COS30015 IT Security

Week 3

Presented by Dr Rory Coulter

14 August 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.

Operating Systems
Host-based Detection
Access Controls, Authentication, and Policy
Monitoring
System Hardening
Converged Security
Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Operating Systems

SWINBURNE UNIVERSITY OF TECHNOLOGY

Operating Systems

System software which manages hardware, software, provides and enables resources to services/programs

A collection of software that manages computer hardware resources and provides common services for computer programs

- Operating Systems provide some key functions to users, hardware, software
- An operating system manages the ways applications access the resources in a computer, including its disk drives, CPU, main memory, input devices, output devices, and network interfaces, user interface
- Kernel
  - Schedules time and resources to a process
- File system
  - Provides a framework to specify the handling of files and folders, permissions (RWX) for users and groups
- Memory management
  - Provide, manage and isolate memory required for software
- Processes
  - An instance of a program currently running
- Operating Systems are not secured by default typically
- Require additional configuration for security
- Where the computer exists plays an important role

https://csrc.nist.gohttps://csrc.nist.gov/glossary/term/operating_systemv/glossary/term/operating_system
NIST SP 800-152

Security

Provide CIA to the computer system

Typical measures in which this can be achieved

- User or group permissions
  - Specifying who and a collection of users have access too
- Antivirus, Endpoint detection and response
  - Match known signatures, signatures, rules, behaviour, policy
- Policy
  - Specify setting which can be allowed or blocked
- Firewall
  - Block or allow connections incoming or outgoing connections
- Authentication
  - Method to whom can access system

- Access control
  - Fine grain settings
- Monitoring
  - Ability to log what is occurring
- Security software
  - Installation and running of additional programs to aid security (e.g., app locker)

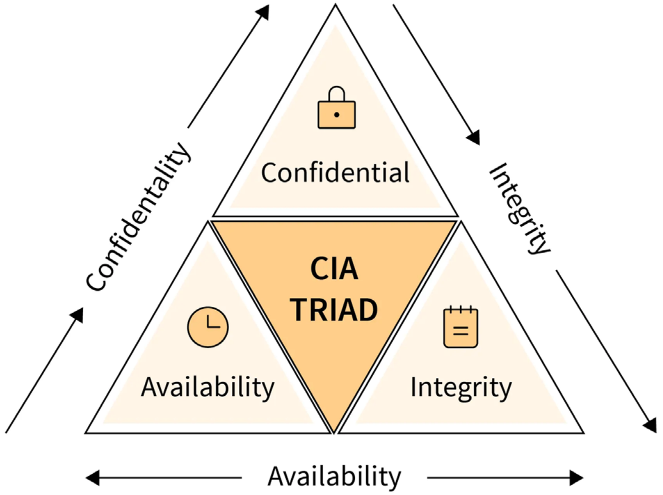


IMAGE SOURCE: https://www.scaler.com/topics/cyber-security/cia-triad/

Host-based Detection

SWINBURNE UNIVERSITY OF TECHNOLOGY

Host-based Detection

A range of tools required to detect and prevent threats for Operating Systems. While signatures are a staple, a behavioural approach behaviour must also be considered

Signature vs Behaviour

- Host may include workstations and servers
- Signature
  - Compare digital signature (hash)
  - Security vendors update known hash signatures
  - Good: Quick, direct match
  - Bad: Only knows what has been observed before
- Behaviour
  - Anomaly focused
  - Detect behaviour and code
  - Good: Detect what hasn't been observed before
  - Bad: Chance for false positives

Network focused? IDS and IPS

Access Controls

SWINBURNE UNIVERSITY OF TECHNOLOGY

Discretionary access control (DAC)

Allows the owner of a resource to control access to that resource and what level of access they are granted

- Access control list (ACL) is a
- List of users or groups who have been granted access to the resource and their corresponding level of access
- Examples ACLs in Windows, Linux: Assumes everyone who has permission exercises it responsibly
- Advantage :
  - simplicity , flexibility
- Limitations
  - not provide any protection against users who abuse their access privileges
  - difficult to manage ACL for large systems with many resources and users

Mandatory access control (MAC)

Access to resources is determined by a security policy that is enforced by the operating system or security software

Every resource (files, folders, and devices) is assigned a security label or classification that indicates the sensitivity or importance of the resource

- The security policy defines the rules for how access is granted based on the labels assigned to resources and users
- Example – SE Linux
  - Assumes no-one who has access can be trusted to exercise it responsibly
- Even root can have no authority
- Advantages:
  - provides a higher level of protection against unauthorised access
  - reduces the risk of accidental data leaks or breaches
- Limitations
  - more complex and difficult to manage than DAC
  - security policy must be carefully designed and maintained

Role-based access control (RBAC)

Provides access based on the roles and responsibilities of users within an organisation

Users can be assigned to multiple roles, each with a different set of permissions

- Users can be assigned to multiple roles, each with a different set of permissions
- These roles are based on the user's job function, responsibilities, and level of authority within the organisation
- Advantages:
  - simplifies the management of access control (central control)
  - more secure?

Attribute-based access control (ABAC)

Grants access to resources based on a set of attributes associated with users, resources, and the environment

Attributes associated with a user or resource can include a wide range of factors such as time of day, location, device type , sensitivity of the data

- Advantages:
  - flexible
  - granular
- Limitations
  - more complex to manage than other access control models
  - it requires a well-defined attribute-based policy and a system for collecting and managing the attributes associated with users and resources

Authentication

SWINBURNE UNIVERSITY OF TECHNOLOGY

Authentication

Verifying the identity of a user, process, or device, often as required to allow access to systems, resources in an information system

Maintain confidentiality

- Authentication is critical in preventing unauthorised access to:
  - Data
  - Systems
  - Resources
  - Applications
- Can lead to system impact, data breaches, financial loss, and reputational damage if breached
- Authentication requires
  - Identity
  - Secret

- User identity and secret is shared to system to authenticate to
  - Password-based authentication is the predominate method for authentication
- Identity and password are passed, password is looked up in table for authenticate*
- Users re-use passwords
- Obtain the password list, adversaries can look up or try to match the password hash

