# 35 Use Cases

splunk>

# SIEM

## *to reduce False Postives*

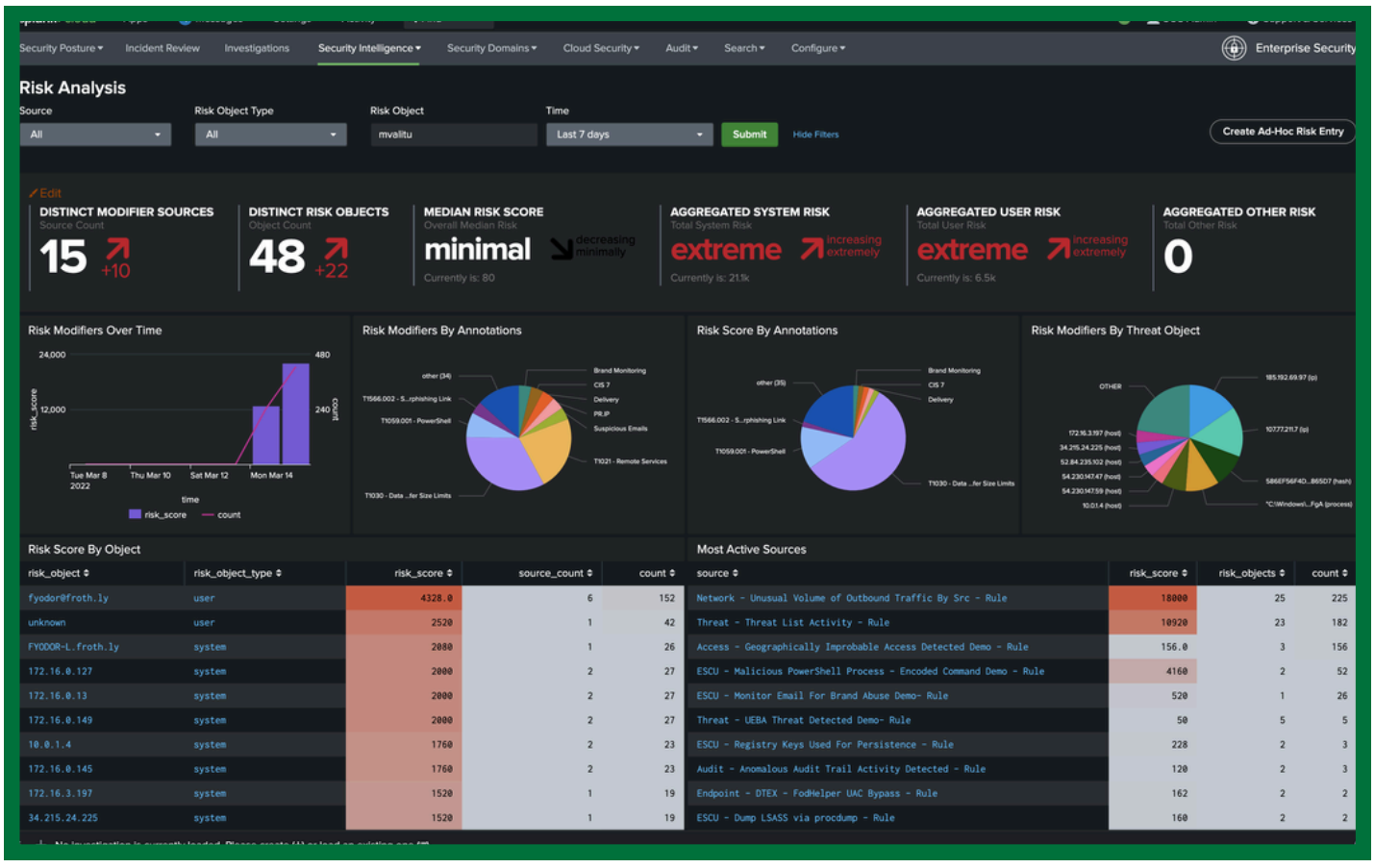
Rajneesh Gupta
Cybersecurity Expert

# TABLE OF CONTENT

# WHAT IS SPLUNK?

Splunk is a data platform primarily used for searching, monitoring, and analyzing machine-generated big data in real-time.

