CSIT302 Cybersecurity

Day 1-2 – Incident Response Process /Cybersecurity Kill Chain

Subject Coordinator: Dr Partha Sarathi Roy

School of Computing and Information Technology

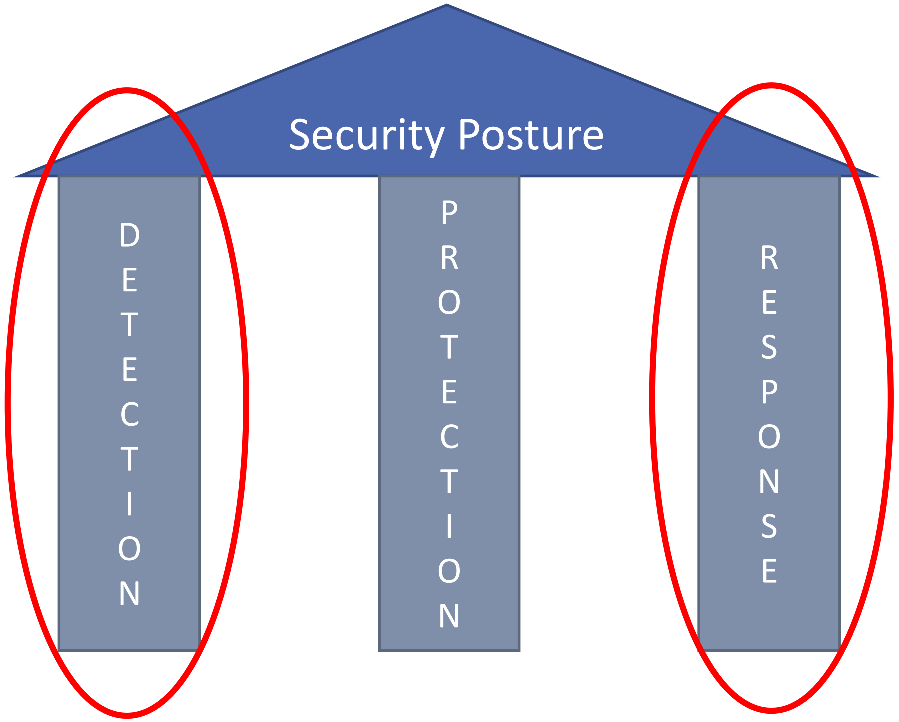
UNIVERSITY OF WOLLONGONG AUSTRALIA

Incident Response Process

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

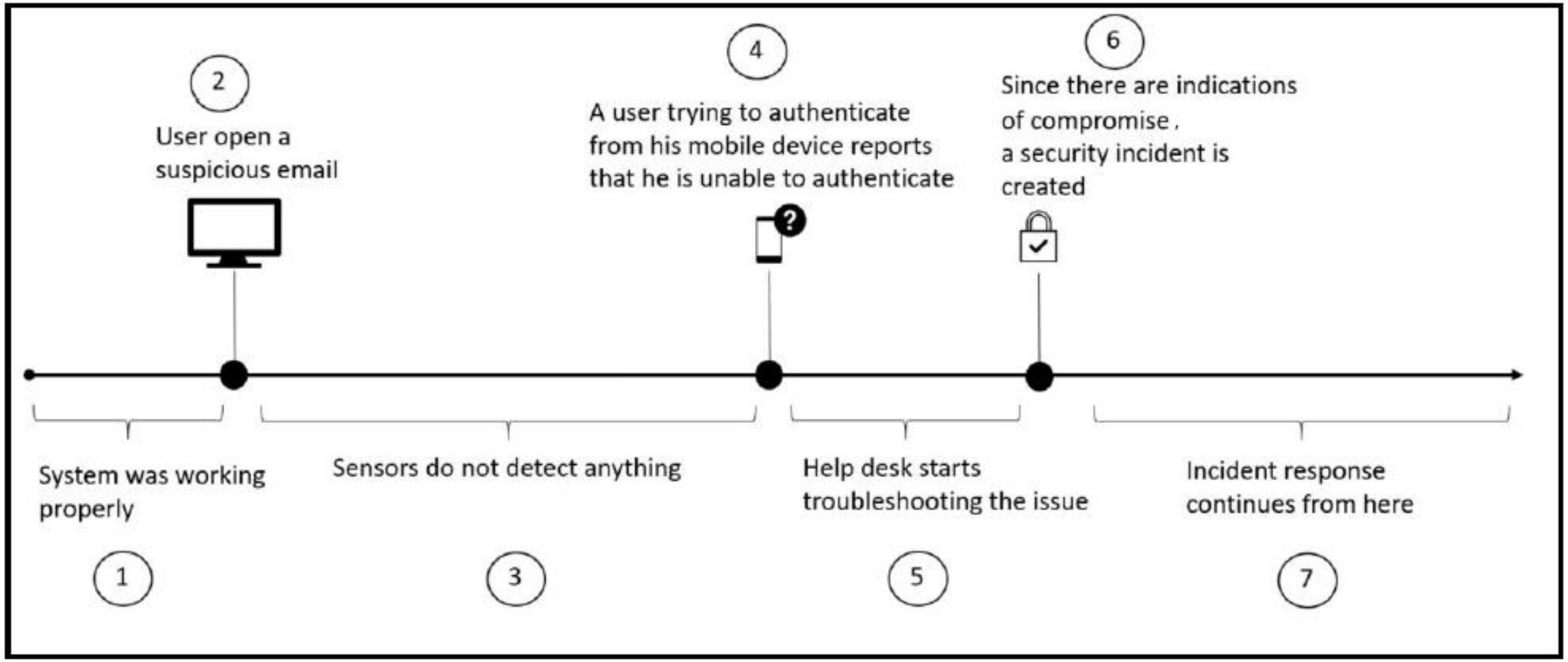
Introduction to IR Process

- Incident Response (IR) process is related to detection and response in the security posture
  - **Detection**: how to handle security incidents.
  - **Response**: how to rapidly respond to them.
- Many companies have an IR process in place, but *they fail to constantly review it* to incorporate lessons learned from previous incidents. → Having addressed this issue well gives us better *protection* in the future.



Introduction to IR Process

- An example of IR process



2
User open a suspicious email
