# Response Containment & Eradication

**TEAM 17** 

## Incident Overview



DATE: September 20, 2023 TimeFrame: 08:10:23 EDT - 17:34:56 EDT



Potential Brute Force Attack Suspicious Network Traffic

Potential SQL Database Compromise Unknown execution file being run

0

### Solutions - Short Term

#### Isolate the affected system

Isolate compromised systems and database from the network to prevent further compromise systems

#### Password reset

Reset passwords for compromised accounts

#### Investigate EXE file

Analyze the unknown EXE using malware analysis tools and remove it from the system.

#### Block suspicious traffic

Block the identified suspicious traffic flows with firewall rules and network-based intrusion prevention systems (IPS)

#### Block malicious IP addresses

Block traffic from the identified suspicious IP addresses with firewall rules and network-based intrusion prevention systems (IPS)



# Solutions - Long Term



Strengthen password policies

Implement strong password requirements (updating passwords more frequently)



Enable
multi-factor
authentication
(MFA)

Require MFA for all user accounts to add an extra layer of security



Regularly patch and update systems

Keep systems and network devices up-to-date with the latest security patches to address vulnerabilities



# Risks For The Company

#### Data Loss

Financial Loss



Unauthorized access to sensitive data can lead to data breaches, financial loss, and reputational damage.

Due to legal expenses, regulatory fines, lost of business, and reputational damage

#### Fines/Penalties



Business Disruption

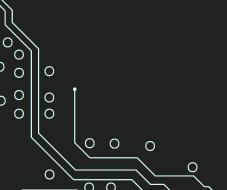


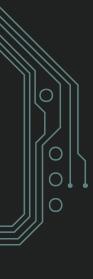
For for not meeting required compliance for Operational/system downtime or disruption, protecting PHI and PII information affecting business operations and productivity

#### Reputational Damage



Lost of trust from customers and damage to company's reputation





## Costs Estimate

\$30,000

Incident response

\$15,000

Forensic Investigation

\$500,000

Regulatory fines

\$20,000

Legal