and other threats
- Make sure AV, IDS/IPS, EDR, Firewall, WAF, SIEM, etc. stay up to date the historical and the latest threats?
- What feeds these tools
- How do we keep track of attacker interests, targets,
- How do we define our strategic aims (what are defending, and from what)?

- Attackers:
- One to multi dimensional Modus Operandi (adversaries may focus on a single to multiple things)
- May be confined to a single industry or objective
- But do they stay static?

Indicators of Compromise (IoC)

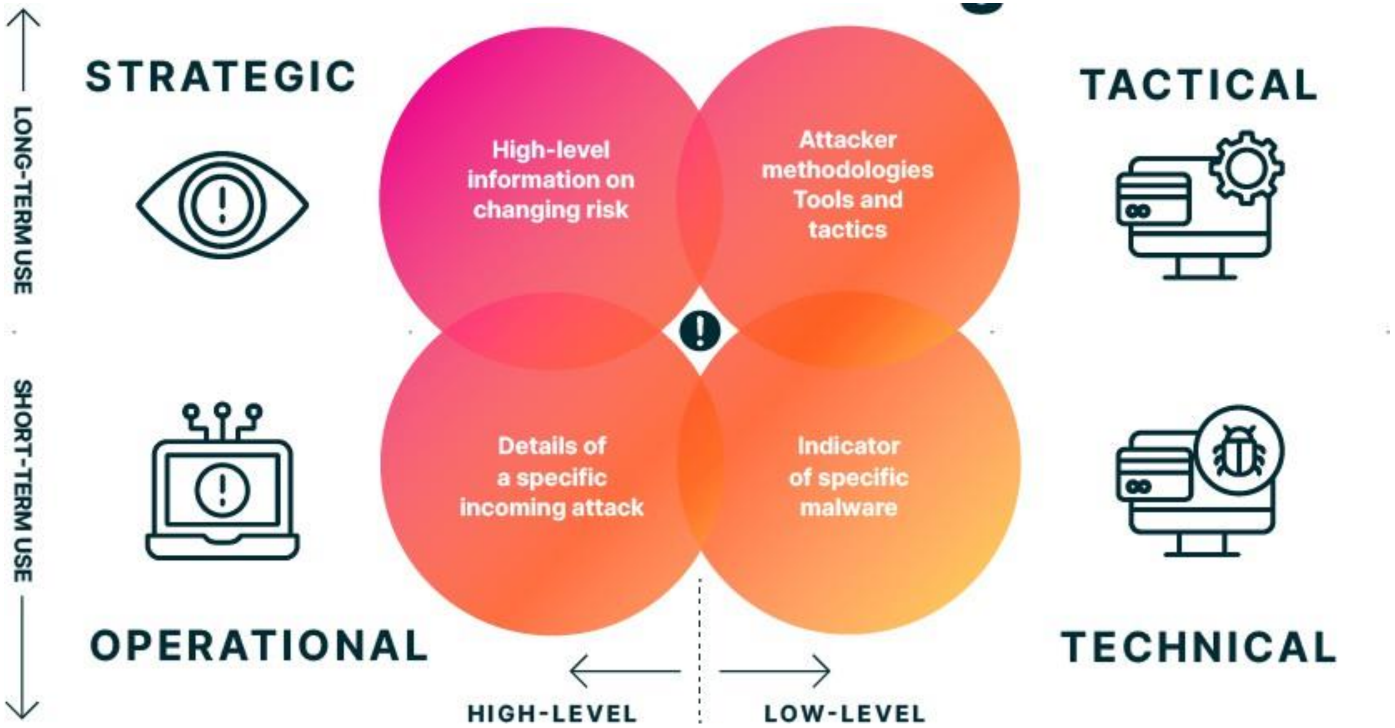
Indicate an incident has taken place

- Help understand the type of incident and its source
- Threat intelligence solutions leverage IoCs to quickly connect cybersecurity incidents to known threat profiles
- For example, if a company has outbound traffic to an IP address known to be used for malicious activity, cyber threat intelligence can connect that IP address to a threat actor, and provide information about malware distributed by that attacker. H
- Drive a lot of the means to answer some previous questions

- File hash
- IP, Domain
- Registry key types
- File extensions
- Directory path
- Etc.

