Theoretical Knowledge

Alert Priority Levels

Priority definition :

1. **Critical**

Meaning : immediate, confirmed threat with major impact
Impact : data breach, ransomware, domain compromise
Urgency : active exploitation / ongoing attack
Examples :

- Ransomware encrypting production servers
- Log4Shell (CVE-2021-44228) exploited on internet-facing server
- Unauthorized domain admin log

SOC action :

- Isolate systems
- Block attacker IPs
- Escalate to IR team
- Management notification

2. **High**

Meaning : serious threat, likely to cause major damage if not handled fast
Impact : privilege escalation,lateral movement
Urgency : high likelihood of exploitation
Examples :

- Brute-force success on admin account
- Known CVE with public exploit on production server

SOC action :

- Contain host
- Reset credentials
- Patch vulnerable services

3. **Medium**

Meaning : suspicious activity, potential threat
Impact : limited or indirect
Urgency : needs investigation
Examples :

- Multiple failed login attempts
- Suspicious PowerShell command
- Outdated vulnerable service on test VM

SOC action :

- Analyze logs
- Correlate with other alerts
- Monitor user behavior

4. **Low**

Meaning : informational or low-risk
Impact : minimal
Urgency : no immediate action
Examples :

- Port scan from external IP
- Single failed login

SOC action :

- Tune alerts
- Add to threat intel watchlist

How SOC assigns priority

SOC doesn't rely only on CVSS. It combines three factors :

1. **Asset criticality**

ASSET	PRIORITY IMPACT
Production DB server	High
Employee laptop	Medium
Test VM	Low

2. **Exploit likelihood**

SITUATION	RISK
Public exploit available	High
PoC exists	Medium
No exploit known	Low

3. **Business impact**

IMPACT	PRIORITY
Financial loss	Critical
Compliance violation	High
Minor outage	Medium

CVSS → SOC priority mapping

CVSS SCORE	SOC PRIORITY
9.0 - 10.0	Critical
7.0 - 8.9	High
4.0 - 6.9	Medium
0.1 - 3.9	Low

Example :
Log4Shell (CVSS 9.4) on internet-facing Apache → critical
Same CVE on internet test VM → high / medium

Incident classification

Core concepts

Incident categories :

Be able to quickly label what kind of incident it is

- Malware : ransomware, trojans, spyware
- Phishing : credential harvesting, malicious links
- DDoS : service disruption via traffic floods
- Insider threat : employee leaking data
- Data exfiltration : unauthorized data transfer
- Web attacks : SQLi, XSS, brute-force

Taxonomy

Mapping every incident to a framework :
MITRE ATT&CK
Use it to describe how the attack happened :
Phishing → T1566
Credential dumping → T1003
Brute force → T1110
Exfiltration over web → T1041

ENISA incident taxonomy (high level categories) used in EU SOCs & reporting :

- Malicious codes
- Information security
- Availability attacks
- Human errors

VERIS framework (for structured reporting) breaks incident into :
Actor → external, internal
Action → malware, hacking, social
Asset → server, database
Attribute → confidentiality, integrity, availability

Contextual metadata
Every incident report should include :

- Timestamp : when detected
- Affected asset : hostname, IP
- Source IP
- User account
- IOCs
- Log source

Example :
Time : 2026-02-11 10:45
Source IP : 185.222.0.0
Target : HR-PC-01
IOC : malicious.exe
MITRE : T1566(phishing)

Basic incident response

Incident response lifecycle (IR phases)

1. **Preparation**
   Create :
   - IR playbooks(phishing, malware, ransomware, data breach)
   - Asset inventory, critical systems list

   Setup :
   - SIEM
   - Logging, backups, EDR

2. **Identification**
   Detect and confirm incident
   Sources :
   - SIEM alerts
   - IDS/IPS
   - EDR alerts
   - User reports

3. **Containment**
   Stop the spread

Actions :
- Isolate infected VM
- Block IP in firewall
- Disable compromised user account

Types :
- Short-term : unplug network, kill malicious process
- Long-term : patch systems, change credentials

4. **Eradication**
   Remove root cause
   Actions :
- Delete malware
- Patch vulnerability
- Remove persistence

5. **Recovery**
   Bring systems back safely
   Actions :
- Restore from clean backup
- Monitor for re-infection
- Re-enable services

6. **Lessons learned**
   Post-incident review
   Ask :
- What went wrong?
- How can detection be faster?
- What control failed?