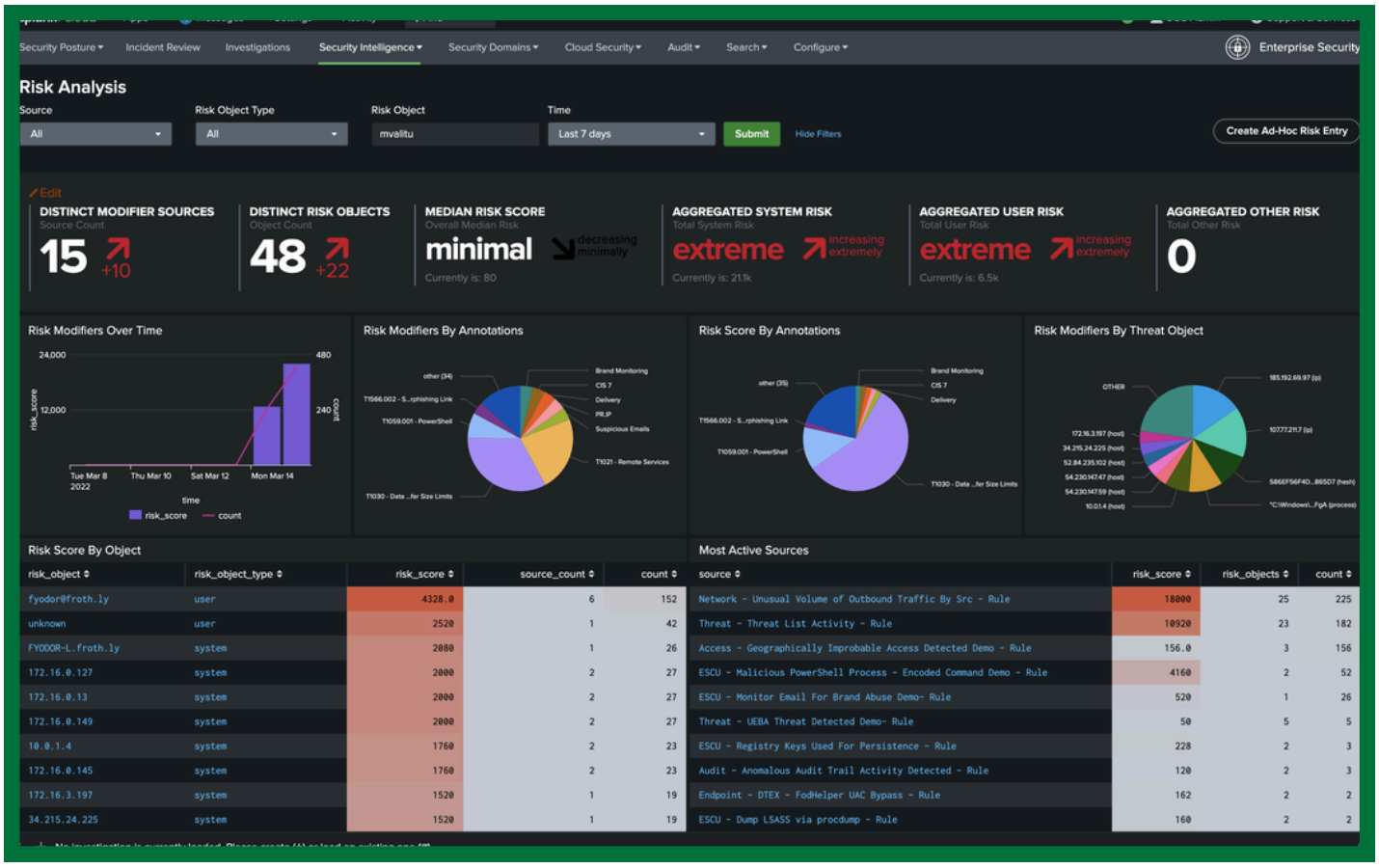
- Data Collection and Indexing: Aggregates logs and metrics from various sources, including servers, devices, applications, and network systems.
- Search and Analysis: Allows users to search, visualize, and analyze data to gain insights and identify trends or issues.
- Real-Time Monitoring and Alerts: Enables real-time monitoring of data with customizable alerts to respond quickly to critical events.



# SPLUNK FOR SECURITY

A comprehensive solution that helps organizations detect, analyze, and respond to security incidents efficiently..

