Maven Clinic

Cyber Security Incident Response Plan & Review

Approved By	*Gemma Chan*
Owner	Head of Cyber Security
Author	*Iswarya Narayanan - Team06*
Audit	Information Security Team
Issue Date	September 20, 2023
Document Name	Cyber Incident Response Process
Version	1.0
Document Class	Restricted
Target Audience	Internal Stakeholders

Table of Contents

1.0 Introduction and Scenario

Maven Clinic, a file transfer platform, recently flagged some unusual network activity that has raised alarms. The senior management is taking this incident very seriously, given the medical data contained on the network. Task is to identify the nature of this alert, its potential impact, suggest mitigation strategies, and compile a review.

This incident response report analyzes a series of security events that occurred on September 20, 2023, on the workstation DESKTOP-1234567. The events indicate a potential compromise of the system, including successful login attempts, policy changes, brute force attacks, resource exhaustion, application errors, and network traffic anomalies.

2.0 Purpose

Incident Response report is a comprehensive document that outlines the details of a cybersecurity incident, the actions taken to address it, and the lessons learned from the experience. Here we follow the guidelines established by the National Institute of Standards and Technology (NIST) for incident response planning and management.

- **Incident Identification and analysis:** Details of how the incident was detected, including the date, time, and source of the alert.
- **Containment:** Describes the actions taken to isolate the affected systems and prevent further damage.
- **Eradication:** Explains the steps taken to remove the threat or malicious code from the affected systems.
- **Recovery:** Outlines the procedures for restoring systems and data to their normal state.
- **Lessons Learned:** Identifies areas for improvement in the organization's security posture and incident response capabilities.

