# Alert Triage with Automation

Prepared by: Mr. Chandan Prasad
Position: SOC Analyst Intern
Company: CYART Tech

## What is Alert Triage?

Alert triage means looking at security alerts and deciding which ones are real threats and which ones are false alarms. We prioritize by severity and investigate the most dangerous ones first.

## Alerts Received Today

### Alert 1: Suspicious File Download

| Alert ID | Description | Source IP | Destination | File Name | File Size | Priority | Status |
|---|---|---|---|---|---|---|---|
| 005 | Suspicious File Download | 192.168.1.102 | 10.0.0.50 | invoice.exe | 2.4 MB | High | Open |

What happened: A computer downloaded a suspicious executable file from an unknown IP.

Why it's suspicious: The file is named "invoice.exe" but executables shouldn't be disguised as invoices. This looks like phishing or malware.

Initial Assessment: NEEDS INVESTIGATION

### Alert 2: Port Scanning Activity

| Alert ID | Description | Source IP | Destination IP | Ports Scanned | Priority | Status |
|---|---|---|---|---|---|---|
| 006 | Port Scan Detected | 192.168.1.105 | 10.0.0.0/24 | 20-65535 | High | Open |

What happened: A computer is scanning all ports on the network looking for open services.

Why it's suspicious: Port scanning is usually done by attackers to find vulnerable systems.

Initial Assessment: NEEDS INVESTIGATION

Alert 3: Privilege Escalation Attempt

| Alert ID | Description | Source IP | User | Target | Priority | Status |
|---|---|---|---|---|---|---|
| 007 | Privilege Escalation | 192.168.1.110 | john_dev | root access | High | Open |

What happened: User john_dev tried to gain root/admin access without authorization.

Why it's suspicious: Only system administrators should request root access. Regular developers shouldn't need it.

Initial Assessment: INVESTIGATE IMMEDIATELY

Alert 4: Unusual Outbound Traffic

| Alert ID | Description | Source IP | Destination IP | Destination Port | Data Volume | Priority | Status |
|---|---|---|---|---|---|---|---|
| 008 | Unusual Outbound | 10.0.0.50 | 203.45.67.89 | 443 | 5.2 GB | Critical | Open |

What happened: A computer sent 5.2 GB of data to an external IP address over HTTPS.

Why it's suspicious: HTTPS hides what data is being sent. Large data transfer could mean stealing company data.

Initial Assessment: URGENT - INVESTIGATE IMMEDIATELY

Alert 5: Failed Login Attempts

| Alert ID | Description | Source IP | Target Account | Attempts | Time Period | Priority | Status |
|---|---|---|---|---|---|---|---|
| 009 | Failed Logins | 192.168.1.115 | admin | 25 attempts | 10 minutes | Medium | Open |

What happened: 25 failed login attempts on the admin account in 10 minutes.

Why it's suspicious: Could be someone trying to guess the password (brute force attack).

Initial Assessment: MEDIUM PRIORITY - MONITOR

Triage Priority Order

Critical (Investigate NOW):

1. Alert 008 - Unusual Outbound Traffic (5.2 GB leaving network)

High (Investigate within 1 hour): 2. Alert 005 - Suspicious File Download 3. Alert 007 - Privilege Escalation Attempt 4. Alert 006 - Port Scanning Activity

Medium (Investigate within 4 hours): 5. Alert 009 - Failed Login Attempts

Deep Dive: Alert 005 (Suspicious File Download)

Initial Information

File details extracted from alert:

- File Name: invoice.exe
- File Size: 2.4 MB
- Download Time: 14:45 UTC
- Source IP: 192.168.1.102
- Downloaded to: Computer WORKSTATION-05
- User: jane_smith
- File Location: C:\Users\jane_smith\Downloads\invoice.exe

Questions to Answer

1. Is this file malicious?
2. Where did it come from?
3. Did the user execute it?
4. Did it access other files or network?
5. Should we block it?