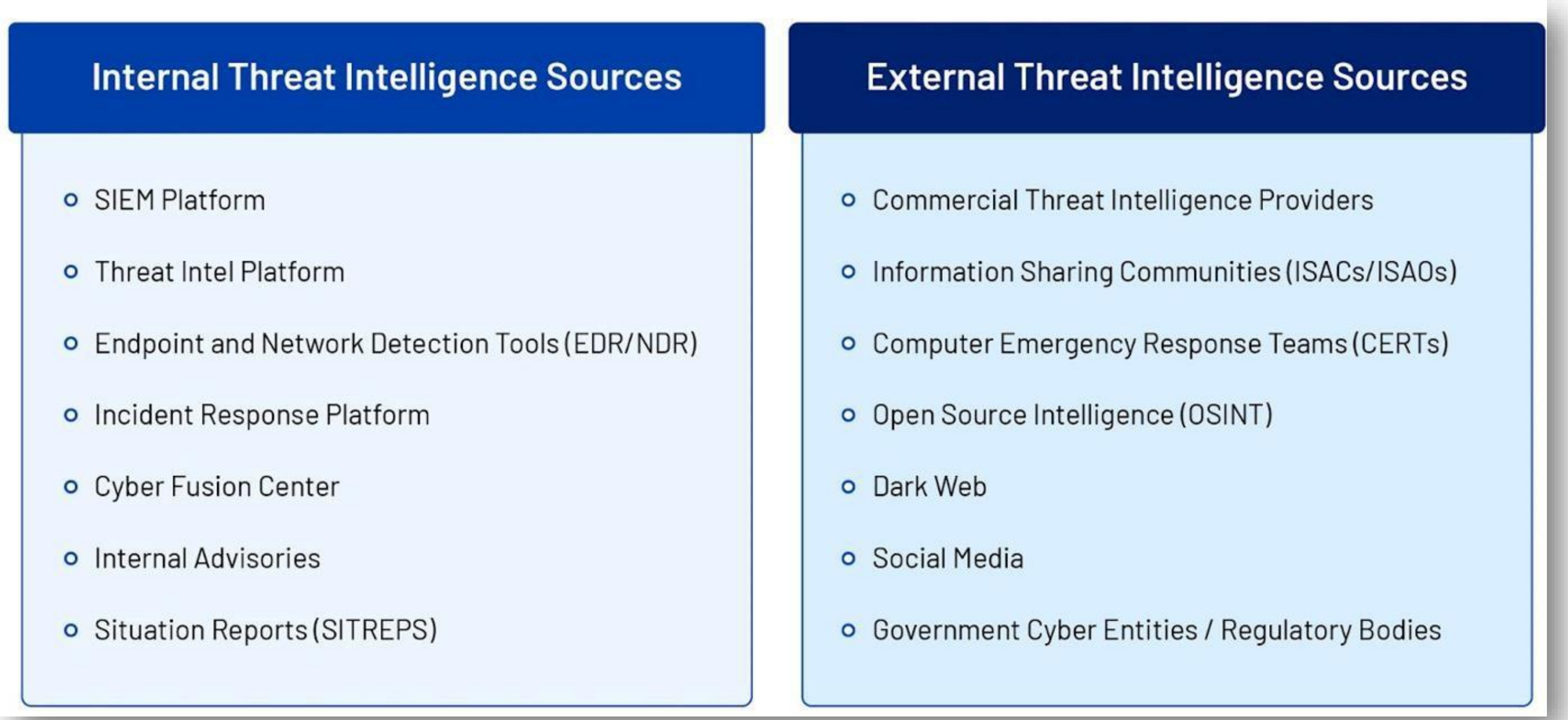
Cyber Threat Intelligence Types

Different uses and stakeholder


STRATEGIC
TACTICAL
High-level information on changing risk
Attacker methodologies Tools and tactics
Details of a specific incoming attack
Indicator of specific malware
OPERATIONAL
TECHNICAL
LONG-TERM USE
SHORT-TERM USE
HIGH-LEVEL
LOW-LEVEL

SOURCE: https://www.plotlights.com/blog/what-is-threat-intelligence-update-for-communicators/

Internal & External Threat Intelligence Sources



Internal Threat Intelligence Sources

- SIEM Platform
- Threat Intel Platform
- Endpoint and Network Detection Tools (EDR/NDR)
- Incident Response Platform
- Cyber Fusion Center
- Internal Advisories
- Situation Reports (SITREPS)

