24 Use Cases

SPLUNK SIEM

for SOC 2 Compliance

Rajneesh Gupta
@rajneeshcyber

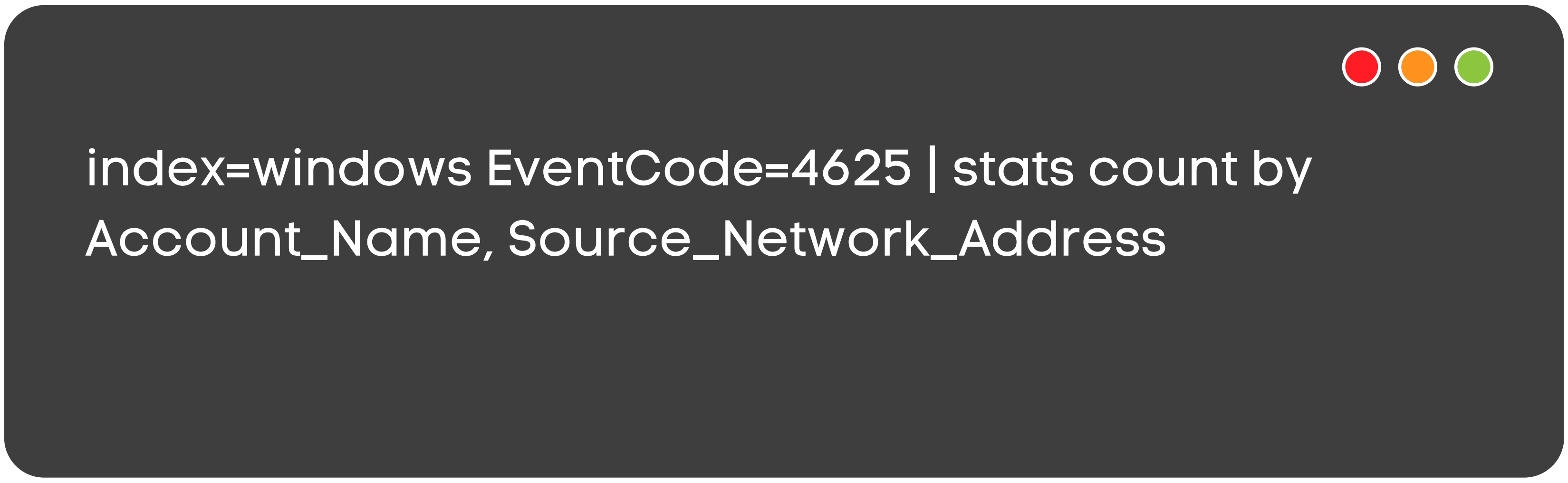
1

UNAUTHORIZED ACCESS ATTEMPTS

Purpose

Detect brute-force or unauthorized access attempts (SOC2 CC6.1 - Logical Access)

Example query



```
index=windows EventCode=4625 | stats count by
Account_Name, Source_Network_Address
```

Outcome

Identifies failed login attempts to accounts from various IP addresses. Helps detect potential brute-force attempts and prevent unauthorized access.

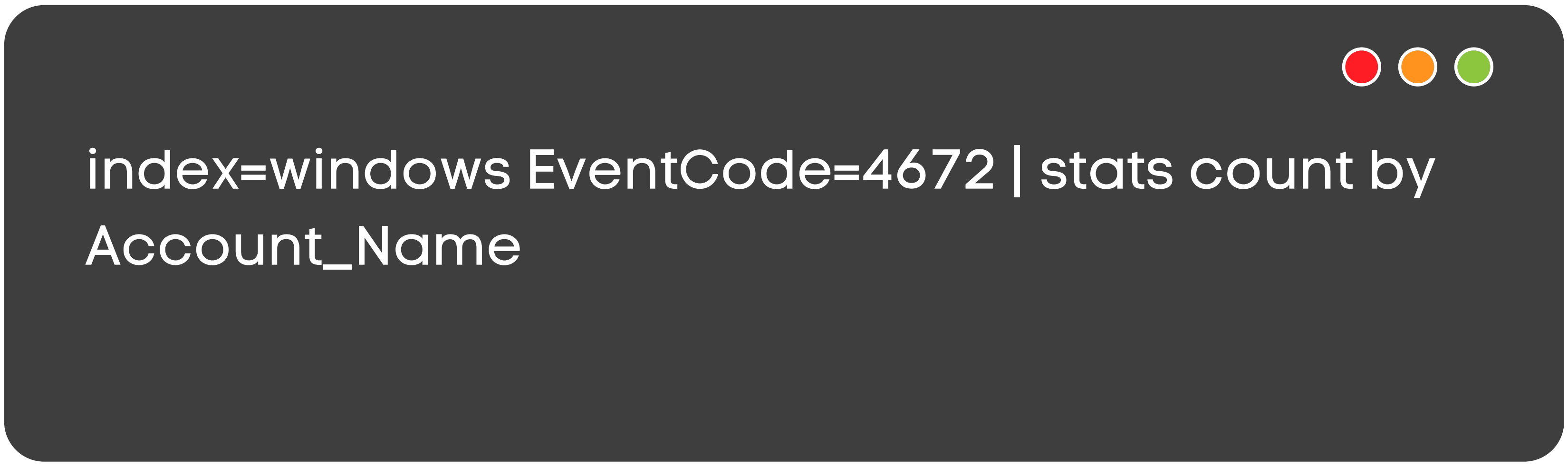
2

PRIVILEGE ESCALATION

Purpose

Monitor attempts to gain unauthorized administrative privileges (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4672 | stats count by
Account_Name
```

Outcome

Provides visibility into accounts assigned special privileges. Allows rapid detection of privilege escalation attempts.

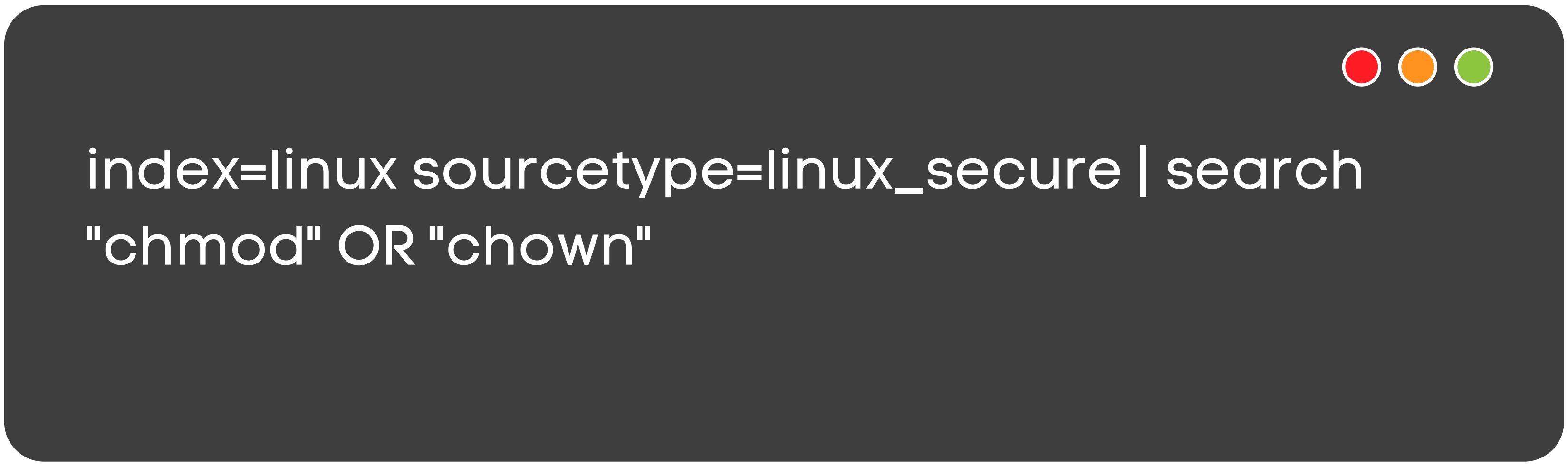
3

MONITORING FILE INTEGRITY

Purpose

Track file changes for sensitive files (SOC2 CC6.7 - System Operations).

Example query