4
A user trying to authenticate from his mobile device reports that he is unable to authenticate
6
Since there are indications of compromise, a security incident is created
System was working properly
1
Sensors do not detect anything
3
Help desk starts troubleshooting the issue
5
Incident response continues from here
7

Introduction to IR Process

- At point (7), the IR process
  - takes over the incidence case:
  - documents *every single step* of the process, and
  - incorporates the *lessons learned* with the aim of enhancing the overall security posture, after the incident is resolved.
- The process may vary according to the company, industry segment and standard.
- No IR process in place results in
  - Bad security posture
  - Waste of human resources

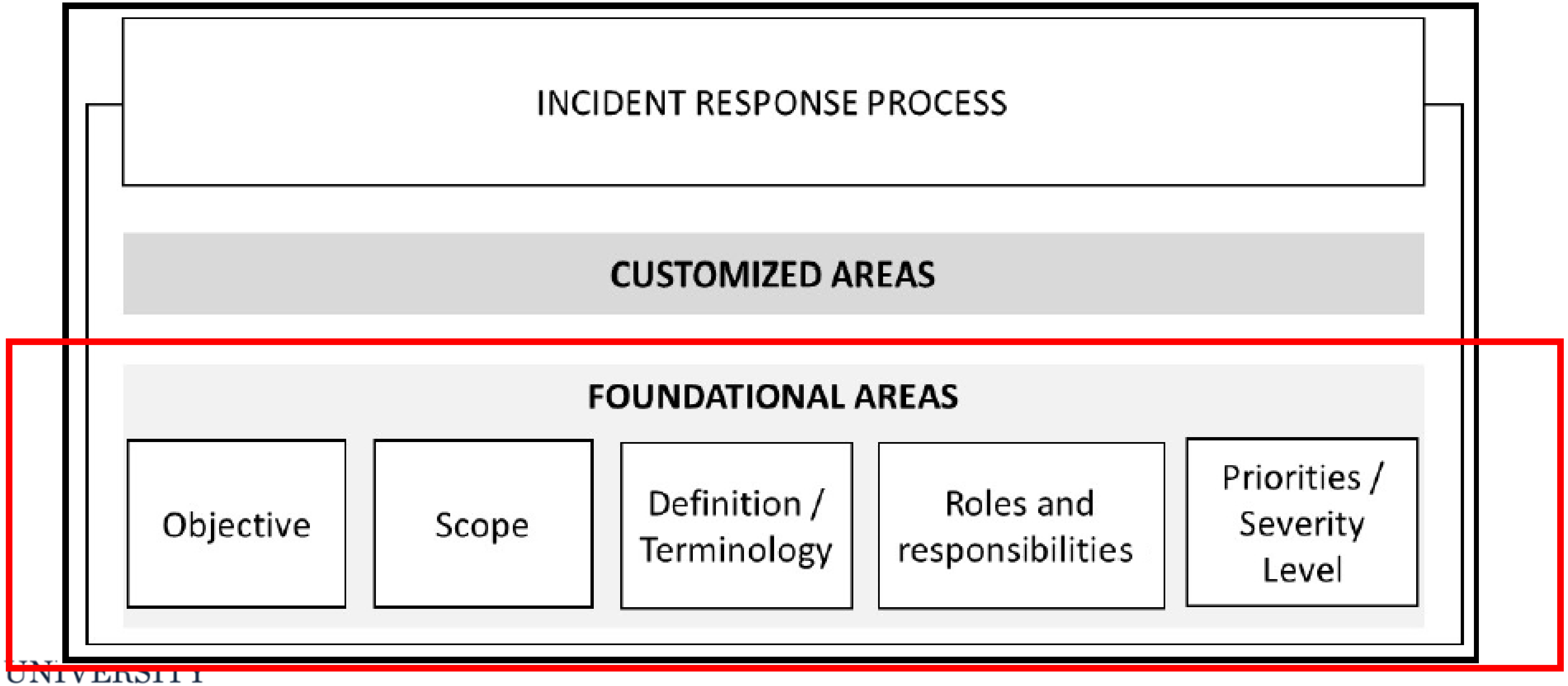
UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Introduction to IR Process