- Security Monitoring: Provides real-time visibility into security events across the organization.
- Incident Management: Streamlines the investigation and resolution of security incidents.
- Compliance: Supports regulatory compliance with detailed logs and audit trails.
- Advanced Threat Detection: Uses analytics to identify sophisticated threats and anomalies.
- Threat Hunting: Empowers proactive threat discovery by enabling deep data exploration.




| risk_object | risk_object_type | risk_score | source_count | count |
|---|---|---|---|---|
| fyodor@froth.ly | user | 4328.0 | 6 | 152 |
| unknown | user | 2520 | 1 | 42 |
| FYODOR-L.froth.ly | system | 2080 | 1 | 26 |
| 172.16.0.127 | system | 2000 | 2 | 27 |
| 172.16.0.13 | system | 2000 | 2 | 27 |
| 172.16.0.149 | system | 2000 | 2 | 27 |
| 10.0.1.4 | system | 1760 | 2 | 23 |
| 172.16.0.145 | system | 1760 | 2 | 23 |
| 172.16.3.197 | system | 1520 | 1 | 19 |
| 34.215.24.225 | system | 1520 | 1 | 19 |

| source | risk_score | risk_objects | count |
|---|---|---|---|
| Network - Unusual Volume of Outbound Traffic By Src - Rule | 18000 | 25 | 225 |
| Threat - Threat List Activity - Rule | 10920 | 23 | 182 |
| Access - Geographically Improbable Access Detected Demo - Rule | 156.0 | 3 | 156 |
| ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule | 4160 | 2 | 52 |
| ESCU - Monitor Email For Brand Abuse Demo- Rule | 520 | 1 | 26 |
| Threat - UEBA Threat Detected Demo- Rule | 50 | 5 | 5 |
| ESCU - Registry Keys Used For Persistence - Rule | 228 | 2 | 3 |
| Audit - Anomalous Audit Trail Activity Detected - Rule | 120 | 2 | 3 |
| Endpoint - DTEX - FodHelper UAC Bypass - Rule | 162 | 2 | 2 |
| ESCU - Dump LSASS via procdump - Rule | 160 | 2 | 2 |

# SPLUNK QUERY

The Splunk Processing Language (SPL) is a powerful query language used to search, analyze, and manipulate data within Splunk.

- Search and Filter Data: Allows users to retrieve and filter specific data from large datasets.
- Statistical Analysis: Performs calculations, aggregations, and statistical analysis on indexed data.
- Data Visualization: Creates charts, graphs, and dashboards for insights and trend analysis.

## *Example query*

```
index="web_logs" | stats count by status_code
```

## *Purpose*

This query searches the web_logs index and counts the occurrences of each HTTP status code, helping to quickly identify the frequency of errors or successful responses in web traffic.

# WHAT IS FALSE POSITIVE?

**False Positive: An alert that mistakenly flags benign activity as a threat, leading to unnecessary investigations.**

## *Example query*

```
index="web_logs" status_code!=200 status_code!=301
| stats count by status_code
```

## *Purpose*

**This query searches the web_logs index and counts the occurrences of each HTTP status code, helping to quickly identify the frequency of errors or successful responses in web traffic.**

# 35 USE CASES OF SPLUNK SIEM TO REDUCE FALSE POSITIVES

NEXT

# 1

# BRUTE FORCE ATTACK DETECTION ON WINDOWS SYSTEMS

## *Goal*

**Identify brute force login attempts by monitoring repeated failed login events within a short period, adjusting thresholds to reduce false positives from user error or network latency.**

## *Detection Rule*

```
index="web_logs" status_code!=200 status_code!=301
| stats count by status_code
```

## *Outcome*

**Excludes routine status codes (200, 301) to reduce noise and focus on potential issues.**

2

# SUSPICIOUS EMAIL ATTACHMENTS DETECTION IN PROOFPOINT

## *Goal*

**Detect emails with potentially malicious attachments using Proofpoint logs and filter out known safe file types.**

## *Detection Rule*

```
index="proofpoint" sourcetype="pp:attachment"
| where attachment_malicious="true" AND NOT
(file_extension IN ("pdf", "docx", "xlsx"))
```

## *Outcome*

**Flags emails with attachments that are likely malicious and have suspicious file types, reducing false positives from commonly used safe file types.**

3

# UNAUTHORIZED IAM ROLE CHANGE IN AWS CLOUDTRAIL

## *Goal*

**Monitor unauthorized changes to IAM roles to prevent privilege escalation, excluding expected changes from trusted service accounts.**

