Quickly Advance Your Security Posture
With Splunk Security Essentials

David Veuve  |  Principal Security Strategist

September 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.
Personal Introduction

David Veuve
Principal Security Strategist, Splunk
SME for UEBA, Security, Architecture
dveuve@splunk.com
Former Splunk Customer
Primary author of the Splunk Security Essentials app

2017 Talks:
- Security Ninjutsu Part Four (Hi!)
- Searching FAST: Start Using tstats and other acceleration techniques
- Quickly Advance Your Security Posture with Splunk Security Essentials

Prior Conf Talks:
- How to Scale Search from _raw to tstats
- Security Ninjutsu Part Two: .conf 2015
- Security Ninjutsu Part One: .conf 2014
- Passwords are for Chumps: .conf 2014
Why Are We Talking About an App?

▶ A showcase of what’s possible in Splunk
▶ Just uses Splunk Enterprise
▶ It’s quick
▶ It’s easy
▶ It’s free
Who Are You?

- Maybe a user of Splunk Security Essentials?
- All Levels of Splunk Experience
- Probably like Security
What Will You Get?

- Detect things better
- Learn about powerful free apps
- Only One Marketing Slide!
1. Splunk Security Essentials Overview
2. SSE Demo
3. End to End Scenario
4. Wrap Up
Technical Components for Successful Security Analytics

Alert Aggregation
- Alert Creation
- Investigation

Threat Detection
- Manage High Volume
- Track Entity Relationships
- Combination ML + Rules

Alert Aggregation

Alert Creation
- Simpler Detection
- ML Based Detection
- Rules & Statistics
- Quick development
- Easy for analysts
- Detect unknown
- New vectors
- Heavy data science

Investigation
- Investigative Platform
- Analyst Flexibility
- Provide access to data analysis solutions
- Record historical context for everything
The Splunk Portfolio

Splunk Premium Solutions

Splunk IT Service Intelligence™

Splunk Enterprise Security™

Splunk User Behavior Analytics™

Rich Ecosystem of Apps & Add-Ons

Splunk>enterprise

Splunk>cloud

Splunk> Platform for Operational Intelligence

Forwarders

Syslog/TCP

Mobile

IoT Devices

Network Wire Data

Hadoop

Relational Databases

Mainframe Data
Identify bad guys:

- 50+ use cases common in Security Analytics products, free on Splunk Enterprise
- Target external and insider threats
- Scales from small to massive companies
- Save from app, send hits to ES/UBA

Solve use cases you can today for free, then use Splunk UBA for advanced ML detection.
What about…

- Ransomware?
- Fraud?
What Can I Detect With Splunk Enterprise?

- Malicious Insiders
- Commodity Malware
- Advanced External Attackers
### Splunk Security Essentials App Inventory

#### DOMAINS
- Access
- Data
- Endpoint
- Network
- Threat

#### DATA SOURCES
- Any Host Logs
- Electronic Medical Record System
- Email Logs
- Firewall
- Netflow
- Print Server Logs
- Salesforce Event Log File
- Source Code Repository Logs
- Splunk Notable Events

#### ALERT VOLUME
- Very Low
- Low
- Medium
- High
- Very High

“Say, aren’t those all recommended data sources for Splunk Security in general?”
Splunk Security Essentials

Types of Use Cases

- First Time Seen powered by stats
- Time Series Analysis with Standard Deviation
- General Security Analytics Searches
Where Can I Install Splunk Security Essentials?

- Your Laptop!
- Your Dev Environment!
- Your Production Environment!
- All Kinds of Production Environments!

Survey Results: Have You Tried to Install the App?

- Tried and Failed
- Installed in Dev
- Installed in Production
- Installed in Distributed Environment
- Installed in a SHC Environment
Getting Started with Splunk Security Essentials

- Download from apps.splunk.com
- Browse use cases that match your needs
- Data Source Check shows other use cases for your existing data
- Evaluate free tools to meet gaps, such as Microsoft Sysmon
  - (links inside the app)
What is Standard Deviation?

A measure of the variance for a series of numbers

<table>
<thead>
<tr>
<th>User</th>
<th>Day One</th>
<th>Day Two</th>
<th>Day Three</th>
<th>Day Four</th>
<th>Avg</th>
<th>Stdev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jane</td>
<td>100</td>
<td>123</td>
<td>79</td>
<td>145</td>
<td>111.75</td>
<td>28.53</td>
</tr>
<tr>
<td>Jack</td>
<td>100</td>
<td>342</td>
<td>3</td>
<td>2</td>
<td>111.75</td>
<td>160.23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>Day Five</th>
<th># StDev Away from Average … aka How Unusual?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jane</td>
<td>500</td>
<td>12.6</td>
</tr>
</tbody>
</table>
| Jack  | 500      | 2.42                                        | SUPER Anomalous!
Apply Splunk to Real Life Scenario

- **Actor:**
  Malicious Insider (because it’s hardest)

