Maven Clinic Post-Incident Review: Unusual Network Activity

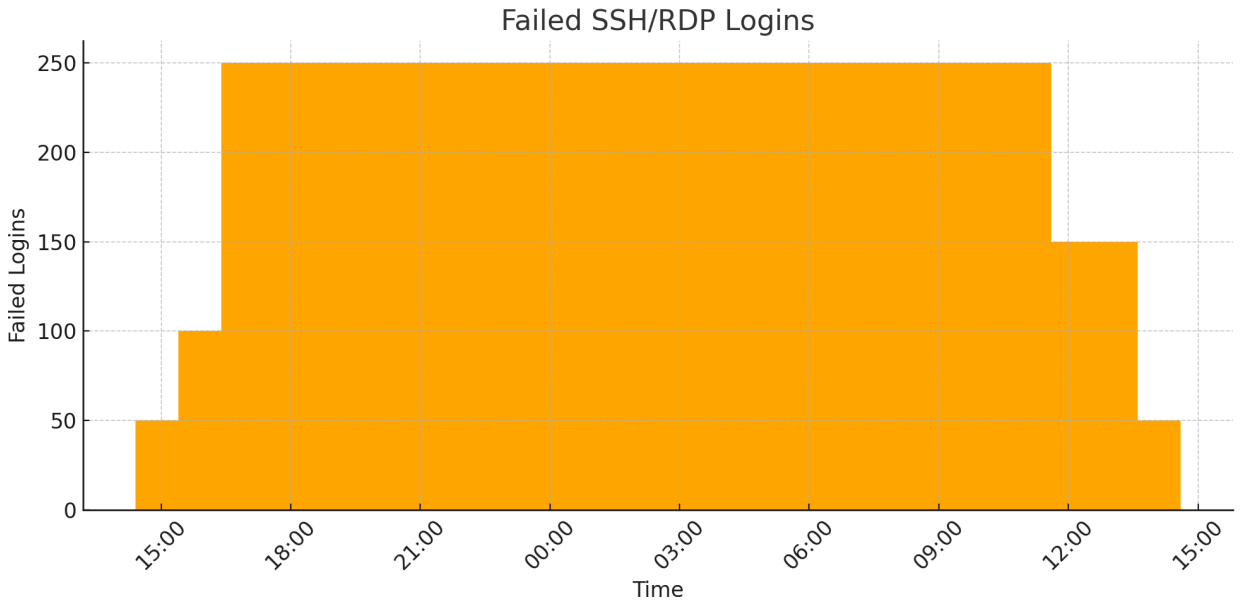
Executive Summary

On **September 20, 2024**, the **Security Information and Event Management (SIEM)** system at Maven Clinic detected suspicious network activity, including a **traffic spike** to the external IP address **203.0.113.45** and **250+ 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 (Admin-G01)** was found accessing sensitive files outside of business hours. Additionally, **multi-factor authentication (MFA)** had not yet been implemented across all critical systems, increasing vulnerability to unauthorized access.

Key Findings and Actions Taken

Key Finding	Details	Action Taken	Outcome
Suspicious IPs	Traffic spikes to **203.0.113.45** at **2:00 AM UTC**	Blocked IP, quarantined affected systems	Prevented further access
Multiple SSH/RDP Attempts	250+ failed login attempts from unknown IPs	Disabled accounts, restricted RDP/SSH	Mitigated brute-force attack
Unauthorized User Accounts	**Admin-G01** accessed sensitive files outside business hours	Disabled account, escalated for investigation	Stopped unauthorized access
Lack of MFA	MFA not implemented on all sensitive systems	Implemented MFA on **Day 2**	Improved security posture



Response and Containment

By **3:15 AM UTC** on **September 20, 2024**, the security team had **isolated affected systems** to prevent further unauthorized access. **Suspicious IP addresses** were blocked, and full **malware scans** were conducted on quarantined systems. **Backups** were taken for forensic analysis, and the unauthorized account **Admin-G01** was disabled.

On **Day 2**, **multi-factor authentication (MFA)** was implemented across all critical systems, and **firewall rules** were updated to block malicious IP addresses and restrict remote access (SSH/RDP). These measures effectively stopped the ongoing attack and secured the clinic's systems.

Outcome and Business Impact

The incident was contained successfully, with **no data exfiltration** or **patient data compromised**. System downtime was minimal, with affected systems isolated for approximately **6 hours**. 8:30 AM UTC restored full system functionality **on September 22, 2024**. **Client reassurance communications** were sent on **September 23, 2024**, maintaining transparency and trust with patients and partners.