```
index=linux sourcetype=linux_secure | search
"chmod" OR "chown"
```

Outcome

Monitors for any modifications to critical files or directories.
Detects unauthorized or suspicious file permission changes.

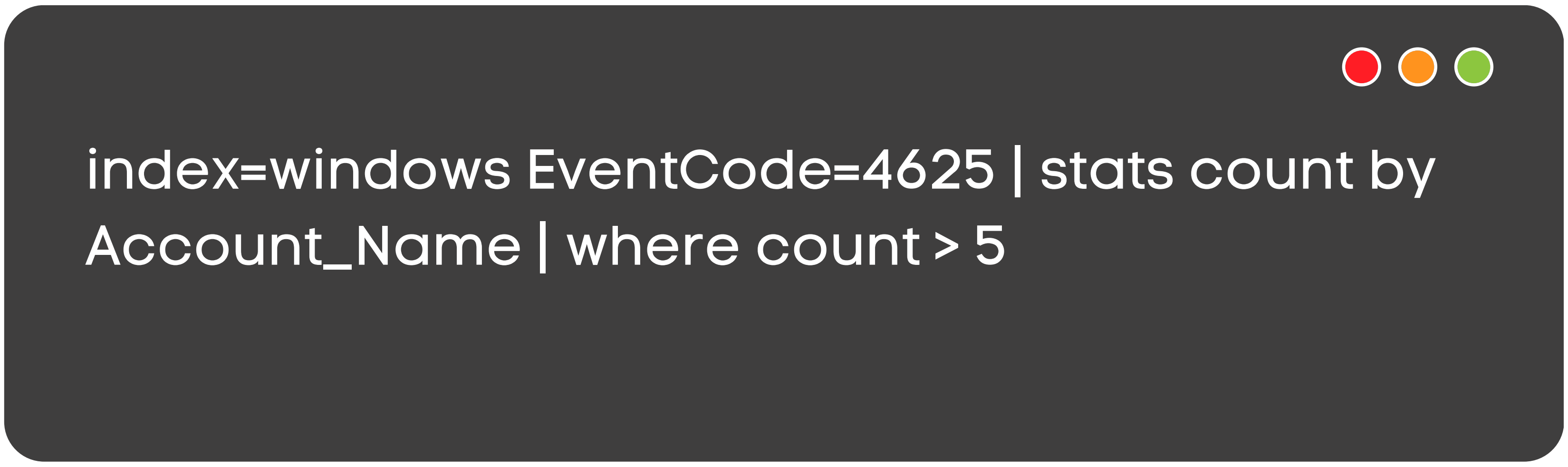
4

EXCESSIVE FAILED LOGINS

Purpose

Detect potential account lockout scenarios (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4625 | stats count by
Account_Name | where count > 5
```

Outcome

Identifies accounts with repeated failed login attempts that could lead to lockout. Helps detect potential password-guessing or brute-force attacks.

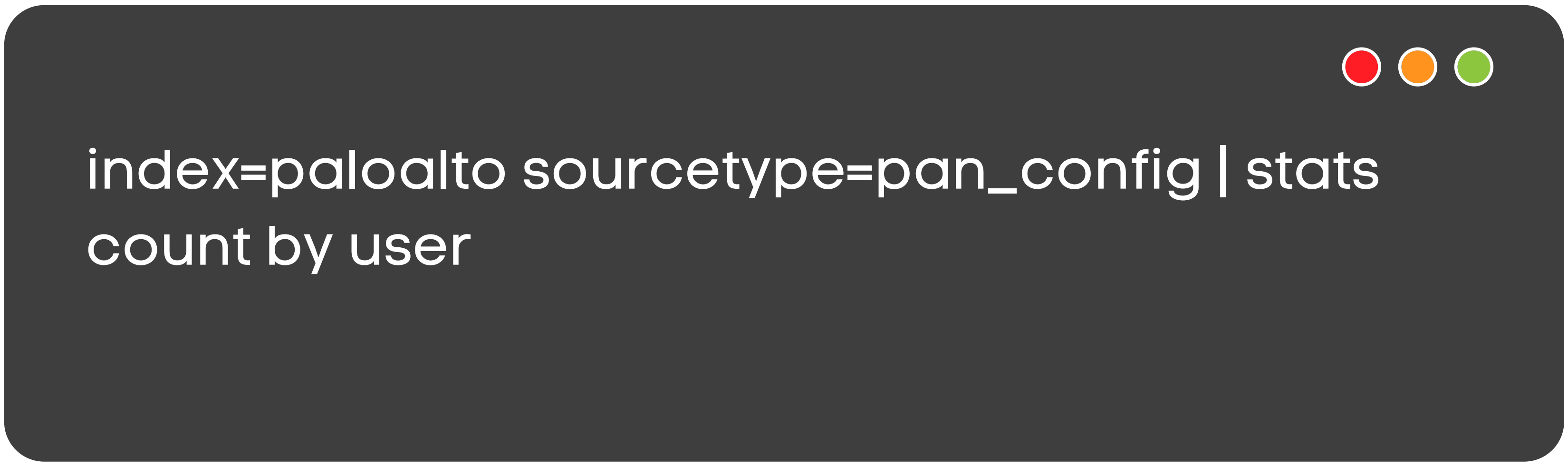
5

FIREWALL POLICY CHANGES

Purpose

Identify unauthorized firewall changes (SOC2 CC6.7 - System Operations).

Example query



```
index=paloalto sourcetype=pan_config | stats
count by user
```

Outcome

Provides a list of users making firewall policy changes. Detects unauthorized or unexpected modifications to firewall configurations.

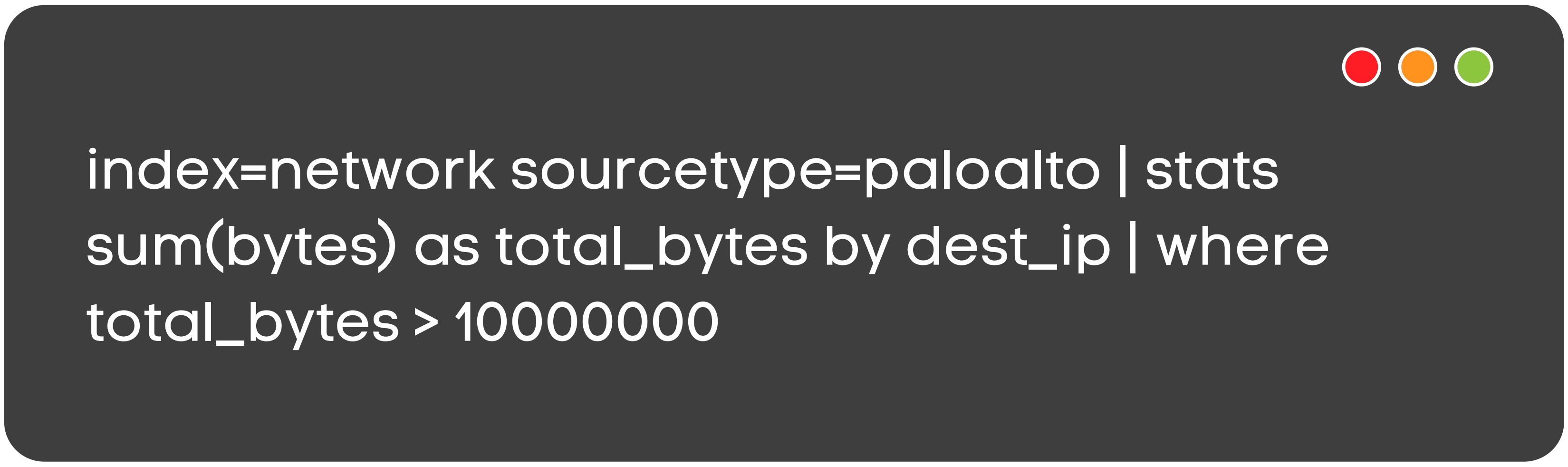
6

DATA EXFILTRATION DETECTION

Purpose

Detect large data transfers indicating possible data exfiltration (SOC2 CC6.7 - System Operations).

Example query



```
index=network sourcetype=paloalto | stats
sum(bytes) as total_bytes by dest_ip | where
total_bytes > 10000000
```

Outcome

Identifies external IPs receiving unusually large amounts of data. Helps detect potential data exfiltration activities.