- **Motivation:**
  Going to work for competitor

- **Target:**
  Accounts, Opportunities, Contacts in Salesforce

- **Additional Target:**
  Sales Proposals in Box

- **Exfiltration:**
  Upload to a remote server

*Photo of Splunker, I promise she is not a malicious insider*
Monitoring Challenges

- No proxy
- No standard file servers
- No agents on laptop
- Cloud Services with their own APIs

How would you detect that?
Set Up Monitoring

- Ingest Salesforce Event Log File
  - https://splunkbase.splunk.com/app/1931/
- Ingest Box Data
  - https://splunkbase.splunk.com/app/2679/
- Install Splunk Security Essentials
  - https://splunkbase.splunk.com/app/3435/
- Schedule Salesforce use cases
- Build a custom Box use case
Splunk Security Essentials Demo
Managing Alert Volume vs Value

Use Low Volume Searches

Splunk ES Risk Framework

Splunk UBA Threat Models

UBA + ES Adaptive Response

Slow Response from Basic Alerts

Fast Response from Advanced Alerts

Managing Alert Volume vs Value
Managing Alert Volume vs Value

Use Low Volume Searches

Splunk ES Risk Framework

Splunk UBA Threat Models

UBA + ES Adaptive Response

Everyone starts here, and spends most of their time here.
Aggregate Alerting with ES Risk

Enterprise Security has a Risk Framework designed for aggregating low severity indicators.

<table>
<thead>
<tr>
<th>risk_object</th>
<th>risk_object_type</th>
<th>risk_score</th>
<th>source_count</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>aseykoski</td>
<td>user</td>
<td>480</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>jsmith</td>
<td>user</td>
<td>270</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Hax0r</td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>agasiewski</td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td><a href="mailto:aseykoski@acmetech.com">aseykoski@acmetech.com</a></td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>cargento</td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>dmsys</td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td><a href="mailto:htrapper@acmetech.com">htrapper@acmetech.com</a></td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>wohler</td>
<td>user</td>
<td>240</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td><a href="mailto:atria@c1z.at">atria@c1z.at</a></td>
<td>user</td>
<td>120</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
Splunk UBA Threat Models leverage Data Science, Machine Learning

- Finds important, inter-related anomalies that analysts should actually view
- Support more advanced anomaly detections!
High Confidence alerts from UBA fed into ES

Take actions like

- Box: “Change Permissions”
- AD: “Reset Password” or “Disable Account”
- PAN: Isolate Host

27 partners!
ES + UBA + SSE Demo
But My Company Is So Custom

► Do you want to build your own detections like this?
► What if your environment is totally custom?
► No product has ever worked out of the box, and that’s why you like Splunk, right?

We’ve got you.

Click Assistants, then “Detect Spikes”
Our Malicious Insider, Jane Smith, also downloaded some proposals from Box

Finding Box downloads spikes is easy, but we want focus on the Proposal Folder

We will use the Detect Spikes assistant to help us
- inputlookup anonymized_box_logs.csv | search folder="PROPOSALS" bucket _time span=1d | stats count by user _time

- Looking for "count" by "user" with "6" standard deviations
| inputlookup anonymized_box_logs.csv | search folder="PROPOSALS" | bucket _time span=1d | stats count by user _time |

Looking for “count” by “user” with “6” standard deviations

<table>
<thead>
<tr>
<th>Outlier(s)</th>
<th>Total Result(s)</th>
<th>Raw Event(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>114</td>
<td>Got Her!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outliers Only</th>
<th>num_data_samples</th>
<th>count</th>
<th>avg</th>
<th>lowerBound</th>
</tr>
</thead>
<tbody>
<tr>
<td>jsmith</td>
<td>15</td>
<td>112</td>
<td>3.071429</td>
<td>-14.61261</td>
</tr>
</tbody>
</table>
Wrap-Up
Splunk Security Portfolio

Splunk Enterprise Detection
- Log Aggregation
- Splunk Security Essentials
- Rules, statistics, correlation

Enterprise Security Response
- OOB key security metrics
- Incident response workflow
- Adaptive response

Splunk UBA Detection
- Risky behavior detection
- Entity profiling, scoring
- Kill chain, graph analysis

Realm of Known
Human-driven

Realm of Unknown
ML-driven
What Do I Want To Do Next?

- Powershell
- Database
- Full Splunk 7.0 Compatibility
- Historical Checking
- Auto-Enable?
What Did We Cover?

1. Splunk Security Essentials shows you new detection use cases
2. Ultimately it just uses Splunk Enterprise – Power of the Platform!
3. You can build your own use cases easily!
4. As you advance, look to ES or UBA to improve threat detection
1. Download Splunk Security Essentials

2. Try the Data Source Check dashboard

3. If you want to learn *how* -- attend Security Ninjutsu tomorrow!

4. If you want to build your own ML: Security Ninjutsu tomorrow Automating Threat Hunting w/ML tomorrow
Thank You

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

I get to come back if you give me good ratings. Rate high, early, and often!