

. . . . .  
. . . . .

# COS80013

# Internet Security

Week 7

**Presented by Dr Rory Coulter**

14 April 2025



. . .  
. . .

. . . . .  
. . . . .

• • • • •  
• • • • •

# 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.

• •  
• •

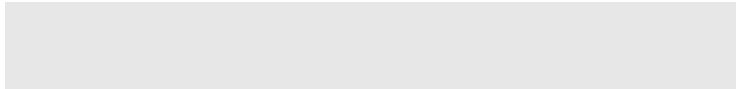
• • • • • • • • • • • • •  
• • • • • • • • • • • • •



. . . . .  
. . . . .  
. . . . .

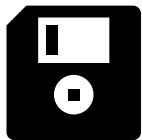
# Data, Information, and Intelligence

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .

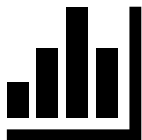


# Data, Information, Intelligence

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 decision
- Not: complete (as possible)

\* as possible



# Data, Information, Intelligence

## In cyber terms

### Data

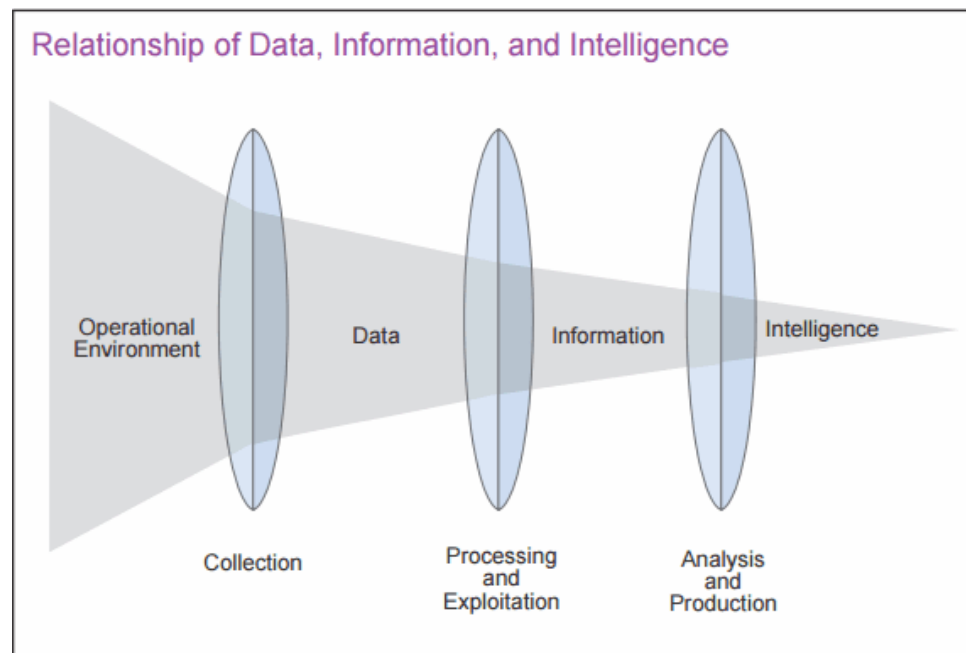
- Easy observed as indicators of compromise (IoC)
- IP, domain name, adversary group, time, hash

### 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

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .

# 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



# 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 use of, processed and transformed into the required format
- Data to information

## Analysis

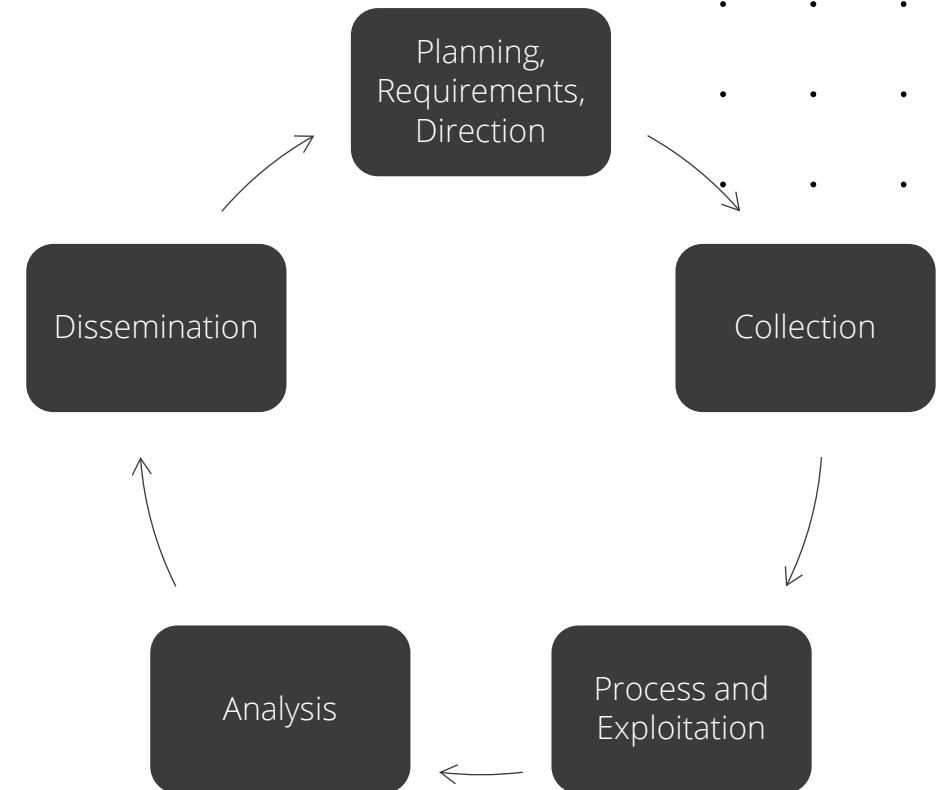
- Refinement of information
- Objective, timely, accurate, and actionable
- Apply induction, deduction, abduction and the scientific method

## Dissemination:

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

## Feedback:

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



# Information Sources

Information of value can be collected from a range of sources

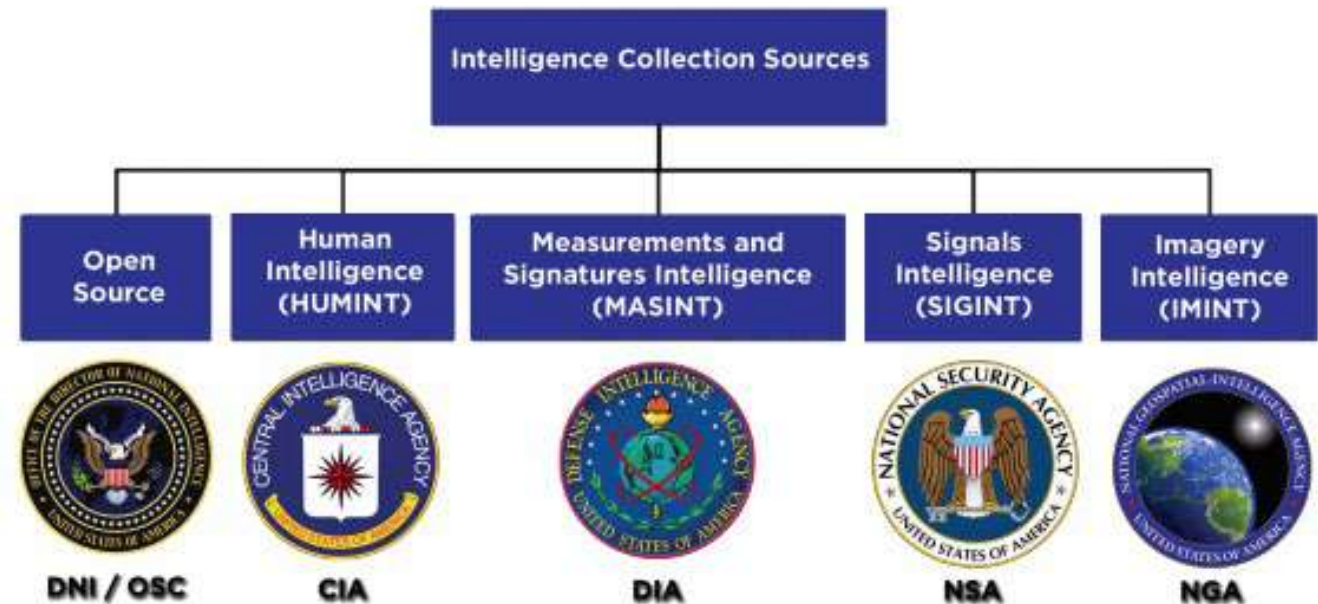
Human Intelligence (HUMINT)