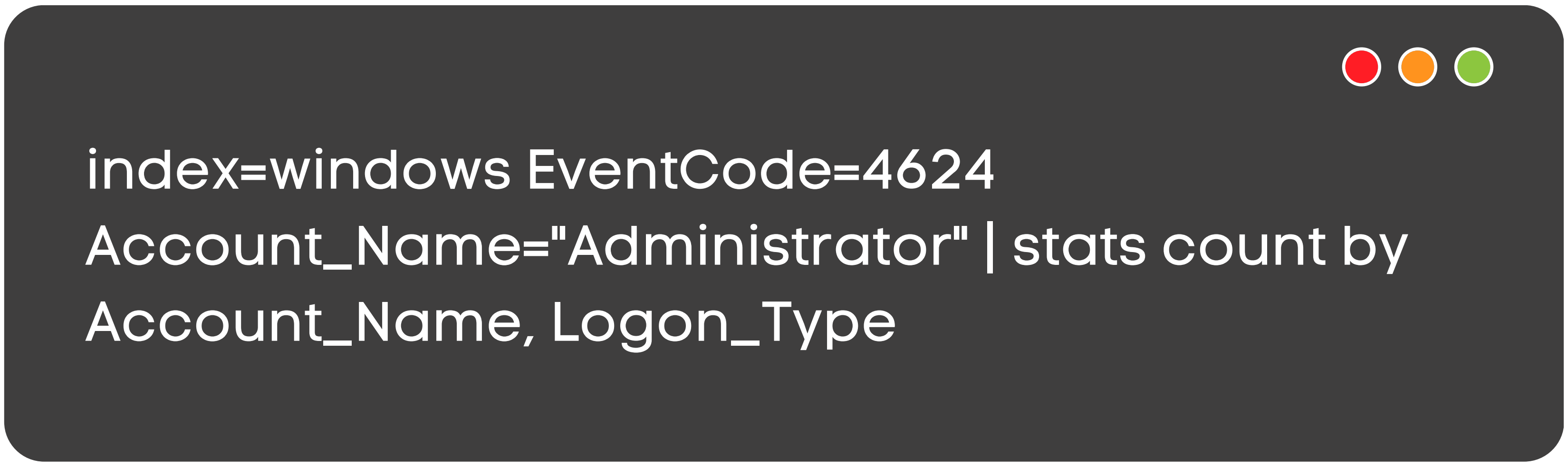
7

MONITORING ADMIN ACCOUNT USAGE

Purpose

Ensure admin accounts are used only when necessary (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4624
Account_Name="Administrator" | stats count by
Account_Name, Logon_Type
```

Outcome

Tracks usage of administrator accounts, monitoring login types. Detects unauthorized or inappropriate use of privileged accounts.

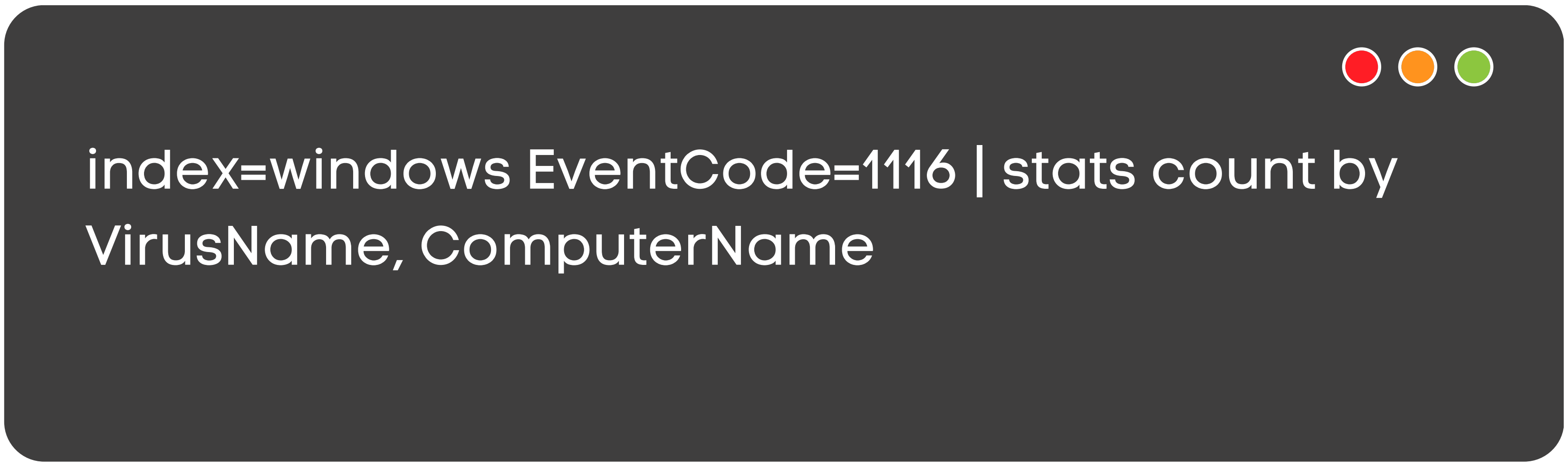
8

MALWARE DETECTION

Purpose

Detect malware infections across endpoints (SOC2 CC6.8 - Risk Mitigation).

Example query



```
index=windows EventCode=1116 | stats count by
VirusName, ComputerName
```

Outcome

Detects instances of malware across systems with relevant details. Enables quick identification of infected endpoints for remediation.

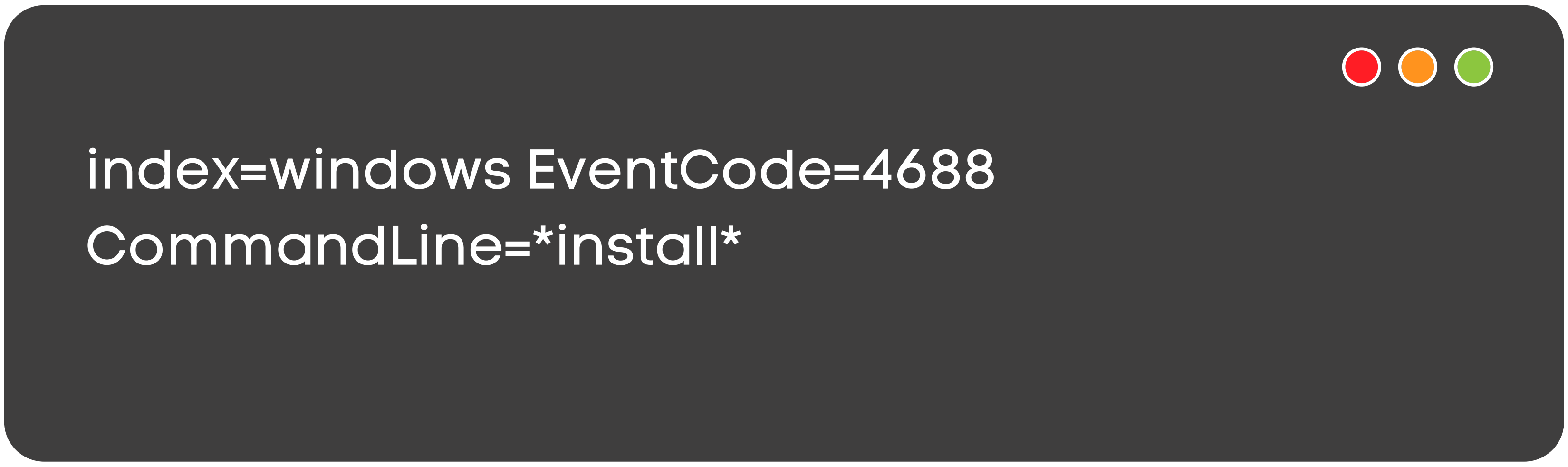
9

UNAUTHORIZED SOFTWARE INSTALLATION

Purpose

Track installation of unauthorized software (SOC2 CC6.7 - System Operations).

Example query