External Threat Intelligence Sources

- Commercial Threat Intelligence Providers
- Information Sharing Communities (ISACs/ISAOs)
- Computer Emergency Response Teams (CERTs)
- Open Source Intelligence (OSINT)
- Dark Web
- Social Media
- Government Cyber Entities / Regulatory Bodies

https://cyware.com/security-guides/cyber-threat-intelligence

Espionage

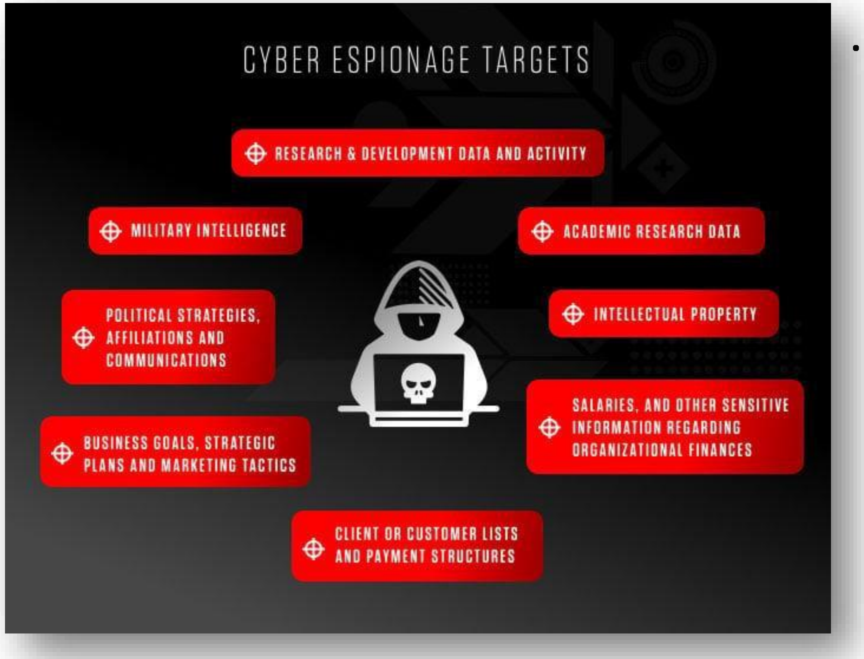
Cyber Espionage

What is Cyber Espionage?

- Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorised user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons
- Cyber espionage is a means for intelligence gathering (Wangen, G., 2015. The role of malware in reported cyber espionage: a review of the impact and mechanism. Information, 6(2), pp.183-211.)

