500++ SIEM USE CASES WITH CATEGORIES

BY IZZMIER IZZUDDIN

SIEM USE CASES

1. **Abnormal Account Lockout Frequency**
2. **Abnormal Changes in Data Retention Policies**
3. **Abnormal Changes to File Ownership**
4. **Abnormal Cloud API Calls**
5. **Abnormal Cloud Resource Terminations**
6. **Abnormal Cloud Service Usage**
7. **Abnormal Cloud Storage Sharing Behavior**
8. **Abnormal Email Reply Patterns**
9. **Abnormal File Deletion Patterns**
10. **Abnormal File Path Access Patterns**
11. **Abnormal Growth in Cloud Storage Usage**
12. **Abnormal Growth of Temporary Files**
13. **Abnormal Increase in Failed Command-Line Operations**
14. **Abnormal Metadata Changes in Digital Files**
15. **Abnormal Metrics in Cloud Workload Activity**
16. **Abnormal Network Time Protocol (NTP) Traffic**
17. **Abnormal Packet Size in Network Traffic**
18. **Abnormal Patterns in Backup Activity**
19. **Abnormal PowerShell Module Import**
20. **Abnormal SSH Key Scanning**
21. **Abnormal SSL Certificate Usage**
22. **Abnormal SSL Certificate Validity Changes**
23. **Abnormal Traffic Spikes from a Single Host**
24. **Abnormal Traffic to Geographically Unusual Locations**
25. **Abnormal Traffic to Rare Domains**
26. **Abnormal Usage of Security Tokens**
27. **Abnormal Use of Debug Privileges**
28. **Abnormal Volume of Web Socket Connections**
29. **Abnormal VPN Session Durations**
30. **Abnormal Web Activity**
31. **Abnormal Web Application Requests**
32. **Abuse of Group Policy Objects (GPO)**
33. **Abuse of Remote Management Tools**
34. **Access Outside Business Hours**
35. **Access to Disallowed Websites**
36. **Account Lockouts**

37. **Active Directory Enumeration**
38. **Anomalous Behavior of Printer Devices**
39. **Anomalous Database Query**
40. **Anomalous Device Connection in Network**
41. **Anomalous Encryption Key Usage**
42. **Anomalous File Deletion Patterns**
43. **Anomalous File Transfers**
44. **Anomalous Outbound Traffic**
45. **Anomalous Resource Scaling in Cloud Environments**
46. **Anomalous SaaS Application Logins**
47. **Anomalous SSL/TLS Handshake Behavior**
48. **Anomalous Use of FTP Servers**
49. **Anomalous User Behavior**
50. **Attempted Deactivation of Endpoint Security**
51. **Attempted Use of Deprecated Protocols**
52. **Beaconing Traffic Detection**
53. **BGP Hijacking Detection**
54. **BGP Route Hijacking Alerts**
55. **Browser Exploit Detection**
56. **Brute Force Attacks**
57. **Brute Force Detection**
58. **Cloud Infrastructure Anomalies**
59. **Cloud Resource Overprovisioning**
60. **Cloud Resource Sharing Violations**
61. **Cloud Security Misconfiguration Alerts**
62. **Cloud Storage Upload Spikes**
63. **Command and Control (C2) Traffic Detection**
64. **Command and Control Traffic**
65. **Compromised Host Communicating with Command and Control (C2) Server**
66. **Credential Dumping Detection**
67. **Credential Harvesting Attempt Detection**
68. **Credential Sharing Alerts**
69. **Data Access Spikes**
70. **Data Exfiltration Attempts**
71. **Data Exfiltration Detection**
72. **Data Loss Prevention (DLP) Violations**
73. **Data Transfer to External Hosts**
74. **Data Uploaded to Unauthorised Cloud Storage**

