COS30015 IT Security

Week 6

Presented by Dr Rory Coulter

4 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.

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
  - Minimise impact, facilitate improvements to handling future incidents
  - Business aims focus on restoring service and operations
- Incident Response Plan:
  - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organisation's information systems(s)

SOURCE: NIST 800-61 R2 Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

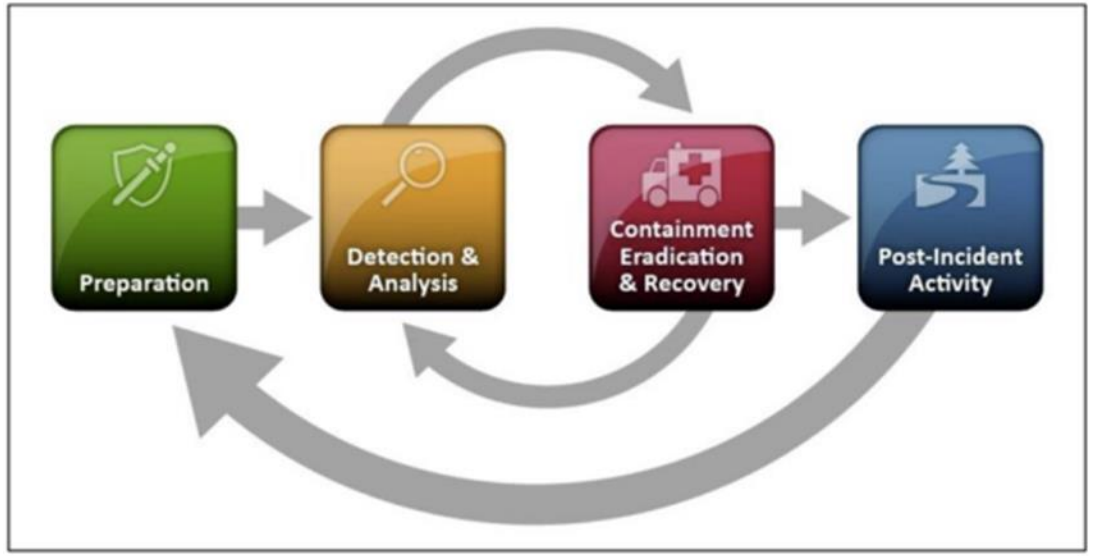
What is Incident Response

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



SOURCE: NIST 800-61 R2 Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

SOURCE: https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

SWINBURNE UNIVERSITY OF TECHNOLOGY

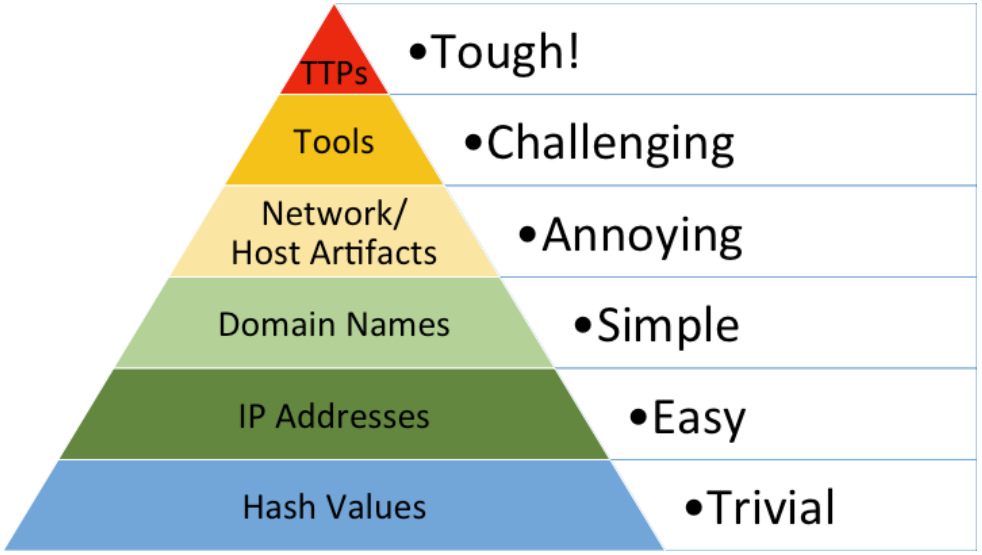
Pyramid of Pain

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



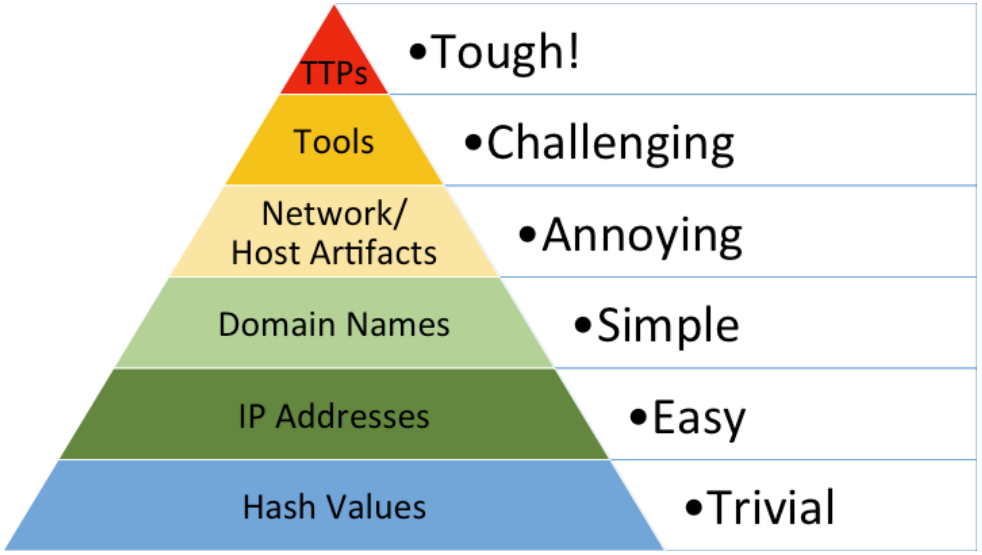
SOURCE: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

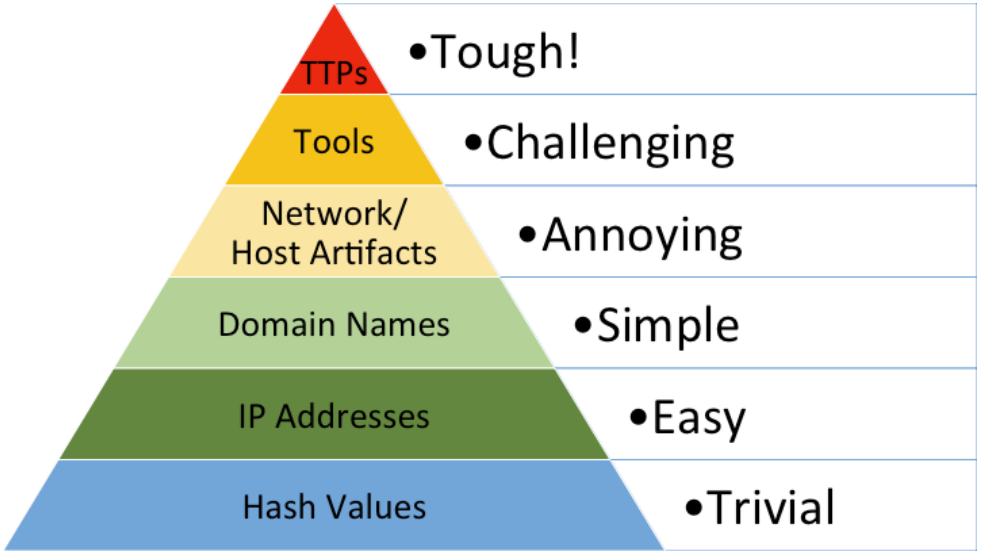


SOURCE: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

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



SOURCE: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

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

Assessment

Assignment 1

Due Thursday

If you don't know when it's due, don’t ask, check the assessment page