- For the successful IR Process:
  - ➢*All IT Personnel* should be trained to know how to handle a security incident.
  - ➢*All Users* should be trained to know the core fundamentals about security.
  - ➢An *integration* between the help desk system and the incident response team.
  - ➢***Good sensors*** (*Intrusion Detection System*) in places. For example, Network sensors + Host sensors for quick and comprehensive detection.
  - ➢IR process must be *compliant with the laws and the industry's regulations*.

Creating an IR Process

- Foundational areas of the incident response process:


INCIDENT RESPONSE PROCESS
CUSTOMIZED AREAS
FOUNDATIONAL AREAS
Objective
Scope
Definition / Terminology
Roles and responsibilities
Priorities / Severity Level

Foundational Areas of IR Process

- Objective:
  - ➢What's the purpose of this process?
    - ✓It is important to define clearly the purpose of process.
    - ✓Everyone should be aware of what this process is trying to accomplish.
- Scope:
  - ➢To whom does this process apply?
    - ✓A company-wide scope vs a departmental scope.
- Define/Terminology:
  - ➢Each company may have a different perception of a security incident.
    - ✓Define what constitutes a security incident and give examples.
    - ✓Create their own glossary using a clearly defined terminology.

Foundational Areas of IR Process

- Roles and responsibilities:
  - ➢Example: Who has the authority to confiscate a computer in order to perform further investigation?
    - ✓Define the users or groups that have this level of authority.
    - ✓Let the entire company be aware of this.
- Priorities/Severity level:
  - ➢Functional impact of the incident in the business
    - ✓Type of information affected by the incident
    - ✓Recoverability
- Additionally, interaction with third parties, partners and customers is needed to be defined.

Incident Response Team

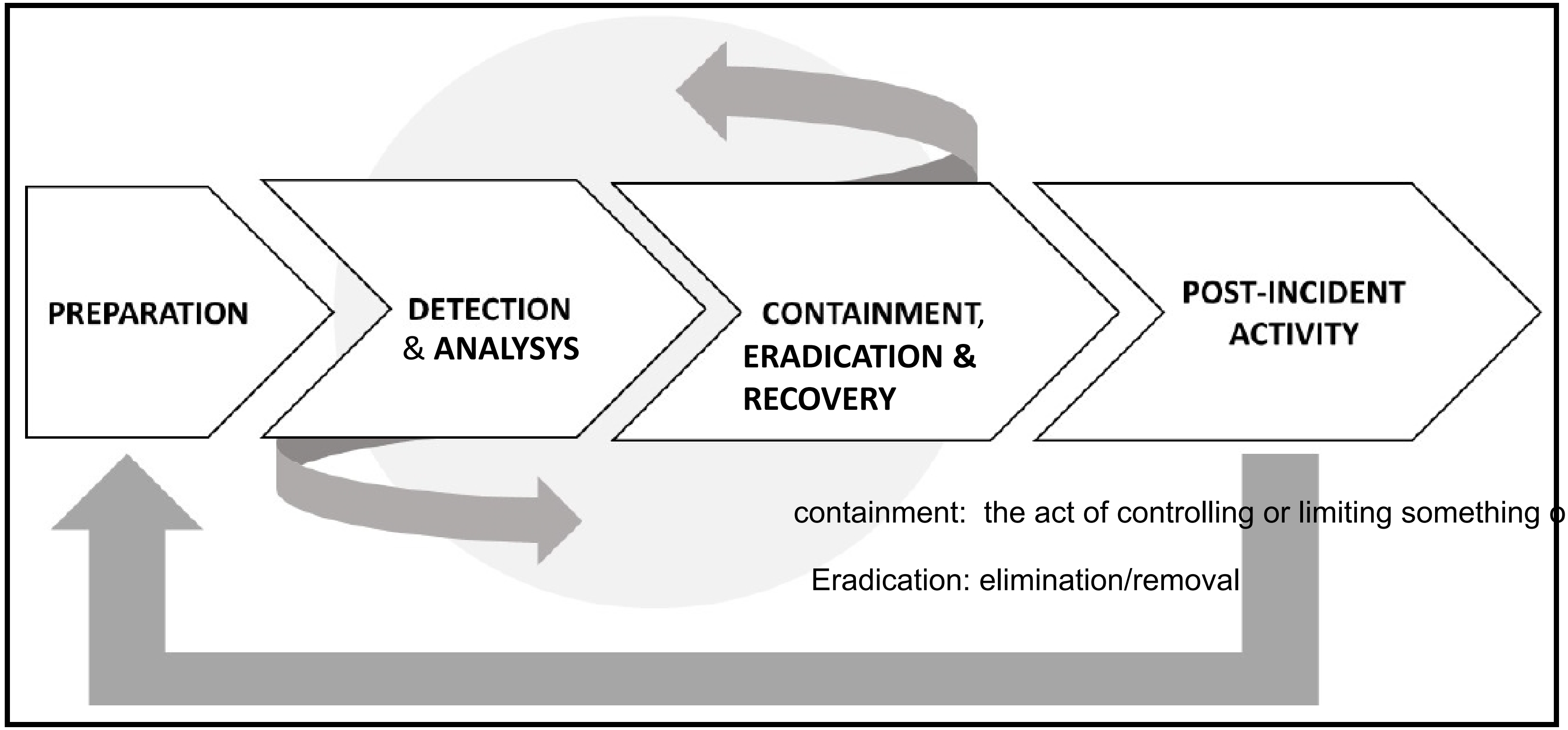
- Incident response team carries out IR process
  - It varies according to the company size, budget and purpose.
  - It requires a personnel who has a technically broad knowledge, but have deep knowledge in some other areas.
  - The budget for IR team must cover the acquisition of proper tools and hardware and training programs for the employees in the company.
- Outsourcing on IR Team
  - Finding proper people who have different skill sets is sometimes difficult. → Outsourcing part of the IR team can be one of the solution.
  - When it is outsourced, well-defined **Service-level-agreement (SLA)** that meets the severity levels is essential.