## *Detection Rule*

```
index="aws-cloudtrail" eventName="UpdateRole"
| where NOT userIdentity.arn IN
("arn:aws:iam::123456789012:role/TrustedRole")
```

## *Outcome*

**Detects suspicious role modifications only from unexpected sources, reducing false positives from known maintenance or automation accounts.**

4

# UNUSUAL FILE DELETION ON WINDOWS SERVERS

## *Goal*

**Detect suspicious file deletions on critical Windows directories while filtering out regular maintenance events.**

## *Detection Rule*

```
index="wineventlog" EventCode=4663 ObjectType="File"
| where Object_Name LIKE "%critical_directory%" AND
Access_Mask="DELETE"
| stats count by User, Computer
| where count > 3
```

## *Outcome*

**Alerts when more than three file deletions occur in critical directories by the same user within an hour, minimizing false positives from typical user actions.**

5

# HIGH DATA TRANSFER TO EXTERNAL IPS IN CLOUD ENVIRONMENT

## *Goal*

**Detect potentially unauthorized data exfiltration by monitoring high data transfer to unknown IP addresses outside the organization.**

## *Detection Rule*

```
index="cloud-traffic" direction="outbound"
| stats sum(bytes_sent) as total_data by dest_ip
| where total_data > 50000000 AND NOT dest_ip IN
("trusted_ip1", "trusted_ip2")
```

## *Outcome*

**Identifies large data transfers to untrusted IPs, reducing false positives by excluding known, trusted destinations.**

6

# SUSPICIOUS COMMAND EXECUTION IN WINDOWS SYSMON

## *Goal*

**Detect execution of potentially malicious commands on Windows systems, filtering out legitimate administrative actions.**

## *Detection Rule*

```
index="sysmon" EventID=1
| search CommandLine IN ("*powershell* -enc*",
"*cmd.exe /c*")
| where NOT Account_Name IN ("admin_user1",
"admin_user2")
```

## *Outcome*

**Flags unusual command-line usage while excluding expected administrative accounts, reducing noise from legitimate actions.**

7

# EXCESSIVE FAILED EMAIL LOGINS IN PROOFPOINT

## *Goal*

**Identify potential account compromise attempts by tracking repeated failed email login attempts.**

## *Detection Rule*

```
index="proofpoint" sourcetype="pp:login"
| stats count by user, src_ip
| where count > 10 AND status="failed"
```

## *Outcome*

**Detects high-volume failed login attempts to email accounts, with thresholds to avoid alerts from typical user errors.**

8

# ABNORMAL CPU USAGE ON CLOUD VM

## *Goal*

**Identify potential cryptocurrency mining or malware infection by monitoring unusual CPU spikes in cloud VMs.**

## *Detection Rule*

```
index="cloud-metrics" metric_name="cpu_usage"
| stats avg(cpu) as avg_cpu by host
| where avg_cpu > 90
```

## *Outcome*

**Flags VMs with unusually high CPU usage, potentially indicating malicious processes while reducing false positives by focusing on high averages.**

9

# C2 COMMUNICATION DETECTION IN SURICATA IDS

## *Goal*

**Identify Command and Control (C2) traffic by monitoring connections to suspicious domains or IPs flagged by Suricata, excluding known safe domains.**

## *Detection Rule*

```
index="suricata" event_type="alert"
| search dest_ip IN ("known_c2_ip1", "known_c2_ip2")
| where NOT dest_domain IN ("safe_domain1.com",
"safe_domain2.com")
```

## *Outcome*

**Detects suspected C2 traffic while excluding known safe domains, reducing unnecessary alerts.**

10

# MULTIPLE FILE ACCESS FAILURES ON WINDOWS SHARES

## *Goal*

**Identify possible unauthorized attempts to access sensitive files by tracking repeated access failures on shared directories.**

## *Detection Rule*

```
index="wineventlog" EventCode=4663
Access_Mask="0x2"
| stats count by Object_Name, Account_Name
| where count > 5
```

## *Outcome*

**Triggers alerts when more than five access failures occur on sensitive files, minimizing false positives by focusing on excessive failures.**

11

# SUSPICIOUS OUTBOUND NETWORK ACTIVITY FROM CROWDSTRIKE EDR

## *Goal*

**Identify potentially malicious outbound connections by monitoring unusual network activity flagged by CrowdStrike, excluding known safe applications.**