Cyber Espionage Targets

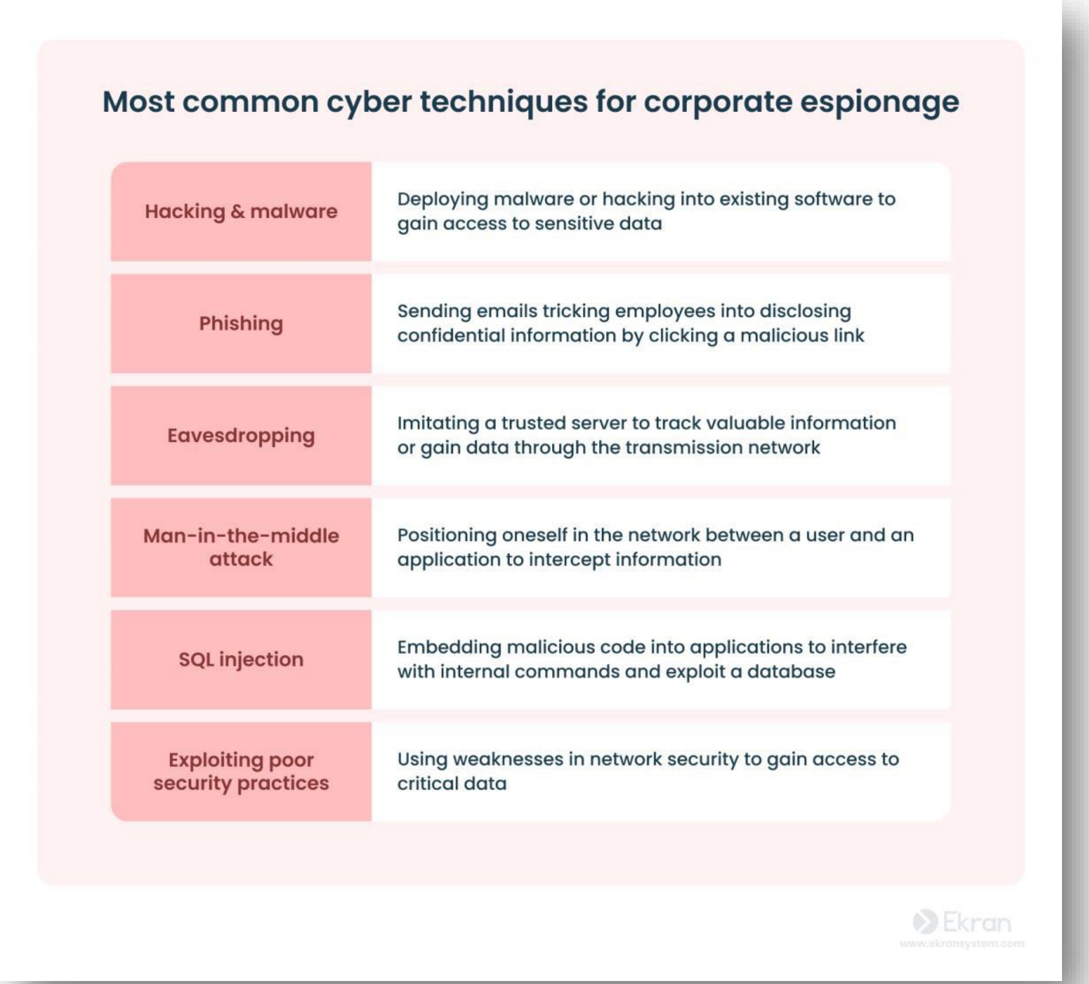
- Organisations :The most common targets of cyber espionage include large corporations, government agencies, academic institutions, think tanks or other organisations that possess valuable IP and technical data that can create a competitive advantage for another organisation or government
- Individuals: Targeted campaigns can also be waged against individuals, such as prominent political leaders and government officials, business executives and even celebrities


CYBER ESPIONAGE TARGETS
RESEARCH & DEVELOPMENT DATA AND ACTIVITY
MILITARY INTELLIGENCE
ACADEMIC RESEARCH DATA
POLITICAL STRATEGIES, AFFILIATIONS AND COMMUNICATIONS
INTELLECTUAL PROPERTY
SALARIES, AND OTHER SENSITIVE INFORMATION REGARDING ORGANIZATIONAL FINANCES
BUSINESS GOALS, STRATEGIC PLANS AND MARKETING TACTICS
CLIENT OR CUSTOMER LISTS AND PAYMENT STRUCTURES

Common Cyber Espionage Tactics

Common attack techniques include:

- Watering hole: Malicious actors are able to infect legitimate websites commonly visited by the victim or people associated with the target with malware for the explicit purpose of compromising the user
- Spear-phishing: A hacker targets specific individuals with fraudulent emails, texts and phone calls in order to steal login credentials or other sensitive information
- Zero-day exploits: Cyberc riminals leverage an unknown security vulnerability or software flaw prior to discovery and patching by the software developer or the customer’s IT team
- Inside actors or insider threat: A threat actor convinces an employee or a contractor to share or sell information or access to the system to unauthorised users

