Security Monitoring and Incident Response Plan

1. Security Monitoring Implementation

Use Case: Unauthorized Network Access Detection

Detection Rules

- **Rule Name**: Unauthorized Network Access
- **Trigger Condition**:
  - Multiple failed login attempts from a single IP address within 5 minutes.
  - Unusual login times outside standard business hours.
  - Login attempts from blacklisted or foreign IP addresses.
- **Detection Tool**:
  - Use **Suricata** or **Snort** for real-time intrusion detection.

Sample Snort Rule:
python
CopyEdit

```
alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH Brute Force
Attack"; flags:S; threshold: type both, track by_src, count 5, seconds
300; sid:1000001;)
```

  -

- **Log Source**:
  - System logs (`/var/log/auth.log` for Linux, Event Viewer for Windows)
  - Firewall logs for unauthorized access attempts

Alert Prioritization Process

Severity Level	Criteria
Critical	Repeated failed logins from an external IP address
High	Multiple failed logins within a short time from an internal source
Medium	Single failed login attempt from a new device
Low	Failed logins from known users with history of mistyped passwords

- **Action for Critical Alerts**:
    - Immediately block the IP using firewall rules.
    - Alert security team via email/SMS notification.

Response Procedures

1. **Analyze Logs** – Review login attempts and cross-check with authorized user activity.

Block Malicious IPs – Apply firewall rules:
css
CopyEdit

```
sudo iptables -A INPUT -s <malicious-IP> -j DROP
```

2.
3. **Notify Security Team** – Send an immediate alert for investigation.
4. **Reset Credentials** – If a legitimate user is affected, force a password reset.
5. **Audit Network** – Conduct a vulnerability scan to check for further signs of compromise.

---

2. Incident Response Scenario

Incident: Brute Force Attack on SSH

Incident Classification

- **Category**: Unauthorized Access Attempt
- **Severity**: High (potential system compromise if successful)
- **Source**: Unknown IP attempting multiple logins to SSH service.

Response Steps Taken

1. **Detection**
    - Logs showed multiple failed login attempts from IP `192.168.1.100`.
    - Suricata flagged the activity as a brute-force attempt.
2. **Containment**

Immediately blocked IP `192.168.1.100` via:
css
CopyEdit

```
sudo iptables -A INPUT -s 192.168.1.100 -j DROP
```

○

Disabled SSH access for root:
nginx
CopyEdit

```
sudo nano /etc/ssh/sshd_config
PermitRootLogin no
sudo systemctl restart sshd
```

   -

3. **Eradication**
   - Reviewed logs to confirm no successful unauthorized logins.

Conducted a full vulnerability scan using Nmap:
css
CopyEdit

```
nmap -sV --script vuln <server-IP>
```

   -
   - Applied security patches and updated SSH configurations.
4. **Recovery**
   - Allowed SSH access only via VPN.

Implemented fail2ban to prevent repeated login attempts:
sql
CopyEdit

```
sudo apt install fail2ban
sudo systemctl start fail2ban
```

   -

5. **Lessons Learned**
   - **Preventative Actions**:
     - Implemented **multi-factor authentication (MFA)** for SSH access.
     - Enabled logging and alerting for login attempts.
   - **Detection Enhancements**:
     - Improved monitoring by integrating logs with **SIEM tools** like Splunk.

Conclusion

- **Monitoring Implementation**: Successfully configured detection for unauthorized network access.
- **Incident Response**: Brute force attack was identified, mitigated, and future risks were minimized.
- **Next Steps**: Regular testing, improved alerting mechanisms, and continuous monitoring.