Sumo Logic Detection & Threat Hunting Playbook (Enterprise Edition 1–100)

Fully explicit queries, copy-paste ready, MITRE ATT&CK mapped, with Severity / Confidence / FP notes and subqueries where applicable.

INITIAL ACCESS

1. External RDP Login (T1078)

```
index=security EventCode=4624 LogonType=10 | stats count by
src_ip,user,host
```

Severity: Medium | Confidence: High | FP Notes: VPN or legit remote work

2. Brute Force Failures (T1110)

```
index=security EventCode=4625 | stats count by src_ip,user | where count>5
```

Severity: High | Confidence: Medium | FP Notes: NAT gateways possible

3. Phishing Email Link Clicks (T1566)

```
index=email EventType=click | stats count by user, sender, link
```

Severity: Medium | Confidence: Medium | FP Notes: Training exercises

4. Suspicious OAuth Consent (T1528)

```
oauth consent granted | where app not in [AUTHORIZED_APPS]
```

Severity: Medium | Confidence: Medium | FP Notes: New SaaS app

5. New Account Creation (T1136)

```
user created | where role matches /(admin|privileged)/
```

Severity: High | Confidence: High | FP Notes: Legit HR onboarding

6. Temporary Account Use (T1078)

```
login success | where user matches /temp/i
```

Severity: Medium | Confidence: Medium | FP Notes: Contractor accounts

7. Password Spray Attempt (T1110)

```
_failed login | stats count by src_ip,user | where count>10
```

Severity: High | Confidence: Medium | FP Notes: High rate of attempts

8. Login From New Geo Location (T1078)

```
login success | geoip src_ip as country | where country not in
[AUTHORIZED_COUNTRIES]
```

Severity: Medium | Confidence: Medium | FP Notes: Travel or VPN

9. Impossible Travel (T1078)

```
login success | timeslice 1h | count_distinct country by user | where
count>2
```

Severity: High | Confidence: Medium | FP Notes: Suspicious geo pattern

10. Disabled Account Login Attempt (T1078)

```
login attempt | where account_status='disabled'
```

Severity: High | Confidence: High | FP Notes: Rare event

EXECUTION

1. PowerShell DownloadString (T1059.001)

```
process | where command matches /downloadstring/i
```

Severity: High | Confidence: High | FP Notes: Admin script

2. Base64 Encoded PowerShell (T1027)

```
process | where command matches /encodedcommand/i
```

Severity: High | Confidence: High | FP Notes: Malware execution

3. Temp Folder Execution (T1204)

```
process | where path matches /temp/i
```

Severity: Medium | Confidence: Medium | FP Notes: Installer

4. Downloads Folder Execution (T1204)

```
process | where path matches /downloads/i
```

Severity: Medium | Confidence: Medium | FP Notes: Installer

5. Registry Run Key Created (T1547)

```
registry | where key matches /Run/i
```

Severity: High | Confidence: Medium | FP Notes: Persistence attempt

6. Scheduled Task Created (T1053)

```
scheduled task created
```

Severity: Medium | Confidence: Medium | FP Notes: Admin automation

7. WMI Persistence (T1047)

```
process | where command matches /wmic/i
```

Severity: Medium | Confidence: Medium | FP Notes: Admin usage

8. Service Install / Modification (T1543)

```
service | where action matches /(install|modify)/i
```

Severity: High | Confidence: Medium | FP Notes: Admin maintenance

9. AV/EDR Stop (T1562.001)

```
service | where name matches /(edr|av)/i AND status='stopped'
```

Severity: High | Confidence: Medium | FP Notes: Admin stop

10. Log Deletion (T1070)

```
log cleared
```

Severity: High | Confidence: Medium | FP Notes: Rotation / evasion

---

LATERAL MOVEMENT & NETWORK

1. SMB Lateral Movement (T1021.002)

```
smb connection | where dest_ip not in [TRUSTED_NETWORK]
```

Severity: High | Confidence: Medium | FP Notes: Admin file copy

2. RDP Brute Force (T1078.001)

```
rdp connection | stats count by src_ip | where count>10
```

Severity: High | Confidence: Medium | FP Notes: Admin access, VPN considered

3. IRC / Chat C2 Beacon (T1071)

```
network connection | where dest_port in (6667,6697) | timeslice 1m | stats
count by src_ip
```

Severity: Medium | Confidence: Medium | FP Notes: Chat server

4. DNS TXT / C2 Check (T1071.004)

```
dns query | where record_type="TXT" | stats count by domain | where count>5
```

Severity: Medium | Confidence: Medium | FP Notes: Rare TXT usage

5. Rare Protocol Use (T1071)

```
network connection | where protocol not in [COMMON_PROTOCOLS]
```

Severity: Medium | Confidence: Medium | FP Notes: Legacy protocols possible

6. High Port Scan Detection (T1046)

```
network connection | stats dc(dest_port) as ports by src_ip | where
ports>50
```

Severity: High | Confidence: Medium | FP Notes: Legit scanner / pentest

7. Outbound Data Threshold (T1041)

```
network bytes_out | stats sum(bytes) as total by src_ip | where
total>100000000
```

