How to detect and analyze

Top 20

Cyber Attacks detected by SIEM Solutions

TOP 20 Cyber Attacks detected by SIEM Solutions

1. Phishing Attacks
2. Malware and Malicious File Detections
3. Unauthorized Access Attempts
4. Brute Force Attacks
5. Suspicious Login Activities
6. Suspicious/Malicious DNS Queries
7. Suspicious Communications with External IPs
8. DoS/DDoS Attacks
9. Man-in-the-Middle (MitM) Attacks
10. Lateral Movement
11. Privileged Access Abuse
12. Insider Threats
13. Advanced Persistent Threats (APTs)
14. Supply Chain Attacks
15. Data Exfiltration
16. Web Application Attacks
17. Suspicious PowerShell and Command Line Activities
18. Ransomware Activities
19. Cloud Security Vulnerabilities
20. Anomalous Privilege Escalation

/in/harunseker/

1. Phishing Attacks

What It is	• Phishing attacks use deceptive emails or messages to trick users into revealing sensitive information or downloading malware. Attackers often impersonate trusted entities.
Threat Indicators	• Suspicious email patterns • Unusual sender domains • User clicking on malicious links or attachments
Where to Investigate	• Email security gateway logs • SIEM email event logs • User-reported phishing attempts
Possible Actions	• Block and quarantine phishing emails • Alert affected users and reset compromised credentials • Educate users on phishing awareness • Implement email filtering and anti-phishing solutions

/in/harunseker/

2. Malware and Malicious File Detections

What It is	• Malware refers to malicious software designed to disrupt, damage, or gain unauthorized access to systems.
Threat Indicators	• Detection by antivirus/EDR • Unusual file executions • Unexpected system behavior
Where to Investigate	• Endpoint security alerts • File integrity monitoring • SIEM malware detection logs
Possible Actions	• Isolate infected systems • Remove malware • Patch vulnerabilities and update defenses

3. Unauthorized Access Attempts

What It is	• Attempts to access systems, applications, or data without proper authorization, often as a precursor to further attacks.
Threat Indicators	• - Access denied logs • - Unusual access times • - Use of expired or disabled accounts
Where to Investigate	• - Authentication logs • - Access control lists • - SIEM alerts on unauthorized access
Possible Actions	• - Block suspicious accounts • - Investigate source • - Review and tighten access controls

/in/harunseker/

5. Suspicious Login Activities

What It is	• Login attempts that deviate from normal patterns, such as logins from new locations or at odd times, possibly indicating account compromise.
Threat Indicators	• Impossible travel • Non-working hours • Repeated login failures
Where to Investigate	• Security and audit logs • User account settings • SIEM, EDR, IDS/IPS event analysis
Possible Actions	• Disable account if suspicious • Change password and enforce MFA • Monitor and educate users

/in/harunseker/

6. Suspicious/Malicious DNS Queries

What It is	• DNS requests that may indicate data exfiltration, command and control, or access to malicious domains.
Threat Indicators	• Unusual DNS query patterns • Queries to known bad domains • High volume of DNS requests
Where to Investigate	• DNS server logs • SIEM DNS event monitoring • Threat intelligence feeds
Possible Actions	• Block malicious domains • Investigate endpoints • Update DNS filtering rules

7. Suspicious Communications with External IPs

What It is	• Outbound or inbound network traffic to suspicious or blacklisted IP addresses, possibly indicating compromise.
Threat Indicators	• Connections to known C2 servers • High-entropy domains • Unusual data transfers
Where to Investigate	• Firewall logs • SIEM network traffic analysis • Threat intelligence lookups
Possible Actions	• Block external IPs • Analyze affected systems • Update firewall and proxy rules

/in/harunseker/

8. DoS/DDoS Attacks

What It is	• Attempts to overwhelm services or networks with excessive traffic, causing disruption or downtime.
Threat Indicators	• Traffic spikes • Service unavailability • Multiple sources of traffic
Where to Investigate	• - Network traffic logs • - SIEM DDoS alerts • - ISP reports
• Possible Actions	• Engage mitigation services • - Block offending IPs • - Rate-limit traffic

9. Man-in-the-Middle (MitM) Attacks

What It is	• Interception or alteration of communications between two parties, often to steal data or inject malicious content.
Threat Indicators	• Unexpected certificate changes • Unusual ARP/DNS activity • Session hijacking attempts
Where to Investigate	• Network packet captures • SIEM MitM detection rules • Endpoint security logs
Possible Actions	• Enforce encryption • Investigate compromised endpoints • Educate users on secure connections

