Incident Response

<Team Name>

<Event Name>

<Date>

Incident Summary

**Low** – Minimal service impact. Unauthorized network probing, automated system scans, host discovery  
**Medium** – Moderate impact, possible services downtime. Unauthorized system access, tampered configs  
**High** – Sure service downtime. Malicious code, system intrusion, tampered configs, compromised host

Security Severity

Low Medium High   
[ ] [ ] [ ]

Status Open Remediation in Progress Resolved  
[ ] [ ] [ ] [ ]

Incident Outline

|  |  |
| --- | --- |
| **Type of incident** | **Supplemental Information** |
| Unauthorized Access / Use [ ] | Malicious / Source IP [Abstract] |
| Unplanned Downtime [ ] | Asset’s / Destination IP [Author] |
| Malicious Software / Logic [ ] | System [Category] |
| Other [ ] |  |

Overview / Description

This is the heart of your explanation. Please include your system type and OS, how you came to find your discovery, the determination in it being a risk to operations and the malicious objects purpose or what you perceive to be the purpose…

Remediation Plan

|  |  |
| --- | --- |
| **Incident Notification** |  |
| Application / System Owner [ ] | Legal and Risk Team [ ] |
| Law Enforcement [ ] | Full IT Management [ ] |
| Application / System Vendor [ ] | System Administrator [ X ] |
| HR [ ] | CCDC White Team [ X ] |

What are the steps taken to remediate the issue? This is dependent on the Incident Status. Include tools, system-dependent features, etc.

Screenshots