```
index=windows EventCode=4688
CommandLine=*install*
```

Outcome

Identifies unauthorized software installation commands on systems. Helps prevent installation of unapproved or malicious software.

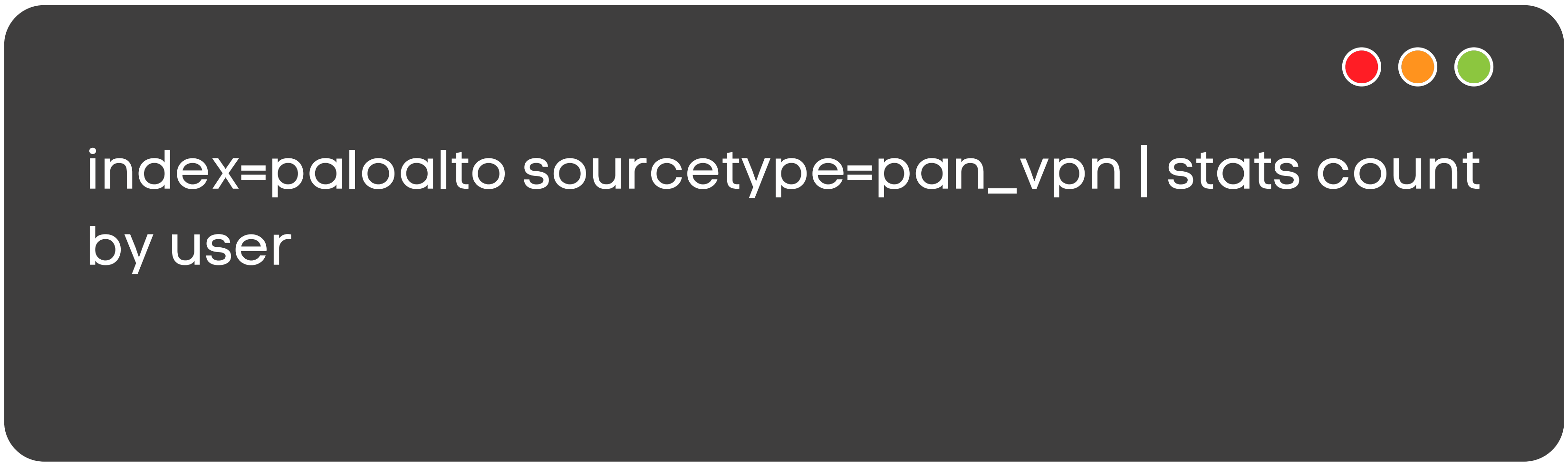
10

VPN ACCESS MONITORING

Purpose

Monitor VPN access to detect unauthorized connections (SOC2 CC6.1 - Logical Access).

Example query



```
index=paloalto sourcetype=pan_vpn | stats count by user
```

Outcome

Provides visibility into VPN connections by user. Detects unauthorized or unusual VPN logins to the network.

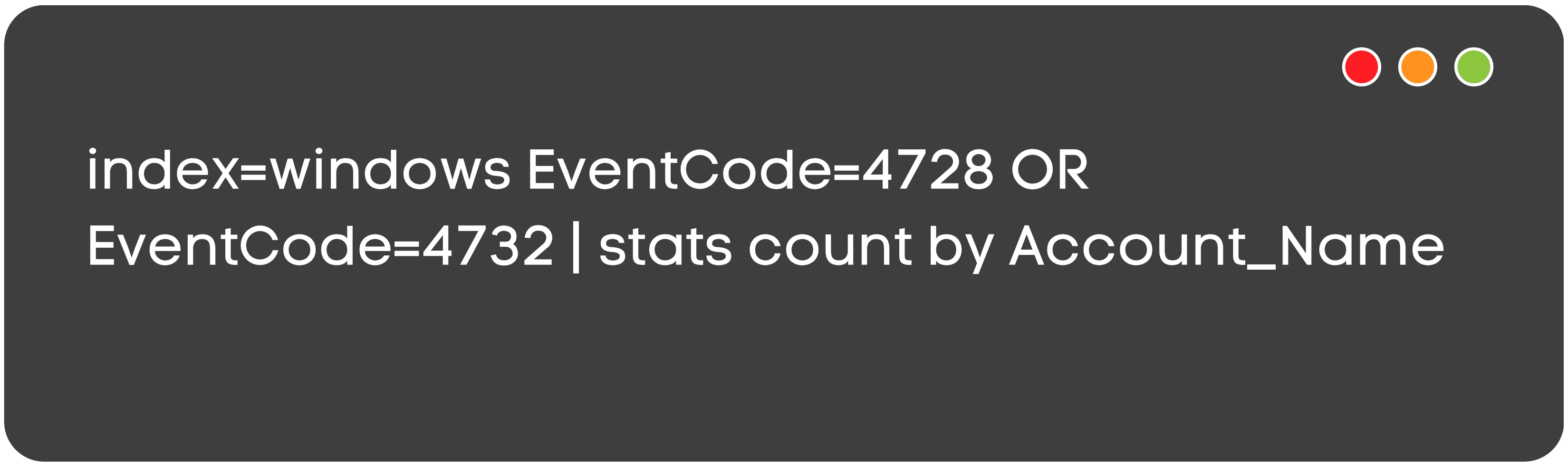
11

PRIVILEGED USER ACCOUNT ACTIVITY

Purpose

Monitor actions by privileged accounts (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4728 OR
EventCode=4732 | stats count by Account_Name
```

Outcome

Tracks changes in user group membership by privileged accounts. Helps detect misuse or escalation of privileges.