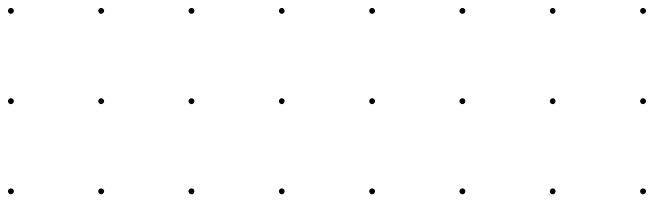
Signals Intelligence (SIGINT)

Imagery Intelligence (IMINT)

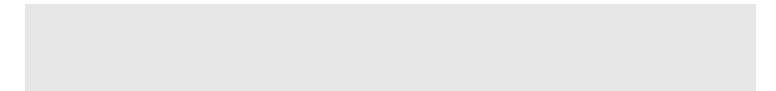
Measurement and Signatures Intelligence (MASINT)

Open-Source Intelligence (OSINT)





# Cyber Intelligence

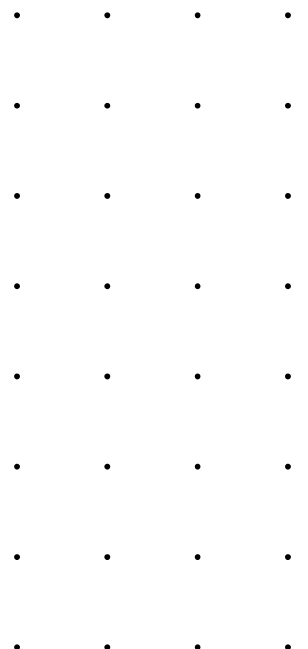


# Detecting and Understanding Threats

**There is a constant evolution of threats, adversaries and challenges**

How do we:

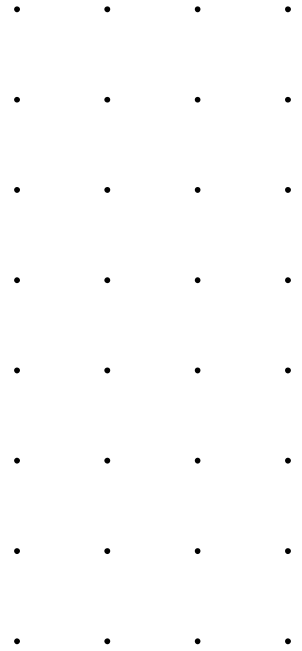
- Keep up to date with different attackers, threats?
  - Stay aware of actor and threat TTPs? (Mitre ATT&CK)
  - Manage to detect malware, network attacks, scams, and other threats
  - Make sure AV, IDS/IPS, EDR, Firewall, WAF, SIEM, etc. stay up to date the historical and the latest threats?
  - What 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)

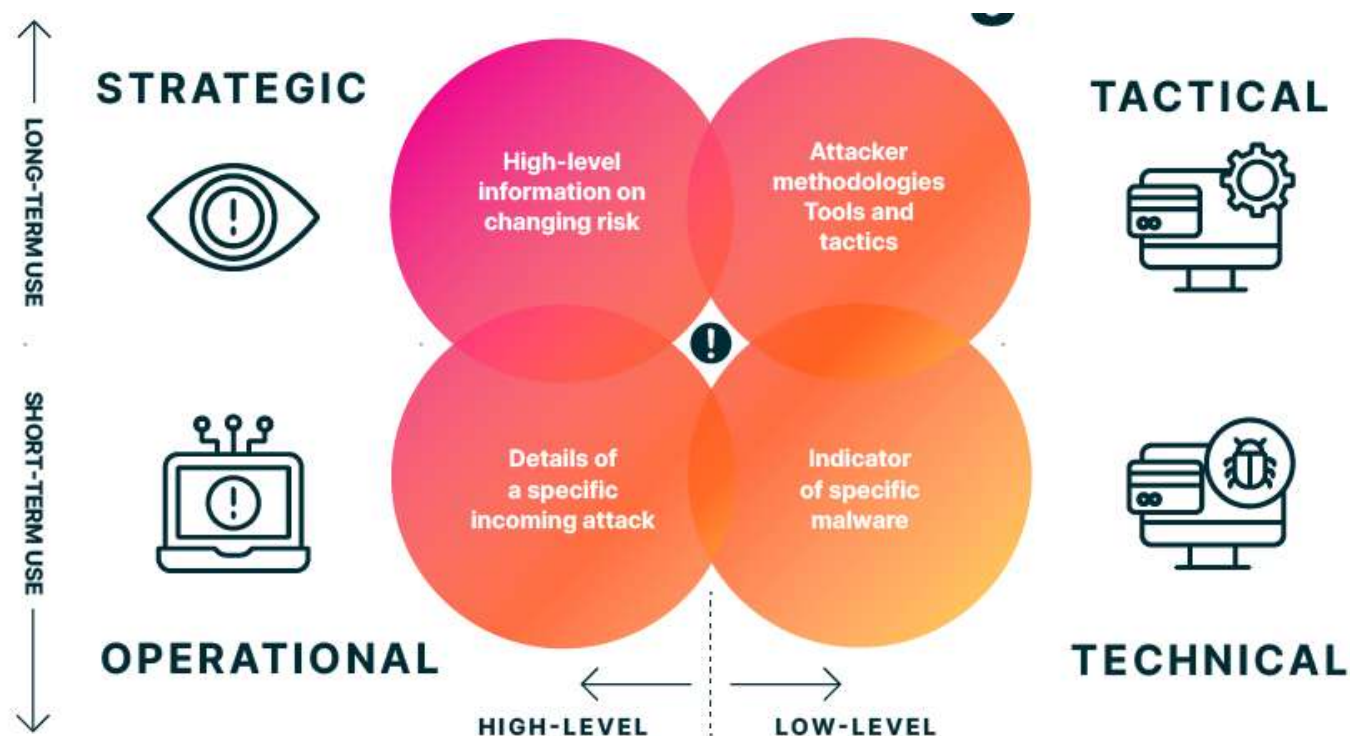
## Indicate an incident has taken place

- 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



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

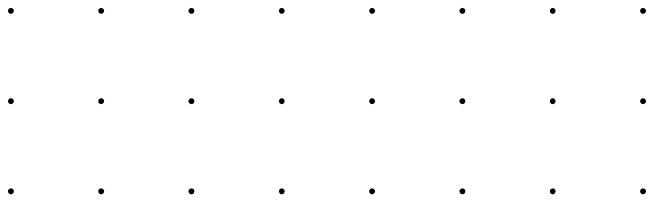
# Internal & External Threat Intelligence Sources