- Back up your work now
- You have unlimited submissions, that could be a way to submit as you go in case something happens
- Lab, library and Office 365 avenues in caser of downtime
- Keep it simple

SWINBURNE UNIVERSITY OF TECHNOLOGY

Quiz

In class week 7

That's right, you need to attend class in week 7 to complete the quiz

- Weeks 1 to 6 lecture, supplementary and lab content
- 30 questions
- 1 hour
- Turn up to your class, log in to Canvas, take quiz, lab machine only
- Closed book
- A practice quiz will be made available
- Answers will be provided a 2 weeks after
- Any funny questions, we will review, don't need to email us
- Medical certificate required is you can't attend
- Attendance will be taken, StudentID cards please
- Attend your assigned class
- We will audit when a quiz was completed and when your class is

Assignment 2

2 parts – 1: Forensic investigation 2: Incident report

The following will help you complete it

- Week 6 supplementary content
- Week 7 lab (hashing and using Cyber Chef)
- Week 8 optional lab (log forensics)
- Week 9 lab and content (analysing email headers)
- Week 10 lab (practice run writing up an incident summary)
- Week 11 lab (exfiltration task)
- Artefacts:
    - Audit logs
    - Hashes
    - Network traffic capture
    - Event logs
    - OSINT
    - Phishing
    - Timestamps
    - Downloads

SWINBURNE UNIVERSITY OF TECHNOLOGY