

**UMass Lowell**

**Cyber Security Team Blue Team XX**

Blue Team XX

*UML Cyber Security Team*

*Lowell, MA*

<Recipient>

NECCDC

Lowell, MA

**March X, 2023**

Dear <Recipient>,

Below, you will see our report regarding a recent request made to our team.

Thank you,

Blue Team XX

Original Request

**Sender:** Sample: Sashank

**Receiver:** Sample: Blue Team XX

**Timestamp:** Sample: January 1, 2023 5:50pm

**Original Communication:**

Sample: Enable SFTP connections on machine 1.

**Original time to complete:** Sample: 45 minutes

1. Executive Summary

Sample: The original task was to complete X for the purpose of Y. After working on the request, our team was able to complete [a subset] [all] [none] of the task.

2. Assets Affected

1. Sample: <hostname possibly> (IP: X.X.X.X)
2. Sample: <hostname possibly>(IP: X.X.X.X)
3. Sample: Network name

3. Fulfilled Tasks

1. Sample: We had installed [X service name] on machine 1
2. Sample: We had made changes to the firewall on machine 2 that would block the FTP port.

4a. Unfulfilled Tasks

1. Sample: We were not able to complete the installation of the 100GB machine onto machine 1 because of storage constraints. The system can only handle 20GB and so this would overload the system.

4b. Steps to complete unfilled tasks

1. Sample: If we were allocated additional time, we would have created and mounted an additional logical volume that could handle this 100GB machine so machine 1 could in fact utilize the machine.

5. Compromises Made

1. Sample: Instead of blocking every single IP address from the known attack IP database, we had simply created a rule to allow whitelisted IP addresses (meaning IP addresses that we specify that are trusted).

6. Next Steps

1. Sample: Please notify your development team that they will not be able to log into their systems without Multi-factor authentication enabled starting from 5 pm on the date of this communication.