Cyber Attacks
Matrix Incident Handler
SOC

By : Ammar Hakim Haris

1. Social Engineering Phishing Attacks

Description	Phishing is a type of social engineering where an attacker sends fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.
Indicators	• Suspicious Email artifacts like SPF, DKIM, DMARK , suspicious sender, subject and message. • Suspicious URL Link and IP Addresses (like sender's IP) • Suspicious Attachments, File name and File Hashes
Investigate	• Email header, email logs, Email Security Logs (Proofpoint logs) • Proxy logs, DNS Logs • EDR/XDR Log
Actions	• Block malicious File hashes, URLs and IPs • Block sender's email address • Use Multi Factor Authentication, Regularly Update Software, Implement Strong password, Two-factor Authentication, Encryption, AV, Spam filter and Educate Employees.

LinkedIn : Ammar Hakim Haris

2. Suspicious/Malicious DNS Queries

Description	Suspicious or malicious DNS queries are requests made to the Domain Name System (DNS) that are intended to connect to domains associated with malicious activities, such as command and control servers for malware, phishing sites, or domains involved in data exfiltration. These queries can indicate a compromised system within a network or attempts to breach a network's security
Indicators	• High Volume of Queries • Queries for Known Malicious Domains • Unusual Query Patterns (Queries at odd times)
Investigate	• DNS Logs • Endpoint Security Tools • Network Traffic Analysis • Threat Intelligence Platforms
Actions	Block malicious domains, Monitor and Analyze DNS Traffic, Implement DNS Filtering, Regularly Update Security Software, Use Threat Intelligence, Network Segmentation and Educate Users

LinkedIn : Ammar Hakim Haris

3. Malwares / Malicious File Detections (AV, EDR, XDR)

LinkedIn : Ammar Hakim Haris

Description	Malware, or malicious software, refers to any program or file that is harmful to a computer user. Malicious file detection is the process of identifying and neutralizing malware using various security tools, such as Antivirus (AV), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) systems. These tools scan for, detect, and respond to threats by analyzing file signatures, behaviors, and patterns.
Threat Indicators	• Suspicious Network Operations • Suspicious Disk Operations • Suspicious DNS Requests • Suspicious Registry Operations • Suspicious Process Operations • Security Alerts • Unexpected System Behavior • Suspicious File Activity • Unauthorized User Access
Investigate	Security Tool Logs EDR/XDR , System and Network Logs, Endpoint Devicesand Threat Intelligence Platforms
Possible Actions	Block malicious Hashes, IPs and URLs, Regular Updates, Use Comprehensive Security Solutions, Educate Users, Implement Access Controls, Regular Backups and Network Segmentation

4. Web Application Attacks

Description	A web application attack is an attempt by malicious actors to exploit vulnerabilities and weaknesses in web applications or mobile apps. These vulnerabilities can arise during the development process due to improper coding, misconfigured web servers, application design flaws, or failure to validate forms. Attackers may seek to gain unauthorized access,obtain confidential information, introduce malicious content, or alter the website’s content.
Threat Indicators	• Unexpected system behavior such as slow performance or crashing • Suspicious network traffic or connections to known malicious IP addresses • Unauthorized changes to files or creation of unknown files • Security alerts from web application firewalls (WAFs), intrusion detection systems (IDS), or other security solutions indicating detected threats
Investigate	• Security Tool Logs WAFs, IDS, and antivirus for alerts • System and Network Logs • Endpoint Devices • Threat Intelligence Platforms
Actions	Conduct regular Vulnerability Scanning, Regular Updates, Use Comprehensive Security Solutions, Educate Users, Implement Access Controls, Regular Backups and Network Segmentation