75. **Database Access Anomalies**
76. **DDoS Attack Detection**
77. **Detection of Abnormal Device Enrollment in MDM**
78. **Detection of Brute Force Attacks on Email Accounts**
79. **Detection of Default or Weak Credentials**
80. **Detection of Denial of Service (DoS) Attacks on Web Servers**
81. **Detection of Deprecated Protocol Usage**
82. **Detection of Hidden Network Tunnels**
83. **Detection of Hidden Root Certificates**
84. **Detection of Malicious PowerShell Commands with Encoded Payloads**
85. **Detection of Network Scanning Tools**
86. **Detection of New Public Key Infrastructure (PKI) Certificates Issued**
87. **Detection of Non-Standard Port Traffic Spikes**
88. **Detection of Packet Fragmentation Attacks**
89. **Detection of Phishing URLs in Email Body or Attachments**
90. **Detection of Rogue DHCP Server**
91. **Detection of Stenographic File Activity**
92. **Detection of Suspicious Browser Extensions**
93. **Detection of Suspicious Cross-Site Scripting (XSS) Attempts**
94. **Detection of Suspicious Network Broadcasts**
95. **Detection of Suspicious Outbound FTP Activity**
96. **Detection of Suspicious Service Account Password Changes**
97. **Detection of Unauthorised IoT Device Registrations**
98. **Detection of Unauthorised Modifications in Server Configurations**
99. **Detection of Unauthorised Remote Access Tools (RATs)**
100. **Detection of Web Shell Installation**
101. **DNS Anomalies**
102. **DNS Query for Known Malicious Domains**
103. **DNS Tunneling Detection**
104. **DNS Zone Transfer Attempt Detection**
105. **Elevated Error Rates in Application Logs**
106. **Elevated Privilege Token Usage**
107. **Email Attachment with Executable Files**
108. **Email Spoofing Detection**
109. **Endpoint Antivirus Alerts**
110. **Endpoint Beaconing to Non-Standard Port**
111. **Endpoint Device Compromise**
112. **Endpoint Isolation Trigger**

113. **Excessive Admin Privilege Assignments**
114. **Excessive Anomalies in Email Bounce Rates**
115. **Excessive Anomalies in SSL/TLS Certificates**
116. **Excessive Changes to Monitoring Thresholds**
117. **Excessive Changes to Security Group Rules in Cloud Environments**
118. **Excessive Connections to Public Git Repositories**
119. **Excessive DNS Requests to External Servers**
120. **Excessive Failed File Access Attempts**
121. **Excessive Failed File Decryption Attempts**
122. **Excessive Failed Logins**
123. **Excessive File Access by a Single User**
124. **Excessive File Copying Activity**
125. **Excessive File Write Operations**
126. **Excessive Log Clearing or Modification Attempts**
127. **Excessive Network Scanning**
128. **Excessive Number of Queries to WHOIS Services**
129. **Excessive SSH Authentication Failures from Known IPs**
130. **Excessive Unsuccessful Password Resets**
131. **Excessive Use of Email Distribution Lists**
132. **Expired Certificate Usage**
133. **Exploit Attempt Detection**
134. **Exploit Attempts on Known CVEs**
135. **Exploit Kit Activity Detection**
136. **Exploit Kit Indicators**
137. **Exploitation of a Known Vulnerability in Software**
138. **Failed Attempts to Escalate Privileges in Containers**
139. **Failed Login Attempts Threshold**
140. **Failed Password Change Attempts**
141. **Failed Two-Factor Authentication Attempts**
142. **File Encryption Activities**
143. **File Encryption Activity Detection**
144. **File Integrity Monitoring**
145. **File Integrity Monitoring Alerts**
146. **File Sharing Service Anomalies**
147. **File Uploads to Unauthorised Servers**
148. **Fileless Malware Detection**
149. **Firewall Policy Change Detection**
150. **Firewall Rule Changes**

151. **Geolocation Access Policy Breach**
152. **Guest Account Activity**
153. **Hidden File Creation on Endpoints**
154. **High Frequency of HTTP 503 Errors**
155. **High Frequency of Network Disconnects**
156. **High Latency in Database Queries**
157. **High Rate of Packet Fragmentation in Network Traffic**
158. **High Volume of 404 Errors**
159. **High Volume of Access Requests to Privileged Directories**
160. **High Volume of Alerts for Default Network Shares**
161. **High Volume of Alerts from Unidentified Devices**
162. **High Volume of Data Retrieval from EDR Systems**
163. **High Volume of Failed SFTP Transfers**
164. **High Volume of Malformed Packets**
165. **High Volume of TCP Reset Packets**
166. **High-Volume Access Requests**
167. **Honeypot Alerts**
168. **HTTP Anomalies Detection**
169. **Inactive Account Usage**
170. **Insecure Protocol Usage**
171. **Insider Threat Data Exfiltration**
172. **Insider Threat Detection**
173. **IoT Device Anomalies**
174. **Keylogger Detection**
175. **Lateral Movement Detection**
176. **Lateral Movement in Cloud Environments**
177. **Lateral Movement in the Network**
178. **Lateral Movement via Remote Desktop Protocol (RDP)**
179. **Lateral Traffic Between Containers**
180. **Malicious Process Injection**
181. **Malware Callback Detection**
182. **Malware Detection**
183. **Misuse of Command-Line Interfaces**
184. **Misuse of Default Credentials in New Devices**
185. **Misuse of Multi-Factor Authentication Tokens**
186. **Misuse of Security Clearance Levels**
187. **Multiple Concurrent Sessions**
188. **Multiple Device MAC Address Spoofing**

