Take Your SIEM to the Next Level with 3rd Party Tools and Scripts

SIEM & Tactical Analytics SUMMIT
November 2017
Who Am I?
Austin Taylor

Chief Security Research Engineer @ IronNet Cybersecurity

Cyber Warfare Operator @ USAF (MDANG)

Security Consultant @ HA Security Solutions
Austin Taylor

Chief Security Research Engineer @ IronNet Cybersecurity

Cyber Warfare Operator @ USAF (MDANG)

Security Consultant @ HA Security Solutions

www.austintaylor.io
Austin Taylor
Chief Security Research Engineer @ IronNet Cybersecurity
Cyber Warfare Operator @ USAF (MDANG)
Security Consultant @ HA Security Solutions
www.austintaylor.io
@HuntOperator
Next Level?

- Content rich data
- Answer many questions at once
- Intended Use? Maybe?
  - Use the API to retrieve data

This talk focuses on:

- Beaconing Detection
- Vulnerability Scans
Your SIEM
Your SIEM
Your SIEM
Your SIEM
Getting Data

Python

elasticsearch
Beaconing Detection
from elasticsearch import Elasticsearch, helpers

query = {
    "query": {
        self.filt: {
            self.query: {
                "query_string": {
                    "query": "*",
                    "analyze_wildcard": 'true'
                }
            }
        }
    }
}

helpers.scan(query=query,
             client=localhost,
             scroll="90m",
             index=logstash-flow-*,
             timeout="10m")
Data Out

- Most SIEMs focus on getting data In
- We’re going to....
  - Retrieve the data through the SIEMs API
  - Enrich it
  - Reprocess it
Beaconing: Detection

- Free Open Source Software
- Designed for data scientists, security researchers
- Written in Python
- Used for rapid prototyping and development of behavioral analytics
- Intended to help identify new anomalous behavior and potentially malicious
- Thank you to Justin Henderson and Jonathan Burkert!

https://github.com/austin-taylor/flare
Beaconing: Detection

[beacon]
es_host=localhost  # IP address of ES Host, which we forwarded to localhost
es_index=logstash-flow-*  # ES index
es_port=9200  # Logstash port (we forwarded earlier)
es_timeout=480  # Timeout limit for elasticsearch retrieval
min_occur=50  # Minimum of 50 network occurrences to appear in traffic
min_interval=30  # Minimum interval of 30 seconds per beacon
min_percent=30  # Beacons must represent 30% of network traffic per dyad
window=3  # Accounts for jitter... For example, if 60 second beacons occurred at 58 seconds or 62 seconds, a window of 3 would factor in that traffic.
threads=8  # Use 8 threads to process (Should be configured)
period=24  # Retrieve all flows for the last 24 hours.
kibana_version=5  # Your Kibana version. Currently works with 4 and 5
verbose=True  # Display output while running script

https://github.com/austin-taylor/flare
Beaconing Detection

<table>
<thead>
<tr>
<th>Time</th>
<th>EveBox</th>
<th>src_ip</th>
<th>src_port</th>
<th>proto</th>
<th>dest_ip</th>
<th>dest_port</th>
<th>http.http_method</th>
<th>http.hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 13th 2017, 10:49:01.935</td>
<td><strong>Correlate Flow</strong></td>
<td>192.168.0.53</td>
<td>49,182</td>
<td>TCP</td>
<td>160.153.76.125</td>
<td>80</td>
<td>GET</td>
<td><a href="http://www.huntoperator.com">www.huntoperator.com</a></td>
</tr>
</tbody>
</table>
Beaconing Detection

- Identify Beaconing
Beaconing Detection

- Identify Beaconing
  - Time
Beaconing Detection

- Identify Beaconing
  - Time
  - IP address
Beaconing Detection

- Identify Beaconing
  - Time
  - IP address
  - Ports
Beaconing Detection

• Identify Beaconing
  • Time
  • IP address
  • Ports
  • Protocol

<table>
<thead>
<tr>
<th>Time</th>
<th>EveBox</th>
<th>src_ip</th>
<th>src_port</th>
<th>proto</th>
<th>dest_ip</th>
<th>dest_port</th>
<th>http.http_method</th>
<th>http.hostname</th>
</tr>
</thead>
</table>
Beaconing Detection

