SEC-202: Secure Start-Up

Lecture 6 – Incident Response & Crisis Communications

"Resilience."
It is not a matter of if, but when. How you respond determines if the company survives.

Instructed By:

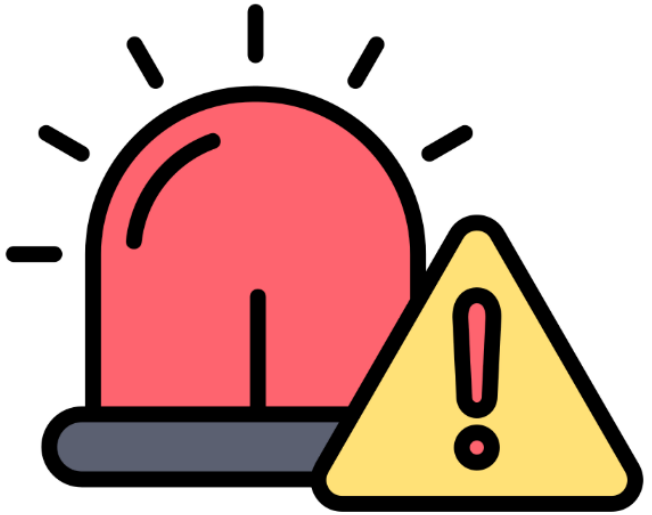
Dr. Charnon Pattiyanon

Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer Engineering (AICE) Program

Today’s Outline

- The Reality of a Breach
- The Incident Response Lifecycle
- Roles in the War Room
- Forensic Basics
- Ransomware Special Case
- Crisis Communication
- Legal Privilege



The Reality of a Breach

- **The Fog of War:** “The day the phone rings at 3 AM”
  - Incomplete Information
  - High stress and panic.
  - Time pressure.
- **Dwell Time:** (No Prevention, but Resilience)
  - The time between the breach and detection.
  - **Goal:** Reduce this from weeks to hours.
- **Objective:** We aren't trying to prevent the hack (it already happened). We are trying to minimize the impact.

Roles in the War Room

Incident Commander (IC):
The "General." Makes the decisions.
Does *not* touch the keyboard.

Tech Lead:
Directs the investigation.
"Get me the logs from Server A."

Scribe: Writes down everything (Timestamp + Action). Vital for legal defense.

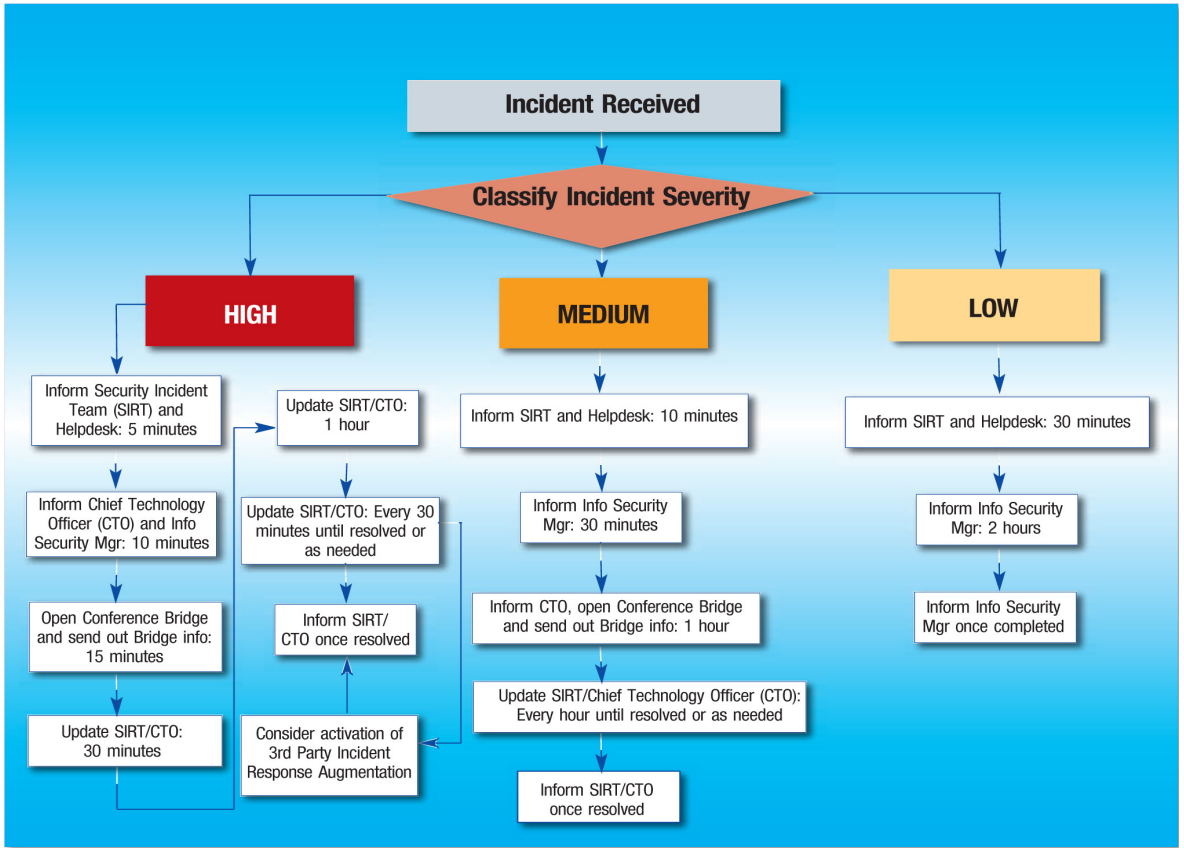
Communications (Comms):
Manages the message to employees, customers, and press.