10. Lateral Movement

What It is	• Attackers move within a network after initial compromise to access additional systems and data.
Threat Indicators	• Unusual internal traffic • Multiple account logins across systems • Use of admin tools
Where to Investigate	• Lateral movement detection in SIEM • Endpoint logs • Privileged account monitoring
Possible Actions	• Contain affected systems • Reset credentials • Review and limit privileges

/in/harunseker/

11. Privileged Access Abuse

What It is	• Misuse of privileged accounts to access or manipulate sensitive data or systems.
Threat Indicators	• Unauthorized privilege escalation • Unusual admin activity • Access outside job role
Where to Investigate	• Privileged account activity logs • SIEM alerts • Change management records
Possible Actions	• Revoke excessive privileges • Investigate activity • Implement least privilege principle

12. Insider Threats

What It is	Malicious or negligent actions by employees, contractors, or partners that threaten security.
Threat Indicators	- Data access outside normal patterns - Large data downloads - Policy violations
Where to Investigate	- User activity monitoring - SIEM insider threat rules - HR and access records
Possible Actions	- Investigate user behavior - Restrict access - Conduct security awareness training

13. Advanced Persistent Threats (APT

What It is	• Sophisticated, targeted attacks that maintain long-term access to systems to steal data or disrupt operations
Threat Indicators	• Multiple attack vectors • Persistent, stealthy activity • Use of zero-day exploits
Where to Investigate	• SIEM correlation of multiple alerts • Endpoint and network logs • Threat intelligence analysis
Possible Actions	• Conduct full incident response • Remove persistence mechanisms • Patch and harden systems

14. Supply Chain Attacks

What It is	• Compromises originating from third-party vendors, partners, or software updates.
Threat Indicators	• Unusual activity from vendor accounts • Unexpected software changes • New external connections
Where to Investigate	• Vendor access logs • Software update records • SIEM third-party monitoring
Possible Actions	• Vet and monitor vendors • Restrict third-party access • Validate software integrity

15. Data Exfiltration

What It is	• Unauthorized transfer of sensitive data outside the organization, often for theft or ransom.
Threat Indicators	• Large data transfers • Transfers to unknown destinations • Use of unauthorized channels
Where to Investigate	• Data loss prevention (DLP) logs • SIEM exfiltration rules • Network traffic analysis
Possible Actions	• Block data transfers • Investigate endpoints • Enforce DLP policies

16. Web Application Attacks

What It is	• Exploitation of vulnerabilities in web applications, such as SQL injection or cross-site scripting.
Threat Indicators	• Unusual web requests • Error messages in logs • Unauthorized file uploads
Where to Investigate	• Web server and application logs • SIEM web attack alerts • Vulnerability scans
Possible Actions	• Patch vulnerabilities • Enable web application firewall (WAF) • Conduct code reviews

/in/harunseker/

17. Suspicious PowerShell and Command Line Activities

What It is	• Malicious or unauthorized use of command line tools and scripting languages to execute attacks.
Threat Indicators	• Obfuscated commands • Unusual script executions • Elevated privilege use
Where to Investigate	• Endpoint detection logs • SIEM script activity monitoring • PowerShell logs
Possible Actions	• Block unauthorized scripts • Monitor admin tool usage • Restrict scripting permissions

18. Ransomware Activities

What It is	• Malware that encrypts data and demands payment for decryption, disrupting business operations.
Threat Indicators	• Sudden file encryption • Ransom notes • Unusual process activity
Where to Investigate	• Endpoint security alerts • SIEM ransomware detection • Backup integrity checks
Possible Actions	• Isolate infected systems • Restore from backups • Notify authorities

19. Cloud Security Vulnerabilities

What It is	• Weaknesses in cloud configurations, APIs, or access controls that can be exploited for attacks.
Threat Indicators	• Unauthorized cloud access • Misconfigured storage • Suspicious API calls
Where to Investigate	• Cloud provider security logs • SIEM cloud monitoring • Configuration management tools
Possible Actions	• Harden cloud configurations • Enforce access controls • Monitor cloud activity

20. Anomalous Privilege Escalation

What It is	• Unexpected elevation of user privileges, which may indicate compromise or insider abuse.
Threat Indicators	• Privilege changes outside process • Use of admin rights by non-admins • Unusual access grants
Where to Investigate	• Privilege change logs • SIEM privilege escalation alerts • Access review records
Possible Actions	• Revoke unauthorized privileges • Investigate escalation events • Implement approval workflows