End Users

- End users' roles
  - They have important roles in identifying and reporting security incident.
  - They should know the procedure how to create incident ticket.
  - They are required to attend the *security awareness training*.
- Sometimes, *the end user cannot reproduce the issue*. To mitigate scenarios like this, make sure the following is in place:
  - System and network profiles
  - Log-retention policy
  - Clock synchronization across all systems (e.g. using Network Time Protocol (NTP))
  - Instruct the end user to contact support when the issue is currently happening and provide them with the environment to capture data.

NIST Incident Response Process

- NIST Incident Response Process



containment: the act of controlling or limiting something or someone harmful

Eradication: elimination/removal

NIST Incident Response Process

- Preparation
  - ➢Implementation of security controls that were created based on the *initial risk assessment*.
  - ➢Implementation of other security controls such as endpoint protection, malware protection and network security.
  - ➢The preparation phase is not static → This phase will receive input from post-incident activity.

NIST Incident Response Process

- Detection and Analysis
  - ➢Detection system must be aware of the attack vectors.
  - ➢Detection system must be able to dynamically learn more about new threats and new behaviours.
  - ➢Detection system triggers an alert if a *suspicious activity* is encountered.
  - ➢To detect threats more quickly and reduce false positives, the leveraging of security intelligence and advanced analytics are required.
  - ➢Detection and analysis are sometimes done almost in parallel: An attack is still taking place when it is detected.

NIST Incident Response Process

- Manual information gathering is often required to identifying an incident
  - ✓ Data gathering must be done in *compliance with the company's policy*.
  - ✓ In scenarios where you need to bring the data to a court of law, you need to guarantee the *data's integrity*.
- The combination and correlation of the following information to Identify IoC (Indication of Compromise) are required:
  - ✓ Endpoint protection and operating system *logs*: Phishing email, lateral movement
  - ✓ Server logs and network captures: Unauthorized or malicious process
  - ✓ The firewall log and the network capture: Data extraction and submission

NIST Incident Response Process

- Containment
  - ➢Perform short-term containment by isolating the portion of the network that is under threat. Then, focus on long-term containment, which requires temporary adjustments to allow systems to be used in production while rebuilding clean systems.
  - ➢Restore affected systems in minimal time.
- Eradication
  - ➢Remove malware from all infected devices, acknowledge the root cause of the attack and take necessary steps to avoid similar attacks in the future.

NIST Incident Response Process

- Recovery
  - ➢To avoid further attacks, put the affected production systems back online.
  - ➢To ensure that they return to normal operation, test, check and track the affected systems.