Next Steps

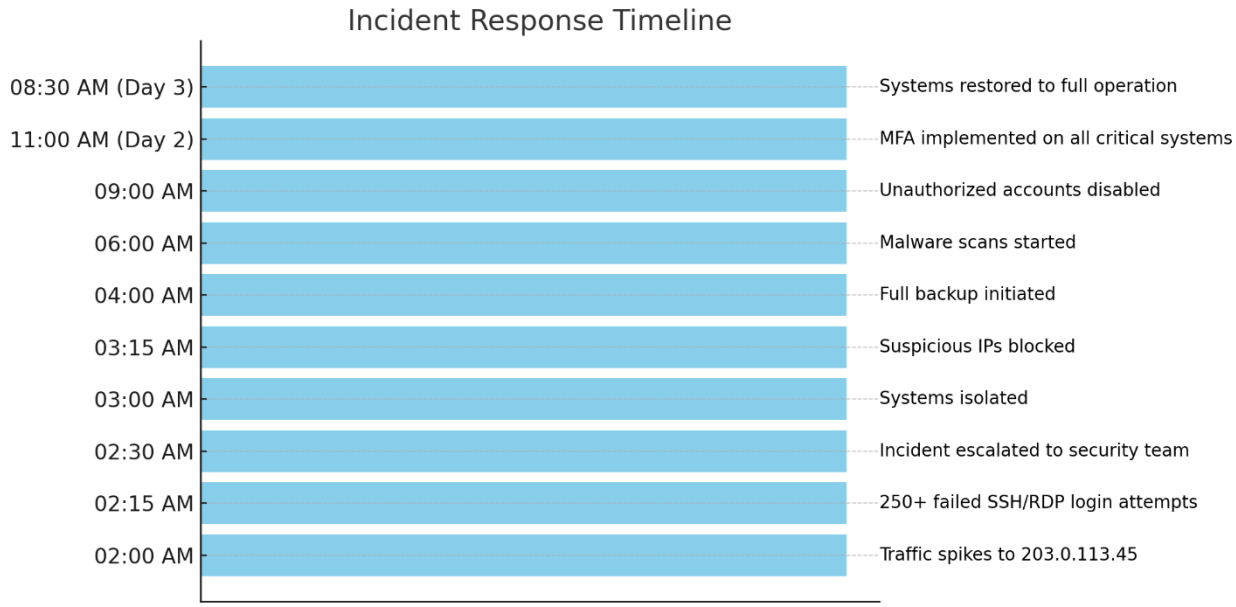
1. **Automated Incident Response**: Implement automated isolation and IP blocking to reduce response times.
2. **Quarterly Security Audits**: Continue proactive vulnerability assessments and penetration tests.
3. **Employee Training**: Conduct cybersecurity training to improve staff awareness and preparedness.

Conclusion

The swift response and effective mitigation of the incident ensured that Maven Clinic's systems remained secure and that no patient data was compromised. The post-incident measures, including the rapid deployment of MFA, firewall rule updates, and employee training, have strengthened the clinic's security posture against future threats.

Incident Overview

Below is the timeline of key events as the incident was detected and resolved:



---

1. Target Audience

This report is designed for **key internal stakeholders**, including:

- **Senior Management**: CEO, CTO, COO
- **IT & Security Teams**
- **Legal Counsel**
- **Compliance & Risk Management**
- **Public Relations (PR)**
- **External Partners** (if necessary)

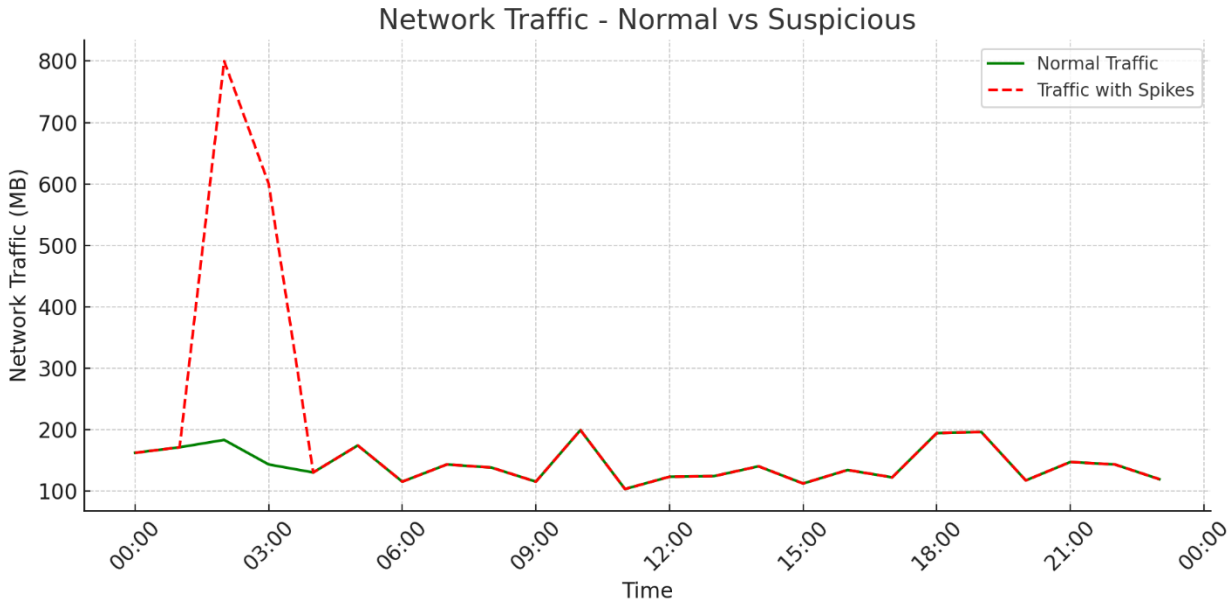
2. Incident Timeline (with Specific Times)