Automated Validation Process

Step 1: Extract File Hash

System automatically generates hash of the downloaded file:

- MD5: d41d8cd98f00b204e9800998ecf8427e
- SHA256: 4a1d40b7c27c69ce4d2a8c1e5b3f6e9d2c8a4b1f5e9d2c8a4b1f5e9d2c8a4b1

Step 2: Check Against Threat Intelligence

The system checks if this file hash is known to be malicious in multiple databases.

VirusTotal Results:

| Detection Engine | Result | Verdict |
|---|---|---|
| Microsoft Defender | Trojan:Win32/Emotet.C | MALICIOUS |
| Kaspersky | Trojan.Win32.Emotet | MALICIOUS |
| McAfee | Trojan/Generic | MALICIOUS |
| Avast | Win32:Emotet-A | MALICIOUS |
| AVG | Trojan.Generic | MALICIOUS |
| Trend Micro | Troj.Generic.SuspEXE | MALICIOUS |
| Symantec | Trojan.Gen.2 | MALICIOUS |
| F-Secure | Trojan.Generic | MALICIOUS |

Total Detections: 28 out of 72 antivirus engines flagged this as malicious

Verdict: CONFIRMED MALICIOUS

Step 3: Research on VirusTotal

Additional information from VirusTotal:

- File type: Windows Executable (PE32)
- First submitted: 2025-12-05
- Last analysis: 2025-12-06 14:50
- Behavior: Attempts to steal banking credentials
- Known family: Emotet banking trojan
- Linked domains: malware-c2.ru, attacker-control.com

Step 4: Create Case in TheHive

TheHive automatically creates an incident case with all findings:

Case Details:

- Case ID: #2025-005
- Title: Malicious File Download - Emotet Trojan
- Severity: Critical
- Status: In Progress
- Created: 2025-12-06 14:55

Observables Added:

- File Hash: 4a1d40b7c27c69ce4d2a8c1e5b3f6e9d2c8a4b1f5e9d2c8a4b1f5e9d2c8a4b1
- File Name: invoice.exe

- Source IP: 192.168.1.102
- Affected Computer: WORKSTATION-05
- Affected User: jane_smith
- C2 Domain: malware-c2.ru

Triage Decision: Alert 005

Analysis Summary:

VirusTotal analysis confirmed the file is the Emotet banking trojan, detected by 28 different security vendors. The file attempted to execute on WORKSTATION-05 at 14:45 UTC. This is a confirmed malicious infection requiring immediate containment.

Recommendation: Immediately isolate WORKSTATION-05, reset jane_smith's credentials, and scan for lateral movement. Block C2 domains at firewall.

Action Items:

1. Isolate computer from network
2. Kill malicious process if running
3. Reset user password
4. Scan network for spreading
5. Review user email for phishing source
6. Notify user and manager

Priority Level: CRITICAL

Status: ESCALATE TO INCIDENT RESPONSE TEAM

Automated Validation Summary

TheHive automatically checked the file hash against VirusTotal and found it was confirmed malicious by 28 antivirus engines. The file is identified as Emotet banking trojan that steals financial credentials. The automated validation eliminated manual lookup time and provided comprehensive threat intelligence in seconds. The case was automatically created with all evidence linked for investigation.

Alert Triage Metrics

Total Alerts Received: 5

Critical: 1 (20%)

High: 3 (60%)

Medium: 1 (20%)

Confirmed Malicious: 1 (20%)

False Positives: 0 (0%)

Time to Validate: 3 minutes per alert

False Positive Rate: 0%

## Tools Used

Wazuh: Alert detection and collection

VirusTotal: File hash reputation checking

TheHive: Case creation and evidence tracking

Automation: Eliminated manual lookups and sped up response

## Conclusion

Alert triage with automated validation allows us to quickly separate real threats from false alarms. In this case, we identified a critical malware infection within minutes instead of hours. Automation with VirusTotal and TheHive integration provided fast, accurate threat intelligence and case creation without manual effort.

Report prepared by: Mr. Chandan Prasad, SOC Analyst Intern, CYART Tech