Output :
- Updated playbooks
- New detection rules

Key procedures
System isolation :
- Disconnect network
- Quarantine host in EDR
- Snapshot VM

SOAR (Security Orchestration, Automation & Response)
Purpose :
Automate repetitive response actions

Example tools :

- Splunk Phantom
- Cortex XSOAR
- Shuffle

Example SOAR workflow :

1. SIEM detects phishing email
2. SOAR :
    - Extracts URL
    - Checks VirusTotal
    - Blocks domain
    - Disables user account
    - Opens ticket in jira

Practical application

Alert management practice

Alert classification system :

	A	B	C	D	E	F
1	**Alert ID**	**Alert Name**	**Type**	**Priority**	**MITRE Tactic**	**MITRE Technique**
2	1	Phishing email-suspicious link	Phishing	High	Initial access	T1566
3	2	Log4Shell exploit attempt	Exploit	Critical	Initial access	T1190
4	3	Port scan detected	Recon	Low	Reconnaissance	T1046
5	4	Brute force login attempt	Auth abuse	Medium	Credential access	T1110

Mock alert scan :
Alert : phishing email : suspicious link
Map it as :

- Priority : high
- MITRE T1566 - phishing

Prioritize alerts using CVSS

	A	B	C
1	**Alert**	**CVSS Score**	**Severity**
2	Log4Shell exploit detected	9.8	Critical
3	Port scan detected	3.5	Low

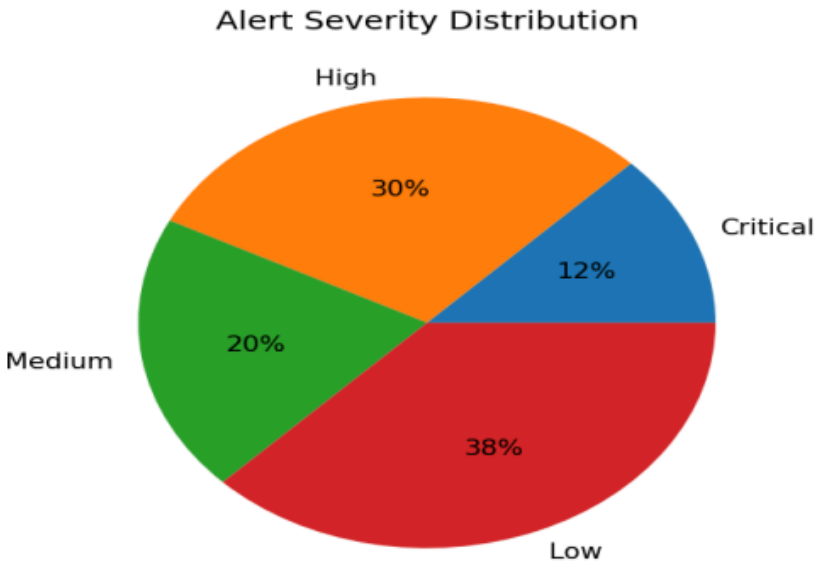
Severity mapping formula :
=IF(B2>=9,"critical",IF(B2>=7,"high",IF(B2>=4,"medium","low")))
Scoring :

- Log4Shell(CVSS 9.8) → critical
- Port Scan (CVSS 3.5) → low

Install wazuh dashboard
Quick install :
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a

To access dashboard :
https://<WAZUH-IP>

Create visualization
Type : pie chart
Visualization for SOC monitoring



Create incident ticket in TheHive
Install TheHive
docker run -d –name thehive -p 9000:9000 strangebee/thehive

Create incident case :
Title :
[critical] Ransomware Detected

Description :
Ransomware activity observed on Server-X. File encryption behavior detected.