NIST Incident Response Process

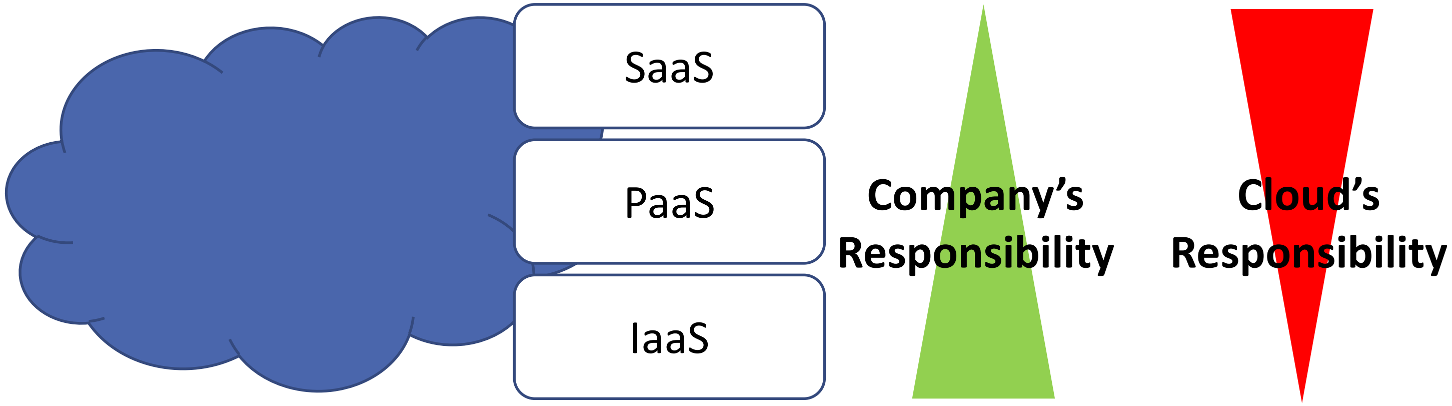
- Post-Incident Activity
  - ➢Documenting Lesson Learned
    - ✓It is one of the *most valuable* pieces of information that you have in the post-incident activity phase.
    - ✓It helps to keep *refining the process* through the identification of gaps in the current process and areas of improvement.
    - ✓This documentation must be very *detailed* with the *full timeline* of the incident.
    - ✓Content: The *steps that were taken* to resolve the problem, what happened during each step and how the issue was finally resolved outlined in depth.

NIST Incident Response Process

- The lesson learned will include the answers of the following:
  - ✓ **Who identified** the security issue? A user or the detection system?
  - ✓ Was the incident opened with the **right priority**?
  - ✓ Did the security operations team perform **the initial assessment** correctly?
  - ✓ Was the **data analysis** done correctly?
  - ✓ Were the **containment, eradication and recovery** done correctly?
  - ✓ Is there anything that could be improved at this point?
  - ✓ How **long** did it take to resolve this incident?
- *Evidence retention*
  - ✓ All the artifacts should be stored according to the company's retention policy.
  - ✓ The evidence must be kept intact until legal actions are completely settled.

Incident Response in the Cloud

- A shared responsibility between the cloud provider and the company that is contracting the service



PaaS (Platform as a Service) provides a platform allowing customers to develop, run, and manage applications such as OS and middleware.

Incident Response in the Cloud

- For the IaaS model:
  - ➢Customers have full control of the **virtual machine** and have complete access to **all logs** provided by the operating system.
  - ➢Cloud provider has the information of the underlying network infrastructure and hypervisor logs.
  - ➢Customers should review the cloud provider policy before requesting any data.
- For the SaaS model:
  - ➢The vast majority of the **information** relevant to an incident response is in possession of the cloud provider. → contact the cloud provider directly, or open an incident via a portal.
  - ➢Customers review the SLA to better understand the rules of engagement in an incident response scenario.

Updating Your IR Process to Include Cloud

- The IR process must include cloud-computing-related aspects
- Preparation
  - ➢needs to update the contact list to include the cloud provider contact information, on-call process, and so on.
- Detection
  - ➢include the cloud provider solution for detection in order to assist you during the investigation
- Containment
  - ➢Revisit the cloud provider capabilities to isolate an incident (e.g, isolate compromised VM for the others)

