**detections/ Folder Content**

**1. Brute Force Attack Detection → brute-force-detection.spl**

index=wineventlog OR index=auth\_logs

| stats count by src\_ip, user, host

| where count > 5

| table \_time, src\_ip, user, host, count

| sort - count

🔎 *Detects multiple failed login attempts (possible brute force). Threshold can be tuned (e.g., > 5 attempts in 5 min).*

**2. Ransomware Behavior Detection → ransomware-detection.spl**

index=file\_logs OR index=sysmon

| where like(file\_name, "%.locked%") OR like(file\_name, "%.encrypted%")

| stats count by user, file\_path, process\_name

| sort - count

🔎 *Flags unusual file extensions (e.g., .locked, .encrypted) that ransomware often generates.*

**3. Suspicious DNS Requests → suspicious-dns.spl**

index=dns\_logs

| where match(query, "\.xyz$|\.top$|\.pw$|\.ru$")

| stats count by src\_ip, query

| sort - count

🔎 *Detects outbound DNS queries to risky TLDs (.xyz, .top, .ru). Can be enriched with threat intel feeds.*

**4. Privilege Escalation Detection → privilege-escalation.spl**

index=wineventlog

EventCode=4672

| table \_time, user, host, Privileges

| where Privileges="SeDebugPrivilege" OR Privileges="SeTcbPrivilege" OR Privileges="SeImpersonatePrivilege"

🔎 *Monitors Windows Event ID 4672 → “Special Privileges Assigned to New Logon” (commonly abused for privilege escalation).*