Tossing Splunk in Your PAN

Ninja’s Guide to the Galaxy of Splunk and Palo Alto Networks

Kevin Gonzalez | Security Operations Manager

September 25, 2017 | Washington, DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
1. Utilizing Splunk Enterprise Security to:
   • Reduce alert chaos
   • Tame your PANW Threat Intelligence Feeds

2. Saving time with a Splunk/PANW API Fusion

3. Knowing the “who” at all times by populating PANW’s User-ID

4. Utilizing the Splunk Universal Forwarder to fix all of your problems
Splunk Enterprise Security & Palo Alto Networks

- Incident Response
  - Single pane of glass
  - Adaptive response based on correlated information

- Threat Intelligence
  - Centralized repository
  - Easy to maintain
  - Deduplication and content filtering
Splunk Enterprise Security & Palo Alto Networks
Integrating PANW into Enterprise Security

- Create Notable Events geared towards your PAN Firewall
  - Auto-Wildfire submissions
  - Per-Notable event tagging for PAN Dynamic Block Lists

- Utilize Threat Intelligence Data Models to feed your Palo Alto Network Firewalls:
  - De-duplicate and publish filtered threat intel
  - Auto-add trusted intel to dynamic block lists via tags
Splunk Enterprise Security & Palo Alto Networks
Splunk Enterprise Security & Palo Alto Networks

Correlation Search
- Search Name: PAN - Threat Intel Update
- Application Context: Enterprise Security
- Description: Auto-tags malicious IPs into a dynamic blocklist
- Node: Guided

Search:
- from datamodel: "Threat_Intelligence.IP_Intelligence"
- search threat_key="trusted_threat_source"
- pantan device="x.x.x.x" action="add" ip_field=ip tag="no_bueno"

Time Range
- Earliest time: 24h
- Latest time: now
- Cron Schedule: 0001***

Scheduling
- Real-time
- Continuous
The `pantag` command shares context with the firewall by tagging IP addresses found in Splunk into Dynamic Address Groups.

Command added in App version 4.1. New parameters added in App version 5.0.

Syntax:

```
pantag device=<hostname>|panorama=<hostname>
[serial=<serial-of-device-in-panorama>] [vsys=<vsys>]
[action=<add>|<remove>] [ip_field=<field-containing-IPs>]
tag=<tag>|tag_field=<field-containing-tags>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Added in</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td></td>
<td>4.1</td>
<td>IP or hostname of firewall</td>
</tr>
<tr>
<td>panorama</td>
<td></td>
<td>5.0</td>
<td>IP or hostname of Panorama</td>
</tr>
<tr>
<td>serial</td>
<td></td>
<td>5.0</td>
<td>Serial of firewall (required if using panorama parameter)</td>
</tr>
<tr>
<td>vsys</td>
<td>vsys1</td>
<td>5.0</td>
<td>VSYS ID (eg. vsys2)</td>
</tr>
<tr>
<td>action</td>
<td></td>
<td>4.1</td>
<td>Add or remove the tag</td>
</tr>
<tr>
<td>ip_field</td>
<td>src_ip</td>
<td>4.1</td>
<td>Same as ip_field parameter (deprecated in 5.0, use ip_field)</td>
</tr>
<tr>
<td>tag</td>
<td></td>
<td>4.1</td>
<td>Tag for the IP, referenced in the Dynamic Address Group</td>
</tr>
<tr>
<td>tag_field</td>
<td>src_ip</td>
<td>5.0</td>
<td>Log field containing the tag for IP address in the same log</td>
</tr>
</tbody>
</table>
API Harmony
Splunk, Palo Alto Networks, and their API’s
Splunk SDK for Python

https://github.com/splunk/splunk-sdk-python
PAN-OS XML API

https://www.paloaltonetworks.com/documentation/71/pan-os/xml-api
pantag - Extended
Auto-tag trusted Domain and HTTP IOCs to Dynamic Block Lists

- Use your Splunk Enterprise Security Data Models
- Splunk Cloud customers are currently limited to IP and HTTP

```python
#!/usr/bin/env python
import splunklib.client as client
import requests
import re

service = client.connect(
    username='admin',
    password='password!',
    port='8089',
)

urlstart = 'https://10.1.1.1/itb/configAction=set&key=xxxxxxxxx&path/config/shared/profiles/custom-url-category/entry[?name="Malicious-Domains"]/list&element=members'
urlend = '&member=

search = '[] from datamodel="Threat_Intelligence.HTTP_Intelligence" | search threat_key="trusted_threat_source" | table threat_key url'
results = service.jobs.oneshot(search)
rexRemover = re.compile(r'\{\[\{value\}\{\}\{\}\}'}