**Simple:** `src_ip, dest_ip, dest_port -> hash`

**More Complex:** Discrete Fourier Transform (DFT)/Fast Fourier transform (FFT)
Beaconing: Hunt

`flare_beacon -c configs/selks4.ini -html beacons.html`

```
Austins-MacBook-Pro:flare huntoperator$ flare_beacon -c configs/selks4.ini -csv beacons.csv
[INFO] Attempting to connect to elasticsearch...
[SUCCESS] Connected to elasticsearch on localhost:9200
[INFO] Gathering flow data... this may take a while...
[INFO] Calculating destination degree.
[SUCCESS] Writing csv to beacons.csv
```

108 events to process
Beaconing: Hunt

flare_beacon -c configs/selks4.ini -html —group —whois —focus_outbound beacons_filtered.csv

Austins-MacBook-Pro:flare huntoperator$ flare_beacon -c configs/selks4.ini --whois --focus_outbound -csv beacons_filtered.csv

[INFO] Attempting to connect to elasticsearch...
[SUCCESS] Connected to elasticsearch on localhost:9200
[INFO] Gathering flow data... this may take a while...
[INFO] Calculating destination degree.
[INFO] Enriching IP addresses with whois information
[INFO] Applying outbound focus - filtering multicast, reserved, and private IP space
[SUCCESS] Writing csv to beacons_filtered.csv

31

events to process
Beaconing: Hunt

```
flake_beacon -c configs/selks4.ini -html --group --whois --focus_outbound beacons_filtered.csv
```

What was applied?

–group: This will group the results making it visually easier to identify anomalies.

–whois: Enriches IP addresses with WHOIS information through ASN Lookups.

–focus_outbound: Filters out multicast, private and broadcast addresses from destination IPs
Beaconing: Hunt

```
flare_beacon -c configs/selks4.ini -html --group --whois --focus_outbound beacons_filtered.csv
```

What was applied?

--group: This will group the results making it visually easier to identify anomalies.

--whois: Enriches IP addresses with WHOIS information through ASN Lookups.

--focus_outbound: Filters out multicast, private and broadcast addresses from destination IPs
Beaconing: Hunt

<table>
<thead>
<tr>
<th>src_ip</th>
<th>dest_whois</th>
<th>dest_ip</th>
<th>dest_port</th>
<th>bytes_toserver</th>
<th>dest_degree</th>
<th>occurrences</th>
<th>percent</th>
<th>interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.100</td>
<td>GOOGLE - Google Inc., US</td>
<td>8.8.8.8</td>
<td>53</td>
<td>82</td>
<td>16</td>
<td>71</td>
<td>98</td>
<td>3601</td>
</tr>
<tr>
<td></td>
<td>SOFTLAYER - SoftLayer Technologies Inc., US</td>
<td>198.23.79.227</td>
<td>123</td>
<td>90</td>
<td>1</td>
<td>71</td>
<td>98</td>
<td>3601</td>
</tr>
<tr>
<td>192.168.0.120</td>
<td>AMAZON-02 - Amazon.com, Inc., US</td>
<td>52.192.78.22</td>
<td>80</td>
<td>1432</td>
<td>3</td>
<td>34</td>
<td>70</td>
<td>1201</td>
</tr>
<tr>
<td></td>
<td>GOOGLE - Google Inc., US</td>
<td>8.8.4.4</td>
<td>53</td>
<td>74</td>
<td>7</td>
<td>139</td>
<td>63</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.8.8.8</td>
<td>53</td>
<td>74</td>
<td>16</td>
<td>140</td>
<td>62</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>GOOGLE - Google Inc., US</td>
<td>8.8.4.4</td>
<td>53</td>
<td>233</td>
<td>7</td>
<td>386</td>
<td>95</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.8.8.8</td>
<td>53</td>
<td>65</td>
<td>16</td>
<td>386</td>
<td>95</td>
<td>61</td>
</tr>
<tr>
<td>192.168.0.60</td>
<td>AKAMAI-ASN1, US</td>
<td>104.95.176.44</td>
<td>80</td>
<td>8399</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>AMAZON-AES - Amazon.com, Inc., US</td>
<td>174.129.1.163</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>77</td>
<td>38</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>204.236.238.3</td>
<td>80</td>
<td>885</td>
<td>1</td>
<td>84</td>
<td>39</td>
<td>111</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23.21.110.37</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>53</td>
<td>35</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23.21.67.210</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>101</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23.21.98.133</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>65</td>
<td>40</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23.23.173.186</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>43</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23.23.236.78</td>
<td>80</td>
<td>759</td>
<td>1</td>
<td>313</td>
<td>41</td>
<td>112</td>
</tr>
<tr>
<td></td>
<td></td>
<td>50.16.215.193</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>25</td>
<td>40</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>50.17.254.18</td>
<td>80</td>
<td>1691</td>
<td>1</td>
<td>25</td>
<td>40</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>DROPBOX - Dropbox, Inc., US</td>
<td>162.125.32.5</td>
<td>443</td>
<td>60</td>
<td>1</td>
<td>53</td>
<td>35</td>
<td>602</td>
</tr>
<tr>
<td></td>
<td>EDGECAST - MCI Communications Services, Inc. db/a Verizon Business, US</td>
<td>152.195.54.20</td>
<td>80</td>
<td>556</td>
<td>2</td>
<td>69</td>
<td>49</td>
<td>601</td>
</tr>
<tr>
<td></td>
<td>LLNW - Limelight Networks, Inc., US</td>
<td>69.164.0.0</td>
<td>80</td>
<td>6242</td>
<td>2</td>
<td>3</td>
<td>33</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US</td>
<td>13.107.6.151</td>
<td>443</td>
<td>3985</td>
<td>1</td>
<td>151</td>
<td>41</td>
<td>300</td>
</tr>
</tbody>
</table>