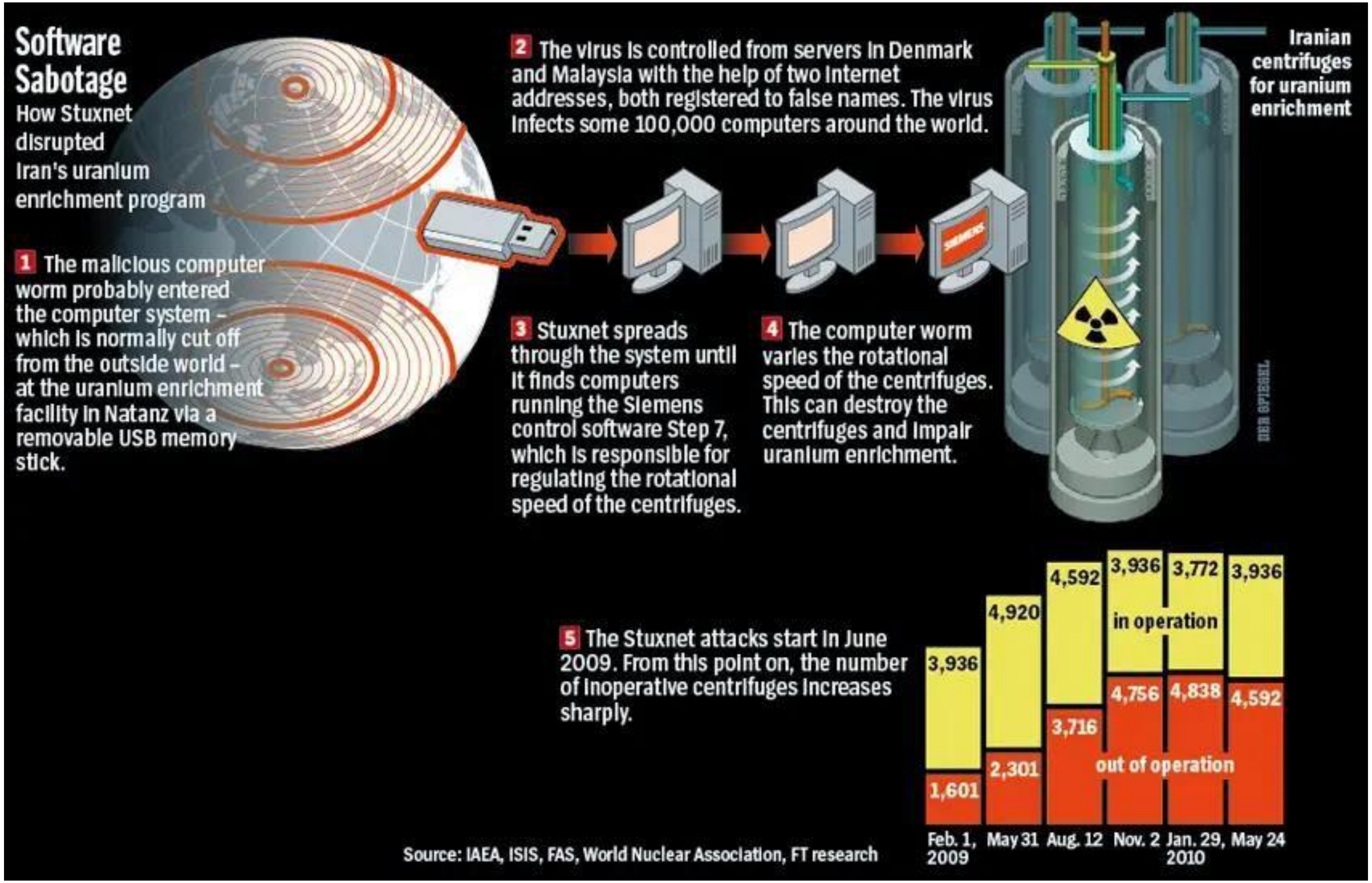


Most common cyber techniques for corporate espionage

Hacking & malware	Deploying malware or hacking into existing software to gain access to sensitive data
Phishing	Sending emails tricking employees into disclosing confidential information by clicking a malicious link
Eavesdropping	Imitating a trusted server to track valuable information or gain data through the transmission network
Man-in-the-middle attack	Positioning oneself in the network between a user and an application to intercept information
SQL injection	Embedding malicious code into applications to interfere with internal commands and exploit a database
Exploiting poor security practices	Using weaknesses in network security to gain access to critical data