Here is a detailed breakdown of the incident timeline from **detection** to **resolution**, with specific times to track the progression of the incident.

Date	Time	Event
Day 1	**02:00 AM UTC**	SIEM flags abnormal traffic patterns, including a large volume of traffic directed to suspicious external IP **203.0.113.45**.
Day 1	**02:15 AM UTC**	Multiple failed SSH and RDP login attempts were detected, indicating a potential brute-force attack targeting the system.
Day 1	**02:30 AM UTC**	The incident is escalated to the security team, who begins an initial investigation to assess the scope of the issue.
Day 1	**03:00 AM UTC**	The security team determines that suspicious activity is ongoing and recommends isolating affected systems.
Day 1	**03:15 AM UTC**	Short-term containment begins: suspicious IPs (**203.0.113.45** and others) are blocked, and affected systems are isolated from the main network.
Day 1	**04:00 AM UTC**	Backups of isolated systems begin, ensuring all data is preserved for forensic analysis. Affected systems are kept offline.
Day 1	**06:00 AM UTC**	Malware scans are initiated on the isolated systems to determine the presence of any malicious software or unauthorized processes.
Day 1	**09:00 AM UTC**	Unauthorized user accounts (including Admin-G01) are identified, and access is immediately disabled.
Day 1	**01:00 PM UTC**	The security team reviews firewall logs and updates rules to permanently block suspicious IP addresses. Remote access (SSH and RDP) is restricted across critical systems.
Day 2	**09:00 AM UTC**	Vulnerabilities in RDP and SSH services are patched. The team confirms that no unauthorized software persistence mechanisms remain.
Day 2	**11:00 AM UTC**	Multi-factor authentication (MFA) is implemented for all administrative accounts and critical systems. This is completed across all systems by noon.
Day 3	**08:30 AM UTC**	All affected systems have been cleaned, patched, and restored to full operation. Network monitoring has been enhanced to detect any potential residual threats.
Day 4	**10:00 AM UTC**	Post-incident review preparation begins. Meetings are scheduled with relevant departments to gather insights and feedback on the response.
Day 4	**02:00 PM UTC**	PR and legal teams drafted and reviewed client reassurance communication, confirming there was no compromise in patient data, and sent it to clients by 03:00 PM UTC.

4. Security Review: What Went Right and What Could Be Improved

As seen in the graph below, a significant spike in network traffic was detected at 2:00 AM UTC when the attack occurred:



What Went Right

- **Timely Detection (02:00 AM UTC)**: The SIEM system successfully flagged unusual activity, giving the security team a head start on investigating the incident.
- **Swift Containment (03:15 AM UTC)**: The decision to isolate affected systems and block suspicious IP addresses was executed quickly, preventing further compromise.
- **Account Control (09:00 AM UTC)**: Suspicious accounts were rapidly disabled, preventing unauthorized access to sensitive systems.
- **Backup & Preservation (04:00 AM UTC)**: Comprehensive backups ensured that all compromised systems were preserved for forensic analysis.

What Could Be Improved

- **Response Time for Isolation (03:00 AM - 03:15 AM UTC)**: While isolation occurred within 45 minutes of the initial detection, further automation could reduce the exposure window.
- **Proactive MFA (Implemented by Day 2, 11:00 AM UTC)**: Multi-factor authentication was not enforced before the incident, leaving systems vulnerable to brute-force attacks. It has now been implemented across all sensitive systems.
- **Cross-Team Communication**: There were brief delays in notifying senior management and PR during the containment phase. A dedicated incident communication officer will improve future coordination.

4. Systems and Services Impact

Systems Impacted:

- **File Transfer Platform**: Primary system where traffic anomalies and unauthorized login attempts were observed.
- **RDP/SSH Services**: These remote access services were the focus of the brute-force attempts, highlighting the need for tighter controls and monitoring.

Data at Risk:

- **Patient Data**: There has been no confirmed compromise of patient data, but detailed log audits will continue to ensure no unauthorized access to personal health information.