## 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



# 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



# Common Cyber Espionage Tactics

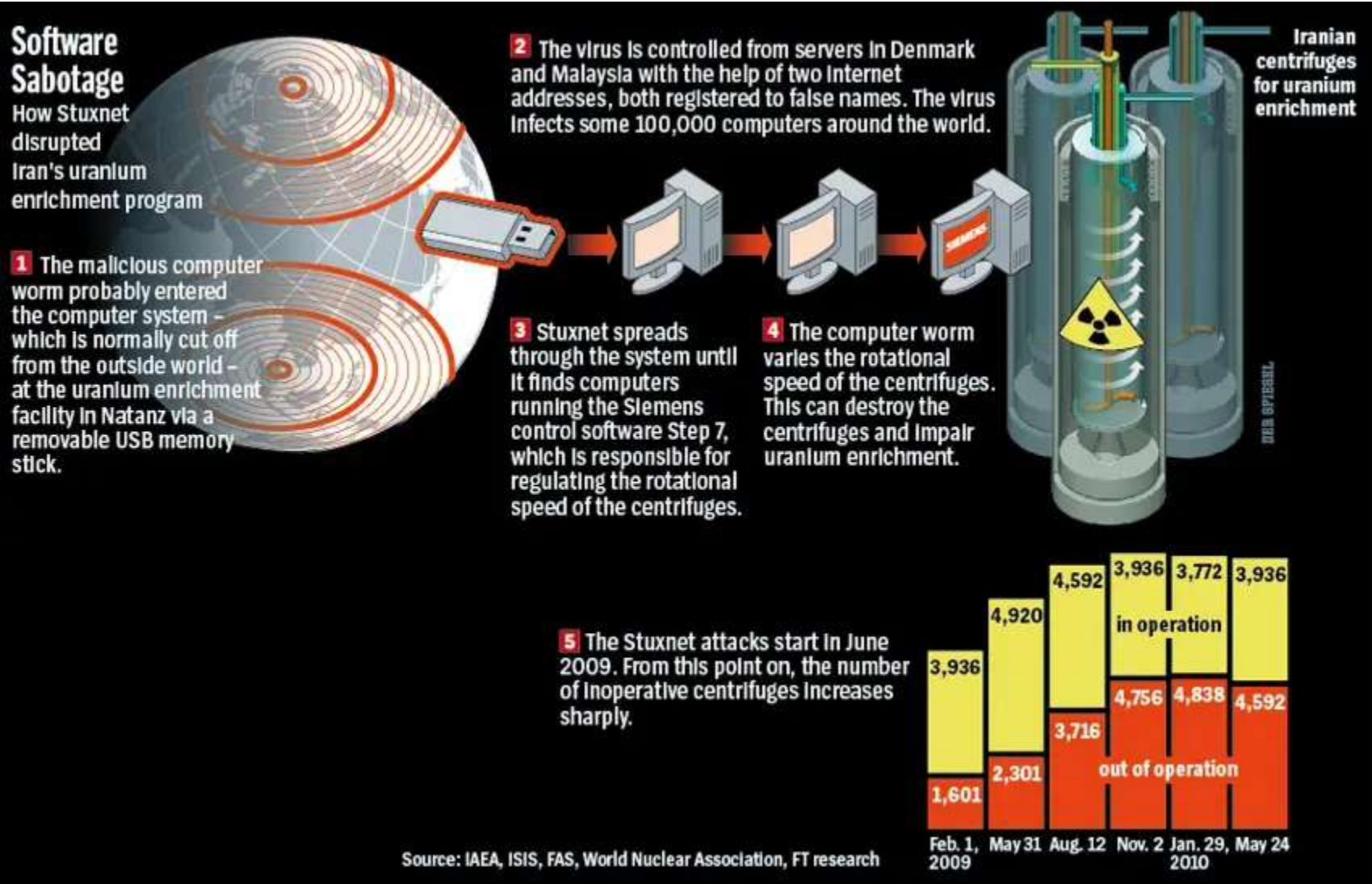
## Common attack techniques include:

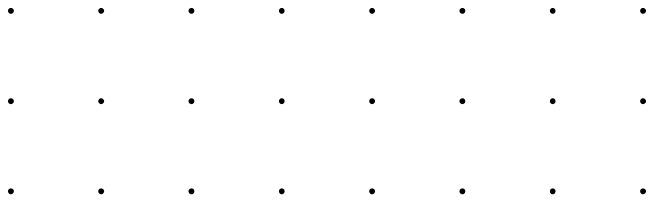
- **Watering hole:** Malicious actors are able to infect legitimate websites commonly visited by the victim or people associated with the target with malware for the explicit purpose of compromising the user
- **Spear-phishing:** A hacker targets specific individuals with fraudulent emails, texts and phone calls in order to steal login credentials or other sensitive information
- **Zero-day exploits:** Cybercriminals 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

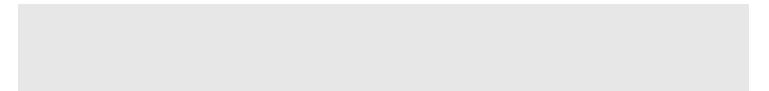
Hacking & malware	Deploying malware or hacking into existing software to gain access to sensitive data
Phishing	Sending emails tricking employees into disclosing confidential information by clicking a malicious link
Eavesdropping	Imitating a trusted server to track valuable information or gain data through 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

# Stuxnet – A Classic Example





# TLP



# Traffic Light Protocol

**The Traffic Light Protocol (TLP) is a system for sharing sensitive information securely**

Uses different colour-coded levels to indicate the degree of restriction on access and use

- Introduced to aid and support information sharing (with appropriate audience)
- TLP isn't a classification scheme (e.g., Secret, Top Secret)
- Designations:
  - TLP:RED
  - TLP:AMBER+STRICT
  - TLP:AMBER
  - TLP:GREEN
  - TLP:CLEAR

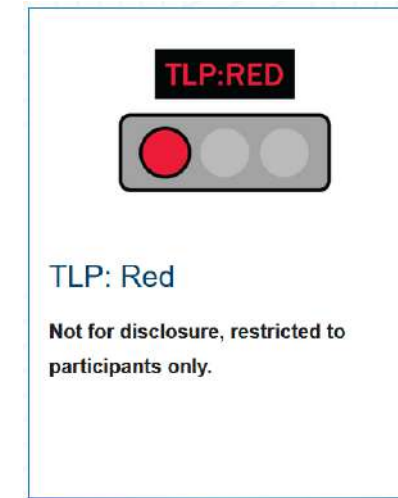


# Traffic Light Protocol(cont.)

## TLP:RED is the highest level of restriction

Information marked as TLP: RED should not be disclosed and is restricted to participants only

- It is used when sharing the information could pose significant risks to privacy, reputation, or operations of the organisations involved
- Recipients may not share TLP: RED information with parties outside of the specific exchange, meeting, or conversation where it was originally disclosed
- TLP: RED information is usually exchanged verbally or in person



# Traffic Light Protocol(cont.)

## TLP:AMBER+STRICT

TLP:AMBER+STRICT indicates a high level of restriction

- It is used when information requires support but still carries risks to privacy, reputation, or operations if shared outside the organisation
- Recipients may only share TLP: AMBER+STRICT information with members of their own organisation on a need-to-know basis to protect their organisation and prevent further harm



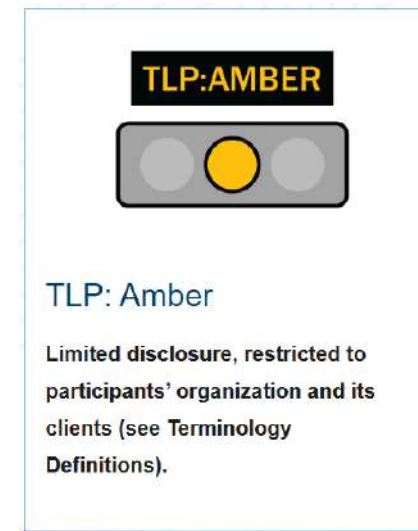


# Traffic Light Protocol(cont.)

## TLP:AMBER

TLP:AMBER signifies limited disclosure

- It is used when information requires support but still carries risks if shared outside the organisations involved
- TLP: AMBER+STRICT should be used to restrict sharing to the recipient organisation only
- Recipients may share TLP: AMBER information with members of their own organisation and its clients on a need-to-know basis to protect their interests





## Traffic Light Protocol(cont.)

**TLP:GREEN indicates limited disclosure**

It is used when information can increase awareness within a specific community

- Recipients may share TLP: GREEN information with peers and partner organisations within their community but not through publicly accessible channels
- TLP: GREEN information is typically shared within the cyber security or cyber defence community