Indicators (IOCs):
File: crypto_locker.exe
IP: 10.209.123.199
Priority: Critical
Assignee: SOC Analyst

Add Tasks:
Isolate host
Block IP
Collect memory dump
Notify IT team

Escalation role play (email)

Hi Tier 2 Team,

We detected a Critical ransomware incident on Server-X. Wazuh generated multiple alerts indicating suspicious process execution and file encryption behavior. The primary indicators of compromise include the file crypto_locker.exe and outbound connections to 10.209.123.199. The affected server has been isolated from the network to prevent further spread. Initial triage is in progress, and logs have been preserved. We need your support for deeper forensic analysis, confirmation of lateral movement, and guidance on eradication and recovery steps. Business impact may be high due to potential service disruption.

Regards,
SOC Analyst

Response documentation

Incident Response Report – Phishing (Mock)

Incident ID: IR-2025-001
Date: 18 Aug 2025
Reported By: SOC Analyst
Severity: High
Status: Closed

1. Executive Summary

On 18 Aug 2025, a phishing email impersonating the IT helpdesk targeted multiple employees. One user clicked the malicious link and entered credentials. The SOC detected suspicious login activity via SIEM alerts. The affected endpoint was isolated, credentials were reset, and no lateral movement was detected.

2. Timeline

Time (IST)	Event
14:00	Phishing email detected by SOC
14:05	User reported suspicious email
14:10	Endpoint isolated from network
14:30	Memory dump and disk image collected
15:00	Password reset enforced
16:00	IOC blocking on firewall & email gateway

3. Impact Analysis

Affected Users: 1
Systems Impacted: Employee workstation
Data Exposure: Credentials potentially compromised
Business Impact: Low (no data exfiltration confirmed)
MITRE ATT&CK:
T1566 – Phishing
T1078 – Valid Accounts (attempted)

4. Remediation Steps

- Isolated infected endpoint from network
- Forced password reset and MFA re-enrollment

- Blocked phishing domain and IPs
- Email gateway rule updated
- User awareness notification sent to all staff

5. Lessons Learned

- Improve phishing detection rules
- Enforce mandatory phishing awareness training
- Implement URL rewriting and sandboxing
- Reduce SOC response time with automated playbooks

Investigation Steps Log (Action Log Table)

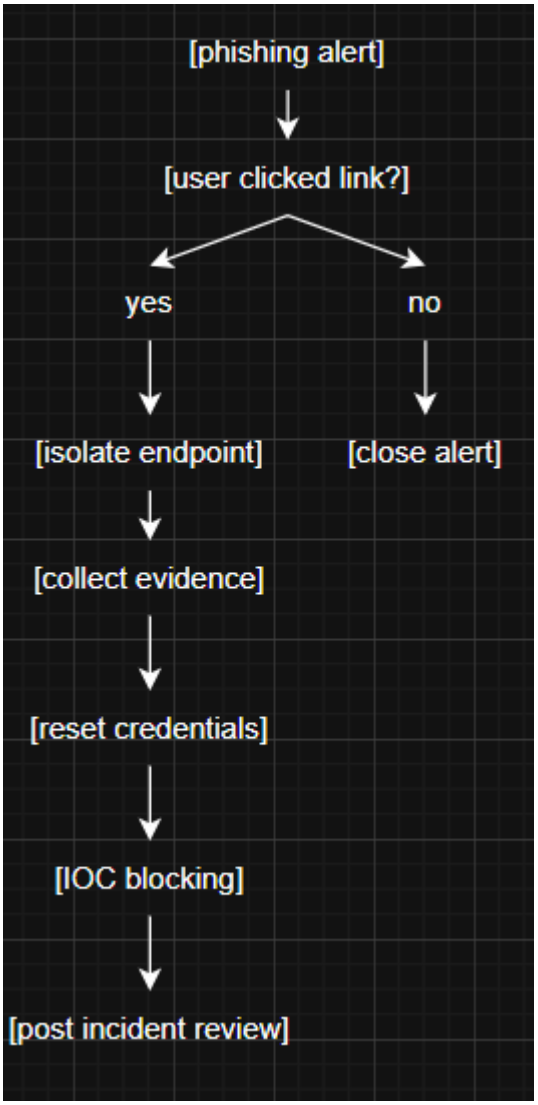
Timestamp (IST)	Action Taken
2025-08-18 14:00:00	Isolated endpoint from network
2025-08-18 14:30:00	Collected memory dump
2025-08-18 14:45:00	Acquired disk image
2025-08-18 15:00:00	Reset user credentials
2025-08-18 15:20:00	Blocked IOC on firewall
2025-08-18 16:00:00	Updated email filtering rules