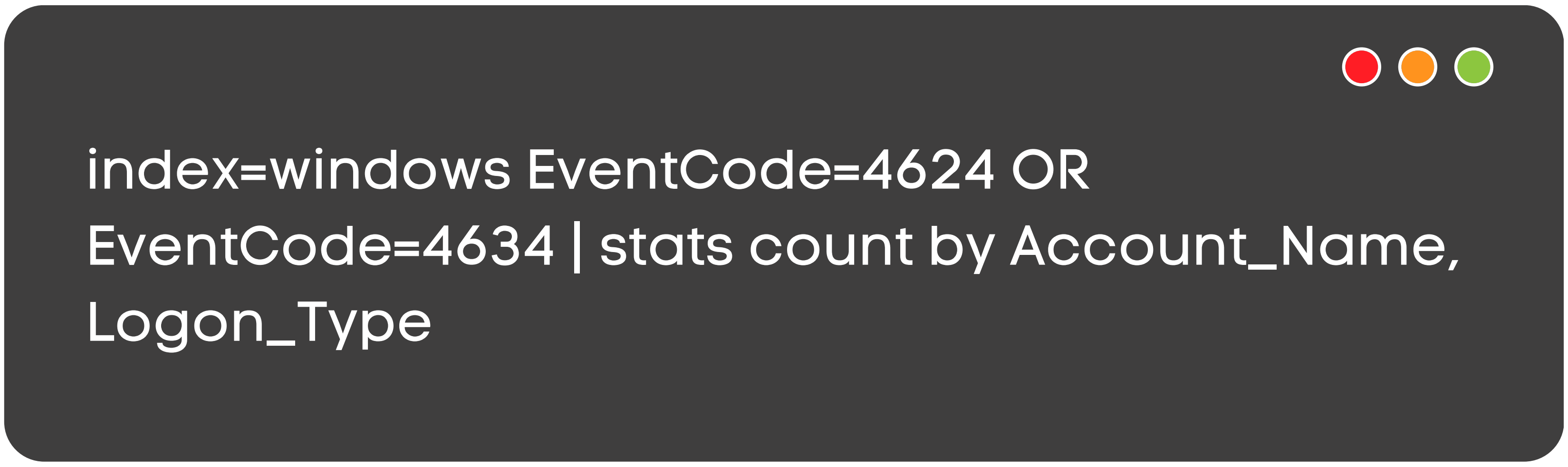
12

MONITORING USER LOGON ACTIVITY

Purpose

Track user logon/logoff events (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4624 OR
EventCode=4634 | stats count by Account_Name,
Logon_Type
```

Outcome

Provides insight into user login and logout patterns. Helps detect unauthorized or suspicious login behavior.

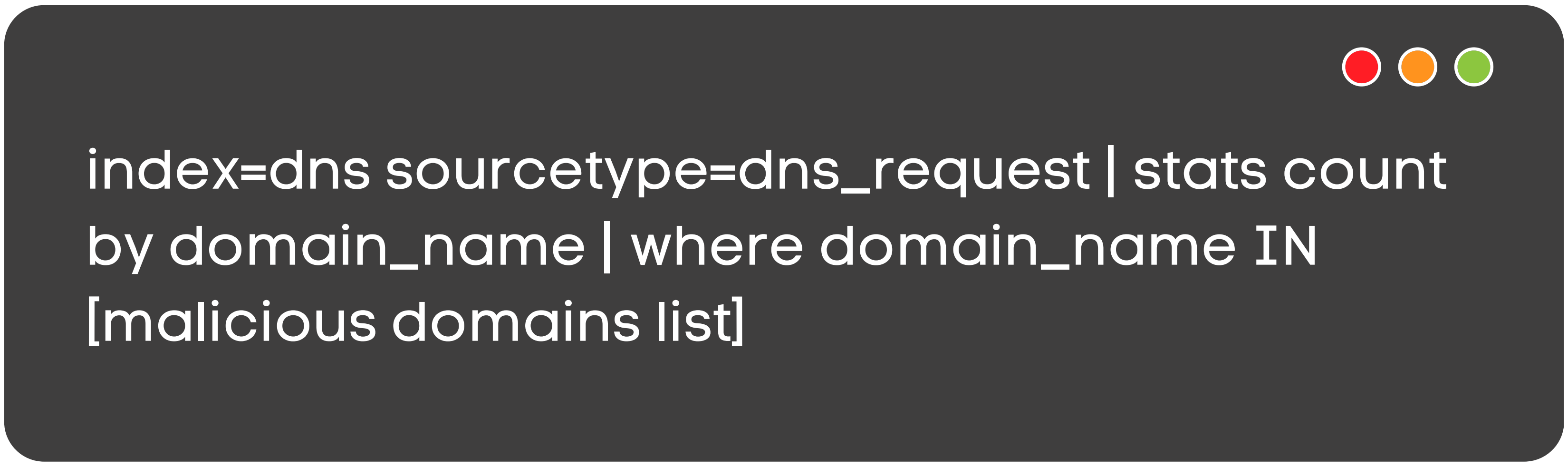
13

SUSPICIOUS DNS REQUESTS

Purpose

Identify DNS queries to malicious or suspicious domains (SOC2 CC6.8 - Risk Mitigation).

Example query



```
index=dns sourcetype=dns_request | stats count
by domain_name | where domain_name IN
[malicious domains list]
```

Outcome

Detects requests to known malicious domains. Helps block further access to risky websites and mitigate threats.

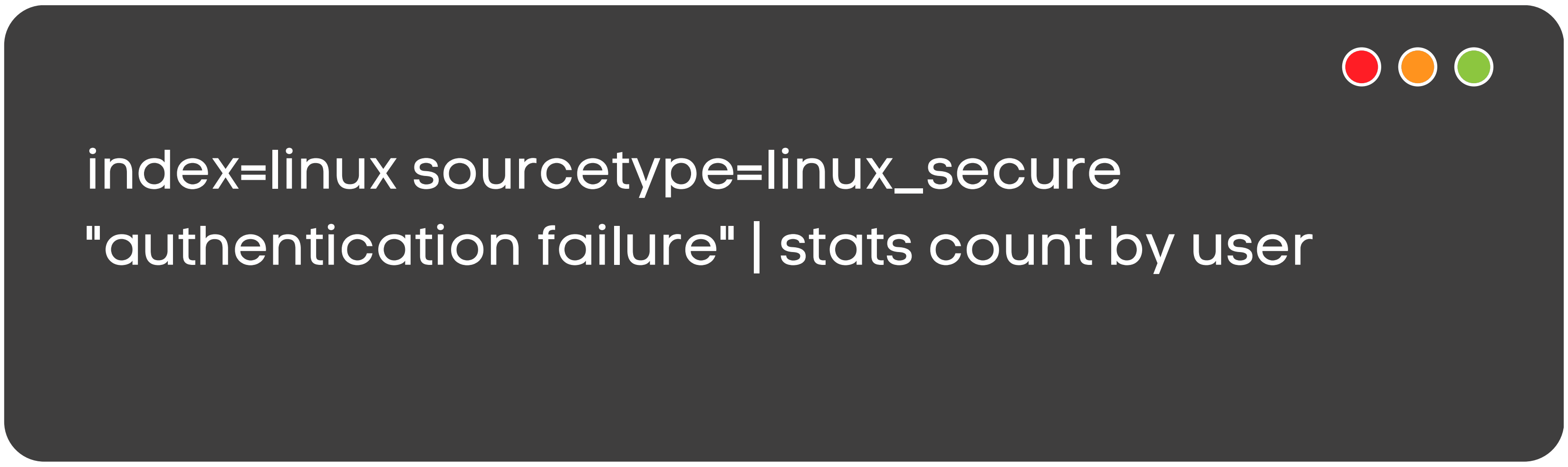
14

FAILED ACCESS TO CRITICAL SYSTEMS

Purpose

Detect failed login attempts to critical servers (SOC2 CC6.1 - Logical Access).

Example query



```
index=linux sourcetype=linux_secure
"authentication failure" | stats count by user
```

Outcome

Tracks failed login attempts on critical Linux servers. Enables quick response to potential unauthorized access attempts.

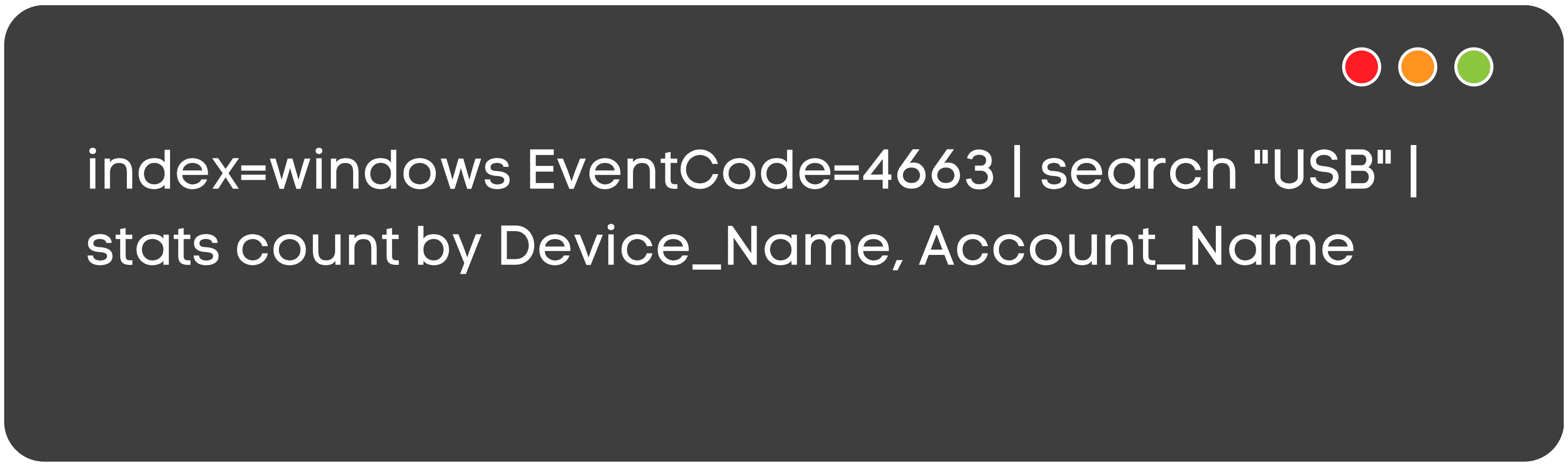
15

USB DEVICE DETECTION

Purpose

Monitor USB device activity (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4663 | search "USB" |
stats count by Device_Name, Account_Name
```

Outcome

Detects and tracks the use of USB storage devices on systems. Helps identify potential data leakage through external devices.

