Task 1. Threat Intelligence Report

In the given scenario, where the attack vector is an unpatched vulnerability in a web application, AWS Security Hub would provide a comprehensive view of the security posture and findings related to the breach. AWS Security Hub would aggregate and present findings related to the vulnerability and exploit, including alerts from integrated services such as AWS GuardDuty and AWS Config. However, if detailed information about the attack is not available, the following steps can be taken:

Types of Attacks:

SQL Injection (SQLi): This attack manipulates a web application's database queries through user inputs, which can lead to unauthorized access to backend and databases.

Cross-Site Scripting (XSS): Injecting malicious scripts into webpages viewed by others, allowing the attacker to potentially steal information or perform actions on behalf of you.

Man-in-the-Middle (MitM): Attackers intercept and alter communications between two parties to steal sensitive data or manipulate the communication for their own gain.

How Exploiting a Vulnerability Can Provide Access: When a vulnerability in a web application is left unpatched, it can allow attackers to exploit that weakness to execute malicious actions, such as gaining access, elevating privileges to move across the network, updating configuration to maintain long-term access and enable the security mechanism to create new open doors.

Preventive Measures:

1. **Regular and Automated Patching and Updates**: All systems, infra, applications are neet to be regularly updated with the latest security patches.
2. **Vulnerability Scanning and Penetration Testing**: Regularly scan for vulnerabilities using tools such as AWS Security Hub identify and remediate findings and create automated remediations.
3. **Web Application Firewalls (WAF)**: Deploy a WAF to filter and monitor HTTP traffic and protect against common web-based attacks.
4. **Secure Software Development Lifecycle (SSDLC)**: With the help of CICD tool using to enhance SDLC integrate security check at all levels with automated process. This will robust the security of infrastructure, software development, including code reviews, threat modeling, and regular testing.

Task 2. Incident Response Plan

Incident Response Plan Outline:

For the incident response plan, the preparation and identification steps are typically determined first. However, since a breach has already occurred, I began with the containment step.

- **Containment:**

Disconnect affected systems from the network to prevent further spread until a secure backup recovered. Apply patches to vulnerable systems, revoke compromised credentials, and update firewall rules.

- **Eradication:**

Remove the malicious files, malware, or files installed by attackers. Identify and patch all vulnerabilities exploited in the breach. Ensure all compromised accounts are reset, and data is secured.

- **Recovery:**

Restore systems from last secure backups. Step by step reconnect affected systems to the network, monitoring for any activities. Retest system to ensure all vulnerabilities have been resolved.

Task 3. Network Security Measures

Recommended Security Technologies and Practices:

- **Intrusion Detection and Prevention Systems (IDS/IPS):**

Deploy IDS/IPS such as AWS Network Firewall or NDR tool to monitor network traffic for malicious activity. These system can detect and prevent attacks by identifying known attack pattern and anomalous behavior. They provide real-rime analysis of network traffic, alerting security team to potential threats and automatically blocking suspicious activities.

- **Network Segmentation:**

Divide the network into smaller, isolated segments to limit an attacker's ability to move laterally within the network. Implement separate zones for sensitive data (like private VPCs) and enforce strict access controls.

- **Multi-Factor Authentication (MFA):**

Enforce MFA for accessing critical systems and data to enhance protection against unauthorized access.

- **Security Information and Event Management (SIEM):**

Utilize a SIEM solution like AWS Security Hub to collect, analyze, centralize and correlate logs from various systems. This will help in real-time threat detection and response.