The Incident Response Lifecycle (NIST)

- There are **four** phases in the IR lifecycle:
  - **Phase 1 - Preparation:** The most important phase. (Plans, Tools, Access).
  - **Phase 2 - Detection & Analysis:** Monitoring alerts and deciding if it's real.
  - **Phase 3 - Containment, Eradication, Recovery:** Stopping the bleeding and fixing the wound.
  - **Phase 4 - Post-Incident Activity:** Learning lessons.

Phase 1 – Preparation

- **The IR Plan:**
  - A "**Playbook**" that tells you who to call.
  - Critical: Have a hard copy (What if the network is down?).
- **Retainers:**
  - Pre-signed contracts with Forensics firms (e.g., Mandiant) and Crisis PR firms.
  - You don't want to be negotiating a contract while your servers are encrypted.
- **Logs:** Ensure your SIEM (Security Information and Event Management) is actually collecting data.

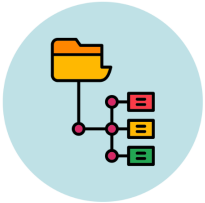


Phase 2 – Detection & Analysis

- **Triage:**
  - False Positive: Looks bad, but is benign (e.g., Admin running a script).
  - True Positive: Actual malicious activity.

1. Detection Intake: Gather alerts from all relevant sources: EDR platforms, Network detection systems, External threat intelligence feeds, and Breach notifications, including from vendors

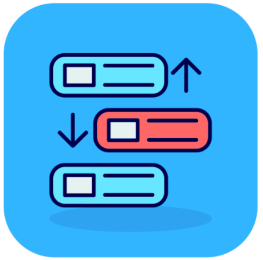
2. Initial Classification: Classify alerts into defined buckets, such as malware, unauthorized access, phishing, or misconfigurations. Using standard tags and categories to sort input can reduce uncertainty when seconds count. Analysts also assess for context and potential errors, such as false positives.



3. Severity Scoring: Assess severity based on: System criticality, Data sensitivity, Exploitability (such as known CVEs or malware indicators), and Level of access involved

4. Business Impact Evaluation: Consider the broader implications of the alert. This step helps shift triage from technical to strategic decision-making:

- Does it impact core systems or customer-facing services?
- Could it disrupt regulatory reporting or revenue?
- Are vendors or partners implicated?



5. Prioritization and Handoff: Escalate based on the inputs collected during the triage process. Route the alert to the appropriate team, whether it's incident response, legal, privacy, or communications. High-priority and critical cases should trigger escalation workflows immediately.

Phase 2 – Detection & Analysis

- **Scoping:**
  - "How big is the fire?"
  - Is it one laptop? Or the entire Customer Database?
- **Declaration:** The moment the IC officially declares "We have an Incident."

A practical evidence-first scoping workflow

Step 1: Preserve evidence before "fixing" systems

Before resets and remediation, capture what will be needed later: access logs, export logs, message routing logs, configuration snapshots, and (where relevant) endpoint telemetry. For cloud tools, preserve audit logs and admin actions that show whether settings were changed during the incident window.

