**Project: Incident Response and Forensics using Generative AI**

**Prompt 1: Roles and Responsibilities of Key Team Members in the Incident Response Team**

**Role 1: Incident Response Team Leader**  
The Incident Response Team Leader oversees the entire incident response process, coordinates the team, and makes critical decisions during the incident, ensuring a timely and effective response.

**Role 2: Communication Liaison**  
The Communication Liaison manages both internal and external communications, keeping management, clients, and other stakeholders informed about the incident’s status and response actions.

**Role 3: Technical Specialist**  
Technical Specialists are responsible for identifying, containing, and eradicating the technical aspects of the incident, including malware removal, forensic analysis, and system recovery.

**Role 4: Incident Documentation Specialist**  
The Incident Documentation Specialist ensures that all actions taken during the incident are documented accurately and in detail, including timelines, decision-making processes, and post-incident analysis.

**Prompt 2: Methods for Monitoring Internal Systems for Unusual Activity**

**Task 1: Intrusion Detection System (IDS)**  
Using an IDS to monitor network traffic for abnormal patterns or unauthorized activities, which can help detect potential threats and provide real-time alerts.

**Task 2: Log Monitoring and Analysis**  
Regularly reviewing and analyzing logs from systems and applications for unusual or suspicious activities, such as failed login attempts, unusual access times, or changes to sensitive files.

**Task 3: Endpoint Security Monitoring**  
Implementing endpoint protection software on all devices to monitor for signs of malware, unauthorized access, or unusual behavior on employee devices.

**Task 4: Network Traffic Analysis**  
Continuously analyzing network traffic for unusual communication patterns, such as large data transfers or connections to unfamiliar external IP addresses, which may indicate data exfiltration attempts.

**Prompt 3: Details to Include When Documenting Detected Incidents**

**Detail 1:** A timeline of the incident from initial detection to resolution, including key milestones and actions taken.

**Detail 2:** A description of the affected systems, data, and departments involved in the incident, including the severity and scope of the impact.

**Detail 3:** The method of attack or breach, such as spear-phishing, and the attack vector used to gain unauthorized access.

**Detail 4:** A summary of the containment, eradication, and recovery actions taken to address the incident and restore normal operations.

**Prompt 4: Containment Strategies**

**Containment Strategy Name 1: Account Isolation**  
By deactivating compromised accounts immediately, SecureSync can prevent further unauthorized access to critical systems, limiting the scope of the breach.

**Containment Strategy Name 2: Network Segmentation**  
Isolating affected network segments from the rest of the infrastructure prevents the attack from spreading to other systems and helps contain the impact.

**Prompt 5: Four Steps for Post-Incident Reviews Based on the NIST Framework**

**Step 1:** Conduct a comprehensive review of the incident, including what occurred, how it was detected, and its impact on the organization.

**Step 2:** Assess the effectiveness of the response efforts, focusing on what worked well and areas where improvements can be made.

**Step 3:** Implement corrective actions to address identified weaknesses, such as patching vulnerabilities, improving security protocols, and enhancing response capabilities.

**Step 4:** Update the incident response plan based on the lessons learned to improve preparedness for future incidents.

**Prompt 6: Checklist for Updating the Response Plan Based on Findings**

**Task 1:** Incorporate newly identified attack vectors and tactics into the response plan, ensuring that the organization is prepared for emerging threats.

**Task 2:** Update training programs to address new security risks and response procedures discovered during the incident.

**Task 3:** Strengthen communication protocols to improve coordination across departments and with external stakeholders during future incidents.

**Prompt 7: Sources of Digital Evidence Necessary for Incident Investigation**

**Source 1:** System and application logs, which provide records of system activities, including login attempts, file access, and error messages that help track the breach.

**Source 2:** Network traffic data, such as packet captures, to analyze any unauthorized communication or data exfiltration occurring during the incident.

**Source 3:** Endpoint security logs, which show activities on compromised devices and can help trace the malware infection path and methods of attack.

**Source 4:** User authentication logs, which help identify unusual login patterns, unauthorized access attempts, or compromised credentials.

**Prompt 8: Steps to Assess Collected Digital Evidence and Verify Its Integrity**

**Step 1:** Verify the source and authenticity of the evidence to ensure it is relevant and accurately represents the incident’s activities.

**Step 2:** Use cryptographic hashing (e.g., MD5, SHA) to ensure that the evidence has not been altered or tampered with since it was collected.

**Step 3:** Document the chain of custody, tracking who accessed the evidence, when, and for what purpose to maintain its integrity.

**Prompt 9: Types of Digital Evidence to Review for Forensic Investigation**

**Evidence Type 1: Email Logs**  
Reviewing email logs helps identify spear-phishing emails that may have been the initial attack vector, which could have compromised user credentials or systems.

**Evidence Type 2: Network Traffic Data**  
Analyzing network traffic data can reveal unusual communication patterns, such as connections to external IP addresses or large data transfers, indicating potential data exfiltration.

**Evidence Type 3: System and Application Logs**  
Examining system and application logs provides a timeline of events leading up to and following the breach, helping to understand the attack’s progression and identify affected systems.

**Prompt 10: Key Components of Structured Reports After Incidents**

**First Key Component: Incident Overview**  
This section summarizes the nature of the incident, including how it was discovered, the attack vector, and the impact on systems and data.

**Second Key Component: Actions Taken**  
Describes the containment, eradication, and recovery steps taken during the incident, outlining the response efforts to mitigate the damage.

**Third Key Component: Lessons Learned**  
Discusses the lessons learned from the incident, identifying weaknesses in security and response protocols and suggesting areas for improvement.

**Fourth Key Component: Preventive Measures**  
Outlines preventive actions, such as implementing additional security controls, patching vulnerabilities, or enhancing employee training to reduce the risk of future incidents.