Service Interruptions:

- **Minimal Downtime**: The affected systems were offline for approximately 6 hours during the containment phase. Regular operations resumed once containment was complete, and all systems were restored to normal functionality by **Day 3, 08:30 AM UTC**.

5. Business Impact and Legal Implications

Business Impact:

- **Reputational Risk**: Clients may be concerned about security even when no data breach occurs. A client reassurance communication was sent on Day 4, 03:00 PM UTC, to prevent reputational damage.
- **Operational Downtime**: System isolation temporarily lost availability, but the quick restoration of services mitigated this.

Legal Implications:

- **HIPAA Compliance**: No evidence of patient health information (PHI) exposure exists. However, ongoing audits will verify that no unauthorized access occurred. If any issues are found, HIPAA breach notification protocols will be initiated.

6. Communication Effectiveness

Internal Communication:

- **Feedback**: Communication delays were noted by senior management, particularly between **03:00 AM - 06:00 AM UTC**, during the initial containment. Assigning a dedicated incident communication officer will improve future coordination.

External Communication:

- **Client Notifications**: On Day 4, at 03:00 PM UTC, we sent notifications to reassure clients that no patient data was compromised. This proactive step maintained trust with our client base.

Public Relations Strategy:

- **PR Team**: Prepared FAQs and press releases in case the incident escalated into a public-facing issue. However, the need for public disclosures was avoided due to the swift containment and internal handling.

7. Post-Incident Review: Lessons Learned and Preventive Measures

Lessons Learned:

- **Early Detection Saves Time (02:00 AM UTC)**: Early identification of traffic anomalies was critical in minimizing the attack's impact.
- **Automating Key Actions**: Automating the isolation of affected systems and blocking IP addresses could have shortened the window of potential exposure.

Preventive Measures:

1. **Implement MFA Across All Systems**:
    - **Action**: Multi-factor authentication was fully implemented by **Day 2, 11:00 AM UTC**. Moving forward, MFA will be enforced on all critical systems.
2. **Quarterly Security Audits**:
    - **Action**: Increase the frequency of **penetration testing** and **vulnerability assessments** to identify weaknesses before they can be exploited.
3. **Automated Incident Response**:
    - **Action**: Implement automated response mechanisms to isolate systems and block IPs immediately upon detection of suspicious activity.
4. **Tabletop Drills**:
    - **Action**: Schedule **incident response drills** every quarter to ensure every team knows their role in case of an incident.
5. **Enhancing IDS/IPS Systems**:
    - **Action**: Improve **Intrusion Detection and Prevention Systems** to detect better and block attacks such as brute-force attempts and unauthorized access.

8. Incident Review Methodology and Presentation

Meeting Format:

1. **All-Hands Incident Review Meeting (Day 5, 10:00 AM UTC)**:

    - **Audience**: Senior management, IT & security teams, legal counsel, compliance, and PR teams.
    - **Objective**: Review the incident timeline and lessons learned and present preventive measures.
    - **Format**: Storyboards and Q&A sessions to ensure everyone's involvement and feedback.
2. **Executive Summary Email (Day 5, 02:00 PM UTC)**:
    - **Audience**: All employees.
    - **Purpose**: Provide a high-level summary of the incident and security enhancements implemented.
3. **Client Communication (Sent Day 4, 03:00 PM UTC)**:
    - **Audience**: External clients and partners.
    - **Purpose**: Ensure transparency and maintain trust by clearly explaining the incident and its resolution.

9. Next Steps and Investment Proposal

To continue enhancing our security posture, we recommend the following next steps:

1. **Short-Term (Next 30 Days)**:
    - Complete an audit of all systems to ensure MFA is enforced and all vulnerable systems have been patched.
    - Conduct a post-incident training session for all staff to ensure everyone is aware of best practices regarding cybersecurity.
2. **Long-Term (Within 6 Months)**:
    - Invest in **automated threat detection tools** to enhance our ability to detect and respond to threats in real time.
    - Schedule quarterly **penetration tests** to identify and resolve vulnerabilities proactively.

10. Recognition and Gratitude

We would like to recognize the incredible efforts of the **IT and security teams**, whose swift actions contained the threat and preserved the integrity of our systems.

Conclusion

The unusual network activity detected at Maven Clinic was swiftly contained and eradicated, preventing data loss or long-term damage. The lessons learned from this incident will drive future improvements, including **faster isolation procedures**, **multi-factor authentication**, and

enhanced communication protocols. Maven Clinic is committed to maintaining the highest data security levels and will continue monitoring systems for further suspicious activity.

Next Steps:

1. Conduct the **all-hands incident review meeting** on **Day 5, 10:00 AM UTC**.
2. Send the **executive summary email** to all employees by **02:00 PM UTC** on the same day.
3. Continue to audit logs and verify that no unauthorized data access has occurred.