Step 2: Define "data at risk" & "data confirmed disclosed"

Separate capability from confirmation. "Data at risk" describes what could have been accessed given permissions. "Confirmed disclosure" requires evidence: exports, file downloads, message sends, portal views, or partner receipts. This separation improves decision-making and prevents premature broad conclusions.

Step 3: Build an exposure pathway map

Map the pathways relevant to the incident type: account access, exports, outbound referrals, shared portal access, vendor support sessions, and partner distribution lists. This map guides which logs to prioritize and which partners may need coordination.

Step 4: Produce a scoping record that supports decisions

Create a scoping record that documents: time window, affected systems, user accounts, log sources reviewed, what was found (and not found), confidence level, and open questions. This record becomes the basis for notification and remediation decisions.

Phase 3 – Containment

- **Containment** in incident response is the critical phase that **stops a cyberattack from spreading**, **limiting damage to systems, data, and reputation**. It acts like a digital firewall, isolating affected network segments, locking down accounts, or severing connections to prevent further unauthorized access, allowing teams to analyze and eradicate threats.
- Purpose: To stop "the bleed," prevent further damage, and gain time to analyze the incident without the threat escalating.
- **Types of Containment:**
  - Short-Term: Immediate actions to limit impact, such as shutting down a server, pulling network cables, or isolating a virtual machine.
  - Long-Term: Strategic measures applied to clean systems, such as patching vulnerabilities, changing all user credentials, or reconfiguring firewall rules.
  - Strategic Isolation:
    - Full: Total isolation from the internet and internal networks.
    - Partial: Restricting traffic to only secure, monitored channels.
    - Selective: Disabling specific compromised IP addresses or accounts.

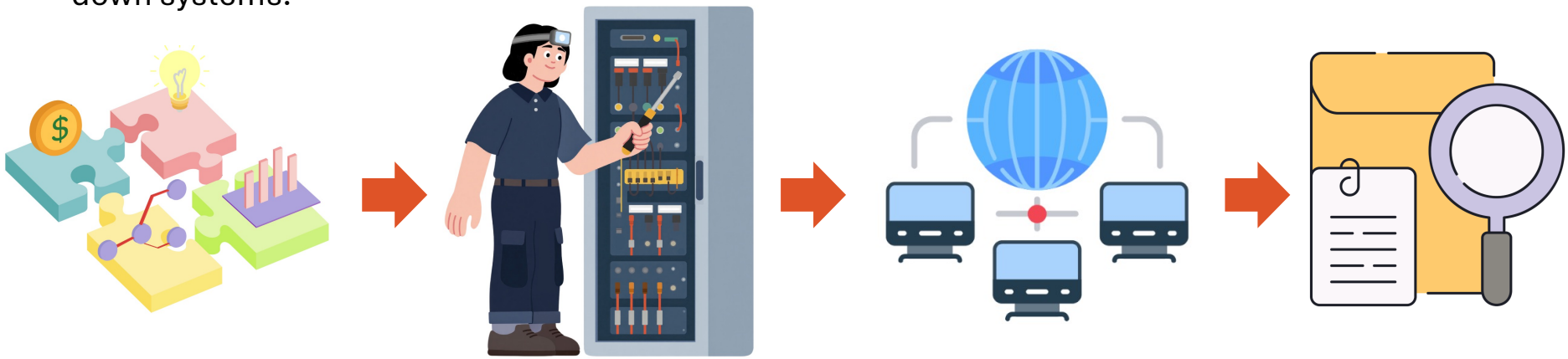
Phase 3 – Containment

- **Strategies & Tactics:**
  - **Network Segmentation:** Restricting lateral movement of attackers.
  - **Account Lockdowns:** Disabling compromised user credentials.
  - **Immutable Infrastructure:** Replacing compromised servers with clean, pre-configured instances rather than trying to clean the infected machine.
  - **Automation:** Using pre-built scripts (Containment as Code) to immediately apply network policies.
- **Golden Rule:** *Do not shut down the machine. You will lose valuable evidence in RAM.*