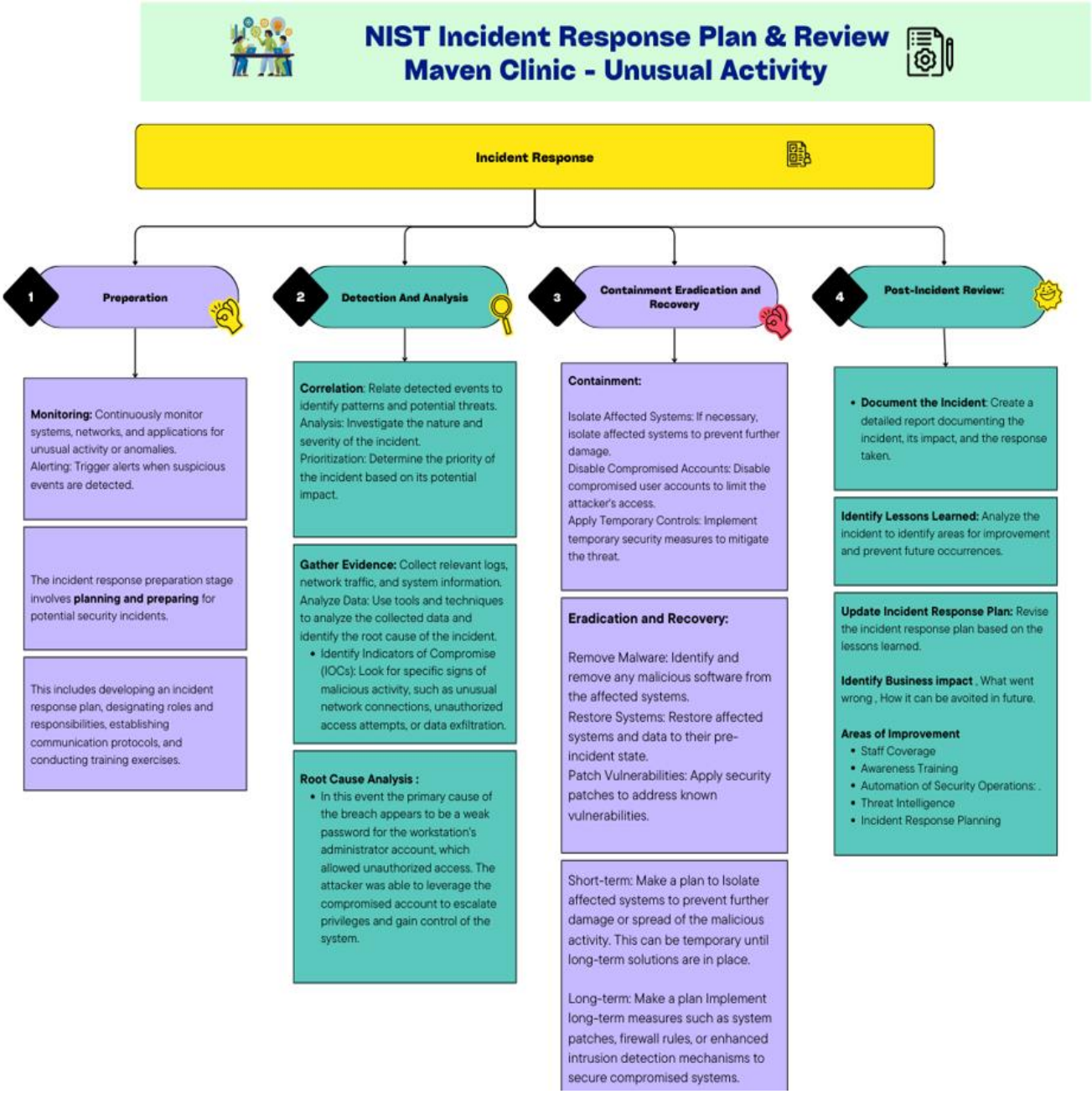
3.0 Scope

The main goals of the incident response are:

- To minimize the damage of the attack.
- To minimize the time of recovery from the attack.
- To create instructions and defensive measures that would prevent such attacks in the future

4.0 Incident Response Process

The incident response process is a structured approach to handling security incidents. It involves a series of steps to identify, contain, eradicate, recover from, and learn from security breaches.Here we follow NIST Incident Response Lifecycle.



4.1 Preparation

The incident response preparation stage involves planning and preparing for potential security incidents. This includes developing an incident response plan, designating roles and responsibilities, establishing communication protocols, and conducting training exercises.

4.2 Identification and Analysis

Once an incident has occurred, it needs to be categorized as the type of incident. The categorization helps in prioritizing the response action.This incident response report analyzes a series of security events

that occurred on September 20, 2023, within the organization's network. The events include a successful login, policy changes, brute force attempts, resource exhaustion, application errors, and network traffic anomalies.

4.2.1 Timeline of Events:

- 10:32:17-10:32:21: Multiple failed login attempts followed by a successful login (brute force).
- 10:33:45: Resource exhaustion detected.
- 12:01:15: Application error (explorer.exe).
- 13:23:15: Resource exhaustion detected again.
- 14:10:12: Traffic blocked by the firewall.
- 15:23:52: Database file corruption error.
- 15:34:56: Failed login attempt.
- 16:45:32: Policy change allowed lateral movement.
- 17:34:56: Failed login attempt.

#	IP	Country	City	Region	ISP	Org	Latitude	Longitude	Ip Reputation
1	31.203.135.126	Kuwait	Kuwait City	Al Asimah	Mobile Telecommunications Company	MTC GPRS AS Number	29.3645	47.9889	
5	106.0.116.228	China	Guangzhou	Guangdong	CHINANET-GD	Chinanet GD	23.1317	113.266	
21	121.196.140.227	China	Hangzhou	Zhejiang	Hangzhou Alibaba Advertising Co	Aliyun Computing Co., LTD	30.2994	120.1612	
23	110.249.206.252	China	Zhangjiakou	Hebei	China Unicom Hebei Province Network	Unknown	40.7687	114.886	
30	188.71.141.239	Kuwait	Kuwait City	Al Asimah	National Mobile Telecommunications Company	Wataniya Mobile IP	29.3645	47.9889	
43	117.80.77.27	China	Nanjing	Jiangsu	China Telecom	Chinanet JS	32.0607	118.763	Flagged Malicious
44	165.202.226.130	Hong Kong	Cheung Sha Wan	Sham Shui Po	CLP Power Hong Kong Ltd	CLP Power Hong Kong Ltd	22.3331	114.16	
48	116.22.77.219	China	Guangzhou	Guangdong	Chinanet	Chinanet GD	23.1181	113.2539	
61	58.30.103.46	China	Beijing	Beijing	Beijing Gehua Catv Network CO	Beijing Gehua Catv Network Co., Ltd.	39.9042	116.407	
68	168.63.143.34	Hong Kong	Hong Kong	Central and Western District	Microsoft Corporation	Microsoft Azure Cloud (eastasia)	22.267	114.188	
87	27.103.217.190	China	Guangzhou	Guangdong	GDHWNET	Gdhwnet	23.1377	113.282	
100	47.52.42.248	Hong Kong	Hong Kong	Kowloon	Alibaba Cloud LLC	Cloud Intelligence Limited	22.3193	114.169	