Assuming a hash-based scheme is employed

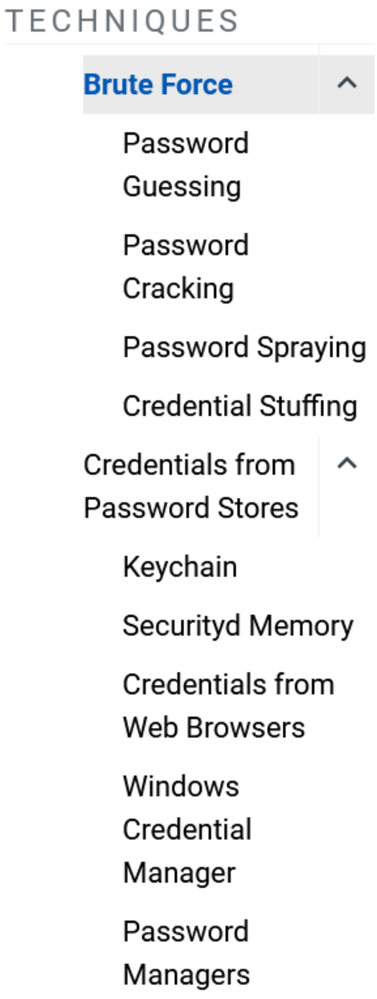
See top 10000 passwords: https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords

Word List & Rainbow Tables

An adversary only needs to guess or compare exposed password hashes

Two key methods

- Word list
- A list of words to pass with identity to guess password
- Rainbow table
- Table of hashed passwords to look up
- Considering MITRE TTPs at a very high and non-exhaustive level, multiple types of password-based attacks
- See Credential Access
- The adversary is trying to steal account names and passwords
- https://attack.mitre.org/tactics/TA0006/