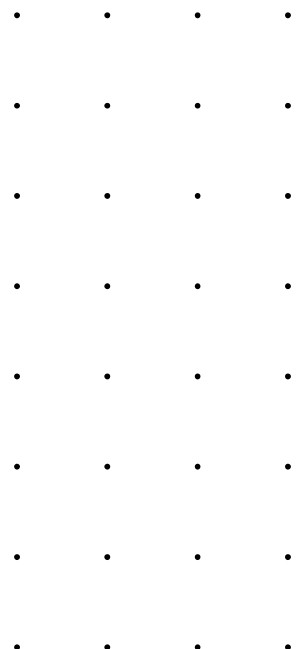


# Traffic Light Protocol(cont.)

## TLP:CLEAR signifies no significant restrictions on disclosure

It is used when information carries minimal or no foreseeable risk of misuse

- Recipients can share TLP:CLEAR information without restriction, following standard copyright rules and procedures for public release



# A Threat Advisory

## Let's look at a way intelligence is shared

TLP:CLEAR The what

- A Cyber Threat Advisory is a formal communication that provides organisations and individuals with critical information about potential or active cyber security threats
- Released by government and vendors
- Cyber Threat Advisories are typically issued by trusted cybersecurity authorities, government agencies, or industry-specific information sharing and analysis centres (ISACs)
- Primary purpose of a Cyber Threat Advisory is to raise awareness about specific cyber threats, vulnerabilities, or incidents that could impact an organisation's security

# A Threat Advisory (cont.)

## Let's look at a way intelligence is shared

TLP:CLEAR What may be covered

- Threat Description: Detailed information about the nature and characteristics of the cyber threat
- Indicators of Compromise (IoCs): Specific data or artifacts associated with the threat
- Vulnerabilities: Information about any software or hardware vulnerabilities being exploited
- Mitigation and Remediation: Guidance on how to detect, prevent, and respond to the threat
- Impact Assessment: An analysis of the potential impact on affected systems or networks
- Recommendations: Actions that organisations should take to protect themselves

# A Threat Advisory (cont.)

Let's look at a way intelligence is shared

Two Examples

- Top Vulnerabilities
  - See below for the link
- Actor Profile
  - See below for the link



[https://www.cyber.gov.au/sites/default/files/2023-08/aa23-215a\\_joint\\_csa\\_2022\\_top\\_routinely\\_exploited\\_vulnerabilities.pdf](https://www.cyber.gov.au/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf)

<https://www.cyber.gov.au/sites/default/files/2023-02/2023-01%20-%20ACSC%20Ransomware%20Profile%20-%20Royal.pdf>

• • • • • • • •  
• • • • • • • •  
• • • • • • • •

# Classification

• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •

# Classification

**Security classification is applied to information to keep sensitive information protected**

We know the levels

- To access sensitive information you're going to need a security clearance
- Should you obtain one, you will be able to access information that is\*:
- Top Secret
- Secret
- Protected
- I just learned about TLP, what's the difference?
- TLP Red is a classification often used in the context of cyber security and information sharing
- Primarily to protect sensitive data related to ongoing cyber threats
- Top Secret, a traditional classification used in the context of national security
- Covers a wide range of sensitive information beyond cyber security
- Much stricter access controls and longer classification durations (TLP:RED could be just for an organisation only)

\* Likely in these ranges, depends where you obtain your clearance

# Levels

## Protected, Secret, Top Secret

Let's get to know all three

- PROTECTED:

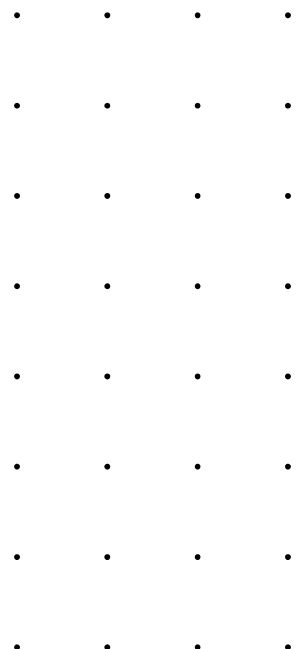
- Damage: Compromise would cause damage, but not exceptionally grave
- Example: Information that, if compromised, would seriously impede the development or operation of major policies. The damage would be significant but not catastrophic

- SECRET:

- Damage: Compromise would cause serious damage
- Example: Information where compromised confidentiality could shut down or substantially disrupt significant national infrastructure. The damage would be severe and could have a substantial impact on critical systems

- TOP SECRET:

- Damage: Compromise would cause exceptionally grave damage
- Example: Information where compromised confidentiality would provoke international conflict. This level of damage is the most severe and could have far-reaching consequences, potentially leading to serious international consequences or conflicts



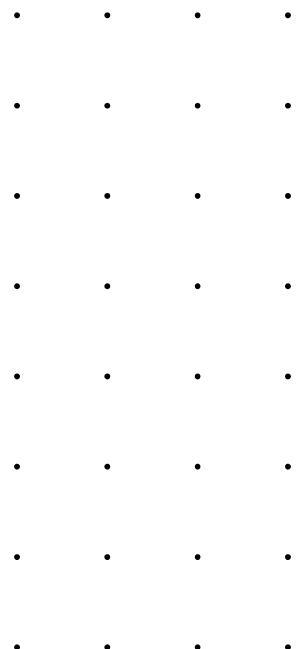


# Protective Security Policy Framework (PSPF)

## How Australian Government entities handle classified information

Security classification can apply to both the information itself and assets like USB drives or laptops

- PSPF also defines three levels of security classified information: Protected, Secret, and Top Secret
- Maybe be Australian, or in collaboration with other Governments
- Restrict information based on citizenship: Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO), and Releasable To (REL)





# Incident Response

# Events and Incidents

## Terms to follow along with

Event, Adverse Event, Computer Security Incident, Incident Response, Incident Response Plan

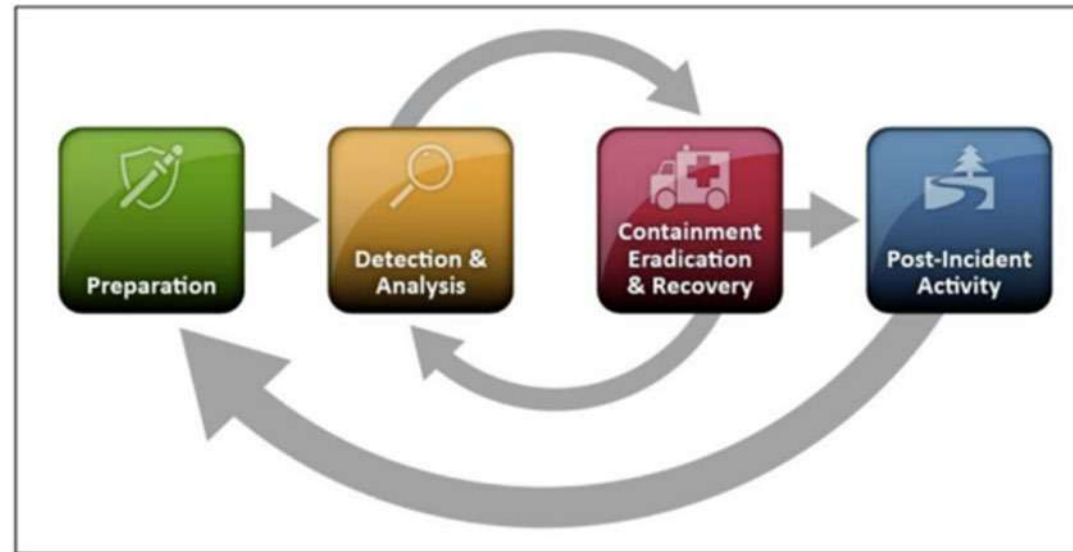
- Event:
  - Any observable occurrence in a system or network
  - Downloading a file, requesting a webpage, logging on, opening a document
- Adverse Event:
  - Event with a negative consequence
  - System crash, destruction of data, unauthorised access (are there non cyber events which are adverse?)
- Computer Security Incident:
  - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
  - Data is encrypted and held to ransom
  - Sensitive data is accessed
- Incident Response:
  - The mitigation of violations of security policies and recommended practices
  - Incident response enables quick best practice response in a systematic way
- Incident Response Plan:
  - Minimise impact, facilitate improvements to handling future incidents
  - Business aims focus on restoring service and operations