- **bytes_toserver**: Total sum of bytes sent from IP address to Server
- **dest_degree**: Amount of source IP addresses that communicate to the same destination
- **occurrences**: Number of network occurrences between dyads identified as beaconing.
- **percent**: Percent of traffic between dyads considered beaconing.
- **interval**: Intervals between each beacon in seconds
Beaconing: Hunt

Validate Results

Dashboard / SN FLOW

SN Application protocol

SN Flow unique count of src and dst IP

SN Mean flow age and count

@HuntOperator
Beaconing: Hunt

Drilling in

@timestamp per minute

Count
app_proto.raw: Descending
@timestamp per minute

2
http
June 12th 2017, 22:08:00.000
Beaconing: Hunt
### Ingest CSV

<table>
<thead>
<tr>
<th>src_ip</th>
<th>dest_whols</th>
<th>dest_ip</th>
<th>dest_port</th>
<th>bytes_toserver</th>
<th>dest_degree</th>
<th>occurrences</th>
<th>percent</th>
<th>interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.120</td>
<td>AMAZON-02 - Amazon.com, Inc., US</td>
<td>52.192.78.22</td>
<td>80</td>
<td>1432</td>
<td>3</td>
<td>34</td>
<td>70</td>
<td>1201</td>
</tr>
<tr>
<td>192.168.0.184</td>
<td>TW CABLE-BACKBONE - Time Warner Cable Internet LLC, US</td>
<td>23.40.38.1</td>
<td>80</td>
<td>312</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>40</td>
</tr>
<tr>
<td>192.168.0.22</td>
<td>EDGECAST - MCI Communications Services, Inc. d/b/a Verizon Business, US</td>
<td>93.184.216.34</td>
<td>80</td>
<td>272</td>
<td>3</td>
<td>34</td>
<td>68</td>
<td>300</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>AMAZON-02 - Amazon.com, Inc., US</td>
<td>52.192.78.22</td>
<td>80</td>
<td>1138</td>
<td>3</td>
<td>34</td>
<td>70</td>
<td>1201</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>ASN-APPNEXUS - AppNexus, Inc, US</td>
<td>66.17.178.132</td>
<td>80</td>
<td>10239</td>
<td>1</td>
<td>5</td>
<td>40</td>
<td>73</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>FORTRUST-SOLUTIONS - FORTRUST, US</td>
<td>66.35.38.76</td>
<td>80</td>
<td>1258</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>12</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>IP not found</td>
<td>193.70.47.153</td>
<td>80</td>
<td>248</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>12</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>IP not found</td>
<td>193.70.47.154</td>
<td>80</td>
<td>1490</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>12</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>IP not found</td>
<td>209.15.36.33</td>
<td>80</td>
<td>1117</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>12</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>OVH , FR</td>
<td>192.99.17.41</td>
<td>80</td>
<td>3652</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>12</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>RACKSPACE - Rackspace Hosting, US</td>
<td>146.20.132.50</td>
<td>80</td>
<td>3518</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>12</td>
</tr>
<tr>
<td>192.168.0.39</td>
<td>EDGECAST - MCI Communications Services, Inc. d/b/a Verizon Business, US</td>
<td>93.184.216.34</td>
<td>80</td>
<td>272</td>
<td>3</td>
<td>3</td>
<td>33</td>
<td>97</td>
</tr>
<tr>
<td>192.168.0.42</td>
<td>EDGECAST - MCI Communications Services, Inc. d/b/a Verizon Business, US</td>
