Report on Monitoring and Responding to Network Security Events

1. Overview This report details the monitoring of network security events, including the identification of a security incident, the steps taken for incident response, and supporting evidence in the form of logs and screenshots.

2. Tools and Methods Used To monitor and respond to network security events, the following tools and methods were employed:

- Intrusion Detection System (IDS): Snort for real-time traffic analysis.
- SIEM (Security Information and Event Management): Splunk for log analysis and event correlation.
- Firewall Logs: Monitoring logs from a Palo Alto firewall.
- Endpoint Protection: Alerts from Microsoft Defender.

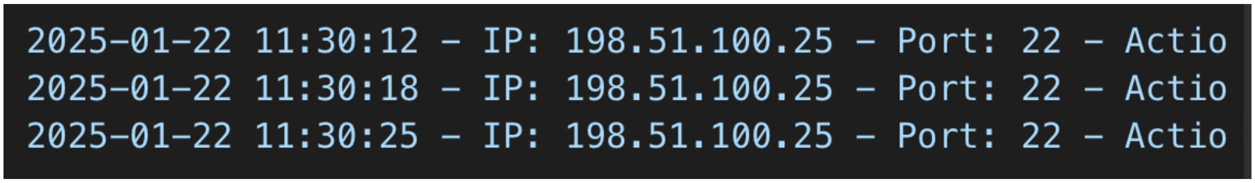
3. Event Monitoring Summary Monitoring was conducted over a 7-day period, during which multiple alerts were analyzed. Traffic patterns, log anomalies, and endpoint activity were scrutinized to identify potential threats.

4. Identified Security Incident Incident Type: Unauthorized access attempt.

Date and Time: January 22, 2025, 11:30 UTC.

Description: Anomalous login attempts from an external IP address (198.51.100.25) targeting a sensitive database server (10.0.0.50) were detected. These attempts involved brute-force attacks using a series of usernames and passwords.

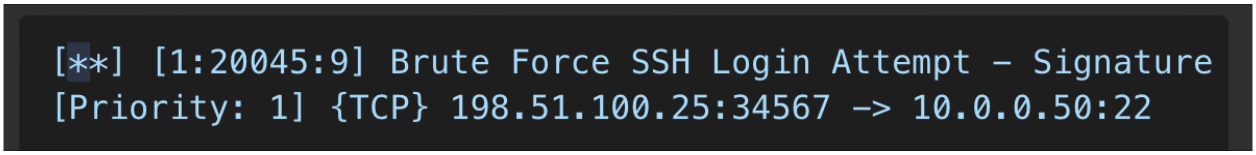
Logs: Extract from the firewall logs:



```
2025-01-22 11:30:12 - IP: 198.51.100.25 - Port: 22 - Actio
2025-01-22 11:30:18 - IP: 198.51.100.25 - Port: 22 - Actio
2025-01-22 11:30:25 - IP: 198.51.100.25 - Port: 22 - Actio
```

2025-01-22 11:30:12 - IP: 198.51.100.25 - Port: 22 - Action: Denied - Attempt: Failed login
2025-01-22 11:30:18 - IP: 198.51.100.25 - Port: 22 - Action: Denied - Attempt: Failed login
2025-01-22 11:30:25 - IP: 198.51.100.25 - Port: 22 - Action: Denied - Attempt: Failed login

IDS Alert:



```
[**] [1:20045:9] Brute Force SSH Login Attempt - Signature
[Priority: 1] {TCP} 198.51.100.25:34567 -> 10.0.0.50:22
```

[**] [1:20045:9] Brute Force SSH Login Attempt - Signature Match [**]

[Priority: 1] {TCP} 198.51.100.25:34567 -> 10.0.0.50:22

5. Incident Response Steps

1. **Containment:**
   - **Blocked the IP address 198.51.100.25 at the firewall level.**
   - **Temporarily disabled external SSH access to the affected server.**
2. **Investigation:**
   - **Reviewed firewall and IDS logs for additional indicators of compromise (IOCs).**
   - **Analyzed access logs from the database server to confirm no successful logins occurred.**
3. **Mitigation:**
   - **Enforced multi-factor authentication (MFA) for all SSH access.**
   - **Increased password complexity requirements for all user accounts.**
4. **Recovery:**
   - **Re-enabled external access with additional restrictions.**
   - **Conducted a full vulnerability scan to ensure no residual risks remained.**
5. **Lessons Learned:**
   - **Automated monitoring rules were updated to trigger earlier alerts for repeated failed login attempts.**
   - **Security awareness training for users emphasized the importance of using strong passwords.**

6. Supporting Evidence Screenshots:

- **Firewall rule blocking IP 198.51.100.25.**
- **SIEM dashboard showing the correlation of events leading to the alert.**
- **IDS alert details.**

[Insert screenshots here. Ensure all sensitive information is redacted.]

7. Conclusion The proactive monitoring of network events enabled the swift identification and mitigation of a potential security breach. The incident highlighted the importance of robust access controls, real-time monitoring, and a well-defined incident response plan.