SOC Analyst Technical Assessment

Assignment Components

Part 1: SIEM Alert Analysis

Alert 1 :

Multiple failed login attempts to database server

1. True Positive
2. Brute Force Attack
3. Block the source IP (203.0.113.42) . Investigate if any login attempt was successful.
4. Priority : Critical

Alert 2 :

Troubleshoot an application (It help)

1. False Positive
2. User reported IT was helping him troubleshoot an application issue today
3. Host: WORKSTATION-FINANCE42
4. User: james.wilson
5. Priority : Low

Alert 3 :

Server used for software development and version control

1. False Positive
2. Priority : Low
3. still need to investigate

Alert 4 :

Malware Detection

1. True Positive
2. Phishing Email Attack
3. Check for any other files downloaded from the same sender. Alert the email security team to block emails from supplierxyz-invoices.com
4. Priority : High

Alert 5 :

Account lockout

1. False positive
2. Priority : Low
3. Device: Recognized device
4. User: admin.helpdesk

Part 2: Log Analysis and Threat Hunting

1. Identify suspicious patterns or anomalies

- Unusual RDP Activity :
- An external IP (198.51.100.73) connected via RDP to 10.10.15.25 multiple times
- A successful interactive login (Logon Type 10) by john.smith from this IP (198.51.100.73) . [2025-03-07 08:25:03 UTC, WORKSTATION-FINANCE10, Microsoft-Windows-Security-Auditing, 4624, Logon Type 10 (RemoteInteractive), Account: john.smith, Domain: CORP, Workstation: WORKSTATION-FINANCE10, Source IP: 198.51.100.73]
- Privilege Escalation:
- created a mimikatz.exe file to assign Special privileges (SeDebugPrivilege) assigned to jhon.smith account

```
2025-03-07 08:30:41 UTC, WORKSTATION-FINANCE10, Microsoft-Windows-Security-Auditing, 4688, Process Created, Process Name: mimikatz.exe, Creator Process ID: 4892, Creator Process Name: cmd.exe, Account: john.smith
```

- SeDebugPrivilege was assigned to john.smith, allowing him to manipulate system processes.

```
2025-03-07 08:32:15 UTC, WORKSTATION-FINANCE10, Microsoft-Windows-Security-Auditing, 4672, Special privileges assigned to new logon, Account: john.smith, Privileges: SeDebugPrivilege
```

- Checking the administrator:
- The attacker is checking if the Administrator account exists in the domain

```
2025-03-07 08:26:55 UTC, WORKSTATION-FINANCE10, Command Line Activity, cmd.exe /c net user administrator /domain
```

- The attacker is checking if they can access the /c admin share on 10.10.15.5.

```
2025-03-07 08:28:12 UTC, WORKSTATION-FINANCE10, Command Line Activity, cmd.exe /c dir \\10.10.15.5\c$
```

2. Correlate events across different log sources

1. Firewall Logs: An external remote access to 10.10.15.25 from 198.51.100.73.
2. Windows Logs: jhon.smith account compromised.
3. windows Logs: created a mimikatz.exe file to assign Special privileges (SeDebugPrivilege) assigned to jhon.smith account.
4. EDR logs : checking for administrator.
5. EDR Logs : Dumbing credentials.
6. Firewall Logs : Sharing files across the network (SMB).

3. Document a potential security incident based on your findings

Summary:

An external attacker (198.51.100.73) remotely connected to a corporate workstation (10.10.15.25) through RDP, authenticated as john.smith, and utilized Mimikatz to dump credentials. The attacker escalated privileges, laterally moved with PsExec, and possibly exfiltrated data through SMB and email.

Potential Impact:

Compromised credentials to privilege escalation.

Lateral movement on key systems.

Possible data exfiltration through SMB.

Recommended Immediate Actions:

Disable account of john.smith and force password reset.

Block external access from 198.51.100.73 at the firewall.

Check email logs for possible data exfiltration.

Perform a complete forensic analysis.