Phishing Incident Checklist

Phishing Response Checklist

[ ] Validate email headers (SPF, DKIM, DMARC)
[ ] Check sender domain reputation
[ ] Analyze URL in VirusTotal
[ ] Check attachment hash in VirusTotal
[ ] Identify affected users
[ ] Search SIEM for similar emails
[ ] Isolate impacted endpoints
[ ] Reset compromised credentials
[ ] Block malicious domain/IP
[ ] Notify IT and Security teams
[ ] Document incident in ticketing system
[ ] Conduct user awareness follow-up

Investigation Flow Diagram



Mock Post-Mortem

The incident revealed delays in phishing triage and user reporting. Improvements include automating phishing alert prioritization, strengthening email gateway filtering, enforcing mandatory security awareness training, and implementing SOAR playbooks to reduce response time. Regular tabletop exercises will enhance cross-team coordination and response maturity.

Alert triage practice

Objective

Simulate alert triage using Wazuh SIEM and validate indicators of compromise (IOCs) using VirusTotal and AlienVault OTX. The goal is to classify alerts, reduce false positives, assign priority, and document actions per SOC standards.

Tool setup

Install & Access Wazuh Dashboard

On Ubuntu Server (example):

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a

Access Dashboard:

URL: https://<Wazuh-IP>

Create Wazuh SSH Brute Force Alert

Enable SSH log monitoring:

sudo nano /var/ossec/etc/ossec.conf

Ensure:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

Restart:

sudo systemctl restart wazuh-manager

Simulate brute-force:

for i in {1..5}; do ssh wronguser@localhost; done

Alert Triage Workflow

Step 1: Alert Review (Wazuh)

Check:

- Alert description
- Rule ID
- Frequency
- Source IP
- Target host

Step 2: Classify Alert

Category : Brute-force

MITRE ATT&CK:

T1110 – Brute Force

Tactic : Credential Access

Step 3: False Positive Check

Verify:

- Is source IP internal?
- Is the user a real user?
- Is this repeated login from admin activity?
- Check time pattern (automated vs manual)

Alert Documentation

ALERT ID	DESCRIPTION	SOURCE IP	PRIORITY	STATUS
002	Brute-force SSH	10.0.2.15	Medium	Open

Priority Justification:

- Medium because : Multiple failed attempts
- No successful login
- Internal IP (less severe than external attacker)

Threat Intel Summary

The source IP was searched in AlienVault OTX and VirusTotal. No malicious pulses or threat intelligence associations were found for the IP address. This suggests the activity is likely internal misconfiguration or a user authentication issue rather than an external attack. The alert is classified as a potential false positive pending further monitoring.

Evidence preservation

Objective:

Practice digital evidence preservation using Velociraptor and FTK Imager, collect volatile and non-volatile evidence from a Windows VM, generate cryptographic hashes, and document chain of custody according to DFIR best practices.