# What is Incident Response

**Incident Response is an organised approach to managing a cyber security incident**

Incident types include

- Ransomware
- Business email compromise
- Phishing
- Data breach
- Denial of service
- Network compromise
- Steps are not always uniform or in succession
- Attacks vary, threat actor tactics are always evolving

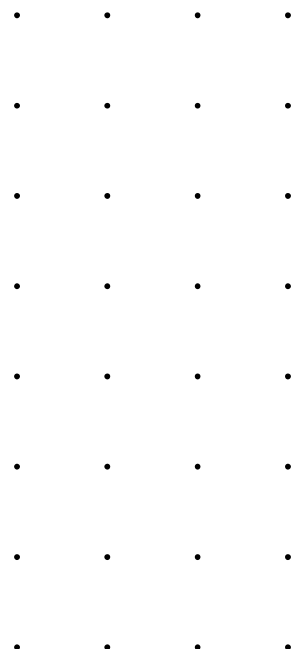


# Main Outcomes of Incident Response

**The overarching outcome is to minimise the impacts for the affected organisation**

This can be achieved through a range of actions

- Answer key forensic questions
- Leverage threat intelligence
- Communicate effectively and accurately to those with a need to know
- Fixing things effectively (that is, doing things that matter and avoiding mistakes)
- Note: A mix of disciplines is desirable to help establish fully effective Incident Response teams



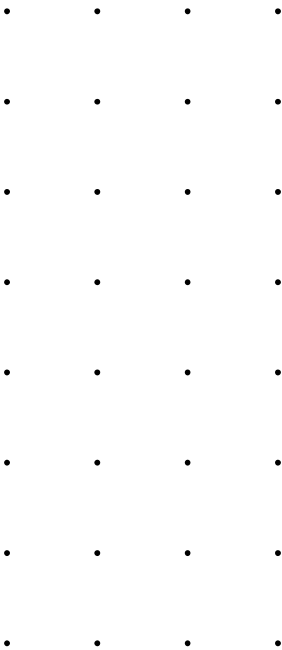
# Common Mistakes

## COMMON MISSTEPS

Common missteps an organization can make when first responding



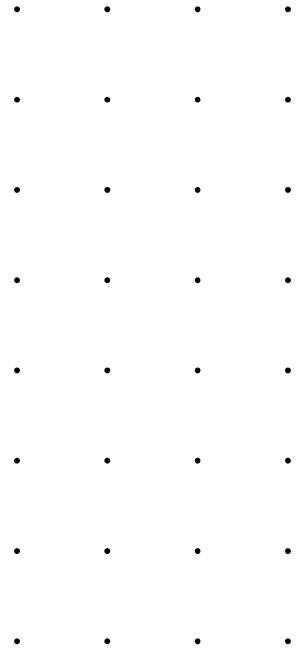
Mitigating the affected systems before responders can protect and recover data	
Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)	
Preemptively blocking adversary infrastructure	
Preemptive credential resets	
Failure to preserve or collect log data that could be critical to identifying access to the compromised systems	
Communicating over the same network as the incident response is being conducted (ensure all communications are held out-of-band)	
Only fixing the symptoms, not the root cause	



SOURCE: US-CERT

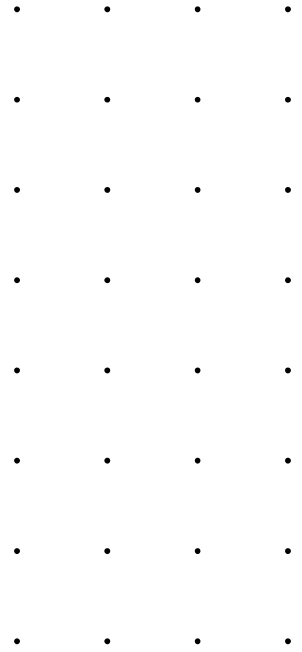
# Preparation Phase

- Develop an incident response policy, plan, and strategy tailored to the organisation's specific needs
- Establish an incident response team with defined roles and responsibilities
- Conduct training and exercises to ensure readiness and familiarity with the incident response plan
- Implement measures for proactive incident detection and prevention
- Establish relationships and lines of communication with external entities such as law enforcement and incident response coordination centres



# Detection and Analysis Phase

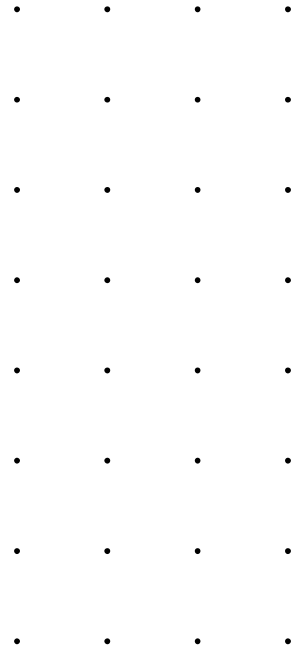
- Deploy systems and technologies to detect and alert on potential security incidents
- Monitor and analyse system logs, network traffic, and other sources of information to identify indications of compromise
- Investigate and assess potential incidents to determine their nature, scope, and impact
- Preserve evidence and maintain a chain of custody for legal and forensic purposes
- Share relevant information with appropriate stakeholders and coordinate response efforts





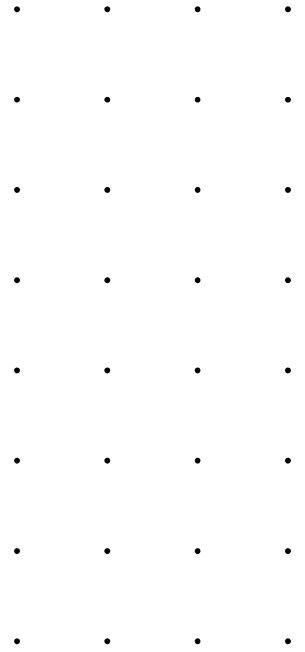
# Containment, Eradication, and Recovery Phase

- Take immediate actions to contain the incident and prevent further damage or unauthorised access
- Remove or mitigate the cause of the incident and restore affected systems to a secure state
- Apply patches, updates, or configurations to address vulnerabilities exploited in the incident
- Recover from the incident by restoring data, systems, and services from secure backups
- Validate the effectiveness of containment, eradication, and recovery measures



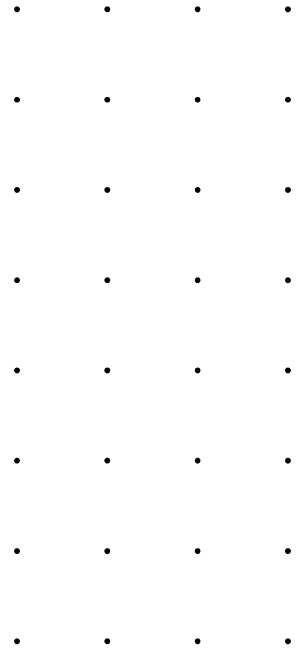
# Post-Incident Activity Phase

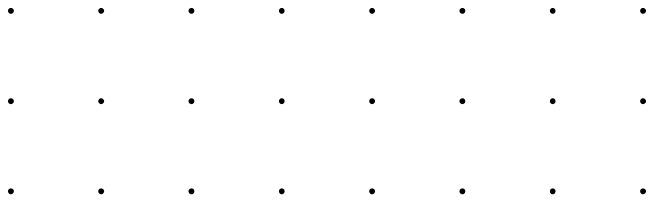
- Conduct a comprehensive review and analysis of the incident response process to identify areas for improvement
- Update incident response plans, policies, and procedures based on lessons learned
- Share information about the incident with appropriate stakeholders to prevent similar incidents
- Provide feedback to external entities such as law enforcement or incident response coordination centres
- Conduct post-incident activities such as reporting, documentation, and debriefing sessions
- Look broadly to identify systemic issues



