Project: Security Monitoring and Incident Response

Objective

Set up a basic security monitoring system using Graylog, define a detection use case, implement an incident response scenario, and document the entire process with mock data.

1. Setup of Security Monitoring

Tools and Environment

- **Log Management Tool:** Graylog
- **Data Source:** Mock Windows Event Logs or Apache Web Server Logs
- **Detection Rule Framework:** Graylog's built-in alerting and pipelines

Steps to Set Up Graylog

1. **Install Graylog:** Use a local virtual machine or cloud-based environment.
   - Follow the official Graylog installation guide.
   - Ensure dependencies like Elasticsearch and MongoDB are set up.
2. **Ingest Logs:**
   - Generate mock data using Windows Event Logs or web server logs.
   - Configure a log input in Graylog (e.g., Syslog UDP/TCP or Filebeat for log shipping).
   - Confirm logs are visible in Graylog’s interface.
3. **Create Alerts:**
   - Navigate to the **Alerts & Events** section.
   - Define an alert condition for the detection use case.

2. Detection Use Case

Scenario: Unauthorized Login Attempts

Objective: Detect multiple failed login attempts from a single IP address, which could indicate a brute-force attack.

Steps to Implement the Use Case:

1. **Define Detection Rule:**
   - Go to Graylog **Pipelines**.

Create a rule to count login failures from a single IP within 5 minutes:

```
rule "Detect Brute Force"
when
   to_long($message.failed_login_count) > 5
then
   create_event("Brute Force Detected", $message);
```

   - end

2. **Set Up Alert Notification:**
   - Define an alert in **Alerts & Events**.
   - Configure it to trigger when the pipeline detects the event "Brute Force Detected."
   - Add email or webhook notifications.

Mock Data Example:

Timestamp	Source IP	Event ID	Username	Action
2025-01-01 12:00:00	192.168.1.10	4625	user1	Failed Login
2025-01-01 12:01:30	192.168.1.10	4625	user1	Failed Login
2025-01-01 12:02:00	192.168.1.10	4625	user1	Failed Login
2025-01-01 12:02:30	192.168.1.10	4625	user1	Failed Login
2025-01-01 12:03:00	192.168.1.10	4625	user1	Failed Login
2025-01-01 12:03:30	192.168.1.10	4625	user1	Failed Login

Detection Trigger: Brute force detection alert created after 5 failed login attempts.

---

3. Incident Response Scenario

Incident: Brute Force Attack

Objective: Respond to an alert of unauthorized login attempts from a single IP address.

Incident Classification:

- **Type:** Brute Force Attack
- **Severity:** Medium

Response Steps Taken:

1. **Containment:**
   - Block the IP address (192.168.1.10) using the firewall.
2. **Eradication:**
   - Review logs to ensure no successful login occurred.
   - Reset the password for the targeted user account (user1).
3. **Recovery:**
   - Monitor further login attempts from other IPs.
   - Ensure system is patched and protected.
4. **Lessons Learned:**
   - Implement rate limiting for login attempts.
   - Educate users about strong password policies.

Mock Data for Response:

Timestamp	Action Taken	Notes
2025-01-01 12:05:00	IP Blocked	Blocked IP 192.168.1.10.
2025-01-01 12:06:00	Password Reset	Reset password for user1.
2025-01-01 12:10:00	Log Review	Verified no successful logins
2025-01-01 12:15:00	Monitoring Enabled	Enabled login rate limiting.

---

4. Documentation and Evidence

Functionality Evidence:

1. Screenshot of Graylog interface showing the detection rule in action.
2. Screenshot of alert triggered in Graylog.
3. Screenshot of logs confirming response steps (e.g., IP block logged).

Process Summary:

- **Setup Completed:** Graylog installed, and logs ingested successfully.
- **Use Case Implemented:** Brute force detection rule with alerts.
- **Incident Response:** IP blocked, user secured, and mitigations applied.

Conclusion

This project demonstrated basic security monitoring using Graylog, the creation of a detection rule, and a structured incident response process with lessons learned. The practical implementation and mock data validate the effectiveness of this setup for identifying and responding to security incidents.