<td>93.184.216.34</td>
<td>80</td>
<td>272</td>
<td>3</td>
<td>3</td>
<td>33</td>
<td>97</td>
</tr>
<tr>
<td>192.168.0.53</td>
<td>AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US</td>
<td>160.153.76.129</td>
<td>80</td>
<td>520</td>
<td>3</td>
<td>3</td>
<td>33</td>
<td>97</td>
</tr>
<tr>
<td>192.168.0.60</td>
<td>AKAMAI-AS1 , US</td>
<td>104.95.176.44</td>
<td>80</td>
<td>8399</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>97</td>
</tr>
</tbody>
</table>
### Ingest CSV

<table>
<thead>
<tr>
<th>src_ip</th>
<th>dest_whols</th>
<th>dest_ip</th>
<th>dest_port</th>
<th>bytes_toserver</th>
<th>dest_degree</th>
<th>occurrences</th>
<th>percent</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.120</td>
<td>AMAZON-02 - Amazon.com, Inc., US</td>
<td>52.192.78.22</td>
<td>80</td>
<td>1432</td>
<td>3</td>
<td>34</td>
<td>70</td>
<td>1201</td>
</tr>
<tr>
<td>192.168.0.184</td>
<td>TWCABLE-BACKBONE - Time Warner Cable Internet LLC, US</td>
<td>23.40.53.81</td>
<td>80</td>
<td>312</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>40</td>
</tr>
<tr>
<td>192.168.0.22</td>
<td>EDGECAST - MCI Communications Services, Inc. d/b/a Verizon Business, US</td>
<td>93.184.216.34</td>
<td>80</td>
<td>272</td>
<td>3</td>
<td>901</td>
<td>68</td>
<td>300</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>AMAZON-02 - Amazon.com, Inc., US</td>
<td>52.192.78.22</td>
<td>80</td>
<td>1138</td>
<td>3</td>
<td>29</td>
<td>79</td>
<td>1201</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>ASN-APPNEXUS - AppNexus, Inc, US</td>
<td>68.67.178.132</td>
<td>80</td>
<td>10239</td>
<td>1</td>
<td>5</td>
<td>40</td>
<td>73</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>FORTRUST-SOLUTIONS - FORTRUST, US</td>
<td>66.35.58.76</td>
<td>80</td>
<td>1258</td>
<td>1</td>
<td>2</td>
<td>50</td>
<td>32</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>IP not found</td>
<td>193.70.47.153</td>
<td>80</td>
<td>2084</td>
<td>1</td>
<td>1</td>
<td>100</td>
<td>53</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>IP not found</td>
<td>193.70.47.154</td>
<td>80</td>
<td>1490</td>
<td>1</td>
<td>2</td>
<td>50</td>
<td>294</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>IP not found</td>
<td>209.15.36.33</td>
<td>80</td>
<td>1117</td>
<td>1</td>
<td>6</td>
<td>33</td>
<td>32</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>OVH , FR</td>
<td>192.99.17.41</td>
<td>80</td>
<td>3652</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>48</td>
</tr>
<tr>
<td>192.168.0.35</td>
<td>RACKSPACE - Rackspace Hosting, US</td>
<td>146.20.132.50</td>
<td>80</td>
<td>3518</td>
<td>1</td>
<td>3</td>
<td>66</td>
<td>30</td>
</tr>
<tr>
<td>192.168.0.39</td>
<td>EDGECAST - MCI Communications Services, Inc. d/b/a Verizon Business, US</td>
<td>93.184.216.34</td>
<td>80</td>
<td>272</td>
<td>3</td>
<td>907</td>
<td>67</td>
<td>300</td>
</tr>
<tr>
<td>192.168.0.42</td>
<td>EDGECAST - MCI Communications Services, Inc. d/b/a Verizon Business, US</td>
<td>93.184.216.34</td>
<td>80</td>
<td>272</td>
<td>3</td>
<td>912</td>
<td>67</td>
<td>300</td>
</tr>
<tr>
<td>192.168.0.60</td>
<td>AKAMAI-ASN1 , US</td>
<td>104.95.176.44</td>
<td>80</td>
<td>8399</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>97</td>
</tr>
</tbody>
</table>