for line in results:
    match = rexRemover.search(line)
    if match:
        value = rexRemover.sub('', line)
        urlMod = urlstart + value + urlend
        requests.get(url=urlMod, verify=False)
```
How About Using the APIs to Maintain Your Address Objects?

- Pre-existing address object library? No problem.
- Need it done now? No problem.
- Create new address object library managed by Splunk data
- Regularly update address objects with pre-defined tags
Updating PAN-OS Address Objects

- Address object:
  - Standardization
  - Creation
  - Modification
- Splunk query that contains all necessary data
- + crontab
Palo Alto Networks User-ID
Why we all want it...

- **Benefits**
  - Improved visibility
  - Policy Control
  - Logging, Reporting and Forensics

- **Use Cases**
  - Security
  - Legal
  - Human Resources
Palo Alto Networks User-ID

Why we had some problems...

- Non-Microsoft endpoints
- No centralized point of reference for User-ID Agent
- Cloud-based systems
- Lack of historical data
Palo Alto Networks User-ID – Solution Overview
Updating User-ID With RADIUS Logs

- X amount of incomplete sources can depict a full picture
- Wireless AP Logs
  - Device MAC
  - Device IP
- RADIUS Logs
  - User
  - Device MAC
  - Automatic Lookups
panuserupdate

The `panuserupdate` command synchronizes user login events with Palo Alto Networks User-ID. More information: User-ID with Splunk

Added in App version 5.0. For previous versions, refer to the `panupdate` command.

Syntax:

```
panuserupdate device=<hostname>|panorama=<hostname> [serial=<serial-of-device-in-panorama>] [vsys=<vsys#>]
[action=<login|logout> [ip_field=<field-containing-IPs>]
user_field=<field-containing-usernames>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td>IP or hostname of firewall</td>
<td></td>
</tr>
<tr>
<td>panorama</td>
<td>IP or hostname of Panorama</td>
<td></td>
</tr>
<tr>
<td>serial</td>
<td>Serial of firewall (required if using panorama parameter)</td>
<td></td>
</tr>
<tr>
<td>vsys</td>
<td>vsys1</td>
<td>VSYS ID (e.g. vsys2)</td>
</tr>
<tr>
<td>action</td>
<td>login</td>
<td>Tell the firewall user logged in or logged out</td>
</tr>
<tr>
<td>ip_field</td>
<td>src_ip</td>
<td>Log field containing IP address</td>
</tr>
<tr>
<td>user_field</td>
<td>user</td>
<td>Log field containing the username</td>
</tr>
</tbody>
</table>
Updating User-ID With SIP and “Best Guess” Scenarios

▶ Know your apps
▶ Know the data from those apps
▶ Now apply that knowledge
▶ Examples:
  • SIP Data from Lync/Skype
  • Raw URL Logs passing user info
“Best Guess” Scenarios and Timeouts...

- Individualized User-ID timeout
- Increased customization
- APIs are your best friend...
Updating User-ID with Custom Scripts

Endpoints are your true source
- Contain LAN/WAN IPs
- Contain User Info

The Splunk Universal Forwarder are also your best friend

Historical evidence of all User/IP mappings... completed.
Other Splunk Universal Forwarder Use Cases
As it relates to Palo Alto Networks...

- GlobalProtect Install Validation
- Version Checks
- Setting Checks
- Assess your egress
- Bug Workarounds
GlobalProtect Bug Workaround Utilizing The Splunk Universal Forwarder

- v3.0.x
- Ubiquitous VPN on Windows
- Ungraceful Network Disconnects
- Internal DNS Settings Frozen

```bash
$CheckGP = gwm -class win32_product | ?{$_ .name -match "globalprotect"}

if($CheckGP -ne $null){
    $n = $CheckGP.name
    $v = $CheckGP.version
    write-host "name = $n"
    write-host "version = $v"
    write-computerosystem get username

    if (((Test-Connection -ComputerName validationurl2.com -Count 2 -ErrorAction SilentlyContinue) -and ((Test-Connection -ComputerName validationurl2.com -Count 2 -ErrorAction SilentlyContinue))){
        write-host "External Test Completed, No Connection Found."
        if (((Test-Connection -ComputerName validationIP1 -Count 1 -ErrorAction SilentlyContinue) -and ((Test-Connection -ComputerName validationIP1 -Count 1 -ErrorAction SilentlyContinue))){
            write-host "Internal Test Completed, No Connection Found."
            C:\Windows\system32\ipconfig.exe /all
            C:\Windows\system32\netsh.exe int ipv4 reset
            C:\Windows\system32\netsh.exe int ipv6 reset
            C:\Windows\system32\netsh.exe winsock reset catalog
            C:\Windows\system32\netsh.exe interface ip set dns name= "Wireless network connection" dhcp
            C:\Windows\system32\netsh.exe interface ip set dns name= "Local Area Connection" dhcp
        }
    }
}
```
Questions, Comments, Concerns?

You're my bestfriend because I wouldn't dare to be this weird with anyone else.
Thank You

Don't forget to rate this session in the .conf2017 mobile app