LinkedIn : Ammar Hakim Haris

5. Suspicious Communications with external IPs and URLs (Command and Control, Botnet / Zombie networks)

Description	Suspicious communications with external IPs and URLs refer to network activities where devices within an organization's network initiate or receive unexpected or unauthorized connections to or from external IP addresses and URLs. These activities can indicate potential security threats, such as malware infections, data exfiltration attempts,command and control (C2) communications, or phishing attacks. Monitoring for such communications is crucial for identifying and mitigating cybersecurity threats
Threat Indicators	• Unusual Traffic Volumes • Connections to Known Malicious IPs/URLs • Geographic Irregularities • Unusual Times • Repeated Failures
Investigate	Firewall and Network Logs, Intrusion Detection/Prevention Systems (IDS/IPS), Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) Tools and DNS Query Logs
Actions	Block malicious IPs and URLs, Implement Network Segmentation, Use Threat Intelligence,Deploy IDS/IPS and EDR/XDR Solutions, Configure DNS Filtering, Apply Firewall Rules,Regularly Update Security Solutions, Educate Users and Monitor and Analyze Network Traffic

LinkedIn : Ammar Hakim Haris

6. Suspicious Powershell Activities

LinkedIn : Ammar Hakim Haris

Description	Suspicious PowerShell activities refer to the use of PowerShell, a powerful scripting language and command-line shell provided by Microsoft, in ways that are indicative of malicious intent. PowerShell is widely used by system administrators for automation and management tasks. However, its powerful capabilities also make it an attractive tool forattackers to execute commands, evade detection, obfuscate malicious activity, download and execute payloads, and perform reconnaissance within a compromised system
Threat Indicators	• Use of Encoded Commands • Execution Policy Bypass • Unusual Script Execution • Anomalous PowerShell Process Behavior
Investigate	• PowerShell Logs • Event Logs -Event ID 4688 - new process is created. • Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) Systems • Antivirus and Antimalware Solutions
Actions	Enable and Configure PowerShell Logging, Implement Execution Policy Restrictions, Use Application Whitelisting, Educate Users and Administrators, Regularly Update and Patch Systems and Monitor and Analyze PowerShell Activity.

7. Brute Force Alarms

LinkedIn : Ammar Hakim Haris

Description	An attacker trying to guess a password by attempting several different passwords.
Threat Indicators	Multiple login failures in a short period of time.
Investigate	• Active Directory logs, Application Logs, Operational System Logs • Contact User
Actions	If not legit action, disable the account and investigate / block attacker and change password and use MFA. Monitor User Logins, Limit Login Attempts,Implement Strong Authentication and Educate Users

8. Suspicious / Malicious Activity Detections from Intranet (Enterprise Network)

Description	Suspicious or malicious activity detection refers to the process of identifying and responding to actions that may compromise the security and integrity of a network or system. This includes detecting malware infections, unauthorized access, data breaches,and other security incidents that could lead to potential harm or exploitation.
Threat Indicators	• Unusual network traffic patterns or volumes • Unexpected system behavior, such as crashes or performance issues • Unauthorized access attempts or changes in user behavior • Security alerts from IDS, IPS, or antivirus solutions
Investigate	• System and network logs to identify unusual patterns or activities • Security tool alerts and reports for signs of potential threats • Endpoint devices for evidence of compromise or malware • User account activities, including logins and access patterns
Actions	Implement strong access controls and password policies, Regularly update and patch systems and software, Deploy and configure IDS, IPS, and antivirus solutions, Educate users on security best practices and potential threats, Monitor network traffic and system logs for anomalies, Use threat intelligence and behavior analytics to detect and respond to unusual activities

LinkedIn : Ammar Hakim Haris

9. Suspicious File Transfers (Sensitive Content, Large Size, etc)

Description	Suspicious file transfers refer to the movement of files that may contain sensitive content, are of unusually large size, or occur under atypical circumstances, which could indicate a security threat such as a data breach, intellectual property theft, or unauthorized data exfiltration.
Threat Indicators	• Transfers of large volumes of data, especially if the size exceeds typical operational thresholds • Files containing sensitive or confidential information being moved or accessed in an unauthorized manner • Transfers occurring at unusual times or at a higher frequency than normal • Files being sent to or received from unknown or untrusted external sources
Investigate	• Network traffic logs to identify unusual data movement patterns • System and access logs for evidence of unauthorized file access or transfers • Endpoint detection and response (EDR) systems for alerts related to file movement • Data loss prevention (DLP) tools that can track and control the transfer of sensitive data
Action	• Implement strict access controls and monitor user activities to ensure that only • authorized personnel can move or access sensitive files Use encryption for data in transit to protect the contents of files being transferred • Employ DLP solutions to detect and block unauthorized transfer of sensitive information