Fig 1: External IP Reputation Details

4.2.2 Incident Logging / Technical Analysis:

The incident appears to be a multi-stage attack involving:

- **Brute Force Attack:** Repeated failed login attempts targeting the administrator account.
  08:10:23: Successful login by user John Doe.
  09:45:32: Admin policy change (event ID 4719).
  Timeline: 10:32:17-10:32:21: Multiple failed login attempts followed by a successful login. This indicates a brute force attack targeting the admin account.

- **Privilege Escalation:** Successful login attempt followed by a policy change granting administrative privileges. The attacker may have gained elevated privileges.

- **Resource Exhaustion:** The resource exhaustion events suggest the attacker may have been attempting to compromise additional systems or execute malicious code.

  An application crash likely triggered by malicious activity.
  10:33:45: Resource exhaustion detected.
  12:01:15: Application error (explorer.exe).
  13:23:15: Resource exhaustion detected again.

- **Malware Infection:** The application error and resource exhaustion incidents point to a potential malware infection on the DESKTOP-1234567 machine.

- **Network Compromise:** The traffic blocked by the firewall and the suspicious network communications suggest the possibility of a network compromise.
  Unusual network traffic patterns indicating malicious activity.

  Traffic Blocked
  14:10:12: Traffic blocked by the firewall.
  File Access
  15:23:52: Database file corruption error.

- **Lateral Movement:** The allowed connection indicates the attacker may have successfully moved laterally within the network.
  15:34:56: Failed login attempt.
  16:45:32: Policy change allowed lateral movement.

4.2.3 Root Cause Analysis

- The primary cause of the breach appears to be a weak password for the workstation's administrator account, which allowed unauthorized access. The attacker was able to leverage the compromised account to escalate privileges and gain control of the system.
- On September 20, 2024, Maven Clinic Security Team detected suspicious network activity, including a traffic spike to the external IP address 203.0.113.45 and Multiple failed SSH and RDP login attempts. The activity indicated a brute-force attack targeting sensitive systems and prompted immediate escalation to the security team.
- Upon investigation, an unauthorized user account was found accessing sensitive files outside of business hours.

Incident Overview

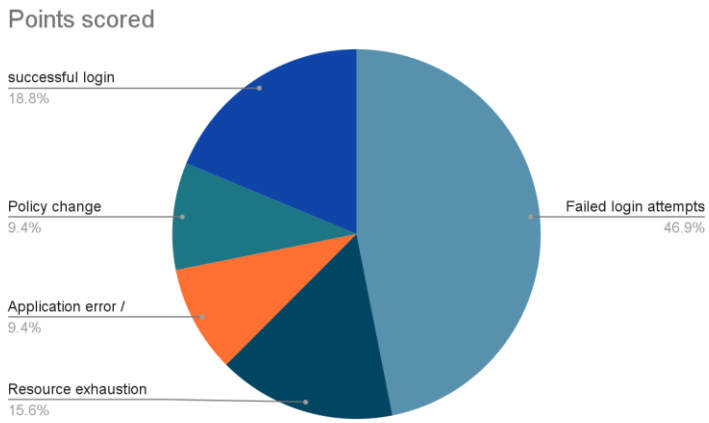


Fig 2 : chart displays Event and its occurrence Percentage .

