1️⃣ HTTP Traffic Spike Detection (DDoS / Bot Activity)

SOC Use: Live monitoring + alert

```
index=main sourcetype=http
| timechart span=5m count as request_count
| where request_count > 1000
```

📌 **Why SOC cares:**
Sudden spikes = DDoS, bot flood, scanning activity

2️⃣ Excessive HTTP Errors (4xx / 5xx Abuse)

SOC Use: Exploitation & brute-force detection

```
index=main sourcetype=http
| where status>=400
| stats count by src_ip status
| where count > 50
```

📌

- 404 → directory brute force
- 401/403 → auth abuse
- 500 → exploitation attempt

3️⃣ Web Login Brute-Force Detection

SOC Use: Account compromise detection

```
index=main sourcetype=http
| search action="login" status="failed"
| stats count as failures by src_ip
| where failures > 10
```

📌
Direct indicator of brute-force or credential stuffing

4️⃣ Web Scanning / Enumeration Detection

SOC Use: Reconnaissance detection

```
index=main sourcetype=http
| where status=404
| stats count by src_ip
| where count > 100
```

📌
High 404s = directory/file scanning tools

5️⃣ Suspicious File Download / Data Exfiltration

SOC Use: Malware delivery / data theft

```
index=main sourcetype=http
| search uri="*.exe" OR uri="*.zip" OR uri="*.rar" OR uri="*.pdf"
| stats count by src_ip uri
| where count > 5
```

📌

- Malware downloads
- Data exfiltration via HTTP