LinkedIn : Ammar Hakim Haris

10. Suspicious Login Activities (Impossible Travel Activity, Non-Working Hours, etc.)

LinkedIn : Ammar Hakim Haris

Description	Suspicious login activities are attempts to access a user's account that deviate from their normal behavior patterns. These can include logins at unusual times, from new or multiple locations, or repeated failed login attempts, which may indicate that an account is compromised or under attack
Threat Indicators	• Impossible Travel • Non-Working Hours • Repeated Login Failures
Investigate	• Security and Audit Logs: Check the logs for failed login attempts, login locations, and times • User Account Settings: Verify any recent changes to account settings or security configurations • Device and Network Security Tools: Use tools like SIEM, EDR, and IDS/IPS to analyze and correlate security events
Action	If not legit action, disable the account and investigate / block attacker and change password and use MFA. Monitor User Logins, Limit Login Attempts, Implement Strong Authentication and Educate Users

11. Ransomware

LinkedIn : Ammar Hakim Haris

Description	A type malware the encrypts files and request a ransom (money payment) from the user to decrypt the traffic
Threat Indicators	User contancting : Burst of "file update" logs; anti-virus alerts;Connection to suspicious IPs;
Investigate	• AV Logs • OS Logs • Network traffic • etc.
Actions	Request AV checks;Isolate the machine;Turn off the mechine

12. Botnets

Description	when attackers are using the victims server to perform DDoS attacks or other malicious activies
Threat Indicators	Connection to suspicious IPs; Abnormal high volume of network traffic;
Investigate	Network traffic; OS logs (new process);Contact server owner; Contact support teams;
Actions	If Confirmed : Isolate the server; Remove malicous processes;Patch the vulnerability utilized for infection;

LinkedIn : Ammar Hakim Haris

13. Advanced Persistent Threats (APTs)

Description	When attackers get access to systems and created backdoors for furner exploitation.Usually hard to detect
Threat Indicators	Connection to suspicious IPs; Abnormal high volume of networks traffic;Off-hours access logs; New admin account creations;
Investigate	Networks traffic;Access logs;OS logs;(new processes,new connections,abnormal users); Contact server owner/support teams;
Actions	If confirmed : Isolate the machine;Start formal forencis process; Star escalation/Communcation plan

LinkedIn : Ammar Hakim Haris

14. Compromised Account

LinkedIn : Ammar Hakim Haris

Description	When attackers get access to one account (via social engineering or any other method)
Threat Indicators	Off-hours account logins;Account group changes; abnormal high network traffic;
Investigate	Active directory logs;OS Logs;Networks Traffics;Contact use for clarifications
Actions	If confirmed:Disable Account; Password changes;Forencis investigations

15. Data Exfiltertion

LinkedIn : Ammar Hakim Haris

Description	When an attackers (or rogue employee) exfiltrate data to external sources
Threat Indicators	Abnormal high networks traffics;Connect to cloud-storage solutions (Dropbox,Google Cloud,etc); Unusual USB sticks;
Investigate	Network traffic; Proxy Logs;OS Logs
Actions	• If Rogue Employee : Contact Manager,Perform full Forencis • if external threat: Isolate

16. Denial of Services (DoS/DDoS)

LinkedIn : Ammar Hakim Haris

Description	When attackers are using the victims server to perform DDoS attacks or other malicous actives
Threat Indicators	Connection to suspicious IPs; abnormal high volume of networks traffic;
Investigate	Network traffic; OS Logs (New Processes); Contact server owner;Contact support teams;
Actions	If Confirmed:Isolate the server;Remove malicious processes;Patch the vulnerability utilized for infection;

THANK YOU

LinkedIn : Ammar Hakim Haris