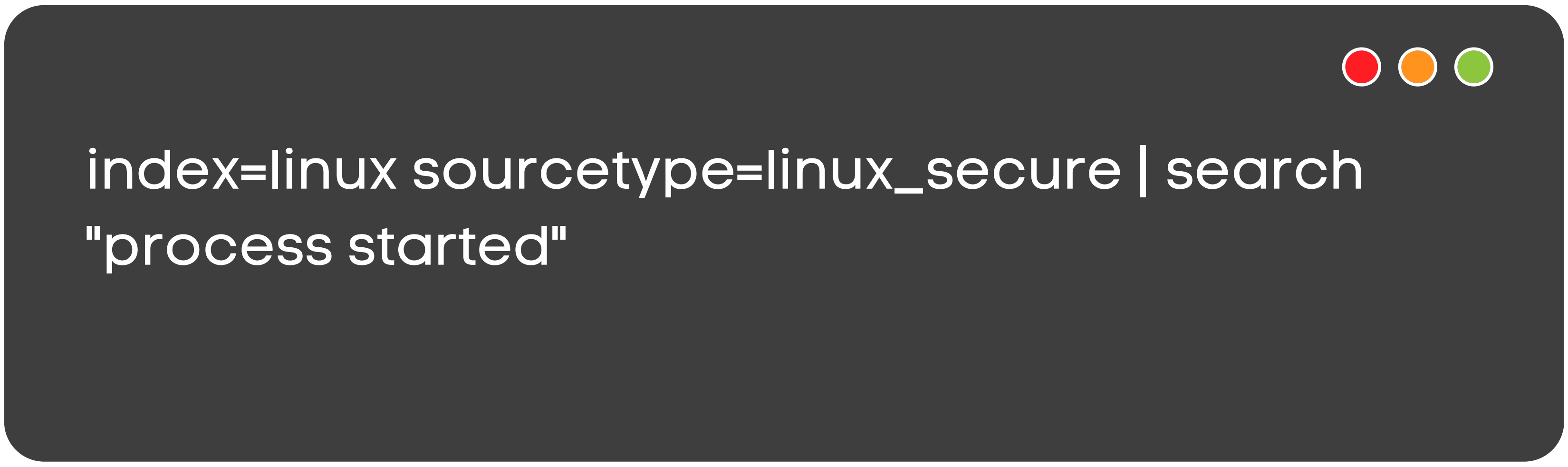
16

SUSPICIOUS PROCESSES

Purpose

Detect suspicious process executions (SOC2 CC6.7 - System Operations).

Example query



```
index=linux sourcetype=linux_secure | search
"process started"
```

Outcome

Monitors for unusual or unauthorized process startups on Linux systems. Enables detection of potential malware or rogue processes.

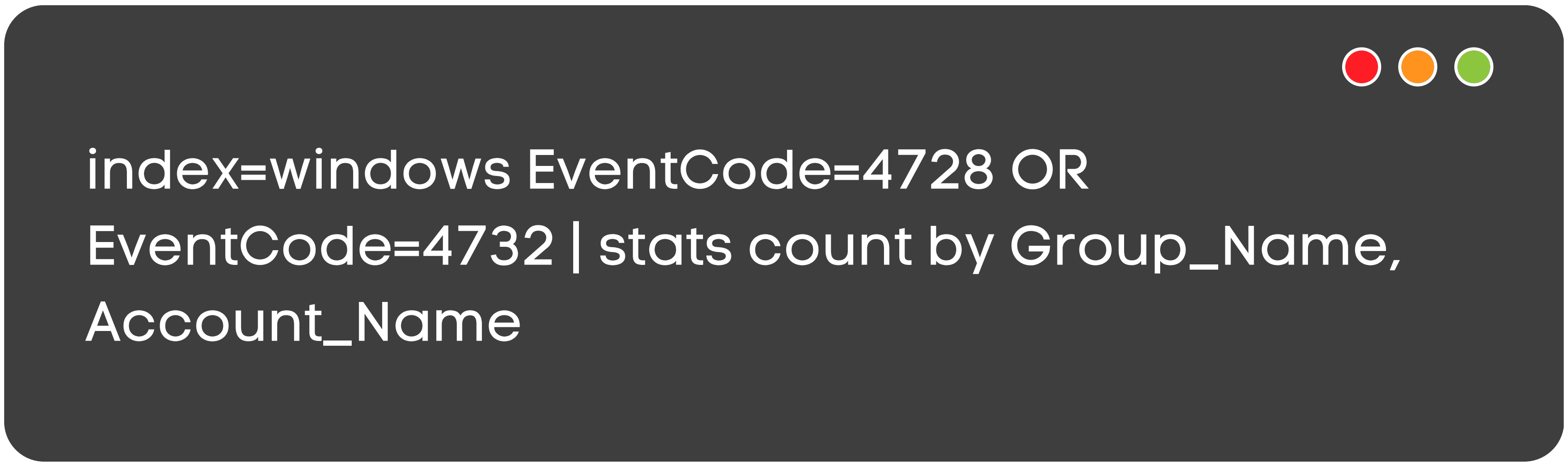
17

CHANGES IN USER ROLES

Purpose

Monitor changes to user roles and permissions (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4728 OR
EventCode=4732 | stats count by Group_Name,
Account_Name
```

Outcome

Tracks changes in user groups and roles across Windows environments. Helps identify unauthorized privilege changes or misuse.

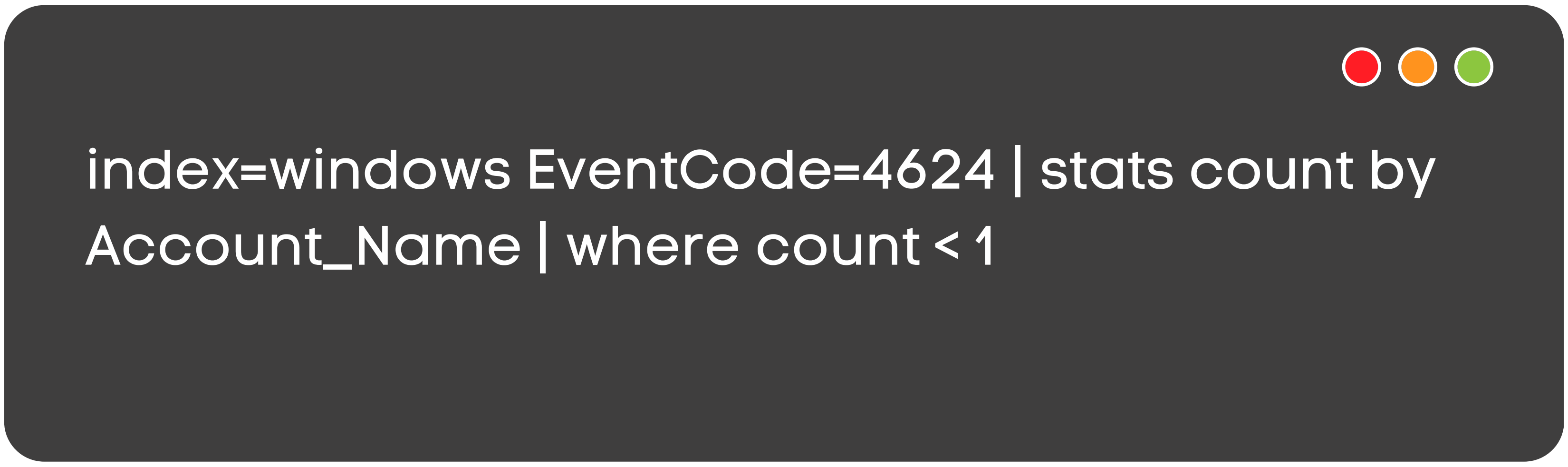
18

INACTIVE USER ACCOUNTS

Purpose

Detect and disable inactive user accounts (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4624 | stats count by
Account_Name | where count < 1
```

Outcome

Identifies inactive accounts that haven't been used for a specific time period. Helps reduce attack surface by deactivating dormant accounts.

