Incident Report

| To: | White Team |
| --- | --- |
| From: | Team XX |
| Date: | March 8th, 2024 |

# Executive Summary

Very short, very sweet – what happened, what is the impact on the business?

# Incident Details

| Time Reported | 03/08/2024 |
| --- | --- |
| Time Occurred |  |
| Affected Assets |  |

# Technical Analysis

| Incident Category |  |
| --- | --- |
| Indicators of Compromise (IoCs) |  |
| Threat Actor(s) |  |
| Attack Methods |  |
| Vulnerabilities Exploited |  |
| Risks to |  |

# Business Impact

| Operational Impact |  |
| --- | --- |
| Financial Implications |  |
| Regulatory and Compliance |  |
| Risk to Business Assets |  |

# Incident Response

| Initial Response Actions |  |
| --- | --- |
| Investigation and Analysis | i.e. Analyzed |
| Containment Strategy | i.e. Quarantined from the network using firewall |
| Remediation Steps | i.e. Changed database user password, disabled file write permissions on website directory |

# Lessons Learned