Ekran
www.ekransystem.com

Stuxnet – A Classic Example



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

https://cyberhoot.com/cybrary/stuxnet/

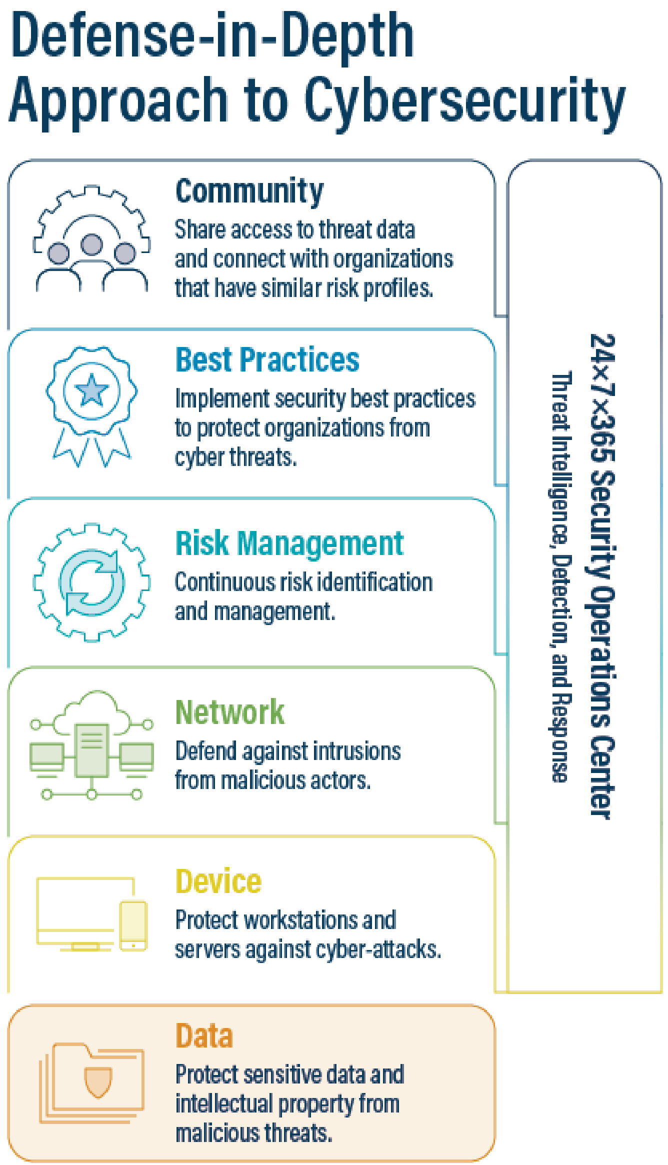
Contemporary Models

Defence in Depth

Not just an outer shell

Security is applied in many layers

- Ensures there is redundancy in security controls, using a range of security layers
- System and network complexity increases
- Restricts and presents a series controls against adversaries
- Also known as onion model



Defense-in-Depth Approach to Cybersecurity

Community
Share access to threat data and connect with organizations that have similar risk profiles.

Best Practices
Implement security best practices to protect organizations from cyber threats.

Risk Management
Continuous risk identification and management.

Network
Defend against intrusions from malicious actors.

Device
Protect workstations and servers against cyber-attacks.

Data
Protect sensitive data and intellectual property from malicious threats.

24×7×365 Security Operations Center
Threat Intelligence, Detection, and Response

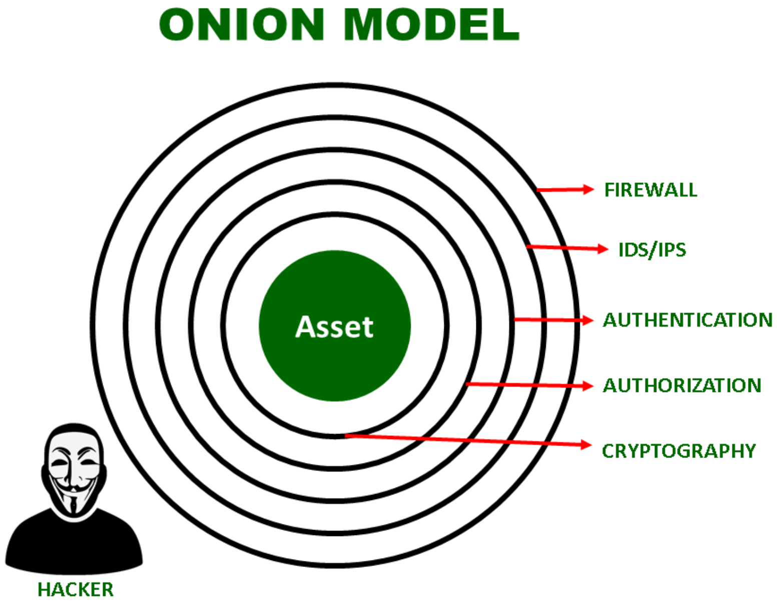
SOURCE: https://www.cisecurity.org/insights/blog/sltt-organizations-and-the-defense-in-depth-strategy