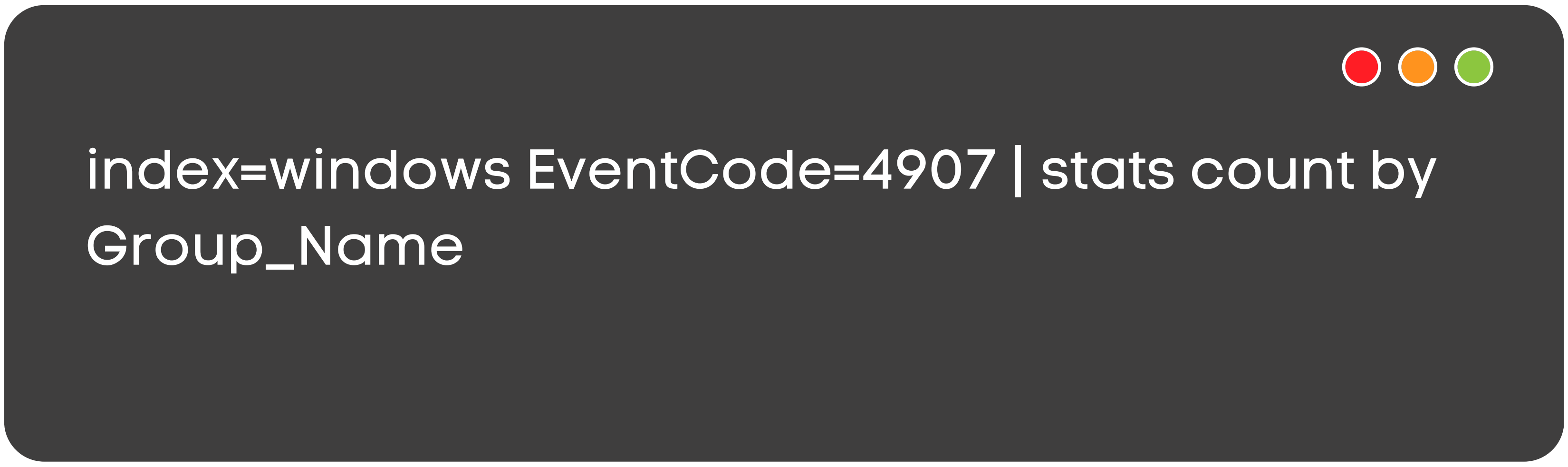
19

SECURITY POLICY MODIFICATIONS

Purpose

Detect changes to security policies (SOC2 CC6.7 - System Operations).

Example query



```
index=windows EventCode=4907 | stats count by Group_Name
```

Outcome

Detects changes to security policies across systems. Ensures that any unauthorized changes are quickly identified and investigated.

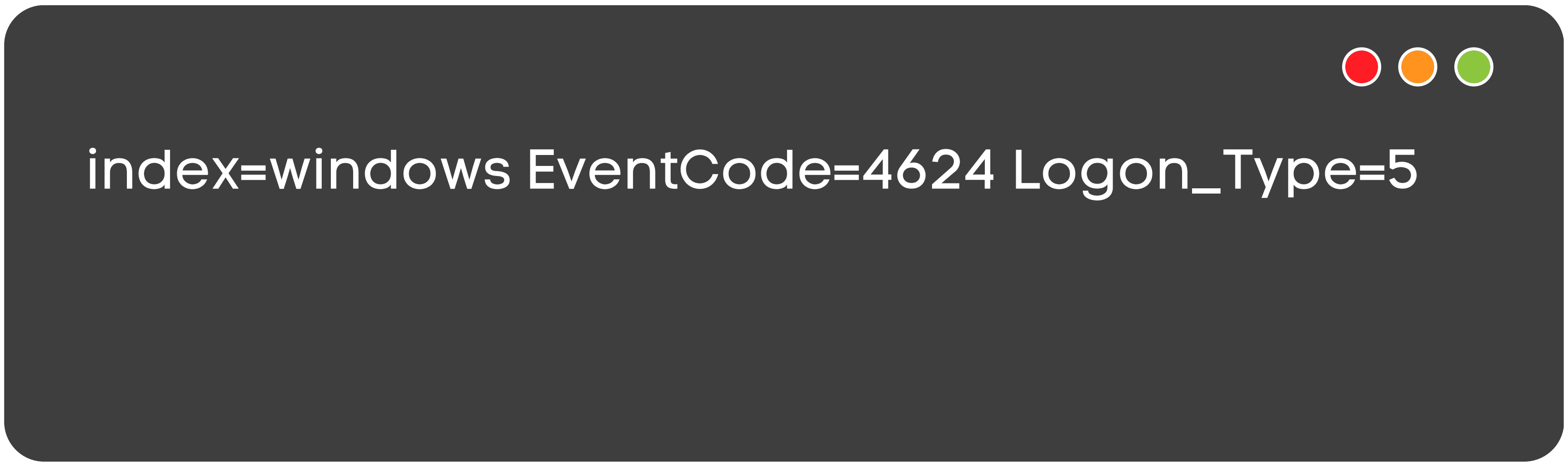
20

TRACKING SERVICE ACCOUNT USAGE

Purpose

Monitor the use of service accounts (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4624 Logon_Type=5
```

Outcome

Tracks logins of service accounts across Windows environments. Helps prevent misuse of these critical accounts.

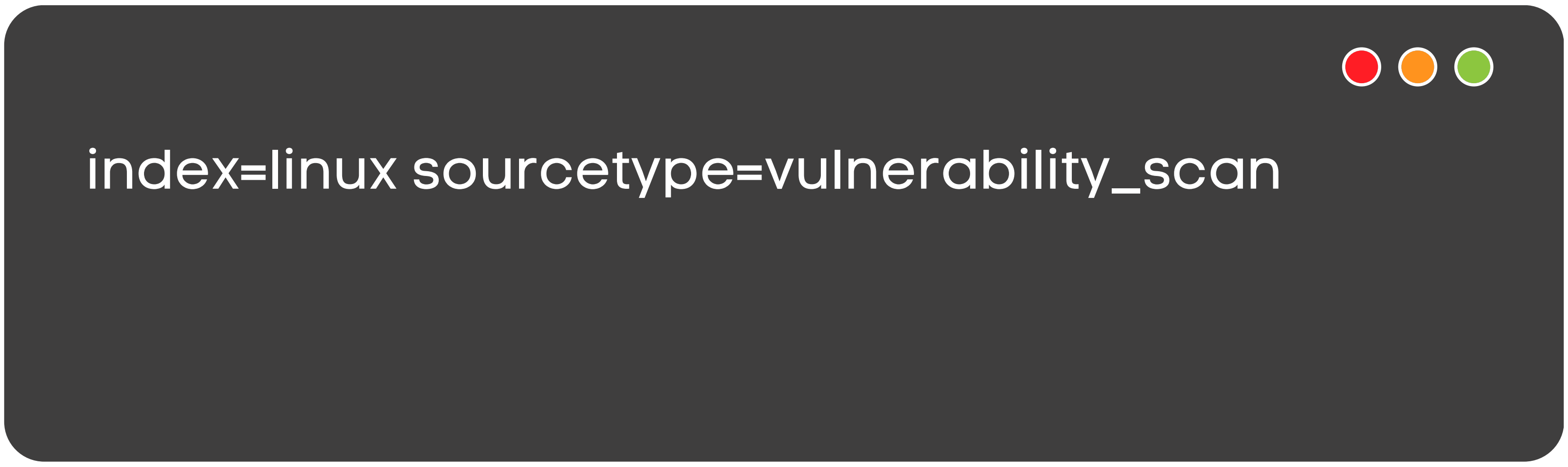
21

SOFTWARE VULNERABILITY SCANNING

Purpose

Ensure regular vulnerability scanning of systems (SOC2 CC6.6 - Change Management).

Example query