4. Outline the attack chain using MITRE ATT&CK framework

Stage	**What Happened**
Initial Access	Attacker logged in using stolen credentials via RDP.
Execution	Ran commands (cmd.exe, net.exe, mimikatz.exe).
Persistence	Installed a backdoor (persistance.dll).
Privilege Escalation	Used mimikatz.exe to steal admin credentials.
Defense Evasion	Deleted traces (net.exe process terminated).
Exfiltration	Possible data theft via email (SMTP traffic).

Part 3: Incident Response Scenario

1. Document your initial response steps

- Disconnect compromised servers and workstations from the network. Disable file transferring protocols like SMB.
- Determine how many systems are affected.
- Determine how it can affect the business.

2. Identify potential indicators of compromise (IOCs)

File-Based Indicators

- Extension : .locked.
- Malicious file : invoice_payment.pdf.exe.
- Payment : 5 Bitcoin

Network-Based Indicators

- URL : .onion
- Unusual SMB activity

Email-Based Indicators

- The phishing email sent to multiple accounting department employees.

Remediation Recommendations

- Isolate infected systems immediately.
- Update AV definitions and EDR rules.

3. Create a basic timeline of the attack

- 02:30 am : Phishing email received by accounting employees.
- 03:00 am : The malicious file executed on one workstation.
- 03:30 am : Malicious file spread across the network.
- 04:00 am : The files encrypted, ransom note displayed.
- 04:30 am : Employees report file access issues to IT helpdesk.

4. Recommend containment and remediation actions

- Disable compromised admin accounts.
- Block SMB communication between endpoints.
- Restore affected systems.
- Patch vulnerabilities and update antivirus definitions.
- Conduct employee phishing awareness training.

Part 4: Written Communication

Incident Report: Ransomware Attack

1. Executive Summary

At 4:30 AM this morning, several employees reported that they could not access files. Investigation verified a ransomware attack on several Windows servers and workstations. Attackers requested payment in Bitcoin and encrypted files with the ".locked" extension. The ransomware is believed to have entered through a phishing email sent to accounting department staff and laterally spread using the SMB protocol. Containment measures have been taken immediately, and a recovery plan is being implemented.

2. Technical Details and Findings

- Attack Vector: A phishing email with a malicious attachment (`invoice_payment.pdf.exe`).

- Malware Execution: The attachment was opened, running the ransomware payload.
- Lateral Movement: The ransomware propagated through SMB, targeting network shares.
- Privilege Escalation: Suspicious logins from domain admin accounts were noted prior to encryption.
- Encryption Activity: Files on several systems were encrypted, and a ransom note was displayed on infected desktops.
- Antivirus Detection: Certain antivirus products detected but did not block the ransomware.
- Backup Availability: A three-day-old system backup is available but potentially incomplete.

3. Business Impact Assessment

- Affected Systems: Several key servers and employee workstations.
- Operational Disruptions: Extensive downtime for impacted employees and possible delay in financial processing.
- Data Loss Risk: Files may be unrecoverable without backups.
- Financial Impact: Costs can be recovery efforts, system restoration, and potential ransom payment.
- Reputational Risk: In case of data exfiltration, regulatory consequences and customer confidence loss are possible.

4. Recommendations for Enhanced Security

Short-Term Actions:

- Isolate affected systems and SMB traffic blocking to limit spread.
- Reset domain admin passwords that were compromised and enable multi-factor authentication (MFA).
- Restore systems from backups that are known to be clean.

Long-Term Security Improvements:

- Phishing Awareness Training: Train employees in security awareness to identify malicious emails.
- Email Filtering and Attachment Scanning: Enforce enhanced filtering to flag and block suspicious attachments.
- Endpoint Detection and Response (EDR): Install state-of-the-art threat detection technology to detect aberrant behavior.

- Network Segmentation: Restrict SMB access to the most critical systems only.

Conclusion

The ransomware attack points to better email security, employee education, and network protections. Containment steps are implemented immediately, and recovery is ongoing. Enhancing cybersecurity controls will be critical in reducing future risks.

Next Steps

- Complete forensic analysis to identify the initial access vector.
- Conduct and update cybersecurity policies and controls.
- Implement security recommendations and test system resilience against similar attacks.

By mohammed k

mohammedbilal.k313@gmail.com

+91 7736762947