TECHNIQUES

Brute Force

Password Guessing

Password Cracking

Password Spraying

Credential Stuffing

Credentials from Password Stores

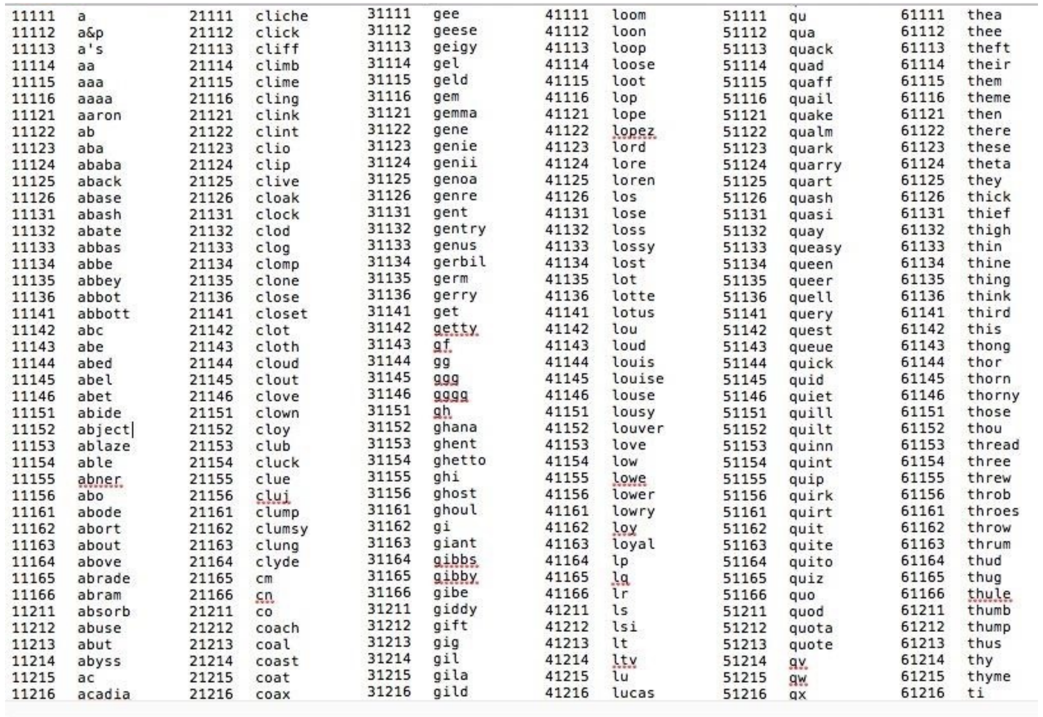
Keychain

Securityd Memory

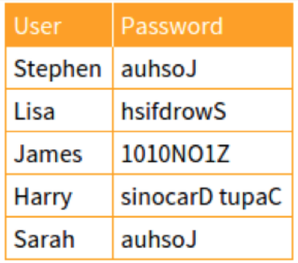
Credentials from Web Browsers

Windows Credential Manager

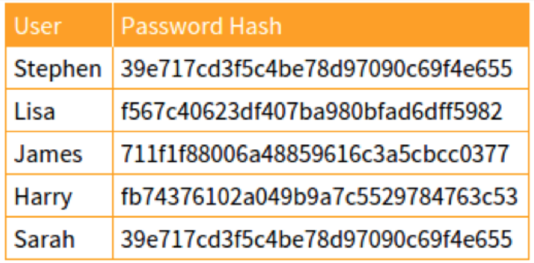
Password Managers



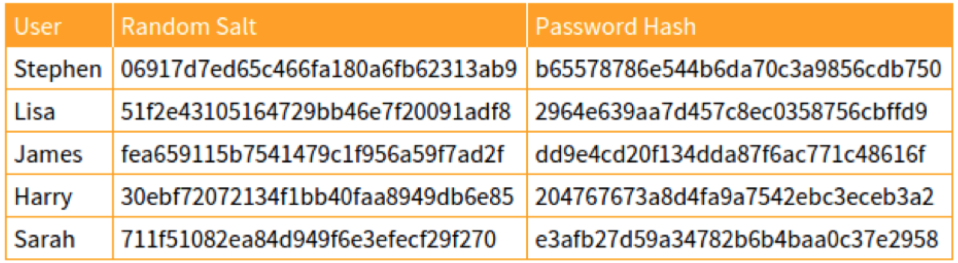
11111	a	21111	cliche	31111	gee	41111	loom	51111	qu	61111	thea
11112	a&p	21112	click	31112	geese	41112	loon	51112	qua	61112	thee
11113	a's	21113	cliff	31113	geigy	41113	loop	51113	quack	61113	theft
11114	aa	21114	climb	31114	gel	41114	loose	51114	quad	61114	their
11115	aaa	21115	clime	31115	geld	41115	loot	51115	quaff	61115	them
11116	aaaa	21116	cling	31116	gem	41116	lop	51116	quail	61116	theme
11121	aaron	21121	clink	31121	gemma	41121	lope	51121	quake	61121	then
11122	ab	21122	clint	31122	gene	41122	lopez	51122	qualm	61122	there
11123	aba	21123	clio	31123	genie	41123	lord	51123	quark	61123	these
11124	ababa	21124	clip	31124	genii	41124	lore	51124	quarry	61124	theta
11125	aback	21125	clive	31125	genoa	41125	loren	51125	quart	61125	they
11126	abase	21126	cloak	31126	genre	41126	los	51126	quash	61126	thick
11131	abash	21131	clock	31131	gent	41131	lose	51131	quasi	61131	thief
11132	abate	21132	clod	31132	gentry	41132	loss	51132	quay	61132	thigh
11133	abbas	21133	clog	31133	genus	41133	lossy	51133	queasy	61133	thin
11134	abbe	21134	clomp	31134	gerbil	41134	lost	51134	queen	61134	thine
11135	abbey	21135	clone	31135	germ	41135	lot	51135	queer	61135	thing
11136	abbot	21136	close	31136	gerry	41136	lotte	51136	quell	61136	think
11141	abbott	21141	closet	31141	get	41141	lotus	51141	query	61141	third
11142	abc	21142	clot	31142	getty	41142	lou	51142	quest	61142	this
11143	abe	21143	cloth	31143	gf	41143	loud	51143	queue	61143	thong
11144	abed	21144	cloud	31144	gg	41144	louis	51144	quick	61144	thor
11145	abel	21145	clout	31145	ggg	41145	louise	51145	quid	61145	thorn
11146	abet	21146	clove	31146	gggg	41146	louse	51146	quiet	61146	thorny
11151	abide	21151	clown	31151	gh	41151	lousy	51151	quill	61151	those
11152	abject	21152	cloy	31152	ghana	41152	louver	51152	quilt	61152	thou
11153	ablaze	21153	club	31153	ghent	41153	love	51153	quinn	61153	thread
11154	able	21154	cluck	31154	ghetto	41154	low	51154	quint	61154	three
11155	abner	21155	clue	31155	ghi	41155	lowe	51155	quip	61155	threw
11156	abo	21156	cluj	31156	ghost	41156	lower	51156	quirk	61156	throb
11161	abode	21161	clump	31161	ghoul	41161	lowry	51161	quirt	61161	throes
11162	abort	21162	clumsy	31162	gi	41162	loy	51162	quit	61162	throw
11163	about	21163	clung	31163	giant	41163	loyal	51163	quite	61163	thrum
11164	above	21164	clyde	31164	gibbs	41164	lp	51164	quito	61164	thud
11165	abrade	21165	cm	31165	gibby	41165	lq	51165	quiz	61165	thug
11166	abram	21166	cn	31166	gibe	41166	lr	51166	quo	61166	thule
11211	absorb	21211	co	31211	giddy	41211	ls	51211	quod	61211	thumb
11212	abuse	21212	coach	31212	gift	41212	lsi	51212	quota	61212	thump
11213	abut	21213	coal	31213	gig	41213	lt	51213	quote	61213	thus
11214	abyss	21214	coast	31214	gil	41214	ltv	51214	qv	61214	thy
11215	ac	21215	coat	31215	gila	41215	lu	51215	qw	61215	thyme
11216	acadia	21216	coax	31216	gild	41216	lucas	51216	qx	61216	ti



User	Password
Stephen	auhsoJ
Lisa	hsifdrowS
James	1010NO1Z
Harry	sinocarD tupaC
Sarah	auhsoJ



User	Password Hash
Stephen	39e717cd3f5c4be78d97090c69f4e655
Lisa	f567c40623df407ba980bfad6dff5982
James	711f1f88006a48859616c3a5cbcc0377
Harry	fb74376102a049b9a7c5529784763c53
Sarah	39e717cd3f5c4be78d97090c69f4e655



User	Random Salt	Password Hash
Stephen	06917d7ed65c466fa180a6fb62313ab9	b65578786e544b6da70c3a9856cdb750
Lisa	51f2e43105164729bb46e7f20091adf8	2964e639aa7d457c8ec0358756cbffd9
James	fea659115b7541479c1f956a59f7ad2f	dd9e4cd20f134dda87f6ac771c48616f
Harry	30ebf72072134f1bb40faa8949db6e85	204767673a8d4fa9a7542ebc3eceb3a2
Sarah	711f51082ea84d949f6e3efecf29f270	e3afb27d59a34782b6b4baa0c37e2958

IMAGE SOURCE: https://www.thesecurityblogger.com/understanding-rainbow-tables/

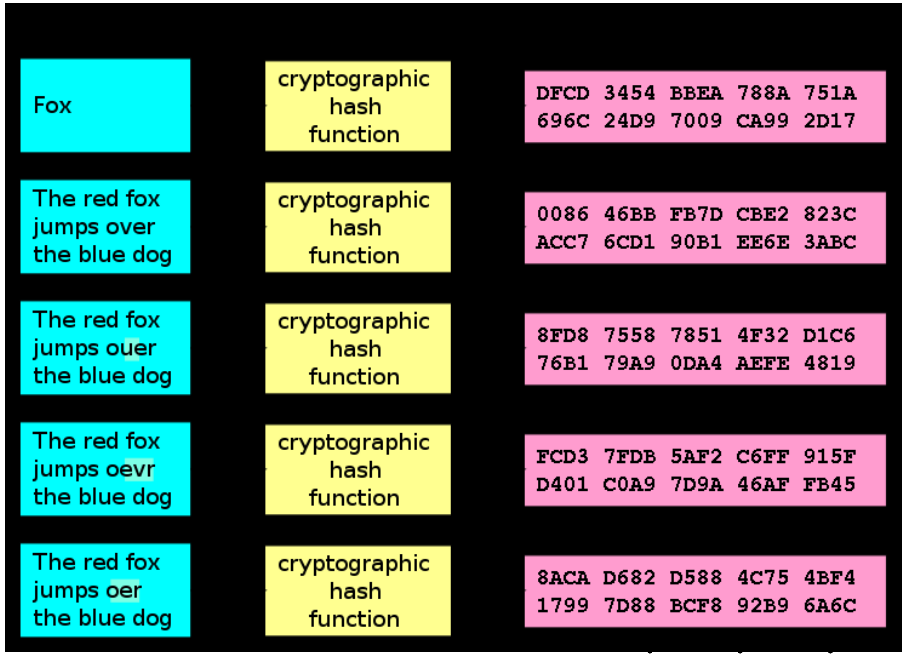
https://latesthackingnews.com/amp/2016/10/30/generate-truly-random-yet-easy-remember-passwc