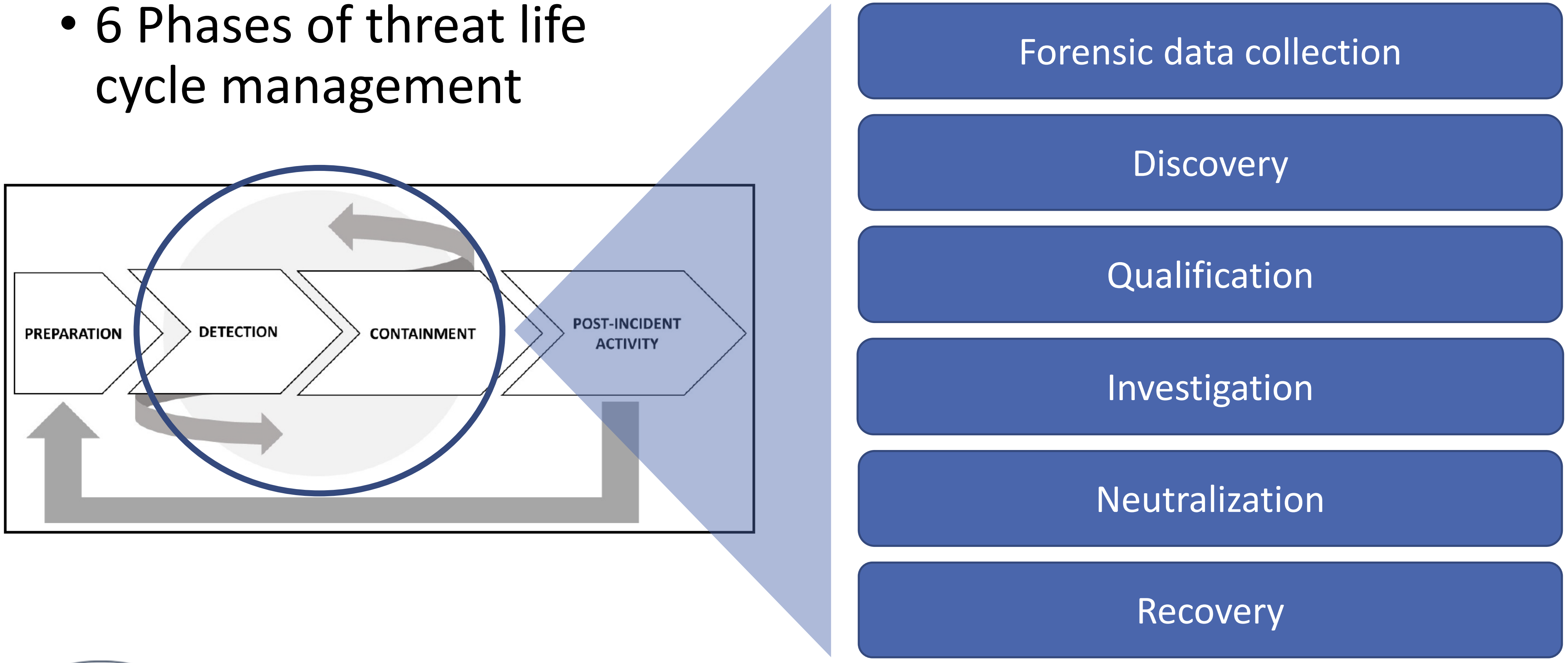
Threat Life Cycle Management

- The Detection and Containment of the NIST IR process can be *more specified by Threat Life Cycle management*.
- An investment in threat life cycle management can enable an organization to *stop attacks just as they happen*.
- New technologies have been adopted, bringing *new vulnerabilities* and *widening the surface* area that cybercriminals can attack.
  - ➢E.g. Internet of Things (IoT)
- 84% of all attacks left evidence in the log data → Appropriate tools and mindset, these attacks could have been mitigated early enough to prevent any damage.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Threat Life Cycle Management

- 6 Phases of threat life cycle management



- Forensic data collection
- Discovery
- Qualification
- Investigation
- Neutralization
- Recovery

Threat Life Cycle Management

- Forensic data collection
  - ➢The threats come through the seven domains of IT. The more of the IT infrastructure the organization can see, the more threats it can detect.
    - ✓Seven Domains of typical IT infrastructure: User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, Remote Access Domain, WAN Domain, and System/Application Domain
  - ➢Collection of security event and alarm data
  - ➢Collection of log and machine data
  - ➢Collection of forensic sensor data

Threat Life Cycle Management

- Discovery phase
  - ➢Search analytics
    - ✓Carrying out software-aided analytics.
    - ✓Review *reports* and identify any known or reported *exceptions* from network and antivirus security tools.
    - ✓Labour-intensive → It should not be sole analytics method.
  - ➢Machine analytics
    - ✓Purely done by *machines/software*.
    - ✓*Autonomously scan* large amounts of data and give brief and simplified results to people using machine learning.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Threat Life Cycle Management

- Qualification phase
  - ➢Threats are assessed to find out
    - ✓their potential impact;
    - ✓urgency of resolution;
    - ✓how to mitigate the threats
  - ➢Inefficient qualification may lead to *true positives being missed and false positives being included*.
  - ➢False positives are a big challenge. → Waste of resources against non-existent threats

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Threat Life Cycle Management

- Investigation phase
  - ➢The qualified threats are fully investigated to *determine whether or not they have caused a security incident*.
  - ➢A threat might have done in the organization *before* it was identified by the security tools → Need to look at any potential damage.
  - ➢Continuous access to forensic data and intelligence about a large amount of threats is required. (It is mostly automated.)
- Neutralization phase
  - ➢Eliminate or reduce the impact of an identified threat.
  - ➢Automated process to ensure a higher throughput of deleting threats, and to ease information sharing and collaboration in the organisation.