Phase 3 – Containment

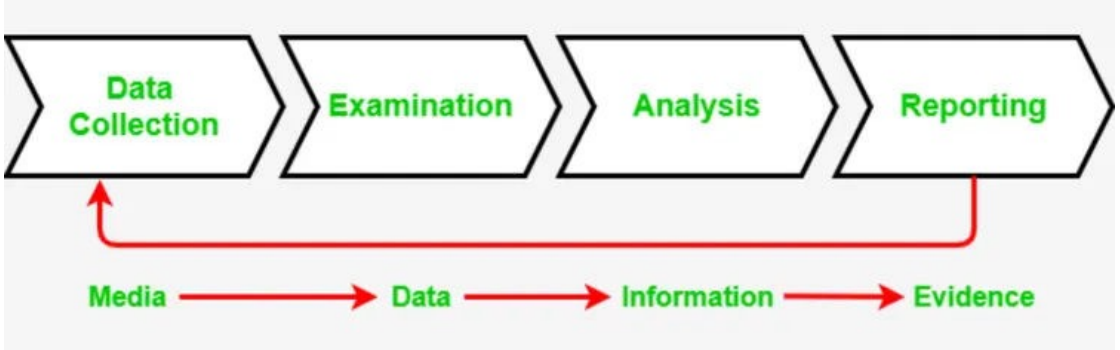
- **Steps in the Containment Process**

1. **Determine Strategy:** Choose based on potential damage, the need for evidence, and service availability.
2. **Identify Affected Systems:** Pinpoint exactly what is compromised to avoid unnecessary downtime.
3. **Execute Isolation**: Implement the chosen strategy (e.g., VLAN isolation, firewall blocks).
4. **Evidence Preservation:** Ensure that volatile evidence (RAM, temporary files) is captured before shutting down systems.



Forensic Basics

- **Chain of Custody:**
  - A legal log proving who held the evidence and when.
  - Without this, evidence is inadmissible in court.
- **Artifacts:**
  - What forensics look for:
    - Registry Keys: Persistence mechanisms.
    - Prefetch Files: "What programs ran recently?"
    - Event Logs: Login attempts.



- **Digital Forensic Chain of Custody:** In digital investigations, this process specifically includes documenting the acquisition, analysis, and storage of electronic data, often using cryptographic hash values to verify that the data remains untampered.

Ransomware Special Case

- **The Dilemma:** To pay or not to pay?
  - FBI Advice: Do not pay (it encourages them).
  - Business Reality: Sometimes it's cheaper than bankruptcy.
- **Double or Triple Extortion:**
  - **Encrypting your data** (Availability attack).
  - **Stealing your data and threatening to leak it** (Confidentiality attack)
  - **Performing DDoS attacks to pressure**.

- **Targeting Critical Infrastructure:** Attacks on essential services, such as the Colonial Pipeline, which led to a $4.4 million ransom payment and caused massive supply shortages.
- **Supply Chain Attacks:** Targeting a single, trusted vendor (like Kaseya) to infect hundreds or thousands of downstream customers, magnifying the impact exponentially.
- **"Digital Parasites" (No Encryption):** A major trend shift in 2025-2026 involves attackers focusing solely on data theft without encrypting files, allowing them to remain embedded longer and avoid triggering security alerts.
- **Virtual Machine (VM) Attacks:** Ransomware running inside a VM (e.g., VirtualBox) to hide from antivirus software while encrypting the host machine.
- **Cross-Claiming (Multiple Gangs):** Cases where one group (e.g., RansomHouse) steals data, and another group (e.g., ALPHV) later claims the same victim, indicating collaboration or data-sharing among attackers.

Crisis Communications

- **The "Golden Hour":** You must control the narrative before Twitter does.
- **The Holding Statement:**
  - "We are aware of an issue and are investigating. We will provide updates as soon as possible."
- **Legal vs. PR:**
  - Legal: "Admit nothing. Say nothing."
  - PR: "Be transparent. maintain trust."
  - The CISO balances these two.

