https://www.linkedin.com/in/harunseker/

TOP 16 Cyber Attacks detected by SIEM Solutions

1. Phishing Attacks
2. **Suspicious/Malicious DNS Queries**
3. Malware / Malicious File Detections (AV, EPP, EDR, XDR)
4. **Web Application Attacks (OWASP Top 10, SQLi, File Upload)**
5. Suspicious Communications with external IPs and URLs (Command and Control, Botnet / Zombie networks)
6. **Suspicious Powershell Activities**
7. Brute Force Alarms
8. **Suspicious / Malicious Activity Detections from Intranet (Enterprise Network)**
9. Suspicious File Transfers (Sensitive Content, Large Size, etc.)
10. **Suspicious Login Activities (Impossible Travel Activity, Non-Working Hours, etc.)**
11. **Ransomware**
12. **Botnets**
13. **Advanced Persistent Threat**
14. **Compromised Accounts**
15. **Data Exfiltration**
16. **DoS / DDoS- Denial of Service**

https://www.linkedin.com/in/harunseker/

1- Social Engineering / Phishing Attacks

What It is	Phishing is a type of social engineering where an attacker sends a 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.
Threat Indicators	• Suspicious Email artifacts like suspicious sender, subject and message. • Suspicious URL Link • Suspicious Attachment
Where to Investigate	Proxy logs, DNS Logs, EDR/XDR Logs
Possible Actions	Block IP and URls Block sender's email address Regularly Update Software, Implement Strong Authentication, Educate Employees

2- Suspicious/Malicious DNS Queries

What It is	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
Threat Indicators	• High Volume of Queries • Queries for Known Malicious Domains • Unusual Query Patterns (Queries at odd times)
Where to Investigate	DNS Logs Endpoint Security Tools Network Traffic Analysis Threat Intelligence Platforms
Possible Actions	Monitor and Analyze DNS Traffic, Implement DNS Filtering, Regularly Update Security Software, Use Threat Intelligence, Network Segmentation and Educate Users

https://www.linkedin.com/in/harunseker/

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

What It is	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	• Security Alerts • Unexpected System Behavior • Suspicious File Activity • Network Anomalies • Unauthorized User Access
Where to Investigate	Security Tool Logs EDR/XDR , System and Network Logs, Endpoint Devices and Threat Intelligence Platforms
Possible Actions	Regular Updates, Use Comprehensive Security Solutions, Educate Users, Implement Access Controls, Regular Backups and Network Segmentation

https://www.linkedin.com/in/harunseker/

4 - Web Application Attacks

What It is	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
Where to Investigate	• Security Tool Logs WAFs, IDS, and antivirus for alerts • System and Network Logs • Endpoint Devices • Threat Intelligence Platforms
Possible Actions	Regular Updates, Use Comprehensive Security Solutions, Educate Users, Implement Access Controls, Regular Backups and Network Segmentation

https://www.linkedin.com/in/harunseker/

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

What It is	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
Where to 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**
Possible Actions	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.

https://www.linkedin.com/in/harunseker/

6 - Suspicious Powershell Activities

What It is	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 for attackers 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
Where to Investigate	• PowerShell Logs • Event Logs • Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) Systems • Antivirus and Antimalware Solutions
Possible 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

Brute Forcing

What It Is	An attacker trying to guess a password by attempting several different passwords
Threat Indicators	Multiple login failures in a short period of time
Where to Investigate	Active Directory logs; Application logs; Operational System logs; Contact User
Possible Actions	If not legit action, disable the account and investigate/block attacker

https://www.linkedin.com/in/harunseker/

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

What It is	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
Where to 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
Possible 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

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

What It is	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
Where to 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
Possible Actions	• 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 • Conduct regular security awareness training for employees to recognize and report potential threats • Establish clear policies for data handling and transfer, and enforce them with technical controls • Utilize advanced threat detection and response tools to identify and respond to suspicious activities

10. Suspicious Login Activities

(Impossible Travel Activity, Non-Working Hours, etc.)

What It is	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
Where to 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
Possible Actions	Monitor User Logins, Limit Login Attempts, Implement Strong Authentication and Educate Users

Ransomware

What It Is	A type of malware that encrypts files and requests a ransom (money payment) from the user to decrypt the traffic
Threat Indicators	User contacting; Burst of "file update" logs; Anti-virus alerts; Connection to suspicious IPs;
Where to Investigate	AV Logs; OS logs; Account logs; Network traffic; etc.
Possible Actions	Request AV checks; Isolate the machine; Turn off the machine*

https://www.linkedin.com/in/harunseker/

Botnets

What It Is	When attackers are using the victim server to perform DDoS attacks or other malicious activities
Threat Indicators	Connection to suspicious IPs; Abnormal high volume of network traffic;
Where to Investigate	Network traffic; OS logs (new processes); Contact server owner; Contact support teams;
Possible Actions	If confirmed: Isolate the server; Remove malicious processes; Patch the vulnerability utilized for infection;

https://www.linkedin.com/in/harunseker/

Advanced Persistent Threats (APTs)

What It Is	When attackers get access to the system and create backdoors for further exploitation. Usually hard to detect.
Threat Indicators	Connection to suspicious IPs; Abnormal high volume of network traffic; Off-hours access logs; New admin account creations;
Where to Investigate	Network traffic; Access logs; OS logs (new processes, new connections, abnormal users); Contact server owner/support teams;
Possible Actions	If confirmed: Isolate the machine; Start formal forensics process; Start escalation/communication plan

https://www.linkedin.com/in/harunseker/

Compromised Accounts

What It Is	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;
Where to Investigate	Active directory logs; OS logs; Network traffic; Contact user for clarifications
Possible Actions	If confirmed: Disable account; Password changes; Forensic investigations

https://www.linkedin.com/in/harunseker/

Data Exfiltration

What It Is	When an attacker (or rogue employee) exfiltrate data to external sources
Threat Indicators	Abnormal high network traffic; Connection to cloud-storage solutions (Dropbox, Google Cloud, etc); Unusual USB sticks;
Where to Investigate	Network traffic; Proxy logs; OS logs
Possible Actions	If rogue employee: contact manager, perform full forensics If external threat: isolate the machine, disconnect from network

https://www.linkedin.com/in/harunseker/

Denial of Service (DoS / DDoS)

What It Is	When an attacker is able to cause interference in a system by exploiting DoS vulnerabilities or by generating a high volume of traffic
Threat Indicators	Abnormal high network traffic in public facing servers;
Where to Investigate	Network traffic; Firewall logs; OS logs;
Possible Actions	If DoS due to vulnerabilities: Contact patching team for remediation If DDoS due to network traffic: Contact network support or ISP

https://www.linkedin.com/in/harunseker/