SOC Incident Response – Week 4 Capstone

By: Mr. Chandan Prasad
Role: SOC Analyst Intern
Company: CYART Tech

What Happened

Today I detected and helped contain a security incident on the network. An employee received a phishing email with a malicious attachment. They opened it, and our detection systems caught it. I helped investigate and shut it down.

The Attack Timeline

Time	What Happened	Alert?
08:00	Phishing email sent	No
08:15	Employee opened attachment	No
08:25	Malware file executed	No
08:35	Wazuh detected suspicious process	YES ✓
08:45	I started investigating	Yes
09:00	Confirmed it was malware	Yes
09:15	Workstation isolated from network	Done
10:00	System cleaned and recovered	Done

Total time from detection to containment: About 1.5 hours

Alerts I Saw

When I checked the SOC dashboard, I saw these alerts:

Alert	Severity	What It Meant
Suspicious file download	High	EXE file in Downloads folder
Process execution from Downloads	High	File was trying to run
Child process cmd.exe	High	Malware spawning command prompt
Privilege escalation attempt	Critical	Trying to get admin rights

All 4 alerts pointed to the same attack. Good detection.

What I Did - Investigation

1. Looked at the alerts - Checked what Wazuh found
2. Checked the file hash - Used VirusTotal to verify it's malicious (confirmed Emotet trojan)
3. Checked network connections - Looked at netstat to see what the malware was trying to connect to
4. Documented the evidence - Saved file hashes and logs with timestamps
5. Reported to team - Told the SOC lead about the incident

Evidence Collected

Files I found and documented:

File	Hash (SHA256)	What It Is
netstat log	2A89028B4F8576845961D7B376C3CA361205B079C111822FC20FC6094B0229D7	Network connections
Process list	25BB6DC849B2F01C21EE209AD41649ED9BDB08CC62CBFAAFA371E011A623570D	Running processes
Event log	19622D96256A170085CACA800B3A63B8AAA9261FFCC7B9659626962CAADEB08F	System events

All hashes match original files. No tampering.

Root Cause - Why It Happened

Why was the malware executed?

- Employee opened email attachment

Why did they open it?

- Email looked like a legitimate invoice

Why wasn't it blocked?

- Email filtering didn't catch it because sender spoofed company domain

Why did spoofing work?

- Email authentication (SPF/DKIM) not properly configured

Real cause: Email security wasn't strong enough

What Went Right

- Detection system worked - caught it in 45 minutes
- Alerts were accurate - no false alarms
- Contained quickly - isolated workstation before damage
- No data was stolen

What Needs Fixing

1. Email authentication needs improvement
2. Users need phishing training
3. Detection could be faster (took 45 min, should be 30 min)
4. More network monitoring needed

What I Learned

- Real attacks happen in steps: email → download → execute → escalate
- Good alert rules catch multiple stages of attack
- Speed matters - faster containment = less damage
- Documentation is important for evidence

Recommendations

This week:

- Set up SPF/DKIM for email
- Send phishing training to staff

Next month:

- Add more detection rules
- Test our response procedures
- Review what happened

Timeline of My Investigation

Time	Action	Who
08:35	Alert received	Wazuh system
08:40	I read the alerts	Me (SOC Analyst)
08:45	Started investigation	Me

Time	Action	Who
09:00	Confirmed malware	Me + VirusTotal
09:15	Told team to isolate	Me
09:30	Workstation isolated	IT team
10:00	System verified clean	IT team

Quick Stats

- Detection Time: 45 minutes
- Response Time: 1.5 hours total
- Alerts Generated: 4 correct alerts
- False Alarms: 0 (all real)
- Data Loss: None
- Systems Affected: 1 workstation

Incident Status

CLOSED – Threat contained, system cleaned, investigation complete

---

Report by: Chandan Prasad, SOC Analyst Intern, CYART Tech