4.3 Communication plan:

Key Stakeholders:

Stakeholders and the team must be quickly notified about the incident.

- **IT Department:** All members of the IT team, including system administrator, network engineers must be notified and take necessary steps to closely monitor the network.
- **Executives:** C-level executives, board members, and other key decision-makers.
- **Affected Users:** Employees, customers, or partners who may be impacted by the incident.This case Host machine DESKTOP-1234567 and user John doe must be notified , the file or server owner must be informed about the incident.
- **External Parties:** Law enforcement, regulatory agencies, or other third parties as needed.In case of data breach of sensitive information that involves other parties must be communicated directly.

5.0 Response Containment and Eradication

Fig 3: Best Practices for Preventing and Responding to Cyber incidents

5.1 Response:

Response to Affected Customers and Stakeholders of Maven Clinic

When a healthcare organization experiences a data breach, it's crucial to respond promptly, transparently, and empathetically to affected customers.

1. **Rapid Assessment and Containment:** Quickly determine the scope and severity of the breach and Implement measures to prevent further data loss and limit the impact of the incident.
2. **Notification and Communication:** Contact affected individuals as soon as possible, providing clear and concise information about the breach, the types of data compromised, and the steps being taken to address the situation.
3. **Empathy and Support:** Express empathy for the inconvenience and potential distress caused by the breach. Offer support like credit monitoring/financial settlement etc., based on the breach information and resources to help affected individuals protect themselves like network monitoring, suggesting security measures and training.
4. **Communication and Updates:** Provide regular updates to affected individuals and stakeholders about the progress of the investigation and remediation efforts. Be responsive to their questions and concerns.

5.2 Containment and Eradication:

The goal of containment is to stop the attack before it overwhelms resources or causes damage. Your containment strategy will depend on the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the duration of the solution—a temporary solution for a few hours, days or weeks, or a permanent solution.

1. Short-term: Make a plan to Isolate affected systems to prevent further damage or spread of the malicious activity. This can be temporary until long-term solutions are in place.

Contain and Eradicate:
Splunk and other SIEM solutions can be used to analyze large data logs. In this case the target source is Desktop-12345 and the data provided was analyzed by the event viewer. Depending how critical the attacks or incidents are the following steps can be taken.
Noncritical-

- Close the unwanted ports such as 50793 ,50791 and stop the unnecessary service.
- Move to a separate Vlan to limit access.
- Immediate change of username and password or adding MFA.
- Rechecking access controls to access any critical data as in this case the PII data of the patients.
- In log 13 the log shows a RADAR, monitor resource usage to identify the top three memory consuming processes. Limit the resource for the time until the investigation is ongoing. Also if there is no service running on port 445 then it can be restricted.
- Log 7 shows a DNS query to a domain which may be malicious hence isolate the system and scans thoroughly. Eradicate by restricting the DNS queries to illegitimate sites.

Critical-

- Disconnect the server or target from the Internet and disable network interfaces.
- Disable remote access.
- Monitor data from all the detection or IDS systems.

As the application log shows some input validation failures it could be cross site Scripting. Temporally take off the suspected application.

Authentication logs show several failed attempts which may be brute force attempts. Hence using firewall configurations these IPs can be blocked.

Firewall log-
Insider threats- the log from the system shows a successful login as an admin. Checking with the administrator and the timings when the system was logged into.

2. Long-term: Make a plan Implement long-term measures such as system patches, firewall rules, or enhanced intrusion detection mechanisms to secure compromised systems.

- Patching the system in case of any vulnerability update.
- Next gen Antimalware
- Making sure the system is backed up and has a regular schedule for backups.
- Reviewing the security Policies and access control to the critical data
- Documenting all the findings and every step taken the isolate and eradicate.
- Informing and communicating with the associated teams and stakeholders.

Recommended Actions:

- Implement strong password policies and multi-factor authentication.
- Conduct regular security assessments and vulnerability scans.
- Provide security awareness training to employees.
- Develop and test a comprehensive incident response plan.
- Invest in automated security tools to streamline incident response and improve efficiency.
- Stay informed about emerging threats and trends through threat intelligence feeds.