```
index=linux sourcetype=vulnerability_scan
```

Outcome

Provides a list of detected vulnerabilities from regular scans. Helps ensure timely patching of identified security risks.

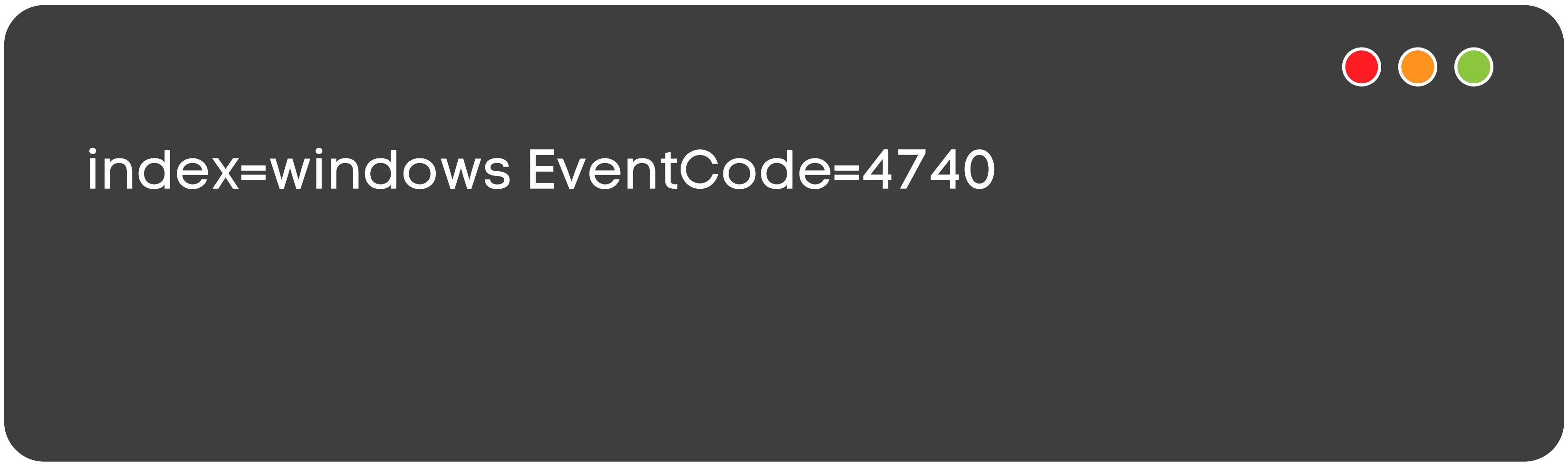
22

MONITORING ACCOUNT LOCKOUTS

Purpose

Detect when accounts are locked due to failed logins (SOC2 CC6.1 - Logical Access).

Example query



```
index=windows EventCode=4740
```

Outcome

Identifies accounts that are being locked out due to excessive failed logins. Helps investigate potential brute-force attacks or misconfigured systems.

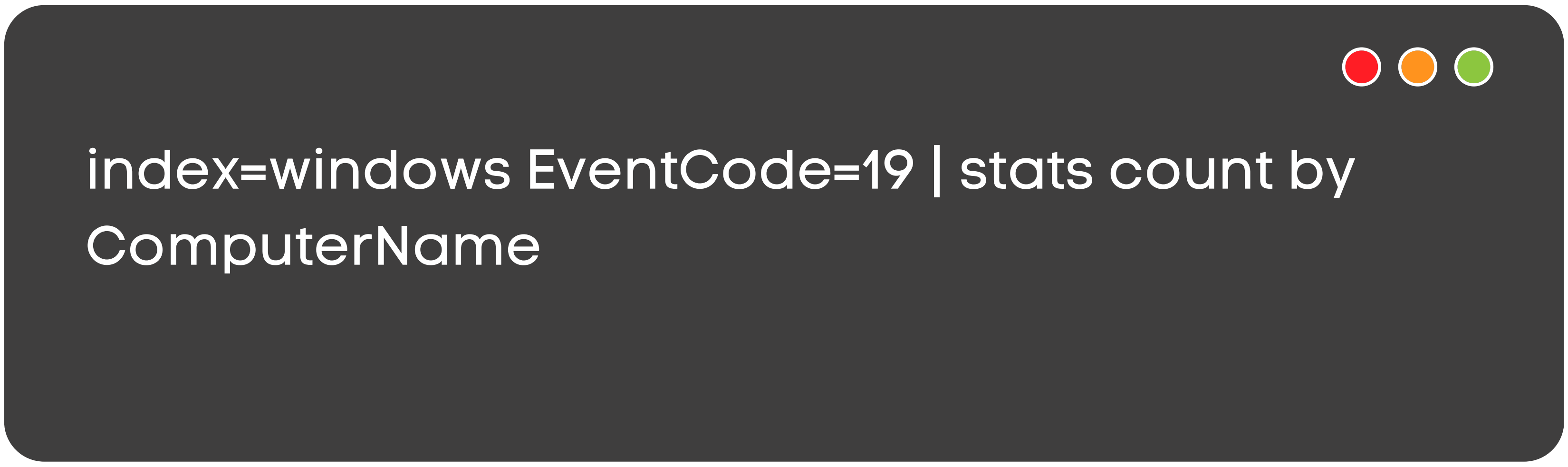
23

SECURITY PATCH INSTALLATION

Purpose

Monitor installation of security patches (SOC2 CC6.7 - System Operations).

Example query



```
index=windows EventCode=19 | stats count by
ComputerName
```

Outcome

Tracks systems where security patches have been installed. Ensures that all systems are up to date with the latest security patches.

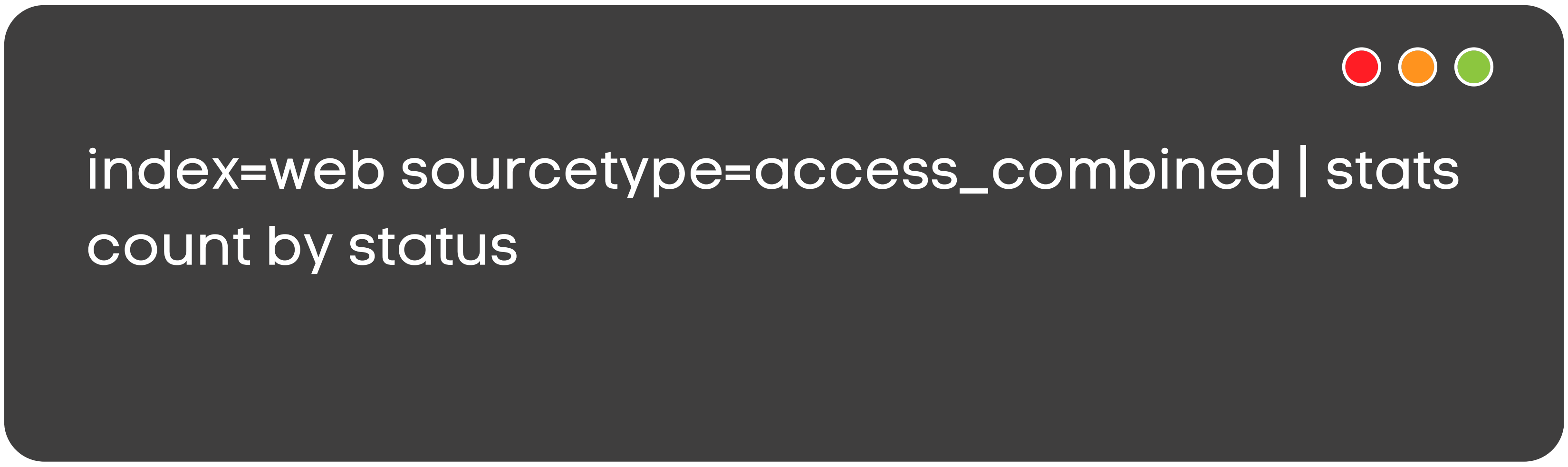
24

WEB SERVER LOG MONITORING

Purpose

Detect abnormal activity in web server logs (SOC2 CC6.7 - System Operations).

Example query



```
index=web sourcetype=access_combined | stats
count by status
```

Outcome

Monitors HTTP status codes to detect anomalies such as 404 or 500 errors. Helps identify potential web server misconfigurations or attacks.

CONCLUSION

Here’s the conclusion summarizing the 24 Splunk SIEM use cases for SOC 2 compliance:

- Splunk SIEM streamlines SOC 2 compliance by automating security monitoring and detection.
- It tracks unauthorized access, privilege escalations, and suspicious activities in real-time.
- Monitoring file integrity, system changes, and patch management ensures compliance with operational controls.
- Use cases focus on detecting data exfiltration, malware, and abnormal traffic patterns.
- Automated tracking of inactive accounts and service account usage enhances access control.
- Vulnerability scans and web server monitoring reduce system vulnerabilities and potential breaches.

ADDITIONAL RESOURCES

- What is SOC 2? [LINK]
- SOC 2 Compliance: The Complete Introduction [LINK]
- SOC 1, 2, 3 Compliance: Understanding & Achieving SOC Compliance [LINK]
- How to Achieve SOC 2 Compliance in the Cloud [LINK]

Reach us at hi@haxsecurity.com