## *Detection Rule*

```
index="crowdstrike" event_type="network_activity"
direction="outbound"
| where NOT process_name IN ("chrome.exe",
"outlook.exe")
```

## *Outcome*

**Detects unusual outbound connections by unknown processes, reducing noise by filtering out known, legitimate applications.**

# 12

# UNAUTHORIZED ACCESS TO CRITICAL DATABASES

## *Goal*

**Monitor unexpected access to critical databases to identify potential insider threats or unauthorized access attempts.**

## *Detection Rule*

```
index="db-logs" event_type="login"
| where database_name="critical_db" AND user NOT IN
("db_admin1", "db_admin2")
```

## *Outcome*

**Flags unauthorized login attempts to sensitive databases, reducing alerts by excluding expected administrative users.**

13

# DETECTION OF LARGE EMAIL ATTACHMENTS WITH SUSPICIOUS CONTENT

## *Goal*

**Identify potential data exfiltration or phishing attempts by monitoring large email attachments flagged as suspicious.**

## *Detection Rule*

```
index="proofpoint" sourcetype="pp:email"
| where attachment_size > 10485760 AND
attachment_malicious="true"
```

## *Outcome*

**Detects suspicious large email attachments, reducing false positives by filtering for both size and malicious indicators.**

14

# MONITORING FOR ANOMALOUS NETWORK SCANNING BEHAVIOR

## *Goal*

**Detect potential recon activity by monitoring for IPs performing a high number of port scans, filtering known vulnerability scanners.**

## *Detection Rule*

```
index="network-traffic" event="port_scan"
| stats count by src_ip
| where count > 50 AND NOT src_ip IN
("trusted_scanner_ip")
```

## *Outcome*

**Alerts on scanning behavior, reducing noise by excluding trusted network scanners.**

# 15

# SUSPICIOUS POWERSHELL COMMANDS WITH BASE64 ENCODING

## *Goal*

**Detect potential obfuscation or malware execution through PowerShell commands with encoded payloads.**

## *Detection Rule*

```
index="wineventlog" EventCode=4104
| where CommandLine IN ("* -enc *")
| stats count by User, Computer
```

## *Outcome*

**Flags encoded PowerShell commands, reducing false positives by focusing on encoding indicators.**

16

# UNUSUAL NETWORK ACTIVITY IN SURICATA FOR INTERNAL HOSTS

## *Goal*

**Detect internal hosts generating unusual traffic patterns consistent with malware or botnet activity, excluding known backup or scanning IPs.**

## *Detection Rule*

```
index="suricata" event_type="network"
| stats count by src_ip
| where count > 100 AND NOT src_ip IN ("backup_ip",
"scanner_ip")
```

## *Outcome*

**Flags suspicious network patterns from internal hosts, reducing false positives from known sources.**

17

# EXCESSIVE FILE DOWNLOADS FROM CLOUD STORAGE

## *Goal*

**Identify potential data exfiltration by monitoring unusual bulk downloads from cloud storage services.**

## *Detection Rule*

```
index="cloud-storage-logs" action="download"
| stats count by user, bucket
| where count > 100 AND NOT user IN ("backup_service",
"trusted_user")
```

## *Outcome*

**Detects high-volume downloads, filtering out trusted services and regular backup activities to minimize false positives.**

# 18

# EXMULTIPLE FAILED LOGIN ATTEMPTS ON CRITICAL DATABASESCESSIVE FILE DOWNLOADS FROM CLOUD STORAGE

## *Goal*

**Detect potential brute force attempts on database logins.**

## *Detection Rule*

```
index="db-logs" action="failed_login"
| stats count by user, db_name
| where count > 5 AND db_name="critical_db"
```

## *Outcome*

**Flags accounts with more than five failed login attempts on critical databases, reducing noise by focusing on high-value assets.**

19

# DETECTION OF UNUSUAL SERVICE STARTUP IN WINDOWS SERVERS

## *Goal*

**Identify malicious persistence by monitoring unusual service startups on Windows servers.**

## *Detection Rule*

```
index="wineventlog" EventCode=7045
| where NOT Service_Name IN ("expected_service1",
"expected_service2")
```

## *Outcome*

**Flags startup of unexpected services, excluding known and safe services to avoid false positives.**

20

# LARGE VOLUME OF OUTBOUND DNS REQUESTS FROM A SINGLE HOST

## *Goal*

**Detect potential data exfiltration or tunneling by monitoring high volumes of DNS requests from a single host.**

## *Detection Rule*

```
index="dns-logs"
| stats count by src_ip
| where count > 1000 AND NOT src_ip IN
("trusted_dns_ip")
```

