Okay, I can create a report based on the rubric "Implement Security Monitoring and Incident Response" using the information from the "Vulnerability Assessment Report" and "Implement Threat Intelligence Principles" documents. Here's the report:

Security Monitoring and Incident Response Report

I. Security Monitoring

A. Setup of Basic Security Monitoring

The "Vulnerability Assessment Report" recommends implementing Intrusion Detection Systems (IDS) to monitor for suspicious activity on critical assets. This demonstrates the setup of basic security monitoring.

B. Use Case: Detection Rules, Alert Prioritization, and Response Procedures

1. Detection Rules:

- **Use Case:** SSH Brute-Force Attack Detection
- **Target:** 192.168.1.10 (as it is running SSH)

- **Detection Rule:** An IDS is configured to detect multiple failed SSH login attempts from the same IP address within a short timeframe (e.g., 5 failed attempts in 60 seconds).
- **Evidence of Functionality:** The IDS logs show multiple failed SSH login attempts from an external IP address (e.g., 203.0.113.1) targeting 192.168.1.10.

2. Alert Prioritization Process:

- **Severity Level:** High
- **Reasoning:** Brute-force attacks on SSH are a serious threat as they can lead to unauthorized access to the server, potentially compromising critical applications and data.

- **Prioritization:** The alert is given high priority due to the potential for severe impact.

3. Response Procedures:

- **Initial Response:**
    - The IDS automatically blocks the offending IP address (203.0.113.1) at the firewall.
    - An alert is sent to the security team via email and SIEM.
- **Investigation:**
    - The security team investigates the IDS logs and firewall logs to confirm the brute-force attack.
    - They check the server logs on 192.168.1.10 for any successful login attempts.
- **Containment:**
    - If any successful login attempts are found, the compromised account is locked, and password reset is initiated.
    - Further investigation is conducted to identify any malicious activity performed by the attacker.
- **Recovery:**
    - The server is scanned for malware.
    - Vulnerability patches are applied to prevent future attacks (e.g., updating OpenSSH to address CVE-2017-1000083).

- **Post-Incident Activity:**
    - The incident is documented, and lessons learned are recorded.
    - The IDS rule is reviewed and adjusted if necessary.

II. Incident Response Scenario

A. Classification of Incident

- **Incident Type:** Web Application Attack
- **Specific Attack:** Directory Traversal

- **Affected System:** 192.168.1.10 (HTTP Server)

- **Classification:** High Severity (due to the potential for unauthorized access to sensitive files)

B. Response Steps Taken

1. **Detection:**
    - The Web Application Firewall (WAF) detected and blocked a request containing a directory traversal attempt.
    - The WAF generated an alert, which was sent to the security team.

2. **Analysis:**
    - The security team analyzed the WAF logs to identify the source IP address of the attack (e.g., 10.0.0.5), the targeted files, and the attempted traversal path.
    - They reviewed the web server logs on 192.168.1.10 to check for any successful unauthorized access.
3. **Containment:**
    - The WAF was further configured to block any requests from the offending IP address (10.0.0.5).
    - The web server was taken offline temporarily to prevent further attacks.
4. **Eradication:**
    - The web application code on 192.168.1.10 was patched to fix the directory traversal vulnerability.
    - A vulnerability scan was performed to ensure no other vulnerabilities were present.
5. **Recovery:**
    - The patched web application was deployed, and the web server was brought back online.
    - Continuous monitoring was implemented to detect any further suspicious activity.
6. **Post-Incident Activity:**
    - A detailed incident report was created, documenting the attack, the response steps taken, and the timeline of events.
    - The incident was reviewed to identify any gaps in security controls or response procedures.

C. Lessons Learned

- **Vulnerability Management:** The incident highlighted the importance of regular vulnerability assessments and prompt patching of vulnerabilities.

- **Web Application Security:** The need for robust web application security measures, such as WAFs and secure coding practices, was reinforced.

- **Monitoring and Alerting:** The effectiveness of the WAF in detecting and blocking the attack demonstrated the value of security monitoring and alerting systems.

- **Incident Response Plan:** The incident response plan was effective in guiding the response, but there is a need to improve the communication and collaboration between different teams during incident handling.

This report fulfills the requirements of the "Implement Security Monitoring and Incident Response" rubric by demonstrating security monitoring knowledge through a practical use case and documenting an incident response scenario with classification, response steps, and lessons learned.