Password Attacks

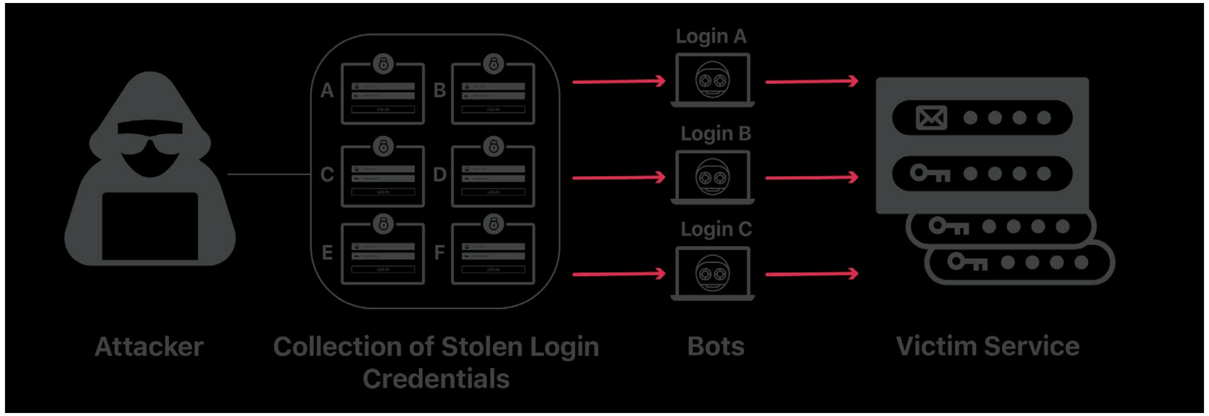
Brute Force: T1110

Just a single technique and sub-techniques

Technique	Name	Details
T1110.001	Password Guessing	Guess password in attempt to login into account
T1110.002	Password Cracking	Try to crack or recover passwords, when pass the hash is not applicable*
T1110.003	Password Spraying	Single or small list of passwords across a range of accounts
T1110.003	Credential Stuffing	Using credentials obtained from data breach



Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C



Credential hashes are passed to authenticate

IMAGE SOURCE:

https://medium.com/@cmcorrales3/password-hashes-how-they-work-how-theyre-hacked-and-how-to-maximize-security-e04b15ed98d

https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Other Authentication Methods

Non-Exhaustive List

Other methods and factors

- Certificate-based authentication
- Biometric authentication: e.g., fingerprint
- Token-based authentication: time-based one-time PIN (TOTP), reset every n seconds
- One-time password: generated for a specific login
- Push notification: approve or deny request
- Voice authentication
- Multifactor authentication
  - Something you know
  - Something you have
  - Something you are

Which are secure?

Security Policy

SWINBURNE UNIVERSITY OF TECHNOLOGY

Policy

Organisation intent, processes and objectives

Policy document outlines these in the management of risk

- Organisations will have a range of policy, outlining:
  - Technology
  - Information assets
  - Associated rules and objectives, controls
- Policy is an excellent tool to "enforce" standards, requirements, specification, processes

- It outlines things like
  - Acceptable use
  - Specification
  - Process
  - Delegation

Policy Types

Scope for policy is broad

There are many moving parts to an organisation

- Aim: employees clear on their role, what is to be done, what is acceptable
- Acceptable use policy
- Digital signature policy
- Email retention, or logging policy in general
- Removable media policy

- Too many policies can become an issue

DEMO: https://www.sans.org/information-security-policy/

USB & External Media Policy Case Study

Many organisations and government ban (through policy and technology)

Policy defines, technology implements

- Initial Ban in 2008:
- Date: November 20, 2008
- The DoD implemented a complete ban on USB thumb drives and other removable media devices. This decision came after a worm infiltrated Army networks, highlighting the security risks associated with these devices
- Restrictions: All units were prohibited from using any USB mass storage devices, including hard drives, cameras, and printers

USB & External Media Policy Case Study (cont.)

Many organisations and government ban (through policy and technology)

Policy defines, technology implements

- Partial Lift of the Ban in 2010:
- Date: February 19, 20102
- Gen. Kevin Chilton, commander of the U.S. Strategic Command, partially lifted the ban on removable devices. However, this was only allowed as a "last resort" when necessary for mission-critical tasks and when no other means of data transfer were available
- Current usage:
- Use only removable media approved by your organisation
- Do not use personally owned/non-organisational removable media on your organisation's systems
- Never plug unauthorised devices into a government system

Authorisation

While you might be able to authentication, you might not have authorisation to the request

Compare the pair

- As discussed, authentication allows a user to confirm who they are
- When authenticating, they might not be authorised to access
- The user may or may not have the permission

Monitoring

SWINBURNE UNIVERSITY OF TECHNOLOGY

System Monitoring

How are systems events handled

Broadly between Unix-based (let's just say Linux) and Windows

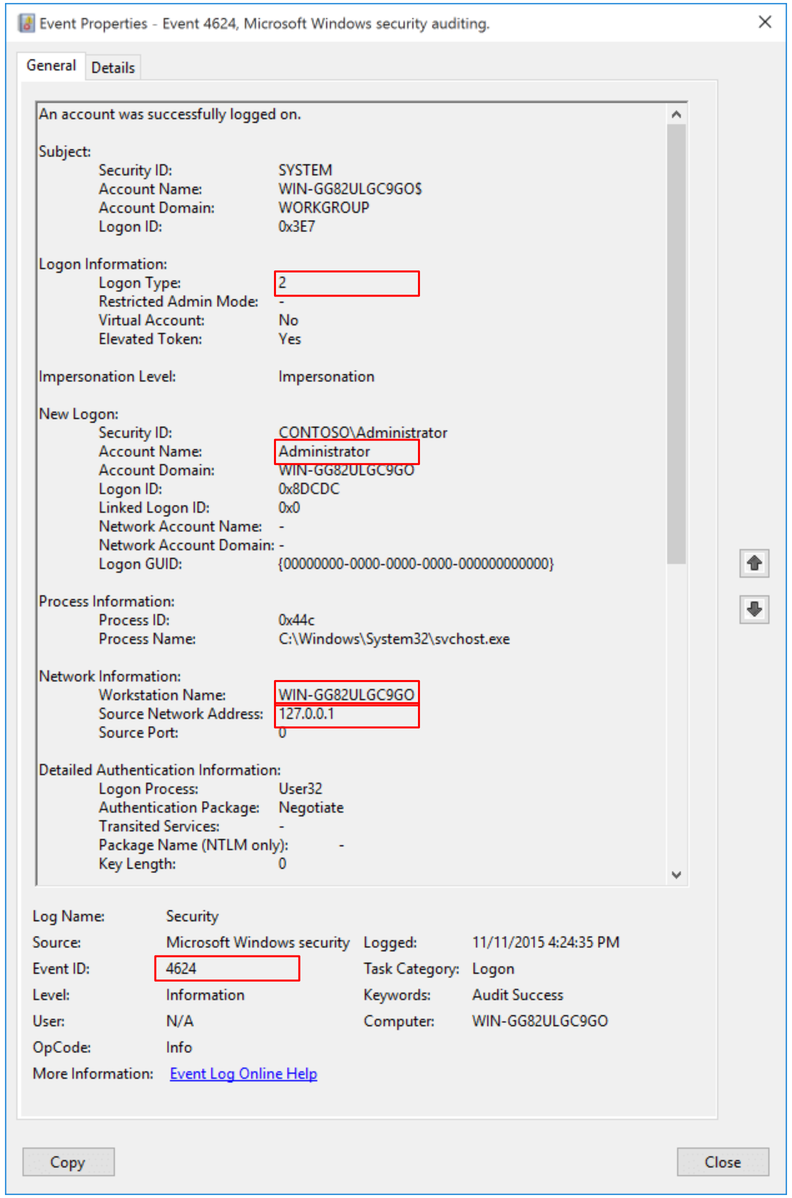
- Events occur within a system
- Event logs capture:
  - Date, time
  - Device
  - Description
  - Level
  - Associated application/process
  - Specific event type
  - Characteristic
  - Networking information in relevant
- Typically, Operating system event logs relate to
- System events from the operating system itself
- E.g., Syslog/Auth (Linux), Sysmon (Windows)
- Applications
  - Security events
  - Application logging may include
  - Request type
  - Status
  - Message
  - Networking
  - Event type
- Log structures are standardised, structured
- Logs should be centralised for monitoring
- Not everything is logged from install