Severity: High | Confidence: Medium | FP Notes: Cloud backup / file sync

8. Cloud API Mass Reads (T1537)

```
GetObject | stats count by user | where count>500
```

Severity: High | Confidence: Medium | FP Notes: Admin bulk operation

9. Unusual Cloud Region Access (T1078)

```
cloud login | where region not in [AUTHORIZED_REGIONS]
```

Severity: Medium | Confidence: Medium | FP Notes: Travel or attacker

10. Suspicious Cloud Function Download (T1105)

```
http_request | where uri matches /(\.exe|\.bin)/
```

Severity: High | Confidence: Medium | FP Notes: Cloud C2 staging

11. Container Privileged Pod Creation (T1611)

```
pod created | where securityContext.privileged=true
```

Severity: High | Confidence: Medium | FP Notes: Escalation risk

12. New Container From Unknown Image (T1610)

```
container start | where image !matches /(approved1|approved2)/
```

Severity: High | Confidence: Medium | FP Notes: Suspicious image

13. IAM Policy Change (T1098)

```
policy updated | where change_type matches /(admin|full_access)/
```

Severity: High | Confidence: Medium | FP Notes: Privilege escalation

14. Logging Disabled in Cloud (T1562.008)

```
logging disabled
```

Severity: High | Confidence: High | FP Notes: Evading detection

15. API Key Use From New IP (T1528)

```
api key used | stats dc(src_ip) as ip_count by key | where ip_count>1
```

Severity: Medium | Confidence: Medium | FP Notes: Admin / devops

16. Suspicious Email Forwarding Rules (T1098)

```
email rule created | where action matches /(forward|redirect)/
```

Severity: Medium | Confidence: Medium | FP Notes: Insider / misconfig

17. Multiple Failed Logins After New Account Creation (T1110)

```
_failed login | join user created on user | stats count by user | where
count>5
```

Severity: High | Confidence: Medium | FP Notes: Attack simulation

18. Service Account Interactive Login (T1078)

```
login success | where account_type="service"
```

Severity: High | Confidence: Medium | FP Notes: Suspicious

19. Concurrent Sessions Same User (T1078)

```
login success | stats dc(src_ip) as ip_count by user | where ip_count>3
```

Severity: Medium | Confidence: Medium | FP Notes: VPN usage

20. Login From Blacklisted IP (T1078)

```
login success | where src_ip in [THREAT_INTEL_IPS]
```

Severity: High | Confidence: High | FP Notes: Known threat

INSIDER THREAT & DATA LOSS

1. Sensitive File Download (T1537)

```
file access | where path matches /(confidential|financial|PII)/i | stats
count by user,path
```

Severity: High | Confidence: Medium | FP Notes: Legit work

2. Bulk Data Download (T1537)

```
file access | stats count by user | where count>1000
```

Severity: High | Confidence: Medium | FP Notes: Backup or migration

3. Unusual USB Device (T1091)

```
device connection | where device_type='usb' | stats count by user,device
```

Severity: Medium | Confidence: Medium | FP Notes: Legit admin devices

4. File Permission Change (T1070.006)

```
file modified | where permission changes match /(chmod|chown)/i
```

Severity: Medium | Confidence: Medium | FP Notes: Admin updates

5. Cloud Storage Download From New IP (T1537)

```
cloud storage access | where src_ip not in [AUTHORIZED_IPS]
```

Severity: High | Confidence: Medium | FP Notes: Travel / VPN

6. Mass Email Forwarding Rule (T1098)

```
email rule created | where action matches /forward/i
```

Severity: Medium | Confidence: Medium | FP Notes: Insider attempt

7. Data Exfil via HTTP POST (T1041)

```
http_request | where method='POST' and bytes_out>10000000
```

Severity: High | Confidence: Medium | FP Notes: Cloud backup possible

8. External Drive Copy Detected (T1091)

```
file copy | where dest_device_type='usb'
```

Severity: Medium | Confidence: Medium | FP Notes: Legit backup

9. Archive File Creation (T1560.001)

```
file created | where extension in (".zip", ".rar", ".7z") | stats count by
user,path
```

Severity: Medium | Confidence: Medium | FP Notes: Admin packaging

10. Suspicious Cloud API Delete (T1485)

```
cloud api call | where action='DeleteObject' | stats count by user,bucket
```

