7. Create an Incident Response Report
Activities:

- **Task:** Document an incident using SANS templates**.**

  The SANS incident response lifecycle: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned

- Incident Identification
- Incident Description
- Incident Classification
- Actions Taken
- Recommendations
- Lessons Learned

1. Executive Summary

Report Identifier:	**IR-2024-001**
Incident Title:	Simulated Phishing Campaign Leading to Initial Access
Date of Incident:	August 24, 2024
Report Date:	August 24, 2024
Incident Handler:	[Your Name/Team Name]

Overview: On August 24, 2024, the security team initiated a controlled simulation of a phishing attack against the internal lab environment. The simulated attack successfully tricked a user into executing a malicious payload, granting the simulated adversary initial access to a Windows 10 endpoint. The incident was automatically detected by the Velociraptor EDR platform. The incident response process was followed, resulting in the swift containment and eradication of the threat. The purpose of this simulation was to validate detection and response capabilities.

Impact Assessment: The impact was limited to a single, non-critical lab virtual machine. No sensitive data was accessed or exfiltrated. The primary impact was a temporary loss of availability for the VM during the forensic analysis and reimaging process.

Root Cause: The root cause was the successful execution of a malicious script (phish_sim.bat) delivered via a simulated phishing email. This highlighted a need for enhanced user awareness training against social engineering tactics.

2. Timeline of Events (UTC)

Timestamp	Event Description	Phase
2024-08-24 14:00	Simulation began. Caldera server executed operation "PhishingSim".	Preparation
2024-08-24 14:02	Simulated phishing email delivered to target user's mailbox.	Delivery
2024-08-24 14:05	User executed the attached phish_sim.bat payload.	Initial Access
2024-08-24 14:05:30	Payload established persistence via Registry Run Key.	Persistence
2024-08-24 14:06	Payload performed host discovery (whoami, systeminfo).	Discovery
2024-08-24 14:07	Velociraptor alert triggered based on anomalous process creation.	Detection
2024-08-24 14:10	IR team initiated response. Analysis confirmed compromise.	Analysis
2024-08-24 14:15	Network isolation rule applied to the endpoint.	Containment
2024-08-24 14:25	Endpoint was reimaged from a known-good backup.	Eradication
2024-08-24 14:40	System was validated as clean and returned to service.	Recovery
2024-08-24 15:00	Lessons Learned meeting conducted.	Post-Incident

3. Mitigation Steps & Recommendations

Immediate Mitigation Steps Taken:

