Modernizing InfoSec Training and IT Operations at USF

Goodbye Tedious Tasks!
A Novel Automation Framework Leveraging Splunk

Tim Ip, Senior Security Engineer
Nicholas Recchia, Director & Information Security Officer

September, 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.
About Us

- University of San Francisco (USF) more than 12,000 students, faculty and staff
- Catholic Jesuit Education
About Me

Tim Ip

- **Senior Security Engineer**
- Leverages Splunk to automate processes in USF
- From Hong Kong 2 years ago
- 10+ years experience in security industry and 6+ years experience on SIEM development
- Previous worked for a consulting company as a SIEM consultant
- Primary focus on Security monitoring, process automation and big data analytics
- Holds a master degree, OSCP, GPEN, CISSP, CISA and CISM

GitHub / LinkedIn / Twitter: [timip.net](http://timip.net)
About Me

- Nick Recchia
  - Director & Information Security Officer
  - USF Alumnus
  - 12+ years experience in Information Technology and 8+ years focused on InfoSec with integration
  - Manages the security group and oversee related InfoSec programs
  - Holds doctorate degree in Organization and Leadership, CISSP, PMP, ITILv3, etc.
  - LinkedIn
Agenda
Our Splunk Journey

▶ Ch.1 – Background & Context
• InfoSec training: from manual methods to strategic innovation

▶ Ch.2 – Course Automation
• Methodology and technical highlights

▶ Ch.3 – IT Automation
• Reuse methodology

▶ Key Takeaways
▶ Q&A
Background & Context

InfoSec training: from manual methods to strategic innovation
Background: Technology Transformation

Manual methods to strategic innovations
Background: Technology Transformation
Manual methods to strategic innovations

Current State (2015)

Future State (2017)
Background: Infosec Training @ USF
Timeline: required security training

- ~2007: New employee orientation
- 2010: SANS Security The Human (STH)
  - Orientation revamped cutting ISO
- 2014: ITS Division Re-org
- 2015: Rebuilt InfoSec Team
- 2016: New CIO
  - How? Security Training
  - Model after Harassment training?
Context: Infosec Training @ USF
Conceptual Development

Technology
Process
People

Automation
InfoSec Course
Context: People, Process and Technology

People:
InfoSec Team

Enrollment (3000 people)
Employee, Faculty & Affiliate

Technology:
canvas
SANS

Process:
• Enrollment?
• Monitoring progress?
• Encourage completion?
Context: Enrollment

High-level: Leverage Existing Process

HR processes new employee into Banner

Banner Enterprise Resource Planning (ERP)

Start date confirmed

Nightly update

USF LMS InfoSec Course
Context: Monitor Progress
High-level: Automated Course Alerts & Mgmt. Reports

USF LMS
InfoSec Course

Banner ERP

Course Logs

Correlation and Alerting - SIEM

Staff-Supervisor Data
Faculty Org Data
Affiliate Sponsor Data
# Concept: Auto Alerts

**High-level:** Inform, Remind, Escalate

<table>
<thead>
<tr>
<th>Alert #</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Schedule</strong></td>
<td>Day 1</td>
<td>Day 10</td>
<td>Day 27</td>
<td>Day 31</td>
<td>Monthly</td>
</tr>
<tr>
<td><strong>Email Title</strong></td>
<td>Welcome</td>
<td>Courtesy Reminder</td>
<td>Due Date Approaching</td>
<td>Manager Escalation</td>
<td>Executive Status Report</td>
</tr>
</tbody>
</table>
Context: Infosec Training @ USF

Conceptual formula

Trusted Partnership

Business Intel + Splunk Ninja = Automation
Course Automation
Framework Introduction

Use Case: InfoSec Course Automation

1. Course Data Input
2. Actions
3. Intelligence Input
4. Knowledge

InfoSec Course Automation
How to make it happen?

Knowledge

Actions

Course Data

Intelligence
Splunk@USF

Provides:
- Filtering
- Compression
- Encryption

Splunk Heavy Forwarder

Splunk Cloud>

Search Head

Splunk Heavy Forwarder on AWS

On-Premise

Data from other systems

User Endpoints

Infra.

Data from external 3rd party systems

User Endpoints

Splunk Cloud>

Search Head

Splunk Heavy Forwarder on AWS

On-Premise
Provides:
- Customized Automation
- Development Environment
1. Course Data Input

For InfoSec Course
Architecture

Course Data

Knowledge

Intelligence

Actions

splunk
Canvas Integration

- Gradebook History
- Assignment Submission
- Enrollments
- Section
- User List
- Ana Student Summaries
- Course Assignment

API

CANVAS Raw Data

SPL

InfoSec Student Status Snapshot
Canvas Integration Dashboard

Infosec Course - Monitoring

Statistics (Click the number to drill down details)

- All student(s) exists in ServiceNow
- In progress / current: 1,231 student(s)
- Completed: 1,572 student(s)
- Suspicious enrollment: 335 student(s)
- Bypass: 0 student(s)

Course Completion

Students who completed last assignment yesterday

<table>
<thead>
<tr>
<th>name</th>
<th>division</th>
<th>login_id</th>
<th>graded_at</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>21-ARTS AND SCIENCES</td>
<td>ebr</td>
<td>2017-04-24 20:16:19 PDT</td>
</tr>
<tr>
<td>Dow</td>
<td>25-EDUCATION</td>
<td>daf</td>
<td>2017-04-24 18:32:08 PDT</td>
</tr>
<tr>
<td>José</td>
<td>21-ARTS AND SCIENCES</td>
<td>jil</td>
<td>2017-04-24 17:07:49 PDT</td>
</tr>
<tr>
<td>Brian</td>
<td>21-ARTS AND SCIENCES</td>
<td>den</td>
<td>2017-04-24 16:24:51 PDT</td>
</tr>
</tbody>
</table>

Actionable?
Ninja Brainstorming
We need something more actionable

InfoSec Team Division Leads need to access to the data to monitor their staff progress!

