🎯 Incident Response Plan: Phishing Attack Scenario

🔍 1. Detection Method

Tool: SIEM (e.g., Splunk, QRadar)
Method:

- Monitor for unusual login behavior (e.g., logins from unfamiliar IPs or geolocations).
- Trigger alert when an email contains known Indicators of Compromise (IOCs), such as:
    - Blacklisted URLs or domains
    - Executable attachments
    - Suspicious subject lines

Why it matters: Early detection is critical to prevent the attacker from harvesting credentials or launching further attacks inside the network.

🔒 2. Containment Strategy

Tool: Endpoint Detection & Response (EDR) system (e.g., CrowdStrike, SentinelOne)
Actions:

- Immediately **isolate the affected endpoint** to prevent lateral movement or data exfiltration.
- Block the phishing domain or sender at the email gateway.
- Disable compromised user account credentials in Active Directory.

Why it matters: Fast containment limits the blast radius of the phishing attack and protects other users.

🧹 3. Eradication & Recovery

Steps:

- Perform a full malware scan on the infected system.
- Remove any malicious files, links, or backdoors installed via the phishing payload.
- Patch any identified vulnerabilities used in the attack.
- Reimage the system if necessary.
- Re-enable user account with new credentials.

Recovery Verification:

- Validate that the system is clean and operating normally.
- Monitor account activity for abnormalities for at least 72 hours post-recovery.

☠️ 4. Type of Cyber Attack: Phishing

Definition:
Phishing is a **social engineering attack** where attackers impersonate legitimate sources to trick users into clicking malicious links or revealing sensitive credentials.

Why It's Dangerous:

- Often used as an entry point for more serious attacks like **ransomware** or **credential theft**.
- Can bypass traditional firewalls and anti-virus via user interaction.

Example Scenario:

> An employee receives an email that appears to be from IT requesting a password reset. The link leads to a spoofed login page designed to capture credentials.

Comprehensive Security Policy – SOC Environment

1. 🔐 Key Security Rules & Guidelines

a. User Access Control

- All users must use Multi-Factor Authentication (MFA) to access internal systems.
- Access is granted based on the principle of **least privilege**—users only receive the access necessary for their roles.
- Access reviews will be conducted quarterly.

b. Acceptable Use Policy (AUP)

- Employees may not install unauthorized software or access personal email/social media on corporate devices.
- Any use of removable media (USB, external drives) must be approved and scanned for malware.

c. Data Handling & Encryption

- All sensitive data must be **encrypted at rest and in transit** using AES-256 or equivalent.
- Public sharing of internal files or screenshots is prohibited without security team approval.

---

2. 🚨 Incident Response Plan (Phishing Attack Example)

Step 1: Detection

- Monitor through SIEM (e.g., QRadar) for suspicious email traffic or login behavior.
- Validate alert via user report or IOC match.

Step 2: Containment

- Isolate compromised workstation using EDR.
- Disable the affected user account temporarily.

- Block phishing domain and URLs at the firewall and email gateway.

Step 3: Eradication

- Scan and remove malicious payloads.
- Reimage the device if tampering is confirmed.
- Reset user credentials and force password changes for impacted accounts.

Step 4: Recovery

- Reconnect the clean device to the network.
- Restore affected services from backups if needed.
- Resume normal activity after full verification.

Step 5: Post-Incident

- Conduct root cause analysis (RCA).
- Update detection rules.
- Provide phishing awareness training to users.

---

3. 🧠 CIA Triad Integration

CIA Component	How This Policy Supports It
Confidentiality	Enforced access control, data encryption, and limited sharing of sensitive info.
Integrity	Incident response ensures compromised systems are cleaned and restored properly.
Availability	Containment and recovery steps ensure minimal downtime and quick restoration.

1. AES Encryption (Symmetric Encryption)

Encryption Process:

- **AES** (Advanced Encryption Standard) is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption.
- AES typically works with key sizes of 128, 192, or 256 bits.

Example:

- **Plain Text**: "Confidential data"
- **Key**: "thisisaverysecurekey1234"

Encrypted Text (Ciphertext):

- This would be generated through AES encryption, and you'll see a random-looking ciphertext after applying the algorithm.

Decryption Process:

- To decrypt the ciphertext, the same key must be used to return the original plaintext.

---

2. SHA-256 Hashing (One-Way Function)

Hashing Process:

- **SHA-256** is a hashing algorithm that produces a fixed-size (256-bit) output, known as a **digest**, no matter the input size.
- Hashing is **one-way**: Once the data is hashed, it cannot be decrypted back to the original input. It's primarily used for data integrity checks and password storage.

Example:

- **Plain Text**: "MySecurePassword"

- **SHA-256 Hash**: After hashing, you'll get a fixed-length output, which will look like a random string of characters.

🔐 Encryption and Hashing Example

1. AES Encryption and Decryption Example

- **Plain Text**: "Confidential data"
- **Key**: "thisisaverysecurekey1234"

Encrypted (Ciphertext):

plaintext
CopyEdit
`1a3b4d6e7f8d9b0a1c2e3f4a5d6b7c8d`

Decrypted (Plaintext): "Confidential data"

> **Note**: The encryption and decryption process works using the AES algorithm with the correct key. In a real-world application, tools like OpenSSL or cryptographic libraries in programming languages (e.g., PyCryptodome for Python) can be used to perform AES encryption.