189. **Multiple Logins from Different Geographies**
190. **Multiple User Account Lockouts**
191. **Network Traffic Spikes**
192. **New Domain Registration Accessed**
193. **New Executable in Startup Folder**
194. **New Service Installation**
195. **New User Account Creation**
196. **Out-of-Hours Maintenance Activity**
197. **Out-of-Scope Service Invocations**
198. **Outbound Connections to Known Malicious IPs**
199. **Outdated Application Vulnerabilities Exploited**
200. **Phishing Email Detection**
201. **Phishing Site Access Detection**
202. **Policy Non-Compliance**
203. **Policy-Based Data Access Anomalies**
204. **Policy-Based Email Monitoring**
205. **Port Scanning Activity**
206. **Port Scanning Detection**
207. **Potential Lateral Movement Detected**
208. **Privilege Escalation**
209. **Privilege Escalation Attempt**
210. **Privilege Escalation via Exploit**
211. **Privilege Escalation via Exploited Kernel Vulnerability**
212. **Privilege Escalation via Scheduled Tasks**
213. **Privileged Account Abuse**
214. **Privileged Account Activity Outside Allowed Hours**
215. **Privileged Account Escalation Activity**
216. **Privileged Account Login Failure**
217. **Privileged Account Login Outside Business Hours**
218. **Privileged User Session Monitoring**
219. **Proxy Bypass Attempts**
220. **Ransomware Activity Detection**
221. **Rapid and Repeated Session ID Generation**
222. **Rapid Cloud Security Group Updates**
223. **Rapid File Encryption Events**
224. **Remote Desktop Protocol (RDP) Anomalies**
225. **Repeated Access Denials**
226. **Repeated Attempts to Restart Security Services**

227. **Rogue Access Point Detection**
228. **Rogue Certificate Authority Requests**
229. **Rogue Cloud Storage Bucket Creation**
230. **Rogue Device Detection**
231. **Rogue DNS Tunnel Detection**
232. **Rogue MAC Address Detection**
233. **Rogue Network Device Detection**
234. **Rogue Script Execution in Sandbox**
235. **Rogue Virtual Machine Deployment**
236. **Rogue Wireless Network Beaconing**
237. **Rootkit Detection on Endpoints**
238. **SaaS Application Anomalies**
239. **Security Policy Change Detection**
240. **Sensitive File Access Outside Business Hours**
241. **Service Account Activity**
242. **Service Account Anomalies**
243. **Shadow IT Application Usage**
244. **Shadow IT Detection**
245. **Shared Account Usage**
246. **SMB Lateral Movement Detection**
247. **Social Engineering Indicators**
248. **SQL Injection Attack Attempt**
249. **Sudden Drops in Network Bandwidth Utilization**
250. **Sudden Increase in Cloud Costs (Possible Crypto Mining)**
251. **Sudden Increase in Failed API Requests**
252. **Sudden Increase in File Reads**
253. **Sudden Privilege Downgrades**
254. **Suspected Insider Reconnaissance**
255. **Suspicious Access to Source Code Repositories**
256. **Suspicious Activity in Cloud Billing Accounts**
257. **Suspicious Activity Involving Trusted Third-Party Applications**
258. **Suspicious Application Installation**
259. **Suspicious Archive File Extraction**
260. **Suspicious ARP Cache Poisoning**
261. **Suspicious ARP Spoofing Detection**
262. **Suspicious ARP Traffic**
263. **Suspicious Authentication Token Use**
264. **Suspicious Backup Restoration**