Threat Life Cycle Management

- Recovery phase
  - ➢The phase comes after the all threats are neutralized and risks are put under control.
  - ➢The organization to a position is restored prior to being attacked by threats
    - ✓Changes caused by the attacker or for the recover are needed to be backtracked
  - ➢Automated recovery tools can be used to return systems to a backed-up state.
  - ➢Ensure that no backdoors are introduced or are left behind

Cybersecurity Kill Chain

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Cybersecurity Kill Chain

- Kill chain
  - The term was originally used as a military concept related to the structure of an attack, consisting of the followings:
    - ✓ target identification
    - ✓ dispatch of troops to the target
    - ✓ decision and order to attack the target
    - ✓ the destruction of the target.
- Cybersecurity kill chain
  - *Lockheed Martin* adapted this concept to the cybersecurity, using it as a method for modelling intrusions on a computer network.

Cybersecurity Kill Chain

- Most cyber attackers use a series of similar phases
  - ➢The skilled attackers operate on well-structured and scheduled plans to remain their intrusion undetected until the time is right.
  - ➢Those attacks are often performed through the following steps:
    - ✓External reconnaissance (or information gathering)
    - ✓Compromising the system
    - ✓Lateral movement
    - ✓Privilege escalation
    - ✓Concluding the mission

External Reconnaissance

- The attackers in the external reconnaissance phase
  - ➢harvest as much information as possible to find vulnerabilities;
  - ➢decide on the exploitation techniques that are suitable for each vulnerability.
- The information that the attacker gathers:
  - ➢It is from outside the target's network and systems.
  - ➢It includes the target's supply chain, obsolete device disposal and employee’s social media activities.
  - ➢Anyone in an organization can be targeted including suppliers and customers.

External Reconnaissance

- Commonly used techniques to get an entry point of the organisation’s network: Social engineering attacks
  - ➢ Phishing: Attackers send the target some carefully crafted emails to cause them to reveal secret information or open a network to attacks.
    - ✓ Phishing emails are usually linked to a malware installation.
    - ✓ They claim to be from reputable institutions.
  - ➢ Other types of social engineering attacks: Attackers closely follow targets and collect information about them: This happens mostly through social media

Compromising

- Once either of these or another technique is used, the attacker will find a point of entrance. (i.e. compromise the system) such as through **stolen passwords** or **malware infection**.
- **Stolen passwords** will give the attacker direct access to computers, servers, or devices within the internal network of an organization.
- **Malware** can be used to infect even more computers or servers, thus bringing them under the command of the hacker.

Lateral movement

- Lateral movement phase involves the use of various scanning tools to find loopholes that can be exploited to stage an attack.
- Popular scanning tools (Framework):
  - ➢**Metasploit and Kali Linux:** Linux-based hacking framework. It is made up of numerous hacking tools and frameworks that have been made to effect different types of attacks.
- Popular password cracking tools:
  - ➢**John the Ripper, THC Hydra** and **Cain and Abel:** Those tools support brute force or dictionary attacks on passwords.

Lateral movement

- Popular scanning tools (for Network):
  - ➢**Wireshark**: Very popular tool among both hackers and pen testers to capture the data packets in the network.
  - ➢**Nmap:** NMap is a free and open source network mapping tool.
  - ➢**Aircrack-ng:** a suite of tools that is used for wireless hacking. The suite includes attacks such as FMS, KoreK, and PTW.
    - ✓The FMS attack is used to attack keys that have been encrypted using RC4.
    - ✓KoreK is used to attack Wi-Fi networks that are secured with WEP-encrypted passwords.
    - ✓PTW is used to hack through WEP- and WPA-secured Wi-Fi networks.
  - ➢**Kismet:** Wireless network sniffer and intrusion detection system.
  - ➢**OWASP Zap:** A website vulnerability scanner that hackers use to identify any exploitable loopholes in organizational websites.

Access and Privilege Escalation

- In order to achieve the freedom of movement without being detected, an attacker needs to perform privilege escalation.
- **Vertical privilege escalation**
  - ➢Attacker moves from one account to *another that has a higher level of authority*
  - ➢Tools are used to escalate privileges
- **Horizontal privilege escalation**
  - ➢Attacker uses the account *that has the same level of authority*
  - ➢User account is used to escalate privileges

Access and Privilege Escalation

- In vertical privilege escalation,
  - ➢The attacker gets *access rights and privileges of high level authority* such as administrator and a super user.
  - ➢The attacker can run any unauthorized code (e.g., malwares and ransomwares) through the privileges it acquires.
  - ➢It is complex operation. It may need some kernel-level operations to elevate their access rights.
  - ➢*Buffer overflow* is widely used for vertical privilege escalation.
  - ➢***EternalBlue***, which is a vulnerability that is used for WannaCry, is also based on buffer overflow.

