

## Solution for Unauthorized Login Attempts and Security Breach:

### Step 1: Confirm Unauthorized Login Attempts

Verify the detection of multiple unauthorized login attempts, indicating a potential security breach.

### Step 2: Activate Security Response Team

Immediately activate the security response team to lead the investigation and coordinate security measures.

### Step 3: Assess Breach Impact

Assess the potential impact of the security breach, including identifying compromised accounts and data exposure.

### Step 4: Investigate the Source

Conduct a thorough investigation to identify the source and method of the unauthorized login attempts.

### Step 5: Block Unauthorized Access

Take immediate action to block and restrict access for any unauthorized users or compromised accounts.

### Step 6: Change Passwords

Mandate password changes for affected accounts and implement strong password policies.

#### Step 7: Enhance Security Measures

Implement security enhancements such as multi-factor authentication (MFA), intrusion detection, and log monitoring.

#### Step 8: Communicate with Stakeholders

Maintain open communication with stakeholders, including employees, to provide updates on the security breach resolution.

#### Step 9: Conduct Security Training

Provide security awareness training to employees to prevent future security breaches and unauthorized login attempts.

#### Step 10: Document the Response

Document the details of the security breach response, actions taken, security enhancements, and preventive measures.