Crisis Communications

Legal Privilege

Court Orders

Legal orders that may require disclosure of privileged information

Private Communications

Communications between a client and lawyer that are confidential

Law Enforcement Records

Records held by law enforcement, not privileged

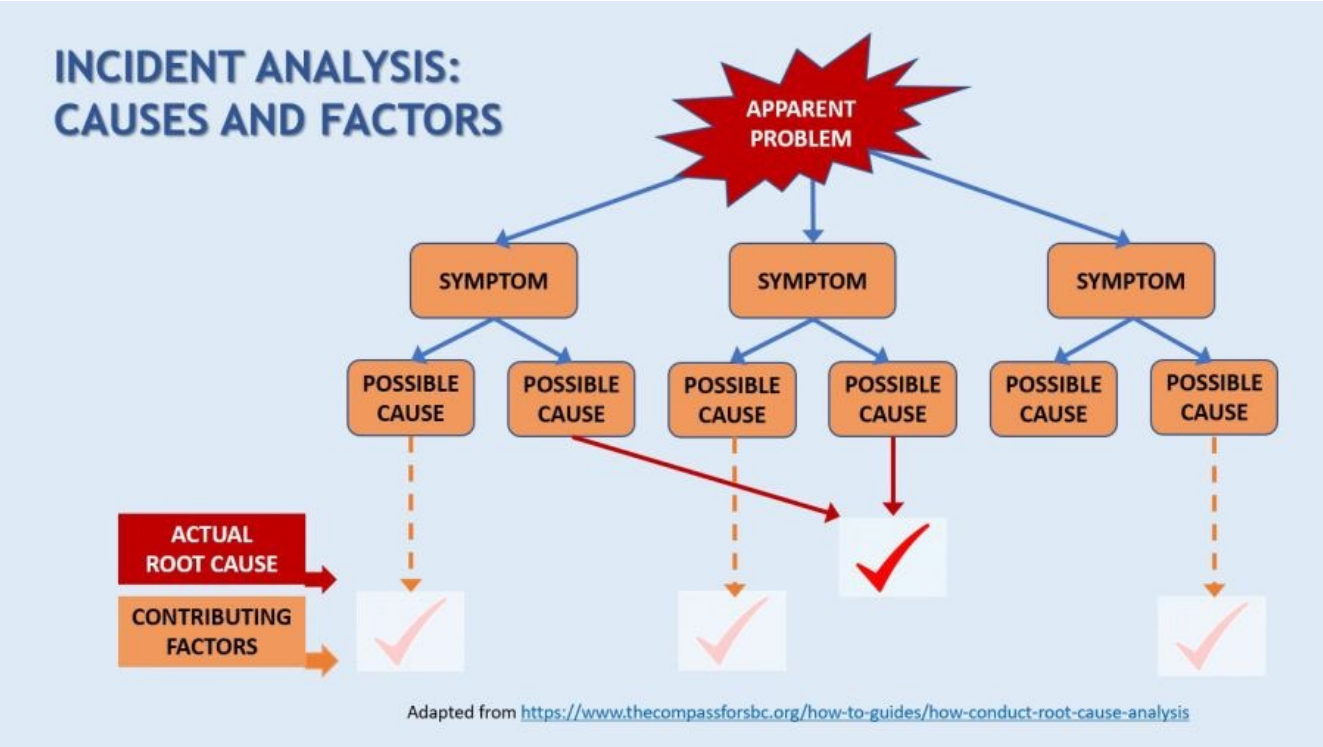
Public Information

Information available to the public, not covered by privilege

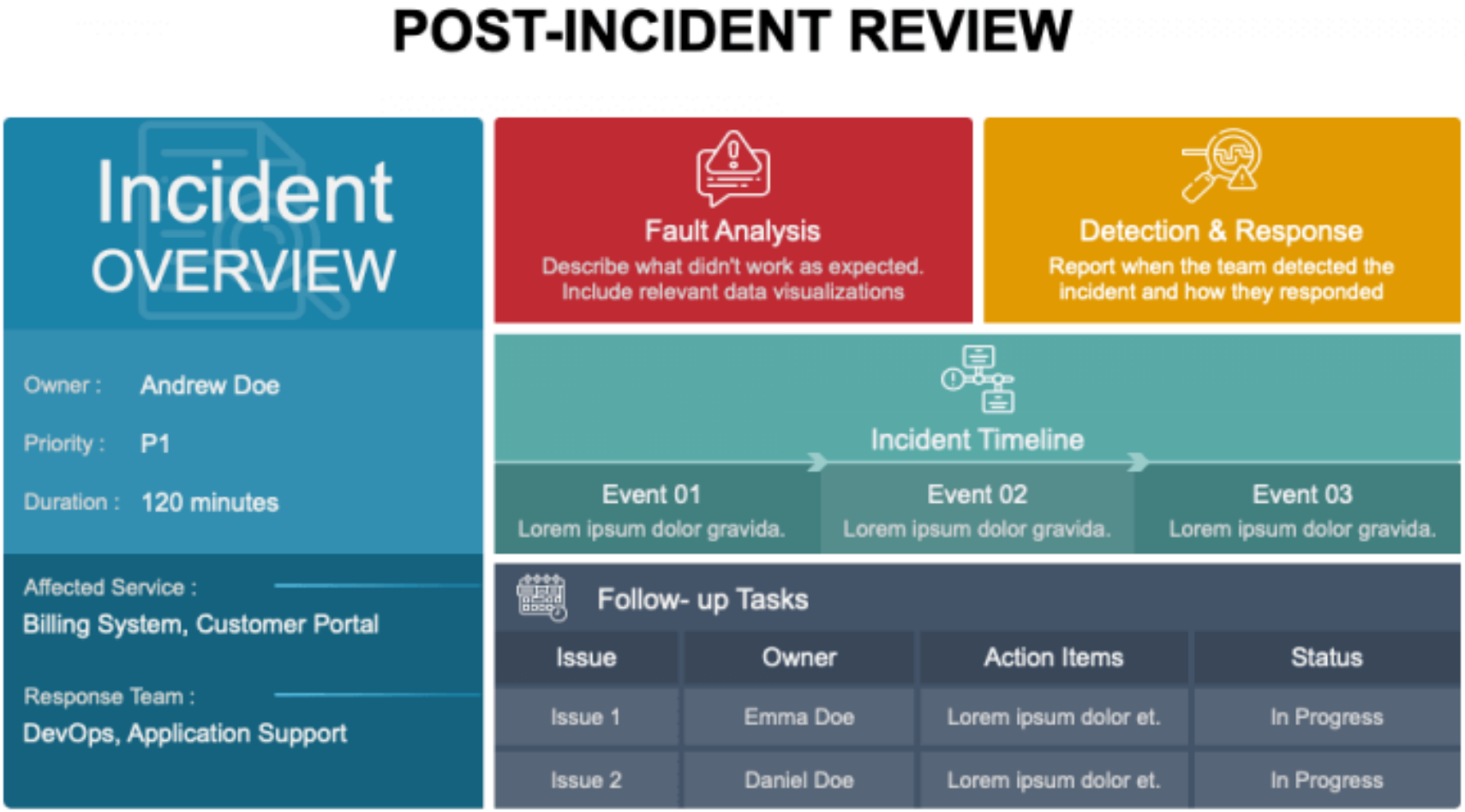
- **Attorney-Client Privilege:**
  - Conducting the investigation at the direction of external counsel.
  - This may protect your internal reports from being discoverable in a lawsuit.
  - **Note:** Never write "This is our fault" in an email during an incident.

Phase 4 – Post-Incident Review

- **The "Post-Mortem":** A blameless meeting held after the dust settles.
- **Root Cause Analysis (5 Whys):**
  - "Why did the server get hacked?" ->
  - "Missing patch." ->
  - "Why missing?" ->
  - "Process failed." -> ...
- **Action Items:**
  - Updating the Playbook so this specific attack cannot happen again.



Phase 4 – Post-Incident Review



Phase 4 – Post-Incident Review

POST-INCIDENT REVIEW

Incident Overview

Fault Analysis

Postmortem owner	Benjamin / Eva Doe
Incident	Type /link to add a ticket
Related incidents	Type /link to add related tickets
Priority	P1 / P2 / P3+
Affected services	Billing Applications
Incident date	Add start and end dates
Incident duration	50 minutes
Incident response teams	E.g., Application support
Incident responders	Responders