Access and Privilege Escalation

- In horizontal privilege escalation,
  - ➢An attacker uses the *same privileges* gained from the initial access.
  - ➢A normal user is erroneously able to *access the account of another user.*
  - ➢Horizontal privilege occurs when an attacker is able to access protected resources using a normal user account.
  - ➢This is normally done through session and cookie theft, cross-site scripting, guessing weak passwords, and logging keystrokes.
  - ➢As a result of this escalation
    - ✓the attacker normally has well-established remote access entry points into a target system.
    - ✓The attacker might also have access to the accounts of several users.
    - ✓The attacker knows how to avoid detection from security tools that the target might have.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Concluding the Mission

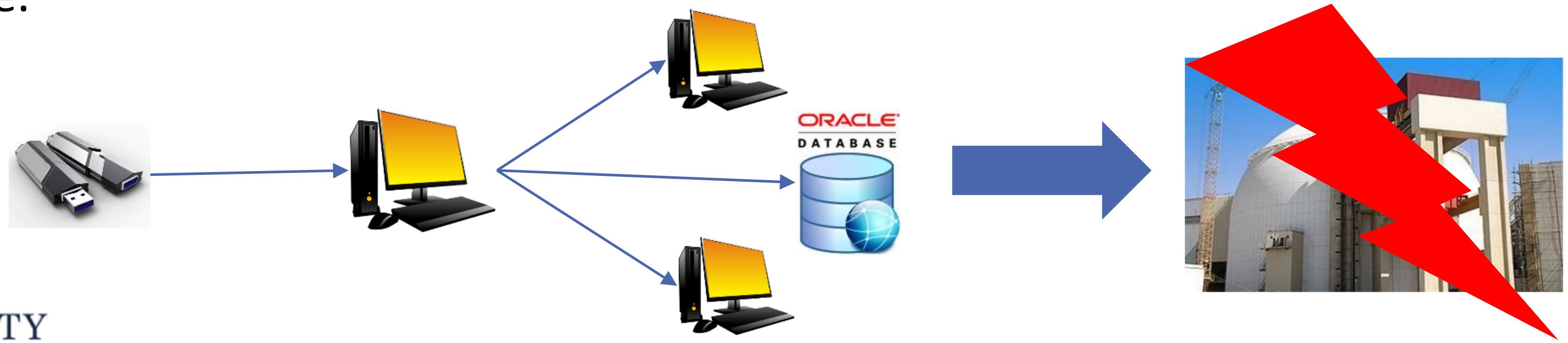
- Exfiltration
  - ➢The attacker will start ***extracting sensitive data*** from an organization.
  - ➢This could include trade secrets, usernames, passwords, personally identifiable data, top-secret documents, and other types of data.
  - ➢Attackers normally steal huge chunks of data in this stage.
  - ➢Example of the data exfiltration
    - ✓Ashley Madison (2015)
    - ✓Yahoo (Happened in 2013, reported to the public in 2016)
    - ✓LinkedIn (2016)
  - ➢The hackers soon put the data on sale for any interested buyers.
  - ➢The hackers could erase or modify the files stored in the compromised computers, systems, and servers

Concluding the Mission

- Sustainment
  - ➢The hackers may decide to *remain silent* even after it exfiltrated all valuable information.
  - ➢Attackers install malware, such as rootkit viruses to assure them of access to the victim's computers and systems *whenever they want*.
  - ➢The victim's security tools are at this point ineffective at either detecting or stopping the attack from proceeding.
  - ➢The attacker normally has *multiple access points* to the victims, such that even if one access point is closed, their access is not compromised.

Concluding the Mission

- Assault
  - ➢most feared stage of any cyber-attack.
  - ➢permanently **damage the data and software**, disable or alter the functioning of the victim's hardware.
  - ➢Stuxnet attacks on Iranian nuclear facility.
    - ✓The first recorded digital weapon to be used to wreak havoc on physical resources
    - ✓The nuclear station was not connected to the Internet. It is transmitted by USB thumb drive.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Concluding the Mission

- Obfuscation
  - ➢The attackers *cover their tracks*.
  - ➢They use various techniques to confuse, deter, or divert the forensic investigation process.
- There are a few techniques to obfuscation:
  - ➢Hackers at times attack outdated servers in small businesses or public schools and then laterally move to attack other servers or targets.
  - ➢Hackers also can use a free WiFi, which is generally not highly protected.
  - ➢Dynamic code obfuscation: This prevents detection from signature-based antivirus and firewall programs.