- Not practical to create alerts for each new IP
- What can we do?
Routes, BGP Dumps and ASN Mappings, Oh My

IP -> ASN -> Owner

8.8.8.8 8.8.8.7 8.8.8.6 8.8.8.5 -> ASN 15169 -> Google Inc., US

```python
In [1]: from flare.tools.whoisip import WhoisLookup

In [2]: who = WhoisLookup()

In [3]: who.get_asn('8.8.8.8')
Out[3]: 15169

In [4]: who.get_name_by_ip('8.8.8.8')
Out[4]: 'GOOGLE - Google Inc., US'
```
Hey SIEM engineer,
Maybe the person who wrote your product made it work that one time, but I don't care unless you make it work for me...
Do You Even Scale, Bro?

• Currently **NOT** suited for large enterprise networks.

• Tested on network with ~10,000 nodes at 10Gbps capture rates for a 24 hour period

• Supports ElasticSearch < 5.x (Currently updating for ES 6)

• Working on integration with GPUs

• Works best with suricata flow records, but customizable
Actionable Next Steps

- Identify New Beacons to ASN
- Create alerts using ElastAlert for new ASNs
- Publish an alert to Slack each time you receive a beacon to a new ASN
- Submit a PR
Level 2: Actionable Vulnerability Scans

864 Low Risk
5,194 Medium Risk
221,808 High Risk
14,971 Critical Risk
VulnWhisperer

• Free Open Source Software
• Currently supports Nessus
• Qualys in progress
• Written in Python
• Custom Risk Scores
• Asset Tagging
• Intended to create actionable data for defenders and metrics for managers (Track risk over time)
• Joint project with Justin Henderson

https://github.com/austin-taylor/VulnWhisperer
Setup Your Environment

vulnWhisperer.ini

[nessus]
enabled=true
hostname=localhost
port=8834
username=nessus_username
password=nessus_password
write_path=/opt/vulnwhisp/scans
db_path=/opt/vulnwhisp/database
trash=false
verbose=true

- Also supports CLI to override Username and Password
Run VulnWhisperer

python bin\vuln_whisperer -c configs\example.ini

[INFO] - Attempting to connect to nessus...
[SUCCESS] - Connected to nessus at 192.168.10.59:8834
[INFO] - Connected to database at /opt/nessus/database/report_tracker.db
[INFO] - Gathering all scan data... this may take a while...

Download for file id 1456454420.