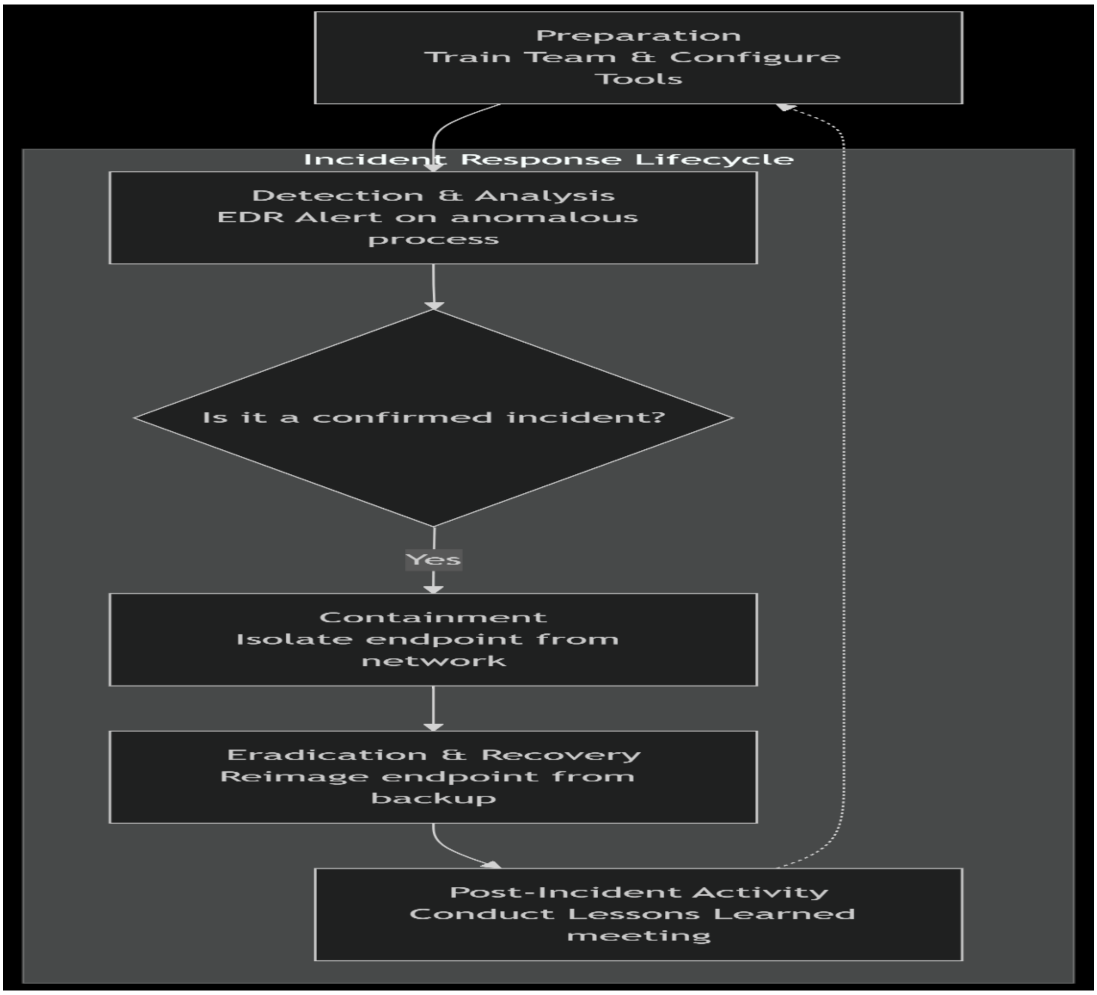
1. **Containment:** The affected VM was immediately isolated from the network via a firewall rule on the hypervisor to prevent any potential lateral movement.
2. **Eradication:** The VM was powered down and reimaged from a clean snapshot to ensure complete removal of the simulated threat actor's artifacts.
3. **Recovery:** After reimaging, the VM was re-deployed and validated using Velociraptor to ensure no remnants of the incident remained.

Long-Term Recommendations:

1. **User Training:** Implement mandatory annual security awareness training with a focus on identifying phishing attempts and reporting suspicious emails.
2. **Technical Controls:** Enable hardware-level application whitelisting (e.g., Windows AppLocker) to prevent execution of unauthorized scripts from user directories.
3. **Process Improvement:** Integrate Velociraptor alerts with a SIEM (e.g., Elastic Security) to automate alerting and ticketing for faster response times.

4. Incident Response Process Flowchart

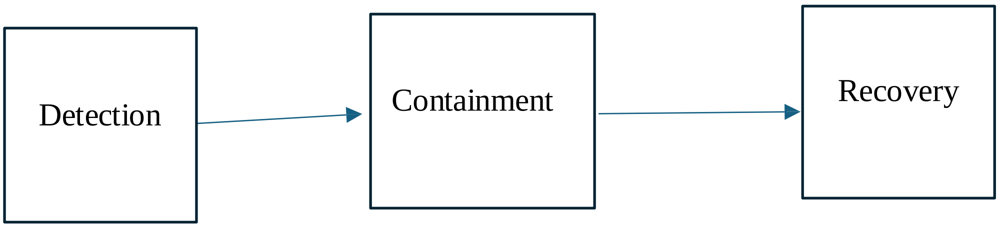
The following diagram outlines the key stages of the incident response process followed during this simulation, based on the NIST framework.


Preparation
Train Team & Configure Tools
Incident Response Lifecycle
Detection & Analysis
EDR Alert on anomalous process
Is it a confirmed incident?
Yes
Containment
Isolate endpoint from network
Eradication & Recovery
Reimage endpoint from backup
Post-Incident Activity
Conduct Lessons Learned meeting

Flowchart Explanation:

- **Preparation:** The cycle begins with preparing tools (Velociraptor, Caldera) and the team.
- **Detection & Analysis:** The simulated attack is detected by an EDR alert and analyzed to confirm the incident.
- **Containment:** The immediate action is to contain the threat, in this case, by isolating the VM.
- **Eradication & Recovery:** The root cause (the malicious script) is removed by wiping and reimaging the system, which is then returned to service.
- **Post-Incident Activity:** The loop is closed by discussing lessons learned, which feeds back into the **Preparation** phase to improve future response efforts. This creates a continuous improvement cycle.

- **Flowchart Creation:** Diagram of the incident response process (Detection → Containment → Recovery**).**


Detection
Containment
Recovery