Environment Setup

Lab Environment:

- Attacker/Analyst VM: Kali Linux or Ubuntu
- Target VM: Windows 10/11

Tools:

- Velociraptor (Server + Windows Agent)
- FTK Imager
- sha256sum (Linux)

Volatile Data Collection (Velociraptor – Network Connections)

Step 1: Deploy Velociraptor Agent on Windows VM

On Velociraptor Server:
Create Windows client installer
Install agent on Windows VM

Step 2: Run Netstat Artifact

In Velociraptor Web UI:
Artifact: Windows.Network.Netstat
Or Custom Query:
SELECT * FROM netstat()

Step 3: Export Results to CSV

In Velociraptor:
Click Results → Export → CSV

Step 4: Preserve Evidence

Move file to evidence folder

Memory Dump Collection (Velociraptor)

Acquire Memory
Run Artifact:
SELECT * FROM Artifact.Windows.Memory.Acquisition

Hashing the Memory Dump (Integrity Verification)

On Kali / Linux:
cd /evidence/case-001/memory
sha256sum ServerX_memory_2025-08-18.raw >
ServerX_memory_2025-08-18.sha256

Chain of Custody Documentation

	A	B	C	D	E
1	**Item**	**Description**	**Collected by**	**Date**	**Hash value(SHA256)**
2	memory dump	RAM dump	SOC analyst	2025-08-18	d41d8cd98f00b204e9800998ecf8427e
3	netstat CSV	network connections	SOC analyst	2025-08-18	9a0364b9e99bb480dd25e1f0284c8555
4	disk image	disk image	SOC analyst	2025-08-18	e3b0c44298fc1c149afbf4c8996fb924
5					

Capstone project

Lab setup

COMPONENT	PURPOSE
Kali linux	Attacker (metasploit)
Metasploitable2	Vulnerable target
Wazuh manager	Detection and alerts
CrowdSec	IP blocking
Google docs	Reporting

Attack simulation

Exploit : VSFTPD Backdoor
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 10.0.2.15
set RPORT 21
run

Detection and triage

FTP exploit detection
On wazuh manager :

```
<rule id="100200" level="10">
  <if_matched_sid>5715</if_matched_sid>
  <description>VSFTPD Backdoor Exploit Attempt</description>
  <mitre>T1190</mitre></rule>
```

Alert triage documentation :

TIMESTAMP	SOURCE IP	ALERT DESCRIPTION	MITRE TECHNIQUE
2025-08-18 11:00:00	10.209.123.199	VSFTPD exploit detected	T1190

Response actions
Isolate metasploitable2 VM :
Shut down network :
Ifconfig eth0 down

Block attacker IP(CrowdSec) :
Sudo cscli decisions add –ip 10.0.2.15 –reason “FTP exploitation attempt”

Evidence collection

EVIDENCE	COMMAND
FTP logs	/var/log/vsftpd.log
Wazuh alerts	Wazuh dashboard
Network capture	tcpdump -i eth0 port 21

Final incident report
Executive Summary
On 18 August 2025, a simulated exploitation of a vulnerable FTP service was detected on a test environment using Wazuh. The attacker leveraged a known VSFTPD backdoor vulnerability to gain unauthorized access to a vulnerable host. The activity was identified as a remote exploitation attempt and classified under MITRE ATT&CK technique T1190 (Exploitation for Initial Access).

Timeline
At 11:00 AM, Wazuh generated a high-severity alert indicating suspicious FTP activity from IP address 10.0.2.15 targeting the Metasploitable2 virtual machine. The SOC analyst validated the alert, confirmed unauthorized access through Metasploit logs, and initiated containment procedures. By 11:05 AM, the compromised system was isolated from the network and the attacker IP was blocked using CrowdSec. Normal operations were restored after validation.

Recommendations
All exposed FTP services should be patched or decommissioned. Vulnerability scanning should be conducted regularly. Network intrusion detection rules must be updated to detect known exploitation patterns. Security awareness training and continuous monitoring should be enforced to minimize exposure to similar attacks.