Executive Summary	Lorem ipsum proin gravida hendrerit ctus a turpis cursus in.

Executive Summary

Detail the incident using UTC to standardize for timezones. Include lead-up events, post-impact events & any decisions or changes made.

Postmortem Report

Instructions	Report
Leadup List the sequence of events that led to the incident	Lorem ipsum.
Fault Describe what didn't work as expected. If available, include relevant data visualizations	Lorem ipsum proin gd hendreit.
Impact Describe how internal and external users were impacted during the incident. Include how many support cases were raised.	Lorem ipsum proin gd hendreit.
Detection Report when the team detected the incident and how they knew it was happening. Describe how the team could've improved time to detection.	Lorem ipsum proin gd hendreit.
Response Report who responded to the incident and describe what they did at what times. Include any delays or obstacles to responding.	Lorem ipsum proin gd hendreit.

Follow- up Tasks

Issue	Owner	Action Items	Documentation
Issue 1	Jane Doe	Lorem ipsum dolor.	Lorem ipsum dolor.
Issue 2	Sophia Doe	Lorem ipsum dolor.	Lorem ipsum dolor.

Summary and Key Takeaways

- **Preparation is key.** You cannot build a fire station while your house is burning.
- **Containment first.** Stop the spread before trying to fix the root cause.
- **Communication matters.** A bad response can damage your reputation more than the hack itself.

End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email (charnon@cmkl.ac.th).