Anatomy of a Tailored PAVO Splunk Use Case for Citrix VPNs

Increasingly, we are asked by clients to help spot various activities via network logs. Here is a relatively small but important use case that we tailored for a Citrix VPN.

Let's break it down and maybe this use case can help you in your environment.

The Use Case: With the current environment around the world, this client knows everyone is working remotely at home. "Bad actors" are attempting now more than ever to access company systems. In order to quickly screen out possible incidents from their Citrix VPN NetScaler, the client would like a chart to show any VPN access (both successful and unsuccessful) and also who is accessing VPN from countries where there are no offices. No personnel is located overseas and travel is currently restricted.

The Search:
Search Title: Citrix VPN Connections Outside Your Business Operations

```
index=netscaler (event_name='SSLVPN LOGIN' OR event_name='AAA LOGIN_FAILED') NOT src_user='scriptChecker'
| iplocation src_ip
| search Country=* NOT (Country='United States' OR Country='Canada')
| table _time event_name src_user src_ip client_ip nat_ip City Country Region
```

Dissecting the Search:
Let's break this down in quick detail.

```
index=netscaler (event_name='SSLVPN LOGIN' OR event_name='AAA LOGIN_FAILED') NOT src_user='scriptRunner'
```

We start by searching the VPN NetScaler logs and narrowing down to the specific events that show users logging in or failing to login. In this case, we know we have 1 automated account that runs various scripts for the BizDev Team called "scriptRunner." The SOC has created its own explicit controls for this account and has chosen to ignore it from this report.

```
| iplocation src_ip
```

Next, we need to lookup (find) the location of each source IP. To do this, we are using the Splunk iplocation command. This command takes the specified IP, checks that IP in the GeoLite2-City.mmdb database, and outputs the fields. (the fields are: city, country, latitude, longitude, and region)
IP Location Reference: https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Iplocation

```
| search Country=* NOT (Country='United States' OR Country='Canada')
```

At this point in the search we have our logins and attempts, plus where they are coming from. We now need to filter down the results, removing any acceptable results from countries where offices are located. We start a sub-search with the search command, ensuring the country is specified. Then, we filter out the countries where the client has offices.

```
| table _time event_name src_user src_ip client_ip nat_ip City Country Region
```

So now, we have all the fields for location and events that meet the use cases's criteria. We are creating the table for the final presentation of results. List the fields in the order that is desired.
Table Reference: https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Table

We concluded this report by scheduling it to search over a small window of 15 minutes.

You may not have Citrix, but the idea of this use case can be applied to any VPN with little effort. A more generalized visualization of this search can be found in the Geo Location Dashboard within the PAVO Network Traffic App. This page will visualize all the network traffic Data Model on your network.