An Example

Windows System Monitor Log: Event Type 4624

4624(S): An account was successfully logged on

- Administrator account logged on
- Logon type is 2, interactive
- Workstation name: WINGG82ULGC9GO
- Source network address is 127.0.0.1


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

```
An account was successfully logged on.

Subject:
        Security ID:                SYSTEM
        Account Name:               WIN-GG82ULGC9GO$
        Account Domain:             WORKGROUP
        Logon ID:                   0x3E7

Logon Information:
        Logon Type:                 2
        Restricted Admin Mode:      -
        Virtual Account:            No
        Elevated Token:             Yes

Impersonation Level:                Impersonation

New Logon:
        Security ID:                CONTOSO\Administrator
        Account Name:               Administrator
        Account Domain:             WIN-GG82ULGC9GO
        Logon ID:                   0x8DCDC
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain:     -
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x44c
        Process Name:               C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:           WIN-GG82ULGC9GO
        Source Network Address:     127.0.0.1
        Source Port:                0

Detailed Authentication Information:
        Logon Process:              User32
        Authentication Package:     Negotiate
        Transited Services:         -
        Package Name (NTLM only):          -
        Key Length:                 0
```

```
Log Name:          Security
Source:            Microsoft Windows security    Logged:          11/11/2015 4:24:35 PM
Event ID:          4624                          Task Category:   Logon
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        WIN-GG82ULGC9GO
OpCode:            Info
More Information:  Event Log Online Help
```

IMAGE SOURCE: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624

Key Windows Events

Logon, Privilege Use, Defender

Key events

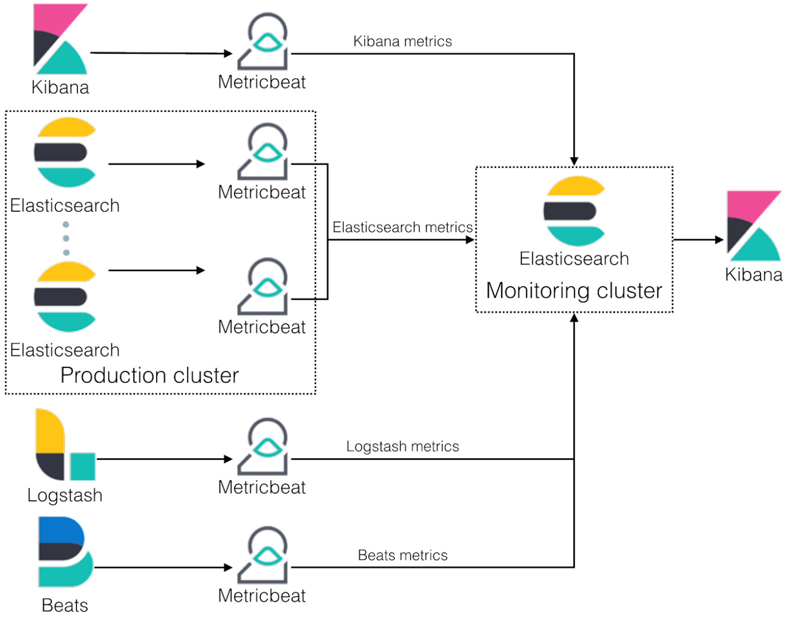
- Logon
  - 4624: User successfully logged on to a computer
  - 4625: Attempt made to logon with unknown user name or bad password and failed
  - 4822: NTLM authentication failed because the account was a member of the Protected User group
- Privilege Use
  - 4660: Object deleted
  - 4698: A scheduled task was created
  - 4699: A scheduled task was deleted
- Defender
  - 1002: malware scan stopped before completing scan
  - 1015: suspicious behaviour detected

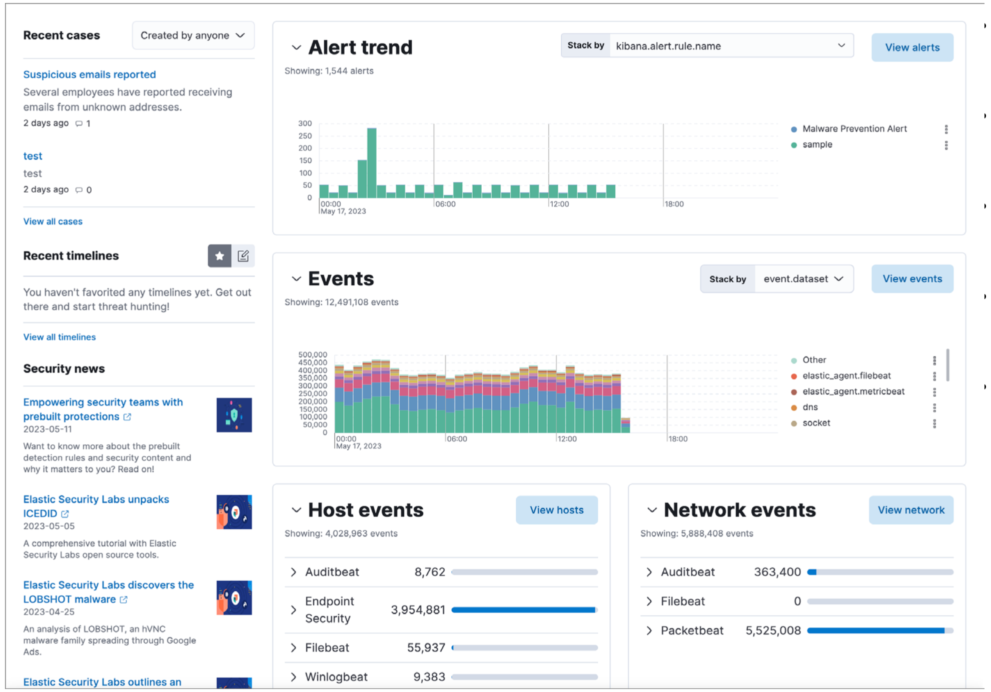
Security Information and Event Management (SIEM)