265. **Suspicious Binary Payload Detection in Network Streams**
266. **Suspicious Browser Extensions**
267. **Suspicious Changes to Group Policies**
268. **Suspicious Changes to OS Kernel Parameters**
269. **Suspicious Changes to System Host Files**
270. **Suspicious Cloud VM Spinning During Off-Hours**
271. **Suspicious Command Execution**
272. **Suspicious Command Execution in CLI**
273. **Suspicious Commands Executed via Command Line**
274. **Suspicious Configurations of Group Memberships**
275. **Suspicious Connections to Obsolete Protocol Endpoints**
276. **Suspicious Cross-Domain Authentication Attempts**
277. **Suspicious Database Query Anomalies**
278. **Suspicious DHCP Activity**
279. **Suspicious Directory Traversal Attempts**
280. **Suspicious DNS TXT Record Queries**
281. **Suspicious Domain Generation Algorithm (DGA) Activity**
282. **Suspicious Dynamic DNS (DDNS) Queries**
283. **Suspicious Email Attachments**
284. **Suspicious Email Header Anomalies**
285. **Suspicious Endpoint Communication**
286. **Suspicious External IP Communication**
287. **Suspicious File Download**
288. **Suspicious File Downloads**
289. **Suspicious File Hash Matching Known Malware**
290. **Suspicious File Integrity Changes**
291. **Suspicious File Replication to External Drives**
292. **Suspicious File Sharing Activities**
293. **Suspicious HTTP 500/400 Error Spike**
294. **Suspicious HTTP/HTTPS Traffic**
295. **Suspicious Hyper-V Activity**
296. **Suspicious Lateral Movement via RDP Shadowing**
297. **Suspicious LNK File Execution**
298. **Suspicious Log Deletions**
299. **Suspicious Mobile Device Management Changes**
300. **Suspicious Modification of Audit Logs**
301. **Suspicious Network Activity**
302. **Suspicious Network Anomalies in DMZ**

303. **Suspicious Network Traffic from Legacy Protocols**
304. **Suspicious Outbound Traffic Volume**
305. **Suspicious PowerShell Command Execution**
306. **Suspicious Powershell Script Logging Disabled**
307. **Suspicious Process Creation**
308. **Suspicious Process Execution**
309. **Suspicious Reconfiguration of Load Balancers**
310. **Suspicious Registry Changes**
311. **Suspicious Registry Key Modification**
312. **Suspicious Removal of Security Agents**
313. **Suspicious Resource Locking in Cloud Environments**
314. **Suspicious Reuse of Authentication Tokens**
315. **Suspicious Scheduled Task Creation**
316. **Suspicious Script Execution in Browsers**
317. **Suspicious SMB Traffic**
318. **Suspicious SMB Traffic to Non-Standard Ports**
319. **Suspicious SQL Queries**
320. **Suspicious Token Generation**
321. **Suspicious Traffic Between VLANs**
322. **Suspicious Traffic to Dynamic DNS Hosts**
323. **Suspicious Usage of Legacy Authentication Methods**
324. **Suspicious USB Device Activity**
325. **Suspicious Use of Automation Tools**
326. **Suspicious Use of Debugging or Tracing Tools**
327. **Suspicious Use of DNS for Data Exfiltration**
328. **Suspicious Use of Email Auto-Forwarding Rules**
329. **Suspicious Use of External Email Addresses**
330. **Suspicious Use of Proxy Avoidance Tools**
331. **Suspicious Use of System Restore Functionality**
332. **Suspicious Use of Web Proxies**
333. **Suspicious Utilization of Cloud IAM Roles**
334. **Suspicious VPN Connection**
335. **Suspicious WMI Activity**
336. **Suspicious YARA Rule Match**
337. **Suspicious ZIP/RAR File Creation**
338. **System Crash Dump Access**
339. **Tampered Security Logs Detection**
340. **Tampering of Application Logs**