Name

- Finance_Office_009_2145_2194_1510554983
- HR_Office_009_2194_1510554953
- Management_Network_009_2194_1510554555
VulnWhisperer Steps

1. Connect to NessusAPI
2. Export **ALL** Results
3. Write Results to Disk
4. Ship Results off to Logstash using FileBeats
5. Prepare and Enrich Data in Logstash
6. Forward to Elastic
7. Mitigate Prioritized Vulnerabilities
Ingest Workflow

Nessus Scan

Magic Happens

Filebeat

plain text log files

Logstash

JSON structured log documents

Elasticsearch

@HuntOperator
File Processing - Grok Filter

FinanceOffice_115_2212_1511836792

match => { "source" => "(?<file_path>\\:\[a-z A-Z_]*\\)(?<scan_name>[a-z-0-9\\.A-Z_\-]*)\{%INT:scan_id\}\{%INT:history_id\}\{%INT:last_updated\}" }
Question

Which site has the most critical vulnerabilities?
<table>
<thead>
<tr>
<th>Scan Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>HomeOffice_LAN_Servers</td>
<td>38,539</td>
</tr>
<tr>
<td>HomeOffice_Workstations</td>
<td>24,962</td>
</tr>
</tbody>
</table>
Could You Answer This?

Show me all of my HIPAA assets that have level 10 risk scores of services we don’t whitelist that belong to our finance office?
Custom Risk Scores

• CVSS Score of 10, but we don’t run Adobe in our Browsers

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>CWE ID</th>
<th># of Exploits</th>
<th>Vulnerability Type(s)</th>
<th>Publish Date</th>
<th>Update Date</th>
<th>Score</th>
<th>Gained Access Level</th>
<th>Access</th>
<th>Complexity</th>
<th>Authentication</th>
<th>Conf.</th>
<th>Integ.</th>
<th>Avail.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-0959</td>
<td>416</td>
<td>1</td>
<td>Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267. Adobe Flash Player Expanded Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.550, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK &amp; Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Reduce the Score in Logstash

```ruby
if [risk_score] != 0 {
    if [plugin_name] =~ "Adobe" and [risk_score] > 6 or [plugin_name] =~ "Java" and [risk_score] > 6 {
        ruby {
            code => "event.set('risk_score', event.get('risk_score') / 3)"
        }
        mutate {
            add_field => { "compensating_control" => "Adobe and Flash removed from browsers unless whitelisted site." }
        }
    }
}
```
Custom Risk Scores

By CVSS

<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Flash Player &lt;= 19.0.0.245 Multiple Vulnerabilities (APSB15-32)</td>
<td>123,570</td>
</tr>
<tr>
<td>Adobe Flash Player &lt;= 22.0.0.192 Multiple Vulnerabilities (APSB16-25)</td>
<td>76,002</td>
</tr>
<tr>
<td>Adobe Flash Player &lt;= 21.0.0.242 Multiple Vulnerabilities (APSB16-18)</td>
<td>51,624</td>
</tr>
<tr>
<td>Adobe Flash Player &lt;= 18.0.0.209 Multiple Vulnerabilities (APSB15-19)</td>
<td>48,888</td>
</tr>
<tr>
<td>MS15-124: Cumulative Security Update for Internet Explorer (3116180)</td>
<td>46,740</td>
</tr>
</tbody>
</table>

By Risk Score

<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB4022722: Windows 7 and Windows 2008 R2 June 2017 Cumulative Update</td>
<td>9,116</td>
</tr>
<tr>
<td>Microsoft XML Parser (MSXML) and XML Core Services Unsupported</td>
<td>1,538</td>
</tr>
<tr>
<td>Apple QuickTime Unsupported on Windows</td>
<td>1,464</td>
</tr>
<tr>
<td>KB4022719: Windows 7 and Windows 2008 R2 June 2017 Cumulative Update</td>
<td>1,431</td>
</tr>
<tr>
<td>Windows 2008 June 2017 Multiple Security Updates</td>
<td>1,248</td>
</tr>
<tr>
<td>Microsoft Excel Viewer Unsupported Version Detection</td>
<td>1,149</td>
</tr>
</tbody>
</table>
Track Risk Over Time

• Managers love this…
Do You Even Scale, Bro?
Do You Even Scale, Bro?

YES
Bringing It All Together

- Invest time up front and save time when it matters
Actionable Next Steps

- Setup VulnWhisperer to start ingesting your vulnerability scans
- Create custom risk scores
- Name scans by Site
- Create tags for your organizations most important assets
- Give back to the community and submit a PR
Questions?

Thank you!

www.austintaylor.io

@HuntOperator