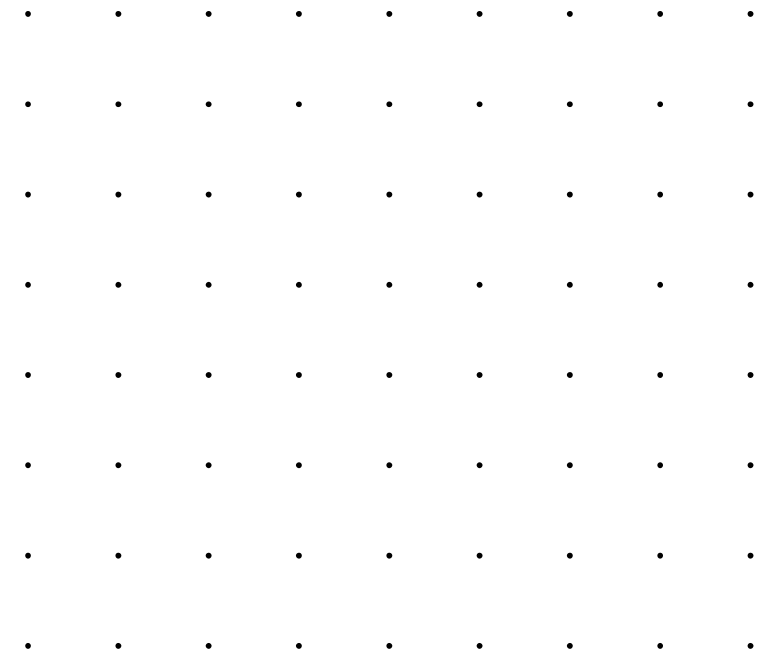
# Incident Response Phases - Ransomware

- Ransomware poses different threats and challenges
- Time is of importance when responding, isolating hosts so the malware does not spread further
- CISA propose the following phases
  - Detection and Analysis
    - Determine which systems, isolate immediately
  - Containment and Eradication
    - Collect evidence, understand threat, rebuild
  - Recovery and Post-Incident Activity
    - Restore and review





# Pyramid of Pain

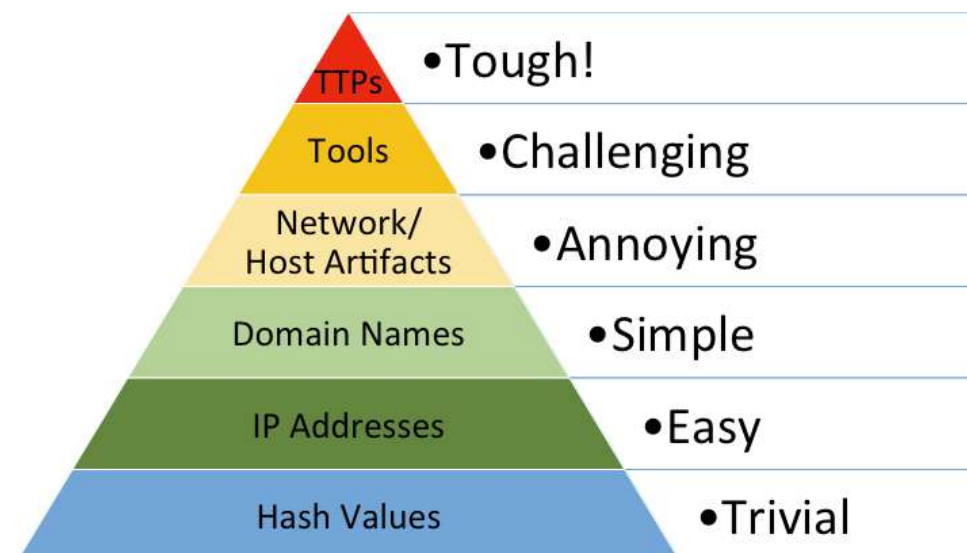


# The Pyramid of Pain

**The Pyramid of Pain classifies indicators based on their level of difficulty for threat actors to alter or evade**

Indicators higher up the pyramid hold greater value for defenders as they signify more enduring and dependable signs of compromise

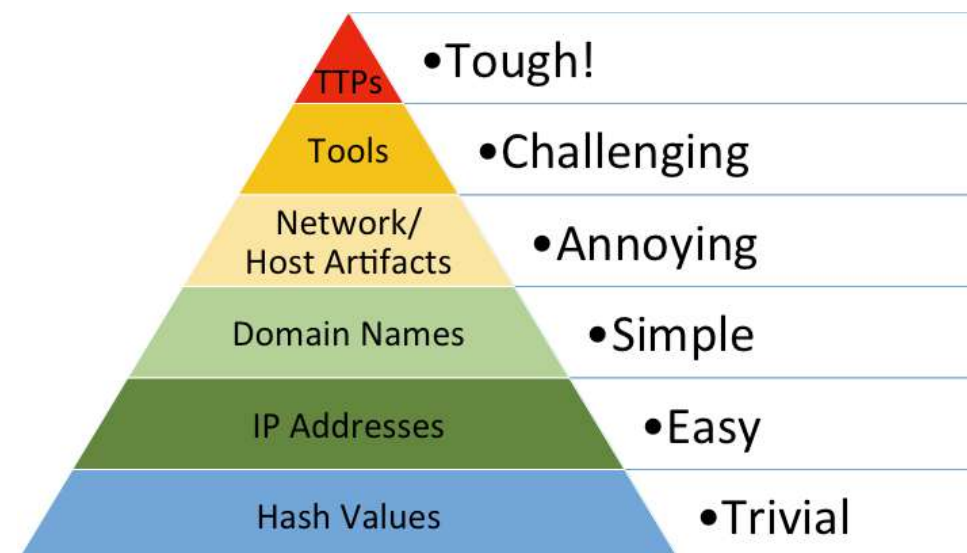
- The Pyramid of Pain represents different levels of indicators, starting from easily changeable indicators like hash values and IP addresses, progressing to more impactful indicators such as network and host artifacts, tools, and ultimately targeting the adversary's tactics, techniques, and procedures (TTPs)
- By focusing on higher levels of the pyramid, defenders can disrupt adversaries' activities and force them to adapt, ultimately increasing the cost and effort required for the adversaries to continue their attacks



# The Pyramid of Pain

## Types of Indicators

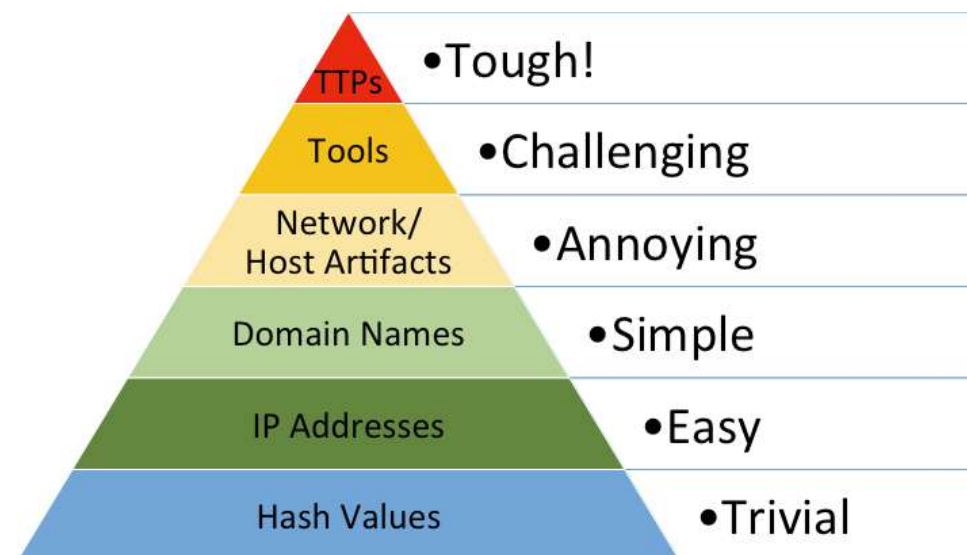
- Hash Values: Unique cryptographic representations of files
- IP Addresses: Numerical labels assigned to network-connected devices
- Domain Names: Human-readable addresses used to access resources on the internet
- Network Artifacts: Observables caused by adversary activities on a network
- Host Artifacts: Observables caused by adversary activities on hosts
- Tools: Software used by adversaries to accomplish their mission
- Tactics, Techniques, and Procedures (TTPs): Adversaries' methods and behaviors throughout the attack lifecycle