341. **Tampering with SIEM or Security Logs**
342. **Threat Intelligence Integration Alerts**
343. **Time-Based Access Violations**
344. **Tor Network Connection Detection**
345. **Traffic Anomalies in VPCs**
346. **Traffic Directed Toward Sinkhole IPs**
347. **Traffic Patterns Resembling Covert Channels**
348. **Traffic Patterns Suggesting Credential Harvesting**
349. **Traffic Spikes to TOR Exit Nodes**
350. **Traffic Spikes Toward Unmonitored Geolocations**
351. **Traffic to Blacklisted IPs**
352. **Unapproved Application Execution**
353. **Unapproved Changes to Firewall Rules**
354. **Unauthorised Access Attempt**
355. **Unauthorised Access to a Database**
356. **Unauthorised Access to Backup Files**
357. **Unauthorised Access to Financial Data**
358. **Unauthorised API Call Detection**
359. **Unauthorised Application Installation**
360. **Unauthorised Backup File Access Attempts**
361. **Unauthorised Change of Critical System Configuration Files**
362. **Unauthorised Cloud Account Login**
363. **Unauthorised Cloud API Key Usage**
364. **Unauthorised Configuration Change**
365. **Unauthorised Database Query Monitoring**
366. **Unauthorised Database Schema Changes**
367. **Unauthorised Execution of Compiled Scripts**
368. **Unauthorised File Access**
369. **Unauthorised File Transfers via Secure Copy Protocol (SCP)**
370. **Unauthorised Firmware Updates**
371. **Unauthorised Modification of Active Directory Group Memberships**
372. **Unauthorised Modification of DNS Records**
373. **Unauthorised Modification of Security Logs**
374. **Unauthorised Network Share Access**
375. **Unauthorised SNMP Queries or Activity**
376. **Unauthorised Software License Activation**
377. **Unauthorised SSH Key Generation**
378. **Unauthorised Use of Debugging Tools**

379. **Unauthorised Use of Security Assessment Tools (e**
380. **Unauthorised Use of Virtual Machines**
381. **Unauthorised Use of Windows Management Instrumentation (WMI)**
382. **Unauthorised Wireless SSID Connection**
383. **Unauthorised Access Attempts**
384. **Unauthorised Access to Archived Data**
385. **Unauthorised Access to Backup Files**
386. **Unauthorised Access to Code Build Systems**
387. **Unauthorised Access to Configuration Management Tools**
388. **Unauthorised Access to CRM Systems**
389. **Unauthorised Access to Encryption Keys**
390. **Unauthorised Access to Human Resources Systems**
391. **Unauthorised Access to Internal Tools**
392. **Unauthorised Access to Key Vaults**
393. **Unauthorised Access to Payment Systems**
394. **Unauthorised Access to Physical Security Systems**
395. **Unauthorised Access to Sensitive Files**
396. **Unauthorised Access to Shared Drives**
397. **Unauthorised Account Merging**
398. **Unauthorised API Gateway Modifications**
399. **Unauthorised API Key Usage**
400. **Unauthorised API Schema Modifications**
401. **Unauthorised Application Installation**
402. **Unauthorised Attempts to Mount Encrypted Disks**
403. **Unauthorised Attempts to Overwrite Database Schemas**
404. **Unauthorised Backup Exports**
405. **Unauthorised Backup Restores**
406. **Unauthorised BIOS Configuration Changes**
407. **Unauthorised Browser Configurations**
408. **Unauthorised Certificate Issuance**
409. **Unauthorised Change in Software Delivery Pipelines**
410. **Unauthorised Changes to DNS Zones**
411. **Unauthorised Changes to Network Time Protocol (NTP) Settings**
412. **Unauthorised Changes to Software Licenses**
413. **Unauthorised Changes to Web Application Firewalls**
414. **Unauthorised Clipboard Monitoring Tools**
415. **Unauthorised Clone of Virtual Machines**
416. **Unauthorised Cloud Resource Allocation**

