

Incident Report

**Team 26**

**Collegiate Cyber Competition Company**

**January 25, 2025**

**1. Executive Summary**

**Incident ID:** INC2025-0125-[2-digit ID Number]

**Incident Priority:**

P1 - Critical P2 – High P3 - Medium P4 - Low

**Incident Classification:**

Compromised System

Compromised User Credentials

Network Attack (e.g., DoS)

Malware (e.g., virus, worm, Trojan)

Reconnaissance (e.g., scanning, sniﬃng)

Lost Equipment/Theft

Physical Break-in

Social Engineering (e.g., phishing)

Policy Violation (e.g., acceptable use)

Other:

**Incident Summary:**

On [date] [time], [team name] detected [incident]. Using [root cause, tools, methods], an unauthorized entity [action (ex. gained access to, compromised, exfiltrated)], impacting [impacted assets].

**2. Incident Detection & Analysis**

**2.1. Evidence Sources & Analysis**

This section lays out security events such as alerts and/or reports that prompted an investigation, and the evidence collected in the investigation. (RS.AN-06, RS.AN-07)[[1]](#footnote-1)



**2.2. Aﬀected Systems & Data**

The following is a list of system(s) impacted by the incident, along with the data on or accessible by the aﬀected systems. (DE.AE-04)

Click or tap here to enter text.

The following is a list of user(s) impacted by the incident, including system access levels and privileges. (DE.AE-04)

**2.3. Indicators of Compromise (IoCs)**

This section lists the key pieces of evidence used to determine that an attack has occurred. (DE.AE-08)

Click or tap here to enter text.

**2.4. Root Cause Analysis**

This section explains the primary factors that enabled the incident to occur. (RS.AN-03)

Click or tap here to enter text.

**2.5. Incident Classification & Priority**

Based on the findings from the investigations, an incident is given an incident priority and classification to help guide and activate response efforts. (RS.MA-03)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Priority**  **Matrix** | | **Impact** | | |
| **High**  Business-critical systems OR multiple departments and customers OR business-critical data is impacted. | **Medium**  Non-business-critical systems are impacted AND one department or multiple customers are affected. | **Low**  Non-business-critical systems are impacted. Partial department, or one customer is impacted. |
| **Urgency** | **High**  Causes immediate and significant disruption affecting critical business functions, security or safely. | **P1 - Critical** | **P2 - High** | **P3 - Medium** |
| **Medium**  Causes immediate and moderate disruption but no critical business functions affected. Workaround may be available. | **P2 - High** | **P3 - Medium** | **P4 - Low** |
| **Low**  Will cause disruption soon if not addressed. Workaround is available. | **P3 - Medium** | **P4 - Low** | **P4 - Low** |

With an impact score of [impact score] and an urgency score of *urgency score*, this incident is given [priority score] priority.

**3. Response and Recovery Analysis**

**3.1. Containment & Immediate Response Actions**

This section describes the immediate response to contain the threat and prevent further damage upon incident identification, such as disabling user accounts, resetting credentials, and isolating devices. (RS.MI-01)

Click or tap here to enter text.

**3.2. Eradication Actions**

This section details the steps taken to patch vulnerabilities and eradicate any malware, backdoors, persistence methods, and other things left by the threat actor. (RS.MI-02)

Click or tap here to enter text.

**3.3. Recovery Actions**

This section outlines the steps taken to validate, rebuild, and restore data and systems to normal operation after verifying the eradication of the threat. (RC.RP)

Click or tap here to enter text.

**4. Recommendations**

**4.1. People**

The following lists recommendations related to users and personnel, such as security awareness training and staffing. (PR.AT)

Click or tap here to enter text.

**4.2. Process**

The following lists recommendations related to policies, procedures and processes for improving incident prevention and response. (GV.PO, ID.IM)

Click or tap here to enter text.

**4.3. Technology**

The following lists recommendations related to technology solutions for improving organizational security posture against threats.

Click or tap here to enter text.

**Appendix: Technical Timeline**

| **Date & Time** | **Activity** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. The NIST Cybersecurity Framework (CSF) 2.0 (https://doi.org/10.6028/NIST.CSWP.29) [↑](#footnote-ref-1)