Post Incident Review Meeting

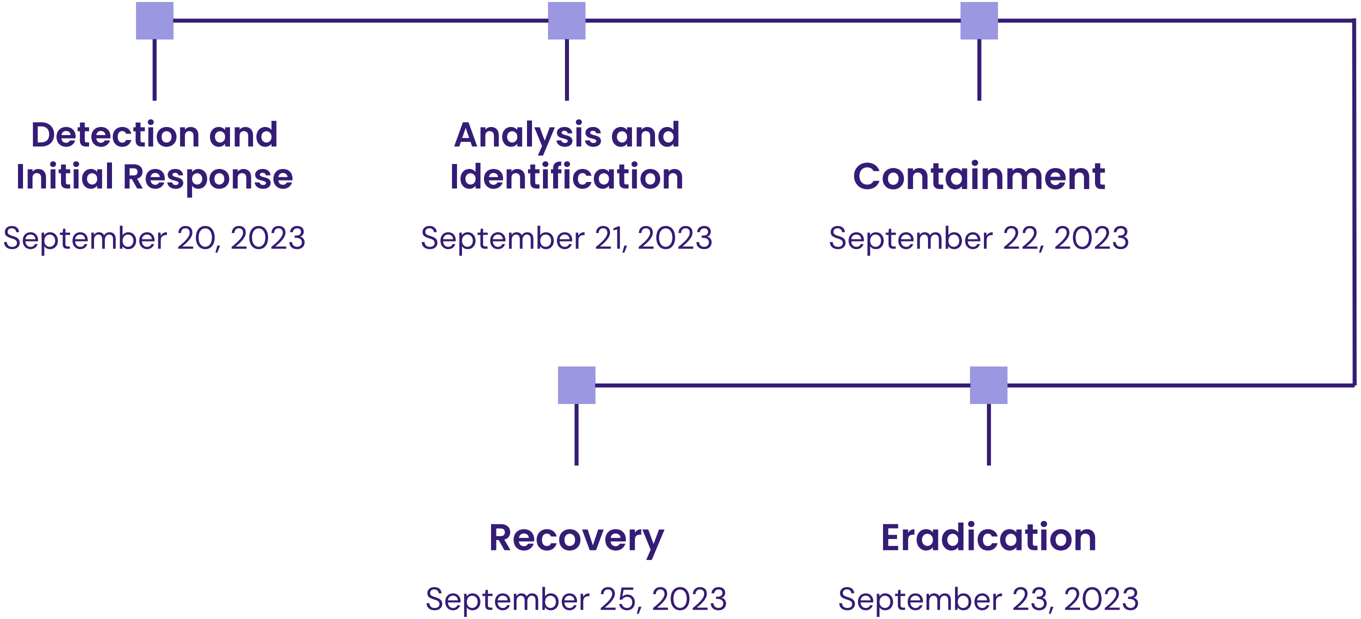
TEAM 17

Purpose

For relevant stakeholders to understand the incident

To refine procedures and prepare for potential future incidents

Timeline Overview



Detection and Initial Response

September 20, 2023

Analysis and Identification

September 21, 2023

Containment

September 22, 2023

Eradication

September 23, 2023

Recovery

September 25, 2023

Timeline Breakdown

Sept 20, 2023

Detection and Initial Response

- Identify suspicious network
- Notify the incident response team and relevant stakeholders
- Initiate investigation: gather logs and evidence from affected systems
- Assess the scope of the incident (determine potential impact and affected assets)

Sept 21, 2023

Analysis and Identification

- Perform deep dive into network traffic analysis to identify all interactions with the suspicious IP
- Cross-check IP reputation and threat intelligence databases for known malicious activities
- Analyze endpoint data for any signs of compromise or suspicious behavior

Sept 22, 2023

Containment

- Quarantine any infected devices or isolate affected systems
- Continue monitoring for unusual traffic or further compromise

Sept 22, 2023 - Sept 23,2023

Eradication

- Remove any identified malware or malicious files
- Patch vulnerabilities or misconfigurations that allowed the suspicious activity
- Conduct a thorough scan of the affected systems to confirm malware or threat is completely removed

Sept 22, 2023 - Sept 23,2023

Recovery

- Restore affected systems from clean backups
- Reconnect systems to the network following confirmation of remediation
- Continue monitoring to ensure no further abnormal behavior or threats

What went right

Identification

Quickly identified suspicious activity indicating an incident

Containment

Isolated compromised system/devices to prevent further spreading

Collaboration

Good communication between different teams involved in the incident response process

Business Continuity

Being able to continue business operations and resilience

Areas of Improvement

Faster Identification

Get alerted faster for suspicious activities

Improving Password Policies

Need to be strengthen against Brute Force Attacks

- Password Retry Delay
- MFA

Awareness Training

For employees to know security best practices

Security Audits and Assessments

More frequent assessments and audits

- Instead of every 6 months, change to every 3 months

Incident Response Plan Refinement

Continuously review and refine the incident response plan to ensure it remains effective and aligns with evolving threats and best practices

Cost

MFA	Awareness Training	Maintenance and Monitoring	Data Monitoring
$15,000	$10,000	$20,000	$30,000
To strengthen security, to enable 2 types of authentication	Increase security best practices amongst employees	To continuously monitor/maintain systems, software updates, patches to keep security systems up to date	For affected customers, to monitor data that were compromised in the incident

Fines for non-compliance

$250,000

HIPAA

$500,000

GDPR

$400,000

CCPA