## *Outcome*

**Detects unusually high DNS query volume, excluding known DNS servers to reduce noise.**

21

# ANOMALOUS PRIVILEGED COMMAND EXECUTION ON LINUX SERVERS

## *Goal*

**Detect potential abuse of sudo commands by monitoring unusual privileged commands on Linux.**

## *Detection Rule*

```
index="linux-logs" command="sudo"
| where Command IN ("*netcat*", "*nc*", "*nmap*")
```

## *Outcome*

**Flags potentially dangerous commands executed with sudo privileges, focusing on network-related tools to avoid false positives.**

22

# UNUSUAL DATA TRANSFER IN AWS CLOUD INFRASTRUCTURE

## *Goal*

**Identify abnormal data transfer volumes to external IP addresses in AWS, excluding trusted endpoints.**

## *Detection Rule*

```
index="aws-logs" action="Transfer"
| stats sum(bytes) as total_bytes by dest_ip
| where total_bytes > 50000000 AND NOT dest_ip IN
("trusted_ip1", "trusted_ip2")
```

## *Outcome*

**Flags large outbound data transfers to unknown IPs, reducing false positives by filtering trusted destinations.**

# 23

# UNAUTHORIZED ACCESS TO S3 BUCKETS

## *Goal*

**Detect potential unauthorized access attempts to sensitive S3 buckets in AWS.**

## *Detection Rule*

```
index="aws-s3" eventName="GetObject" OR
eventName="PutObject"
| where bucket_name IN ("sensitive_bucket") AND user
NOT IN ("trusted_user1", "trusted_user2")
```

## *Outcome*

**Alerts on access to sensitive S3 buckets by unknown users, reducing alerts from trusted users.**

# 24

# SUSPICIOUS BROWSER ACTIVITY INDICATING PHISHING

## *Goal*

**Identify potential phishing activity by monitoring access to known phishing domains.**

## *Detection Rule*

```
index="proxy-logs" action="browse"
| search dest_domain IN
("known_phishing_domain1.com",
"known_phishing_domain2.com")
```

## *Outcome*

**Detects access to known phishing sites, with a rule based on threat intelligence sources.**

25

# MULTIPLE FAILED FILE ACCESS ATTEMPTS ON LINUX SHARES

## *Goal*

**Monitor suspicious activity by tracking failed access attempts on shared Linux directories.**

## *Detection Rule*

```
index="linux-logs" event_type="file_access_failed"
| stats count by user, file_path
| where count > 5
```

## *Outcome*

**Alerts on repeated failed file access attempts, indicating possible unauthorized access attempts.**

26

# DETECTION OF EXECUTABLE FILES IN EMAIL ATTACHMENTS (PROOFPOINT)

## *Goal*

**Identify potentially malicious emails by detecting executable file attachments.**

## *Detection Rule*

```
index="proofpoint" sourcetype="pp:email"
| where attachment_file_type="exe"
```

## *Outcome*

**Flags emails containing executable attachments, which are more likely to be malicious.**

27

# EXCESSIVE PRIVILEGE ESCALATION ATTEMPTS ON WINDOWS SYSTEMS

## *Goal*

**Detect suspicious privilege escalation by monitoring repeated attempts to elevate privileges on Windows.**

## *Detection Rule*

```
index="wineventlog" EventCode=4674
| stats count by User
| where count > 3
```

## *Outcome*

**Flags users with multiple privilege escalation attempts, reducing noise by focusing on excessive attempts.**

# 28

# UNUSUAL COMMAND LINE ARGUMENTS IN LINUX PROCESSES

## *Goal*

**Detect suspicious processes with unexpected command-line arguments, which may indicate malicious activity.**

## *Detection Rule*

```
index="linux-logs" event="process_creation"
| where CommandLine IN ("*curl*", "*wget*")
| where NOT User IN ("safe_user")
```

## *Outcome*

**Flags processes with network-related commands, reducing false positives by excluding expected administrative users.**

# 28

# UNUSUAL COMMAND LINE ARGUMENTS IN LINUX PROCESSES

## *Goal*

**Detect suspicious processes with unexpected command-line arguments, which may indicate malicious activity.**

## *Detection Rule*

```
index="linux-logs" event="process_creation"
| where CommandLine IN ("*curl*", "*wget*")
| where NOT User IN ("safe_user")
```