Defence in Depth

Sources of focus, multiple interpretations

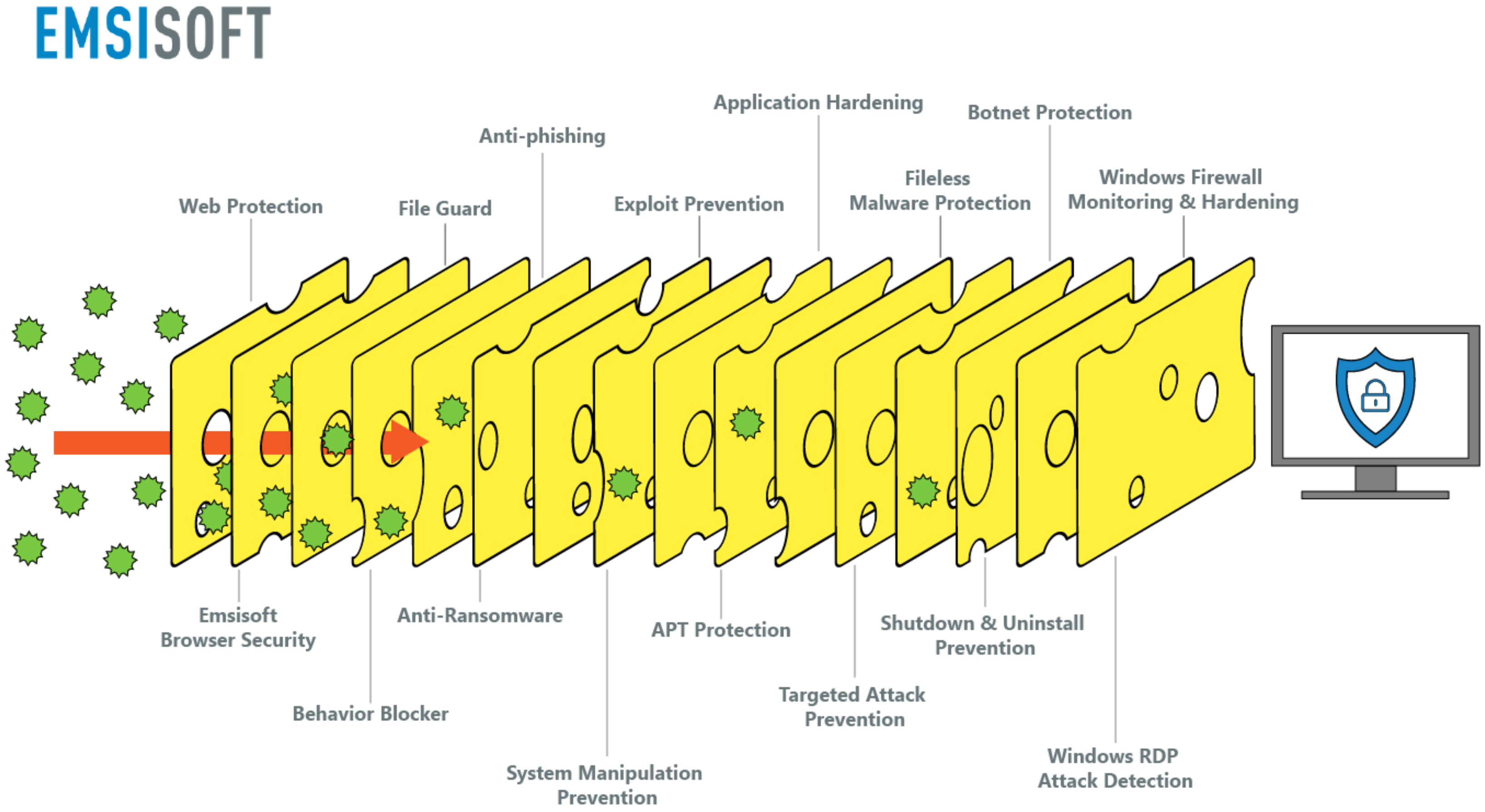
More than just the outside

- Physical
- Perimeter
- Network
- Endpoint
- Application and OS
- Data and Information
- Policy



SOURCE: https://www.geeksforgeeks.org/introduction-to-security-defense-models/

Defense in Depth (cont.)