417. **Unauthorised Cloud Storage Access**
418. **Unauthorised Cluster Node Access**
419. **Unauthorised Code Execution in Memory**
420. **Unauthorised Container Privilege Escalation**
421. **Unauthorised Container Registry Access**
422. **Unauthorised Data Compression Activities**
423. **Unauthorised Database Changes**
424. **Unauthorised Debugging Tool Usage**
425. **Unauthorised Deletion of Incident Records**
426. **Unauthorised Device Connections**
427. **Unauthorised Device Removal**
428. **Unauthorised Disabling of Log Forwarders**
429. **Unauthorised DNS Changes**
430. **Unauthorised Email Forwarding**
431. **Unauthorised Execution of Scheduled Tasks**
432. **Unauthorised Expansion of Firewall Rules**
433. **Unauthorised File Share Permissions Changes**
434. **Unauthorised File Sharing Between VMs**
435. **Unauthorised File Sync Operations**
436. **Unauthorised Firmware Rollbacks**
437. **Unauthorised Firmware Updates**
438. **Unauthorised HTTP Requests to Known Malicious Domains**
439. **Unauthorised Hypervisor Access**
440. **Unauthorised IoT Firmware Modification**
441. **Unauthorised Key Pair Usage in SSH**
442. **Unauthorised LDAP Queries**
443. **Unauthorised Modification of Email Security Settings**
444. **Unauthorised Network Device Configuration**
445. **Unauthorised NTP Server Access**
446. **Unauthorised Password Reset Attempts**
447. **Unauthorised Print Jobs**
448. **Unauthorised RDP Port Access**
449. **Unauthorised Remote Desktop Connections**
450. **Unauthorised Repository Access**
451. **Unauthorised S3 Bucket Policy Changes**
452. **Unauthorised SNMP Access Attempts**
453. **Unauthorised Software Downloads via Web Browsers**
454. **Unauthorised Software License Activations**

455. **Unauthorised Software Patch Installations**
456. **Unauthorised Software Removal**
457. **Unauthorised SSH Key Addition**
458. **Unauthorised Sudo Commands**
459. **Unauthorised Tampering with Security Policies**
460. **Unauthorised Use of Admin Consoles**
461. **Unauthorised Use of Debugging Tools on Live Systems**
462. **Unauthorised Use of Development Tools**
463. **Unauthorised Use of Encryption Tools**
464. **Unauthorised Wireless Network Connections**
465. **Unencrypted Data Transfers**
466. **Unencrypted Passwords in Network Traffic**
467. **Unexpected Alterations in Application Dependencies**
468. **Unexpected Changes to Encryption Policies**
469. **Unexpected Changes to Network Segments**
470. **Unexpected Container Spawning**
471. **Unexpected File System Changes**
472. **Unexpected PowerShell Script Execution**
473. **Unexpected Rate of Archive Extract Operations**
474. **Unexpected Role Changes in IAM Systems**
475. **Unexpected Server Shutdowns**
476. **Unexpected Service Restarts**
477. **Unexpected SSH Access**
478. **Unexpected Traffic to Content Delivery Networks (CDNs)**
479. **Unexpected Use of IPv6 in IPv4 Networks**
480. **Unusual Account Profile Changes**
481. **Unusual Activity on Printer Interfaces**
482. **Unusual Anomalies in Container Logs**
483. **Unusual API Activity**
484. **Unusual Audit Policy Modifications**
485. **Unusual Bandwidth Consumption**
486. **Unusual Beaconing Patterns**
487. **Unusual Binary Execution from Temp Directory**
488. **Unusual Correlation in SIEM Event Sources**
489. **Unusual Correlation of User Actions Across Applications**
490. **Unusual CPU Utilization**
491. **Unusual Credential Use Across Multiple Endpoints**
492. **Unusual Data Movement Between Regions**

493. **Unusual Delays in Network Packet Delivery**
494. **Unusual Deviation in Network Baselines**
495. **Unusual DNS Requests for Non-Existent Domains**
496. **Unusual Email Open Rates**
497. **Unusual Email Sending Patterns**
498. **Unusual File Compression Activity**
499. **Unusual File Transfers via FTP or SFTP**
500. **Unusual Host-to-Host Communication**
501. **Unusual HTTP Methods**
502. **Unusual IoT Device Behavior**
503. **Unusual Log Clearing Activities**
504. **Unusual Login Location**
505. **Unusual Logoff Activity**
506. **Unusual Memory Utilization**
507. **Unusual Modifications in Firmware Logs**
508. **Unusual Network Traffic**
509. **Unusual Number of ARP Requests**
510. **Unusual Number of Failed VPN Logins**
511. **Unusual Outbound Traffic to Tor Exit Nodes**
512. **Unusual Outbound UDP Traffic**
513. **Unusual Pattern in DNS TXT Record Queries**
514. **Unusual Privilege Inheritance**
515. **Unusual Process Parent-Child Relationship**
516. **Unusual Proxy Activity**
517. **Unusual Rate of Role-Based Access Modifications**
518. **Unusual Registry Key Modifications**
519. **Unusual Resource Consumption in Kubernetes Clusters**
520. **Unusual Service Account Activity**
521. **Unusual Spikes in IoT Data Transmission**
522. **Unusual Traffic Between Cloud Regions**
523. **Unusual Traffic on Non-Standard Ports**
524. **Unusual Traffic on Reserved Network Ranges**
525. **Unusual Traffic Patterns from Web Application Firewall (WAF)**
526. **Unusual Traffic Through Proxy Servers**
527. **Unusual Usage of Deprecated APIs**
528. **Unusual Use of Base64 Encoding in Commands**
529. **Unusual Use of Tunneling Protocols**
530. **Unusual User Agent Strings**