6.0 Post-Incident Review

6.1 Relevant Stakeholders

Legal Counsel: To evaluate any legal implications resulting from the breach.
Public Relations: To manage communication with the public and mitigate any potential damage to our corporate image.
• IT Department Heads: To discuss the technical response and future preventive measures.
• Compliance Officer: To ensure adherence to relevant laws and regulations regarding data protection.

6.2 Business Impact

The potential impact of this incident includes:

- **Data Exfiltration:** Sensitive patient data stored on the workstation may have been compromised.
- **Disruption of Services:** The compromised workstation may have affected the availability of critical services.
- **Reputational Damage:** A data breach could damage Maven Clinic's reputation and public trust.
- Regulation compliance such as HIPAA and GDPR must be focused and take steps if any customer data that may have been exposed or compromised.
- Downtime: operational disruption or unavailability of data
- Customer Impact: Take necessary actions if any sensitive data or PII /health related data exposed

- Financial Loss: Estimate of financial costs due to the incident.

6.3 What Went Wrong?

Weak Password Hygiene: The primary cause of the breach was the use of a weak password for the workstation's administrator account. This underscores the importance of enforcing strong password policies and using multi-factor authentication (MFA).

Lack of Regular Security Assessments: The absence of regular vulnerability assessments may have allowed the attacker to exploit known vulnerabilities in the system.

Insufficient Monitoring: The system may not have been adequately monitored for suspicious activity, allowing the attacker to gain a foothold and escalate privileges.

6.4 Lessons Learned

- **Importance of Strong Passwords:** The breach highlights the critical importance of using strong, unique passwords for all accounts.
- **Regular Security Assessments:** Regular vulnerability assessments are essential for identifying and addressing potential risks.
- **Employee Education:** Security awareness training can help employees recognize and prevent phishing attacks.
- **Incident Response Planning:** A well-defined incident response plan can help organizations respond effectively to security incidents.
- **Conduct a Post-Incident Review:** Analyze the incident to identify lessons learned and areas for improvement.
- **Implement Preventive Measures:** Strengthen security measures to prevent similar incidents in the future.

6.5 Preventive Measures

By implementing these preventive measures, Maven clinic can significantly enhance their security posture and reduce the risk of future data breaches.

1. Phishing Awareness Training
2. Strong Password Policies(complex with MFA)
3. Regular Security Assessments
4. Incident Response Planning
5. Data Encryption
6. Strong Access Controls to limit sensitive data access
7. Third-Party Risk Management

6.6 Areas of Improvement

- **Staff Coverage:** Ensure adequate staffing levels within the security operations center (SOC) to maintain 24/7 coverage and timely response to incidents.
- **Awareness Training:** Provide regular security awareness training to employees to help them recognize and prevent phishing attacks and other social engineering tactics.
- **Automation of Security Operations:** Implement automated security tools like SOAR , XDR, ASO (Autonomic SecOps) etc., and processes to reduce the burden on security teams and improve response times.
- **Threat Intelligence:** Leverage threat intelligence feeds to stay informed about emerging threats and trends.
- **Incident Response Planning:** Develop and regularly test a comprehensive incident response plan to ensure a coordinated and effective response to security incidents.
- Implement ZTA , Strong MFA and system Hardening measures to avoid these incidents in future.

6.6.1 Estimated budget:

- More trained staff needs to be employed and existing employee- People (Training and Staff): $250,000 - $800,000/year
- A designated team or staff is needed -Process (Access Control Management): $5,000 - $50,000 (initial setup) + $1,000 - $5,000/year (ongoing)
- A second-generation firewall at the end points are needed- Tech (Systems, Monitoring, and Firewall): $10,000 - $50,000 (initial setup) + $1,500 - $10,000/month (ongoing)
- Insurance (Cyber, Liability, and Malpractice): $4,500 - $10,000/yea

7.0 Conclusion

By addressing these Lesson learned areas and implementing the recommended measures, Maven Clinic can significantly enhance/strengthen its security posture and reduce the risk of future breaches. Regular review and updates of the incident response plan are essential to maintain a proactive and effective approach to cybersecurity.