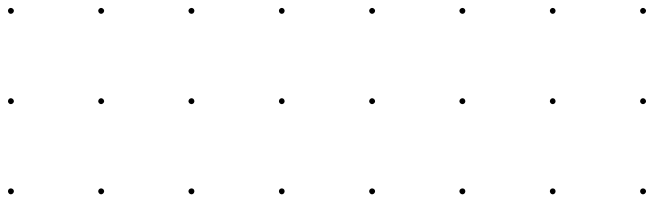


# The Pyramid of Pain

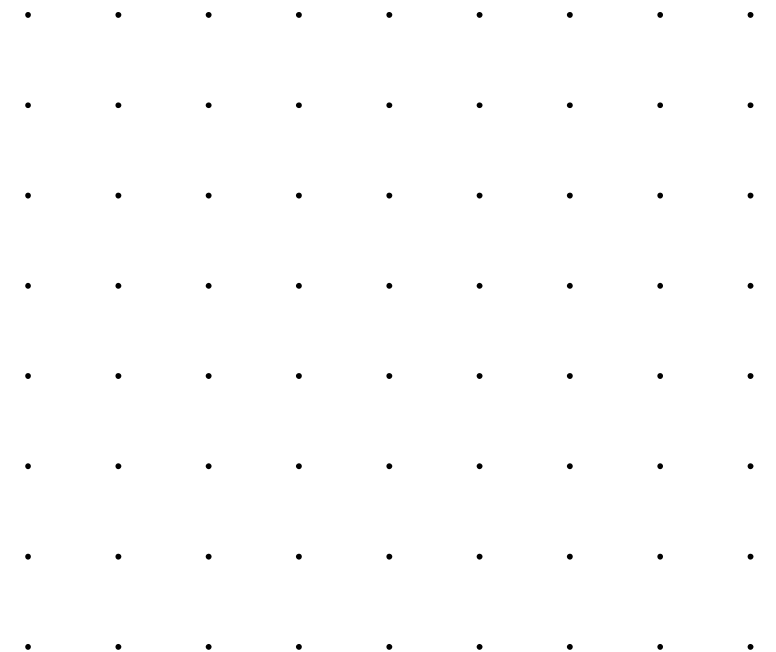
## The Pyramid Explained

- Hash Values: Most accurate indicators but easily changeable
- IP Addresses: Fundamental indicators that can be changed effortlessly
- Domain Names: Slightly harder to change than IP addresses
- Network & Host Artifacts: Impact the adversary and force reconfiguration of tools
- Tools: Taking away the adversary's ability to use specific tools
- Tactics, Techniques, and Procedures: Operating directly on adversary behaviors, the most effective level





# Remediation



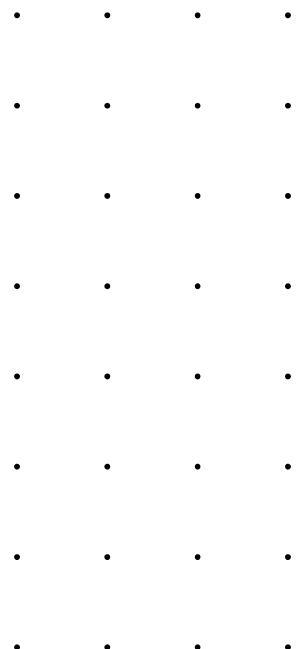


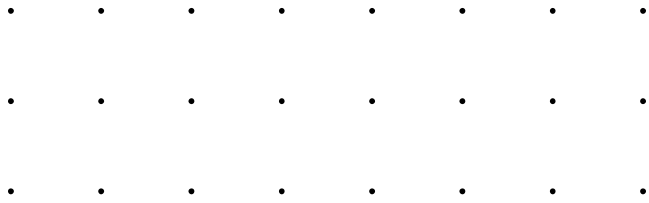
# Remediation

**At what point do you start to remediate the incident?**

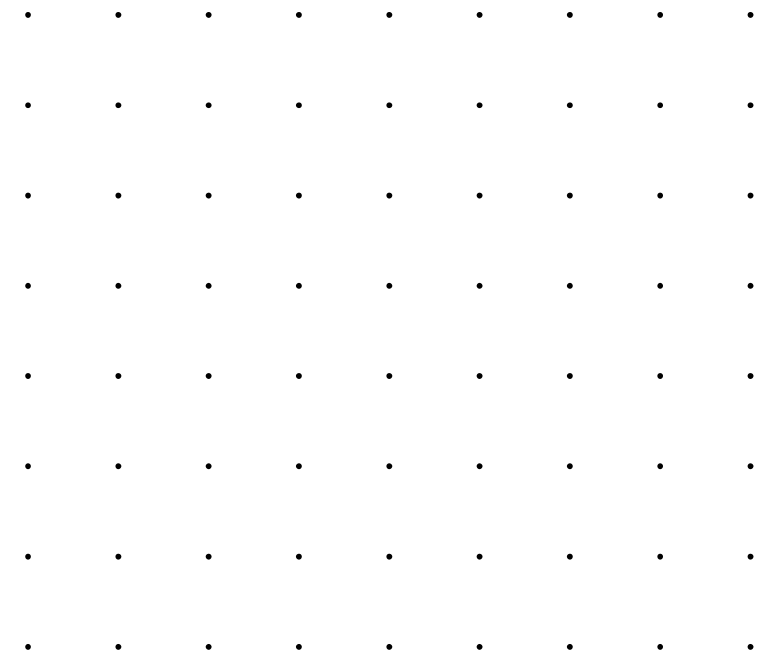
3 types of remediation

- When you see 1 to 2 techniques per tactic, or understand why not
- No remediation
- Ineffective remediation
- Effective remediation





# Forensics

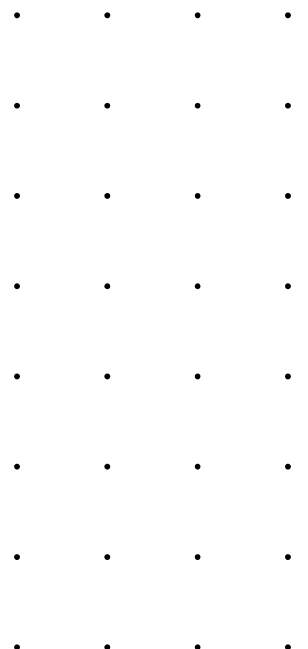


# Forensics

**Digital forensics involves the systematic collection, preservation, and analysis of digital evidence to investigate and respond to cyber crimes and security incidents**

Vital role in cyber security and law enforcement

- Systematic examination of digital devices and data
- Processes to maintain proper handling of data
- Different types of forensic analysis
- Key questions to answer:
  - Adversary status
  - Dwell time
  - Extent of the compromise
  - TTPs
  - IoCs

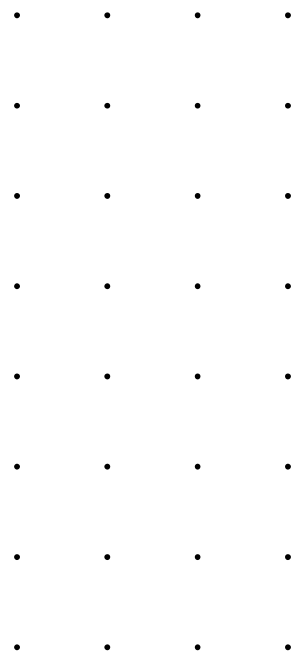


# Artefacts

## Understanding operating system and networking concepts helps greatly

### Understanding computer hardware and software

- Hardware components (e.g., CPU, RAM, storage)
  - CPU (Central Processing Unit): The core processing unit of a computer that executes instructions
  - RAM (Random Access Memory): Temporary memory used for active tasks and data storage
- Storage: Devices for long-term data retention, such as hard drives and solid-state drives (SSDs)
  - Differentiating between software types (e.g., operating systems, applications)
- Operating systems: Software that manages hardware resources and provides a user interface
- Applications: Programs that perform specific tasks or functions on a computer
- Operating systems and file systems:
  - Operating system: The software that manages hardware resources, schedules tasks, and provides user interfaces
- Recognising various file system structures (e.g., NTFS, FAT)
  - File system structures: The organisation and layout of data on storage media
  - NTFS (New Technology File System) and FAT (File Allocation Table): Common file systems used in Windows