2. SHA-256 Hashing Example

- **Plain Text**: "MySecurePassword"

SHA-256 Hash:

plaintext
CopyEdit
`9d5ed678fe57bcca4bf8c0f2c8e8b29b3a5e3fcfc4fe6ab6b8b51bc33a17f7c7`

> **Note**: You cannot reverse the hash back into the original text, as hashing is one-way.

🔑 Code Example (Python)

python
CopyEdit

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
import hashlib
import binascii

# AES Encryption/Decryption Example
key = b'thisisaverysecurekey1234'  # 32-byte key for AES-256
data = b'Confidential data'

# Encrypt data
cipher = AES.new(key, AES.MODE_CBC)
ciphertext = cipher.encrypt(pad(data, AES.block_size))

# Decrypt data
decipher = AES.new(key, AES.MODE_CBC, cipher.iv)
plaintext = unpad(decipher.decrypt(ciphertext), AES.block_size)

# SHA-256 Hash Example
hash_object = hashlib.sha256(b'MySecurePassword')
hashed_password = hash_object.hexdigest()

# Output
print(f"Encrypted: {binascii.hexlify(ciphertext)}")
print(f"Decrypted: {plaintext.decode()}")
print(f"SHA-256 Hash: {hashed_password}")
```

This code will encrypt and decrypt the data with AES and generate a SHA-256 hash for the password.

AES Encryption:

- Encrypts sensitive data and is reversible with the same key.

SHA-256 Hashing:

- Creates a unique, fixed-size output for data integrity and password storage, irreversible.

🚨 Legal and Ethical Compliance in Incident Response

1. Relevant Laws and Regulations

In cybersecurity, adherence to legal frameworks and ethical standards is critical for effective incident management and for protecting both the organization and its stakeholders. Below are two key regulations:

a. General Data Protection Regulation (GDPR) - EU

- **Overview**: GDPR mandates strict data protection and privacy requirements for organizations that handle personal data of EU citizens.

- **Relevance to Incident Response**:

    - **Data Breach Notification**: Under GDPR, organizations are required to notify affected individuals and supervisory authorities within 72 hours of discovering a data breach involving personal data.

    - **Data Protection Impact Assessment (DPIA)**: A DPIA must be conducted if the breach could lead to high risks for individuals' rights and freedoms (e.g., identity theft).

b. Health Insurance Portability and Accountability Act (HIPAA) - US

- **Overview**: HIPAA is a U.S. law that sets national standards for the protection of health information.

- **Relevance to Incident Response**:

    - **Breach Notification**: HIPAA requires covered entities and their business associates to notify affected individuals of a data breach involving Protected Health Information (PHI).

    - **Risk Analysis and Mitigation**: Organizations must conduct risk analyses to assess potential vulnerabilities and ensure PHI remains secure, even during a

breach.

---

2. Ethical Consideration

Privacy and Confidentiality

- **Overview**: Maintaining the privacy and confidentiality of individuals' personal data is a core ethical principle in cybersecurity.

- **Ethical Challenge**: During an incident response, cybersecurity teams often have access to sensitive personal data or organizational secrets. It's essential to handle this information ethically, ensuring it is only accessed by authorized personnel and is protected from unnecessary exposure.

Ethical Dilemma:

- **Balancing Transparency vs. Protection**: In some cases, an organization might face a dilemma between disclosing certain breach details to the public (or customers) and protecting sensitive internal data or exposing further vulnerabilities.

---

3. How the Incident Response Plan Upholds Legal Requirements and Ethical Principles

a. Legal Compliance:

- **GDPR Compliance**: The plan includes **immediate notification** protocols that ensure affected users and authorities are informed within the mandated 72 hours. It also includes procedures for data retention and deletion in line with GDPR's "right to be forgotten" clause.

- **HIPAA Compliance**: The plan includes **protected health information (PHI)** handling guidelines, ensuring that data involved in breaches is documented, and individuals' privacy is safeguarded.

b. Ethical Compliance:

- **Confidentiality of Sensitive Data**: The plan emphasizes that any sensitive data uncovered during incident response (including PHI or financial data) is protected, stored securely, and disclosed only to the minimum necessary parties (e.g., regulatory authorities).

- **Transparency with Affected Parties**: The plan promotes **ethical transparency**, meaning stakeholders, employees, and affected customers are informed honestly and promptly without compromising the investigation's integrity.

---

4. Integration of Legal & Ethical Considerations in the IRP

The Incident Response Plan incorporates both **legal** and **ethical** standards at every stage:

- **Detection**: Logs and alerts are processed in a way that respects privacy and is compliant with data protection laws.

- **Containment**: Ensuring that the isolation of affected systems does not unnecessarily expose or leak sensitive data.

- **Eradication and Recovery**: Eradication procedures comply with legal data destruction requirements and avoid unnecessary retention of sensitive data.

- **Post-Incident**: Ethical reviews are performed to ensure that the organization has acted transparently and communicated appropriately with affected individuals.

Example Table for Your Plan:

Section	Legal Consideration	Ethical Consideration
Detection	GDPR breach detection requirements	Minimize collection of unnecessary personal data
Containment	Ensure compliance with data protection laws	Protect confidentiality of sensitive data during response
Eradication	Follow legal retention and destruction policies	Ensure minimal impact on stakeholders' privacy
Recovery	Notify authorities as required by GDPR/HIPAA	Maintain transparency and honesty with affected parties

Post-Incident	Conduct a data breach impact assessment	Apply lessons learned to improve security measures ethically