Centralise Logs

Event logs from all devices

- Ship logs to a SIEM
- Correlate events
- Investigate trends





Recent cases Created by anyone

Suspicious emails reported
Several employees have reported receiving emails from unknown addresses.
2 days ago 1

test
test
2 days ago 0

View all cases

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Security news

Empowering security teams with prebuilt protections
2023-05-11
Want to know more about the prebuilt detection rules and security content and why it matters to you? Read on!

Elastic Security Labs unpacks ICEDID
2023-05-05
A comprehensive tutorial with Elastic Security Labs open source tools.

Elastic Security Labs discovers the LOBSHOT malware
2023-04-25
An analysis of LOBSHOT, an hVNC malware family spreading through Google Ads.

Elastic Security Labs outlines an

Alert trend
Stack by: kibana.alert.rule.name
Showing: 1,544 alerts

Events
Stack by: event.dataset
Showing: 12,491,108 events

Host events
Showing: 4,028,963 events

Auditbeat	8,762
Endpoint Security	3,954,881
Filebeat	55,937
Winlogbeat	9,383

Network events
Showing: 5,888,408 events

Auditbeat	363,400
Filebeat	0
Packetbeat	5,525,008

IMAGE SOURCE: https://www.elastic.co/guide/en/elasticsearch/reference/current/monitoring-overview.html

https://www.elastic.co/guide/en/security/current/overview-dashboard.html

System Hardening

SWINBURNE UNIVERSITY OF TECHNOLOGY

System Hardening

Reduce the attack surface for a given system

A Windows example, Operating System focused

- Operating System Hardening
  - Operating System selection (secure-by-design and secure-by-default)
  - Operating environment (e.g., Internet facing DMZ, server LAN, user LAN, OT)
  - Hardening operating system configurations
  - Application management
  - Application control
  - Command & PowerShell
  - Host-based Intrusion Prevention System
  - Software Firewall
  - Antivirus
  - Device access control software (external media)
  - Operating system event logging

- But also:
  - User Application Hardening
  - Server Application Hardening
  - Authentication Hardening
  - Virtualisation Hardening

See for resources: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

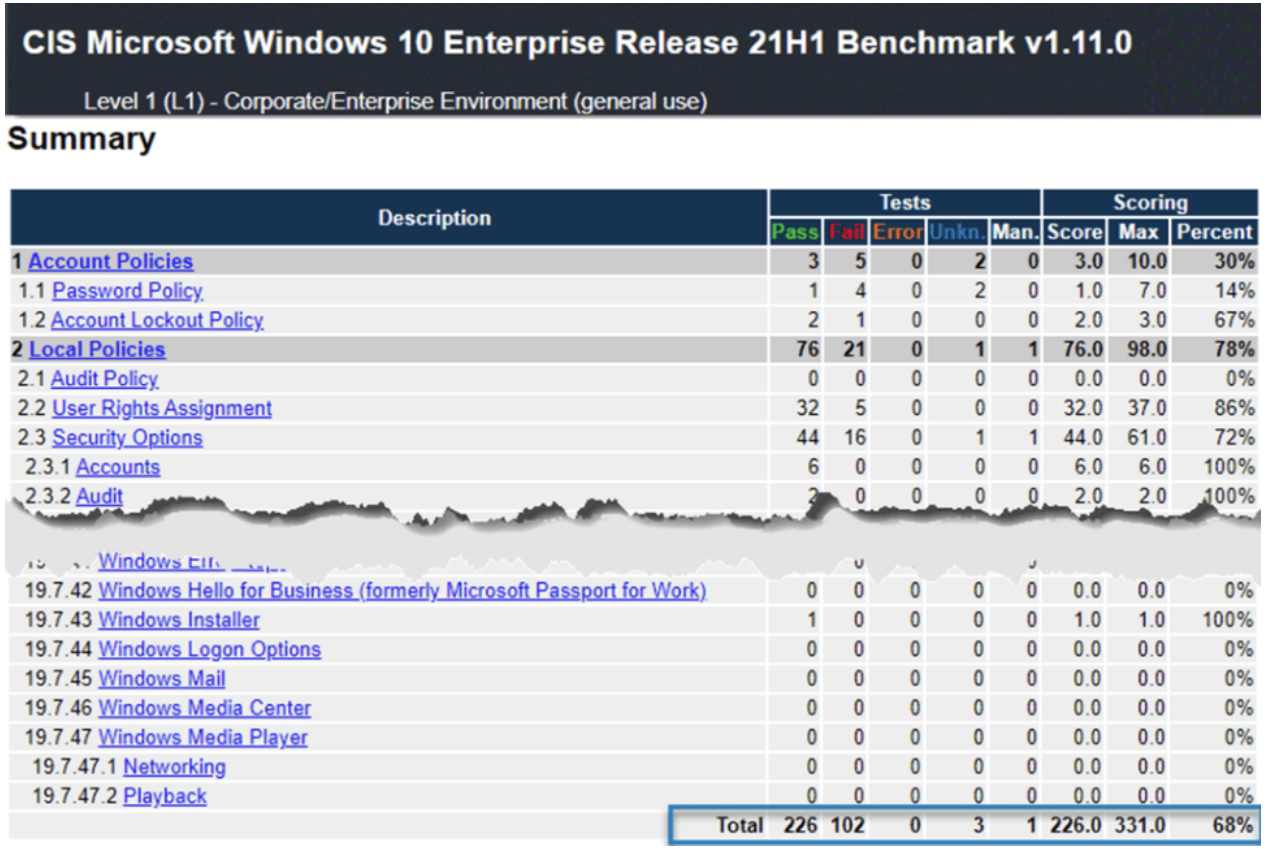
Semi-Automated Hardening

CENTER for INTERNET SECURITY

CIS Benchmarks

Benchmarks provided to harden a range of areas and maturity levels

- Cloud
- Desktop Software
- DevSecOps Tools
- Mobile Devices
- Multi Function Print Devices
- Network Devices
- Operating Systems
- Server Software



CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

Level 1 (L1) - Corporate/Enterprise Environment (general use)

Summary

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Account Policies	**3**	**5**	**0**	**2**	**0**	**3.0**	**10.0**	**30%**
1.1 Password Policy	1	4	0	2	0	1.0	7.0	14%
1.2 Account Lockout Policy	2	1	0	0	0	2.0	3.0	67%
2 Local Policies	**76**	**21**	**0**	**1**	**1**	**76.0**	**98.0**	**78%**
2.1 Audit Policy	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	32	5	0	0	0	32.0	37.0	86%
2.3 Security Options	44	16	0	1	1	44.0	61.0	72%
2.3.1 Accounts	6	0	0	0	0	6.0	6.0	100%
2.3.2 Audit	2	0	0	0	0	2.0	2.0	100%
19.7.42 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0	0.0	0.0	0%
19.7.43 Windows Installer	1	0	0	0	0	1.0	1.0	100%
19.7.44 Windows Logon Options	0	0	0	0	0	0.0	0.0	0%
19.7.45 Windows Mail	0	0	0	0	0	0.0	0.0	0%
19.7.46 Windows Media Center	0	0	0	0	0	0.0	0.0	0%
19.7.47 Windows Media Player	0	0	0	0	0	0.0	0.0	0%
19.7.47.1 Networking	0	0	0	0	0	0.0	0.0	0%
19.7.47.2 Playback	0	0	0	0	0	0.0	0.0	0%
Total	226	102	0	3	1	226.0	331.0	68%

IMAGE SOURCE: https://nira.com/cis-benchmarks-and-compliance/

Physical and Converged Security

SWINBURNE UNIVERSITY OF TECHNOLOGY

Physical Security

Physical security refers to the measures taken to protect physical assets, such as people, property, and resources, from unauthorised access, theft, damage, or harm

Physical security is as much as cyber risk as information security

- Physical security framework is made up of three main components:
  - Access Control
  - Surveillance
  - Testing
- Protection of people, space/dwelling, equipment, inventory, or information

- The success of an organisation's physical security program can often be attributed to how well each of these components is implemented, improved, and maintained

Physical Security Importance

Expected protection

Many similarities to cyber security considerations

- Reputation management: protect a company's reputation by preventing incidents that could damage its image
- Compliance with regulations: banks and financial institutions are required to have certain security measures in place to protect customer information
- Perimeter Barriers: Physical barriers such as walls, fences, and gates can be used to prevent unauthorised access to a facility or area. They can also be used to control the flow of people and vehicles entering and exiting a site.
- Security Personnel: Security personnel such as guards, patrols or on-site officers can provide a physical presence to deter potential intruders, respond to security incidents, and monitor activity in and around a facility
- Alarm Systems: Alarm systems can be used to detect and alert security personnel to potential security breaches. These can include burglar alarms, fire alarms, and motion sensors
- Regular audits: All security checks should be regularly audited to ensure that everything is working as expected.
- Incident Response: The organisation should be prepared to handle incidents to ensure a rapid, organised and effective response

Physical Security Measures

Access Control, Surveillance, Testing

Protection of people, space/dwelling, equipment, inventory, or information

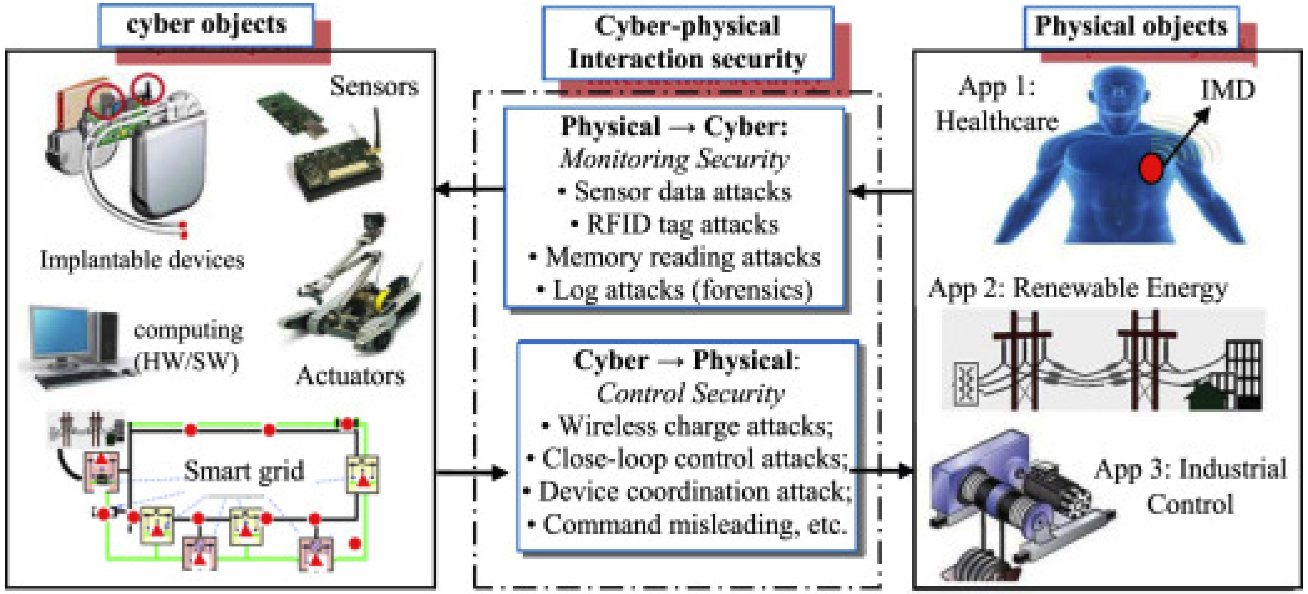
- Access Control
- limit access to certain assets to authorised personnel only
- ID Cards, Card Readers, Biometric Readers, Locks
- Potentially electronic logging
- Surveillance
- Monitoring, CCTV, personal to monitor physical assets
- Testing
- Audit, review, exercise

Physical Meets Cyber

Cyber Physical Systems (CPS)