Severity: High | Confidence: Medium | FP Notes: Admin purge

11. Privilege Escalation Attempt (T1068)

```
policy updated | where change_type matches /role|privilege/i
```

Severity: High | Confidence: Medium | FP Notes: Legit role updates

12. Login During Non-Working Hours (T1078)

```
login success | where hour < 6 OR hour > 22
```

Severity: Medium | Confidence: Medium | FP Notes: Shift work

13. Access to Rare Resources (T1087)

```
file access | where path not in [COMMON_PATHS]
```

Severity: Medium | Confidence: Medium | FP Notes: Rare resource use

14. Suspicious Command Execution (T1059)

```
process | where command matches /(net user|net localgroup)/i
```

Severity: Medium | Confidence: Medium | FP Notes: Admin commands

15. Data Exfil via Email Attachment (T1041)

```
email sent | where attachment_size>10000000
```

Severity: High | Confidence: Medium | FP Notes: Large attachments possible

16. Deleted Sensitive File (T1070.004)

```
file deleted | where path matches /(confidential|financial)/i
```

Severity: High | Confidence: Medium | FP Notes: Admin cleanup

17. Shadow Copy Deleted (T1490)

```
vssadmin delete shadows
```

Severity: Critical | Confidence: High | FP Notes: Ransomware activity

18. Abnormal File Copy (T1030)

```
file copy | stats count by user | where count>500
```

Severity: High | Confidence: Medium | FP Notes: Bulk operation

19. Email Rule Modification (T1098)

```
email rule modified | where action matches /(forward|redirect)/
```

Severity: Medium | Confidence: Medium | FP Notes: Insider attempt

20. Cloud IAM Role Change (T1098)

```
cloud policy updated | where role matches /(admin|full_access)/
```

Severity: High | Confidence: Medium | FP Notes: Privilege escalation

---

RANSOMWARE / MALWARE BEHAVIOR

1. Unusual File Encryption Activity (T1486)

```
file modified | where extension in (".docx", ".xlsx", ".pdf") and
modification_pattern='encrypt'
```

Severity: Critical | Confidence: High | FP Notes: Possible ransomware

2. Multiple Shadow Copy Deletion (T1490)

```
vssadmin delete shadows | stats count by user | where count>1
```

Severity: Critical | Confidence: High | FP Notes: Ransomware behavior

3. Unexpected Process Spawn (T1059)

```
process | where parent_process in [SYSTEM, SERVICES] and command matches /
(powershell|cmd)/i
```

Severity: High | Confidence: Medium | FP Notes: Suspicious execution

4. Mass File Rename (T1486)

```
file rename | stats count by user,path | where count>100
```

Severity: Critical | Confidence: High | FP Notes: Ransomware indicator

5. Office Macro Execution (T1059.003)

```
process | where command matches /excel|winword/ and macro_enabled=true
```

Severity: High | Confidence: Medium | FP Notes: Phishing delivery

6. Suspicious Registry Key for Malware (T1547.001)

```
registry | where key matches /Software\\Microsoft\\Windows\\CurrentVersion\
\Run/ and value matches /(malware|suspicious)/i
```

Severity: High | Confidence: Medium | FP Notes: Persistence attempt

7. Ransom Note Creation (T1486)

```
file created | where content matches /DECRYPT_INSTRUCTIONS/i
```

Severity: Critical | Confidence: High | FP Notes: Ransomware

8. Abnormal CPU Usage (T1499)

```
process cpu_usage | stats avg(cpu) by process | where avg(cpu)>80
```

Severity: Medium | Confidence: Medium | FP Notes: Legit load possible

9. Suspicious Network Beaconing (T1071.001)

```
network connection | stats count by dest_ip,src_ip | where count>50
```

Severity: High | Confidence: Medium | FP Notes: Malware C2

10. Process Renaming to System Name (T1036)

```
process | where name matches /(svchost|explorer)/ and original_name != name
```

Severity: High | Confidence: Medium | FP Notes: Masquerading

11. File Deletion Flood (T1070)

```
file deleted | stats count by user | where count>1000
```

Severity: Critical | Confidence: Medium | FP Notes: Ransomware / Cleanup

12. Malware Dropped Executable (T1204)

```
file created | where extension in (".exe", ".dll") and source_path in
[TEMP_DIRS]
```

Severity: High | Confidence: Medium | FP Notes: Malware staging

13. Registry Persistence Modification (T1547)

```
registry | where key matches /(RunOnce|Run)/ and value matches /(malware)/i
```

Severity: High | Confidence: Medium | FP Notes: Malware persistence

14. Suspicious Service Creation (T1543)

```
service | where name matches /(malware|suspicious)/i
```

Severity: High | Confidence: Medium | FP Notes: Malware persistence

15. Abnormal Outbound Connections (T1041)

```
network bytes_out | stats sum(bytes) as total by dest_ip | where
total>50000000
```

Severity: High | Confidence: Medium | FP Notes: Data exfil

16. Mass Archive Creation (T1560.001)

```
file created | where extension in (".zip", ".rar") | stats count by user |
where count>50
```

Severity: Medium | Confidence: Medium | FP Notes: Packaging for exfil

17. Suspicious Script Execution (T1059)

```
process | where command matches /(powershell|cmd|vbs)/i and path in
[TEMP_DIRS]
```

Severity: High | Confidence: Medium | FP Notes: Malware execution

18. Encryption Tool Execution (T1486)

```
process | where name matches /(encrypt|crypt)/i
```

Severity: Critical | Confidence: High | FP Notes: Ransomware

19. Unusual Task Creation (T1053)

```
scheduled task created | where name matches /(update|service)/i
```

Severity: Medium | Confidence: Medium | FP Notes: Malware persistence