Automated Cybersecurity Actions Using Splunk

Recruit Technologies

Mitsuhiro Nakamura  |  Senior Security Engineer:
September 26, 2017  |  Washington, DC
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.
Agenda

This is a short session.

1. BIO
2. Heuristic Analysis with SPL
3. Threat Profiling using Data Visualization
4. Real World
5. Unmanned Defense System
6. Wrap Up
Bio

Mitsuhiro Nakamura (Hiro)

▶ 10+ years experience in cyber security specializing in Pen-Test, Forensics, and Incident-Response.

▶ Built web application vulnerability assessment methodology.

▶ Data analysis for Threat Detection using Splunk.

▶ I have gave lectures at conf 2016 (Florida), and at SplunkLive 2016 (Japan)

▶ like: Windsurfing (Wave!)
We are committed to creating chances to discover “Opportunities for Life,” connecting users and clients through new channels.

### What A Kind Of Frauds?

<table>
<thead>
<tr>
<th>Frauds</th>
<th>Threats</th>
<th>Risk</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Exploitation and Account Takeover</td>
<td>Spoofing</td>
<td>Data Breach</td>
<td>Automatic Unmanned Defense System</td>
</tr>
<tr>
<td>Unauthorized Agency</td>
<td>Stock Leak</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abuse (dealer)</td>
<td>Nuisance</td>
<td>Business Risk</td>
<td>in preparation..</td>
</tr>
<tr>
<td>First party frauds (Greedy and selfish)</td>
<td>Virtual Currency Fraud</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Heuristic Analysis

Recovering Behavior from fragmented data.

Dig, dig, dig.
Chew this iron bitch up.
**Lookup**: iplocation / dnslookup / Tor-exitnode / Account Attributes & Fingerprint

\(\n\text{SPL (Heuristic)} \)

**INPUT**

**LOG & Attributes**

- Behavior
- Behavior
- Behavior

**OUTPUT**

- Profiling
- Profiling

- Custom Detection Rule
① Building Base Query
(Summary Index)

Whois, TorExitNode, WebAPI, etc
Reverse DNS
Country

② Heuristic Analysis

AnomalyData + Attributes + Statistics + StDev + NextStep-Behavior

We use various data before and after the point of incident, plus, User-Attributes.
Threat Profiling

Using Data Visualization
Kaleidoscope for White & Noise Filtering

Sankey Chart

stats profiling-data (one-million record)
Pipeline for Real-Threat Detection

Browser
FingerPrint - FingerPrint - Country - Speed - Bot/Hand - AccountID - Results - Attributes - Action - LastAction
Real World

The real aim of the attacker
Incident Response of Real World

Preparation | Attack | Account Takeover | Illegal exchange | Attackers say “mission completed”

Timeline

**The Signs of IOC**

- Before
- Just Before
- Just After
- After

RISK-Level

- High
- Low
They Are Coming On The Great Friday Night

Attacker

Hunter

Round 2!! (eternally)
Unmanned Defense System

We call them “Shield”.
The Birth of Unmanned Defense System

Detection | Triage | Respond
--- | --- | ---
Before (Manually)

Auto

Judge

Manual

Execute (only business hour)

Manual

Resettter

AuthDB

After (Unmanned Defense System)

Python or WebHook

Auto

API (Java)

Auto

AuthDB

24/7 Automated Action

Sleep
# WebHook vs InterSplunk

<table>
<thead>
<tr>
<th>Approach</th>
<th>Develop</th>
<th>Format</th>
<th>Multiple</th>
<th>Best Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webhook</td>
<td>a little</td>
<td>Solid</td>
<td>Incompatible</td>
<td>JSON, per record</td>
</tr>
<tr>
<td>InterSplunk</td>
<td>Necessary</td>
<td>Flexible</td>
<td>Supports</td>
<td>without JSON, Per record or Multiple</td>
</tr>
</tbody>
</table>

### WebHook

- **in**: select the time interval in minutes (e.g., 1 minute)
- **Trigger**: select the trigger condition (e.g., Once, For each result)
- **Throttle?**: select if the throttle should be applied

**Trigger Actions**
- Add additional actions if needed

**When triggered**
- Webhook
- URL: `https://account/reset`

### Intersplunk (custom alert)

- **is greater than**: set the comparison value (e.g., 0)
- **Trigger**: select the trigger condition (e.g., Once, For each result)
- **Throttle?**: select if the throttle should be applied

**Trigger Actions**
- Add additional actions if needed

**When triggered**
- Add to Triggered Alerts
- Run a script

**Filename**: `scip_hpr.py`

---

© 2017 SPLUNK INC.
Wrap Up

Splunkers for the Future
Encouragement of Automatic-Defense

Automatic (Task)

Detection → Respond

0-day

Innovation

Reset 🔄 Password

Auto

CAPTHCA

Image-Auth
Splunkers for the Future

Their DeepAnalysis has changed dramatically.

Before

Time & Delivery

Long Hours

(Wild-Samurai)

2014

After

Quality

Right Now

(Shuriken-Ninja)

2015 with SPL

They can judge things calmly..

Later..

Splunk> DASHBOARD

(ZEN)

2016

Later..

Bed

2017
Thank You

Facebook : https://www.facebook.com/hiro.goahead
Hiro : <nakamura@r.recruit.co.jp>

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