Given the interconnection between domains

- Integration of physical and computing components
- Physical process, resources or assets
- Computing algorithms, sensors, networking
- Physical objects become relevant in a digital space
- Cyber tactics applicable in real world physical objects
- A gap in control anomaly detection allows a cyber attack to halt energy production, resulting in loss of power, potential physical loss of life (medical, transport), theft (security systems)
- A gap in access controls allows a commercial printing services allows attackers to compromise kiosk and access to internal networks



cyber objects
Sensors
Implantable devices
computing (HW/SW)
Actuators
Smart grid
Cyber-physical Interaction security
Physical → Cyber: *Monitoring Security*
• Sensor data attacks
• RFID tag attacks
• Memory reading attacks
• Log attacks (forensics)
Cyber → Physical: *Control Security*
• Wireless charge attacks;
• Close-loop control attacks;
• Device coordination attack;
• Command misleading, etc.
Physical objects
App 1: Healthcare
IMD
App 2: Renewable Energy
App 3: Industrial Control

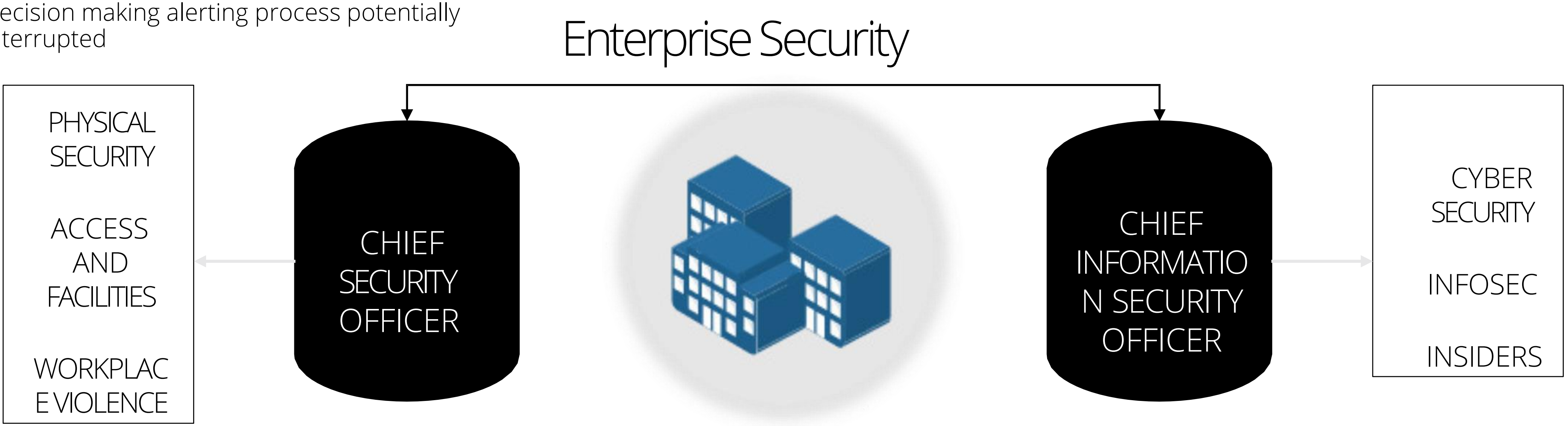
IMAGE SOURCE: Hu et al., Robust Cyber–Physical Systems: Concept, models, and implementation, Future Generation Computer Systems

Converged Security

Traditional practice sees two roles to maintain security

Keeping these functions separated

- Security functions operating separately Management lack visibility and oversight
- Possible counterproductive decision making
- Decision making alerting process potentially interrupted



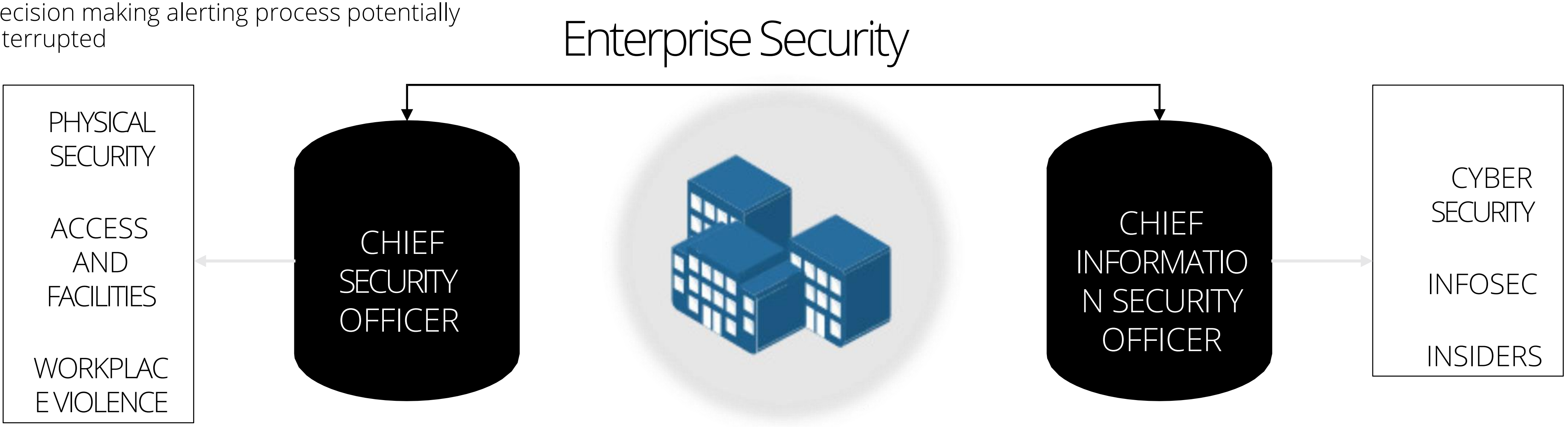
Converged Security

Traditional practice sees two roles to maintain security

Keeping these functions separated

- Security functions operating separately Management lack visibility and oversight
- Possible counterproductive decision making
- Decision making alerting process potentially interrupted

- Blend of controls to better maintain assets, people and processes



Converged Security

Case Study

How to rob a casino

- Has anyone ever walked in the front door and gotten away with it?
- Occasionally yes, these things do happen, possibly a breakdown between physical and cyber systems?
- Why go in through the front door, why not through the fish tank?

IMAGE SOURCE: https://filmthreat.com/features/ranking-the-oceans-movies-from-worst-to-best/
https://www.hackread.com/hackers-casinos-fish-tank-smart-thermometer-hack/

Assignment 1

SWINBURNE
UNIVERSITY OF
TECHNOLOGY