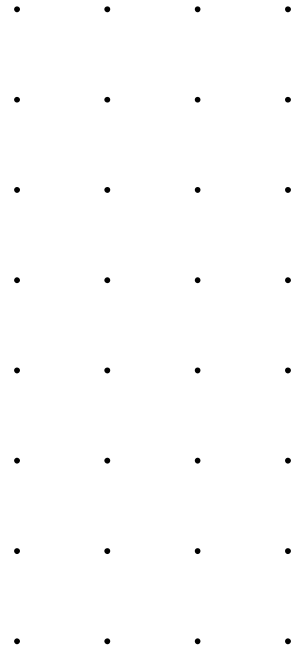


# Evidence Collection

## Structure and control

Methods and procedures for evidence collection

- The importance of proper documentation
  - Proper documentation: Detailed recording of actions taken during evidence collection to maintain integrity
- Distinguishing between physical and logical acquisition
  - Physical acquisition: Direct copying of storage media
  - Logical acquisition: Selective copying of specific files and data
- Chain of custody and preservation:
  - Ensuring the integrity of evidence
    - Chain of custody: A documented trail showing who handled evidence and when
  - Maintaining a detailed record of evidence handling
    - Detailed record: Comprehensive documentation of all actions related to evidence handling



# Acquisition

## Let's obtain data

In conjunction with the others we've spoken of

- Bit-by-bit imaging and data duplication:
  - Creating an exact copy of storage media
    - Bit-by-bit imaging: Making a complete duplicate of every bit on the storage device
  - Safeguarding data integrity
    - Data integrity: Ensuring that data remains unaltered during acquisition
- Write-blocking and forensic hardware tools:
  - Preventing data alteration during acquisition
    - Write-blocking: A technique or device that ensures data on the source media is not modified during copying
  - Utilising both hardware write-blockers and software tools
    - Hardware write-blockers: Physical devices that prevent write access to the source media
- Software tools: Software applications designed for data acquisition and imaging
- File Hashing:
  - File hashing is used in digital forensics to verify the integrity of acquired data. A hash value is generated for the acquired image, and subsequent examinations can compare this hash to detect any changes
- Logs, Volatile memory, network capture, disk
- Targeted
  - Collect only the required data

# File System Analysis

## File system structures (e.g., FAT, NTFS, ext4)

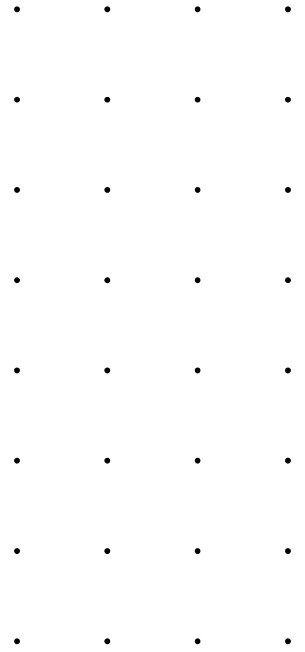
The organisation and layout of data on storage media

- Inodes:
  - Inodes are data structures used in Unix-based file systems (e.g., ext4) to store information about files. In digital forensics, understanding inodes is essential when dealing with Unix-like operating systems
- Master File Table (MFT):
  - MFT is a crucial component in digital forensics, especially in Windows-based systems. It serves as a central index of all files and directories on an NTFS-formatted storage device. Forensic examiners use the MFT to identify and access files, track file metadata, and recover deleted files
- File recovery and reconstruction:
  - File recovery: Methods for retrieving files that have been deleted or lost
- File reconstruction: Reassembling fragmented or damaged files
- Timestamp analysis:
  - Examination of file timestamps, including creation and modification times
    - Timestamps: Metadata associated with files that record their creation, modification, and access times
- Event Logs:
  - Event logs are records of system events from a range of sources
    - Event identifiers can be used to track
  - Auth logs
  - Event logs
  - Security event logs

# Network Forensics

## Traffic, flow, etc.

- Event Logs:
  - Event logs are records of system and application events. In network forensics, these logs provide insights into network activities, user actions, and potential security incidents
- Investigating network traffic and logs:
  - Capturing and analysing data packets
  - Network traffic: Data transmitted over a network
  - Data packets: Units of data sent over a network
- Detecting and analysing network intrusions:
  - Identifying unauthorised access or malicious activity
  - Network intrusion: Unauthorised access or activities on a network
- Internet and email investigations:
  - Online communication: Exchange of information over the internet
  - Web activities: Actions performed by users on websites and online services





# Mobile Device Forensics

## Becoming much more prominent

Not just smart phones, drones and the like

- In-depth examination of mobile device data
  - Mobile devices: Portable computing devices like smartphones and tablets
- Mobile operating systems (iOS, Android):
  - Understanding platform-specific nuances
  - Operating systems: Software that powers mobile devices
- App data extraction and analysis:
  - Extracting data from mobile applications
  - App data: Information stored within mobile apps



# Malware Analysis and Reverse Engineering

## Identifying and analysing malware

Malware: Malicious software designed to harm or compromise systems

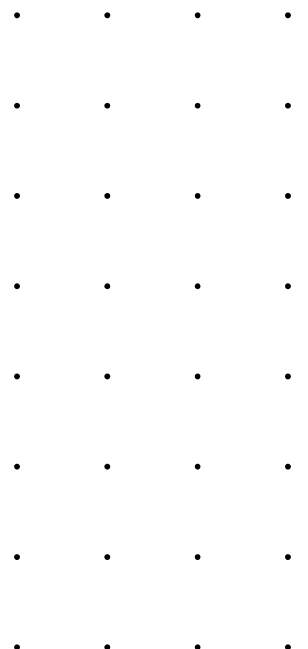
- Static analysis: Static analysis techniques involve examining the code and characteristics of malware without executing it. These methods include:
  - Code review: Reviewing the source code or disassembled code to understand its functionality and potential threats
  - File analysis: Analysing the file structure, headers, and metadata to identify anomalies or suspicious elements
  - Signature-based detection: Matching known malware signatures in files or memory to detect known threats
  - Dependency analysis: Identifying external libraries or resources that malware relies on
- Dynamic analysis: Dynamic analysis involves executing malware in a controlled environment to observe its behaviour. These methods include:
  - Sandboxing: Running malware in an isolated environment (sandbox) to monitor its actions without affecting the host system
  - Behaviour analysis: Observing and recording malware's interactions with the operating system, network, and files during execution
  - API monitoring: Tracking application programming interface (API) calls made by malware to understand its functionality
  - Memory analysis: Analysing memory activities and changes during malware execution
- String analysis and memory dumps:
  - String analysis involves searching for and extracting character strings within binary or memory data. Memory dumps capture the contents of a system's memory, which can contain valuable information for malware analysis

# Memory Forensics

## Volatile memory analysis

Investigation of RAM for live system data

- RAM (Random Access Memory): Temporary memory used by a computer's active processes
- Detecting and analysing memory-resident malware:
  - Identification of malware running in memory
    - Memory-resident malware: Malicious software that operates solely in a computer's memory
- Extracting volatile data:
  - Capturing data from RAM for analysis
- Cached and Resident Files:
  - Cached and resident files stored in memory can contain valuable forensic information. Examining these files can reveal recent activities and data that may not be readily accessible through other means



# Data Recovery and File Carving

## Deleted data recovery

### File carving techniques

- Extracting files from unallocated space
  - Unallocated space: Storage areas that do not contain active data
- Data reconstruction from fragmented files:
  - Reassembling fragmented data
- File Carving:
  - File carving is a technique used to

extract files from storage media without relying on file system metadata. It's particularly useful in recovering fragmented or partially overwritten files

