Splunk Use Cases

Use Case: Checking for Windows Audit Log Tampering

Link = https://education.splunk.com/elearning/splunk-use-case---checking-for-windows-audit-log-tampering

⇨ Using Splunk to check for any tampering done to Windows audit logs.

```
Index=* (sourcetype=wineventlog AND (EventCode=1102 OR EventCode=1100)) OR
(sourcetype=wineventlog AND EventCode=104)
| stats count by _time EventCode Message sourcetype host
```

Use Case: Finding Large Web Uploads

Link = https://education.splunk.com/elearning/use-case---finding-large-web-uploads

⇨ Using Splunk with proxy data to find large file uploads that could point to data exfiltration in your network.

```
Index=* sourcetype=websense*
| where bytes_cut > 35000000
| table _time src_ip bytes* uri
```

Use Case: Detecting Recurring Malware on Host

Link = https://education.splunk.com/elearning/use-case---detecting-recurring-malware-on-host

⇨ Using anti-virus logs to detect if malware is recurring on a host after being removed.

```
Index=* sourcetype=Symantec:*
| stats count range(_time) as TimeRange by Risk_Name, Computer_Name
| where TimeRange > 1800
| eval TimeRange_in_Hours = round(TimeRange/3600,2), TimeRange_in_Days =
round(TimeRange/3600/24,2)
```

Use Case: Detecting Brute Force Attack

Link = https://education.splunk.com/elearning/use-case---detecting-brute-force-attack

⇨ Using Windows security logs to find possible brute force attacks on your network.

```
Index=* sourcetype=win*security user=* user!=""
| stats count(eval(action="success")) as successes count(eval(action="failure")) as failures by user,
ComputerName
| where successes>0 AND failures>10
```

Note: I adjusted detection for failures exceeding 10, I think 100 is a lot and we might miss possible password spraying attacks

Use Case: Detecting Network and Port Scanning

Link = https://education.splunk.com/elearning/use-case---detecting-network-and-port-scanning

- ⇨ Using firewall logs to detect hosts that are running network and port scans.

```
Index=* sourcetype=firewall*
| stats dc(dest_port) as num_dest_port dc(dest_ip) as num_dest_ip by src_ip
| where num_dest_port > 500 OR num_dest_ip > 500
```

Use Case: Basic Tor Traffic Detection

Link = https://education.splunk.com/elearning/user-case---basic-tor-traffic-detection

- ⇨ Using firewall data to find TOR traffic on your network.

```
Index=network sourcetype=firewall_data app=tor src_ip=*
| table _time src_ip src_port dest_ip dest_port bytes app
```

Use Case: Detecting Unencrypted Web Communications

Link = https://education.splunk.com/elearning/use-case---detecting-unencrypted-web-communications

- ⇨ Using Splunk to find unencrypted web communications that could lead to a data breach or expose PII data (Personally Identifiable Information).

```
Index=* sourcetype=firewall_data dest_port!=443 app=workday*
| table _time user app bytes* src_ip dest_ip dest_port
```

Use Case: Identifying Web Users by Country

Link = https://education.splunk.com/elearning/use-case---identifying-web-users-by-country

- ⇨ Using IPs in your data to report and visualize user locations.

```
Index=web sourcetype=access_combined
| iplocation clientip
| stats dc(clientip) by Country  # geostats dc(clientip) by country   => this will output results displayed on a world map
```

Use Case: Identifying Slow Web Content

Link = https://education.splunk.com/elearning/use-case---identifying-slow-web-content

⇨ A slow loading web site can not only frustrate users, but can also hurt search rankings. In this video we will show you how to use Splunk Enterprise to find slow content using web server logs.

```
Index=web sourcetype=ms:iis:auto OR sourcetype=apache:access
| stats avg(time_taken) as art by uri_path
| eval "Average Response Time" = round(art,2)
| sort –"Average Response Time"
| table uri_path, "Average Response Time"
```

Use Case: Finding New Local Admin Accounts

Link = https://education.splunk.com/elearning/use-case---finding-new-local-admin-accounts

⇨ Often an attack will include the creation of a new user, followed by permissions being elevated to an admin level. In this video we show you how to use Splunk to find these accounts so that you can take action if needed.

```
Index=win_servers sourcetype=windows:security EventCode=4720 OR ( EvenCode=4732
Administrators)
| transaction Security_ID maxspan=180m
| search EventCode=4720 EventCode=4732
| table _time, EventCode, Security_ID, SamAccountName
```

Use Case: Find Interactive Logins from Service Accounts

Link = https://education.splunk.com/elearning/use-case---find-interactive-logins-from-service-accounts

⇨ Most service accounts should never interactively log into servers. This video will show you how to actively monitor your servers so you can quickly investigate if this happens.

```
Index=systems sourcetype=audit_logs user=svc_*
| stats earliest(_time) as earliest latest(_time) as latest by user, dest
| eval isOutline= if (earliest >= relative_time(now(), "-1d0d" ), 1, 0)
| convert ctime(earliest) ctime(latest)
```

Use Case: Log Volume Trending

Link = https://education.splunk.com/elearning/use-case---log-volume-trending

⇨ Visualizing the number of events being logged by an application can provide a simple, yet powerful indicator of the state of your application, or changes in the behavior of your code or environment. In this video we show you how to use the tstats command to get a quick "heartbeat" for your data, helping you pinpoint server changes or issues.

```
| tstats prestats=t count where index=apps by host _time span=1m
| timechart partial=f span=1m count by host limit=0                    # Display Visualization
```

Use Case: Measuring Storage I/O Latency

Link = https://education.splunk.com/elearning/use-case---measuring-storage-i/o-latency

- ⇨ Using Splunk Enterprise to quickly find I/O bottlenecks across your systems.

```
Index=main sourcetype=iostat
| timechart avg(latency) by host
```

Use Case: Measuring Storage Speed I/O Utilization by Host

Link = https://education.splunk.com/elearning/use-case---measuring-storage-speed-i/o-utilization-by-host

- ⇨ Splunk Enterprise makes it simple to track disk I/O, helping you quickly discover storage issues on your servers.

```
Index=main sourcetype=iostat
| eval hostdevice=host+":"+Device
| timechart avg(totoal_ops) by hostdevice
```

Use Case: Measuring Memory Utilization by Host

Link = https://education.splunk.com/elearning/use-case---measuring-memory-utilization-by-host

- ⇨ Tracking memory utilization of your systems.

```
Index=main sourcetype=vmstat
| timechart max(memUsedPct) by host
```