## *Outcome*

**Flags processes with network-related commands, reducing false positives by excluding expected administrative users.**

29

# MULTIPLE ACCOUNT LOCKOUTS IN A SHORT PERIOD

## *Goal*

**Detect potential brute-force attacks or password spraying by monitoring frequent account lockouts.**

## *Detection Rule*

```
index="wineventlog" EventCode=4740
| stats count by Account_Name
| where count > 5
```

## *Outcome*

**Flags accounts that have been locked out multiple times, which may indicate a targeted attack.**

# 30

# SUSPICIOUS PORT SCANNING IN NETWORK TRAFFIC

## *Goal*

**Detect internal or external port scans by monitoring for unusual numbers of open port checks.**

## *Detection Rule*

```
index="network-traffic" event="port_scan"
| stats count by src_ip
| where count > 50
```

## *Outcome*

**Detects potential recon activity from IPs scanning multiple ports.**

31

# DETECTION OF MALWARE FILE HASHES IN CROWDSTRIKE EDR

## *Goal*

**Identify potential malware by matching file hashes from CrowdStrike with known malicious hashes.**

## *Detection Rule*

```
index="crowdstrike" event_type="file_event"
| where file_hash IN ("malicious_hash1",
"malicious_hash2")
```

## *Outcome*

**Flags files with hashes matching known malware, reducing noise by filtering safe files.**

# 32

# UNUSUAL USE OF ENCODING OR OBFUSCATION IN POWERSHELL COMMANDS

## *Goal*

**Detect potentially malicious PowerShell activity with obfuscation techniques.**

## *Detection Rule*

```
index="sysmon" EventID=4104
| search CommandLine IN ("* -enc *")
```

## *Outcome*

**Alerts on obfuscated PowerShell commands, typically associated with malicious activities.**

33

# DETECTION OF ANOMALOUS NETWORK TRAFFIC IN SURICATA IDS

## *Goal*

**Identify suspicious network traffic patterns from known attack vectors in Suricata.**

## *Detection Rule*

```
index="suricata" event_type="alert"
| search dest_ip IN ("suspicious_ip1", "suspicious_ip2")
```

## *Outcome*

**Detects connections to known malicious IPs, filtering out known safe connections.**

34

# TRACKING PRIVILEGED FILE ACCESS ATTEMPTS ON WINDOWS

## *Goal*

**Monitor sensitive file access by privileged users, excluding administrative operations.**

## *Detection Rule*

```
index="wineventlog" EventCode=4663
| where Object_Type="file" AND Access_Mask="Write" AND
Account_Name NOT IN ("admin_user")
```

## *Outcome*

**Flags sensitive file access, reducing false positives from known admin activity.**

35

# DETECTION OF RDP CONNECTIONS FROM EXTERNAL IPS

## *Goal*

**Identify unauthorized RDP connections from external sources, excluding known VPN or admin IPs.**

## *Detection Rule*

```
spl
Copy code
index="wineventlog" EventCode=4624 LogonType=10
| where src_ip NOT IN ("vpn_ip1", "vpn_ip2")
```

## *Outcome*

**Detects unauthorized RDP access, reducing noise by excluding legitimate remote access sources.**

# CONCLUSION

These 35 Splunk use cases demonstrate how powerful queries and customized alerts can enhance security monitoring, threat detection, and incident response.

- Real-Time Visibility: Splunk provides continuous, real-time monitoring across systems and networks.
- Threat Detection: Custom rules enable precise detection of suspicious behaviors and attack patterns.
- False Positive Reduction: Fine-tuning alerts helps minimize noise, allowing teams to focus on true threats.
- Incident Investigation: Correlation rules streamline investigations by linking related security events.
- Automation & Response: Integrations with other security tools support automated responses to critical events.
- Comprehensive Coverage: By addressing multiple sources, Splunk ensures thorough monitoring across the security landscape.

# Reach us at hi@haxsecurity.com

### Security Consulting

- Risk assessment
- Security Architecture
- SOC Set up

### Penetration testing

- Internal Pentest
- External Pentest
- Web App Pentest

### Training and Courses

- SOC Training
- Certification Training
- Vendor-specific learning

### Labs

- Hands-on Labs
- Career Path Labs
- Cyberrange for businesses