EMSISOFT
Application Hardening
Botnet Protection
Anti-phishing
Fileless Malware Protection
Windows Firewall Monitoring & Hardening
Web Protection
File Guard
Exploit Prevention
Emsisoft Browser Security
Anti-Ransomware
APT Protection
Shutdown & Uninstall Prevention
Behavior Blocker
Targeted Attack Prevention
System Manipulation Prevention
Windows RDP Attack Detection

SOURCE: https://blog.emsisoft.com/wp-content/uploads/2021/03/logo.png

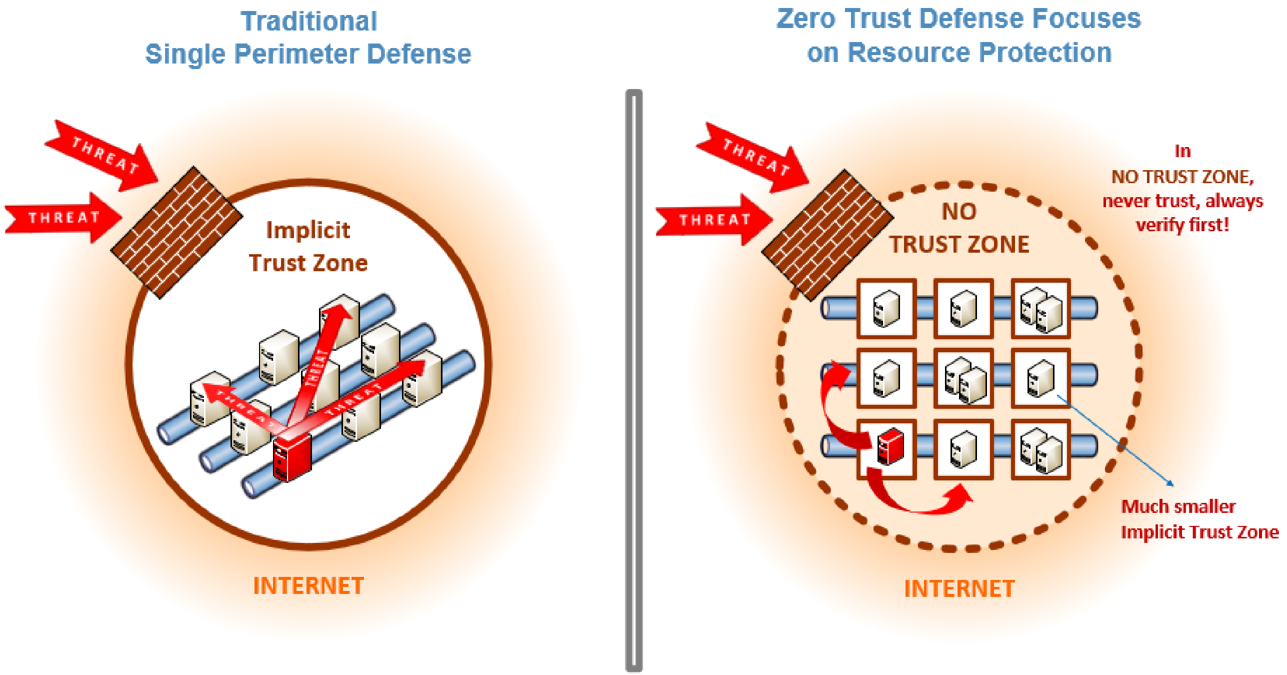
Zero Trust

Focus shifts to verification of users and assets, assumes compromise and not to trust

"Never trust, always verify"

- Previous models still operate on a trusted zone
- Trust, but verify
- Authenticated, in a trusted zone, surrounded by controls – it's ok to trust

- Zero trust removes the idea of a trusted zone
- All services, accounts must be understood ahead of time
- Development of zero trust policies



SOURCE: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Key Principles

Of zero trust architecture (ZTA)

Three key principles applied

- **Continuous verification**
- Verify all access, for all resources, all the time
- **Limit the "blast radius"**
- Reduce the impact regardless on internal or external breach
- **Automate context collection and response**
- Incorporate a range of data/information from the IT stack to get an accurate picture (identity, endpoint, working hours, etc.)

SOURCE: https://csrc.nist.gov/pubs/sp/800/207/final

Continuous Verification

No trusted credentials, zones or devices at any time

Never trust, always verify

- **Risk based conditional access**
- Workflow will be interrupted when risk changes
- **Scalable policy**
- Must also align to organisation specification also

Limit the Blast Radius

Identity and privilege

- **Identity segmentation, not zone**
- Segment based upon identity to required data and systems
- **Least privilege**
- User and service accounts, apply the minimum capability to apply the task

Automate Context Collection And Response

Accurate decisions required data

Realtime decision making from a range of sources

- Credentials
- Workload
- Endpoint
- Network
- Data
- SIEM
- Identity
- Etc.

Assignment 2

SWINBURNE UNIVERSITY OF TECHNOLOGY