531. **Unusual Volume of DNS Queries**
532. **Unusual Web Proxy Bypass Attempts**
533. **Usage of Obsolete or Deprecated Protocols**
534. **USB Device Usage Anomalies**
535. **USB Mass Storage Device Data Transfer**
536. **User Access Policy Violations**
537. **User Account Creation**
538. **User Account Deletion**
539. **VPN Login Anomalies**
540. **Web Server Attack Detection**
541. **Zero-Day Exploit Detection**

CATEGORIES FOR USE CASES

Access Management

- Abnormal Account Lockout Frequency
- Multiple User Account Lockouts
- Privileged Account Abuse
- Access Outside Business Hours
- Shared Account Usage

Cloud Security

- Abnormal Cloud API Calls
- Abnormal Cloud Storage Sharing Behavior
- Cloud Infrastructure Anomalies
- Cloud Resource Sharing Violations
- Sudden Increase in Cloud Costs (Possible Crypto Mining)

Email Security

- Phishing Email Detection
- Detection of Phishing URLs in Email Body or Attachments
- Abnormal Email Reply Patterns
- Email Spoofing Detection
- Suspicious Use of Email Auto-Forwarding Rules

Network Anomalies

- Abnormal Traffic to Rare Domains
- DNS Query for Known Malicious Domains
- Detection of Non-Standard Port Traffic Spikes
- Suspicious Outbound FTP Activity
- Abnormal Network Time Protocol (NTP) Traffic

Malware Detection

- Fileless Malware Detection
- Detection of Malicious PowerShell Commands with Encoded Payloads
- Suspicious File Hash Matching Known Malware
- Malware Callback Detection
- Suspicious Binary Payload Detection in Network Streams

Threat Detection

- Command and Control (C2) Traffic Detection
- Beaconing Traffic Detection
- Suspicious PowerShell Command Execution
- Rogue Access Point Detection
- Exploit Kit Indicators

Privilege Escalation

- Privilege Escalation Attempt
- Privilege Escalation via Exploit
- Suspicious Scheduled Task Creation
- Elevated Privilege Token Usage
- Suspicious Use of Debug Privileges

Data Security

- Data Exfiltration Detection
- Suspicious Use of DNS for Data Exfiltration
- Suspicious File Replication to External Drives
- File Encryption Activity Detection
- Abnormal File Deletion Patterns

Insider Threat

- Insider Threat Detection
- Suspicious Access to Source Code Repositories

- Anomalous Device Connection in Network
- Abuse of Group Policy Objects (GPO)
- Suspicious Activity in Cloud Billing Accounts

Incident Response

- Endpoint Isolation Trigger
- Tampered Security Logs Detection
- Suspicious Log Deletions
- Firewall Policy Change Detection
- Detection of Unauthorised Remote Access Tools (RATs)

Vulnerability Exploits

- Exploit Attempt Detection
- Exploit Attempts on Known CVEs
- Exploitation of a Known Vulnerability in Software
- Detection of Hidden Root Certificates
- Detection of Deprecated Protocol Usage

Lateral Movement

- Lateral Movement in the Network
- Lateral Movement via Remote Desktop Protocol (RDP)
- SMB Lateral Movement Detection
- Suspicious Traffic Between VLANs
- Lateral Movement in Cloud Environments

Compliance and Governance

- Policy Non-Compliance
- Geolocation Access Policy Breach
- Time-Based Access Violations
- Security Policy Change Detection

- Detection of Unauthorised Modifications in Server Configurations

User Behavior

- Anomalous User Behavior
- Detection of Default or Weak Credentials
- Abnormal Growth in Cloud Storage Usage
- Suspicious Commands Executed via Command Line
- Abnormal Metrics in Cloud Workload Activity