How to give access to the division leads?

Send the information to them an email?

Export PDF
Schedule PDF Delivery
Print
Ninja Brainstorming
We need something more actionable

Email Report? No!

I need to make the email more user friendly!
2. Actions

For InfoSec Course
Architecture

Course Data

Intelligence

Knowledge

splunk

Actions
Notification
Type of notification

To Students:
• Welcome Email
• Reminder Email
• Overdue Email

To division leads:
• Monthly Report
• Escalation Report
Default Alert Notification

- Not user friendly
- Lack of enforcement
- Not Actionable
Customized Email Notifications

Goals

- User friendly email
- Dynamic information from Splunk
- Flexible and reusable

Welcome!

Dear [Name],

Welcome! You have been enrolled in the required Information Security Awareness Basic Training course. This course must be completed within 30 business days from today, which is Wednesday, September 13, 2017. This mandatory course helps keep university assets and data secure, and is overseen by USF Information Technology Services & Human Resources.

For your information, failure to complete this requirement could result in suspension of your USF network and email access. Click here to take the course now.

Rather take the course in a day or two? Add to calendar: Google Calendar • Outlook

Additional Information:

As you may know, awareness of cyber security is one of the most important aspects to safeguarding university data. In order to avoid pitfalls and maintain a high level of awareness, participation from all members of the University community is essential.

The following 6 topics will be covered to establish a foundation for our shared responsibilities:

1. Social Engineering: recognizing ways people try to extract information from you
2. Email & Messaging: avoiding suspicious attacks
3. Browsing: safely browsing the Internet
4. Passwords: creating and maintaining quality passwords
Customized Email Notification Scheduler

Search Head

Splunk Query

Results

Email Template

"@C0$9A">&lt;h3&gt;Sheduling&lt;/h3&gt; &lt;table border="0" cellspacing="5" cellpadding="5" width="100%"&gt; &lt;tr&gt; &lt;td&gt;Dear $first_name$ $last_name$&lt;br/&gt;&lt;br/This is a second course.&lt;/td&gt; &lt;/tr&gt; &lt;/table&gt; &lt;font size="3"&gt;&lt;br/Email Scheduler

- Expanding results
- Replace tokens with query results
- Loop
- Send out email
Customized Email Notification
For Student

- Reminder, Due Date Approaching and Due Date Overdue Alert
  - All dynamic information from Splunk query
  - Customized “Add to Calendar” Link

Due Date Approaching Overdue

Dear [Name],

This is a second courtesy reminder notice. Your required Information Security Awareness course completion due date is Monday, August 07, 2017.

Click here to take the course now.

Rather take the course in a day or two? Add to calendar: Google Calendar • Outlook

A copy of the original message is below:

Welcome! You have been enrolled in the required Information Security Awareness Basic Training course. This course must be completed within 30 business days from today, which is Monday, August 07, 2017. This mandatory course helps keep university assets and data secure, and is overseen by USF Information Technology Services & Human Resources.

For your information, failure to complete this requirement could result suspension of your USF network and email access.

Click here to take the course now.

Rather take the course in a day or two? Add to calendar: Google Calendar • Outlook

Additional Information:

As you may know, awareness of cyber security is one of the most important aspects to safeguarding university data. In order to avoid pitfalls and maintain a high level of awareness, participation from all members of the University community is essential.
Executive Report
- Statistics by role
- Overview and details

Monthly Executive Escalation Status Report

Dear [Name],

Below is the Information Security Awareness Course status report for your division. Please review the overdue section and follow-up with those individuals for completion. As a reminder the system has sent each of these people three courtesy reminders.

Sincerely,
Information Security and Compliance (ISC)

This is an automated message. Please do not reply. Contact infosec@usfca.edu with questions or concerns.

Statistics

<table>
<thead>
<tr>
<th>Role</th>
<th>Completion Percentage</th>
<th>No. of Past Due People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affiliate</td>
<td>62%</td>
<td>12</td>
</tr>
<tr>
<td>Employee_FT</td>
<td>100%</td>
<td>0</td>
</tr>
<tr>
<td>Employee_PT</td>
<td>100%</td>
<td>0</td>
</tr>
<tr>
<td>Faculty_PT</td>
<td>58%</td>
<td>4</td>
</tr>
</tbody>
</table>
### Affiliate Details

**Statistics**

<table>
<thead>
<tr>
<th>Total Number</th>
<th>Completed</th>
<th>In Progress</th>
<th>Past Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>31</td>
<td>19</td>
<td>12</td>
</tr>
</tbody>
</table>

**List of Past Due People**

<table>
<thead>
<tr>
<th>Name</th>
<th>Enrollment Date</th>
<th>No. of business day from first enrollment</th>
<th>Total Activity Time (Minutes)</th>
<th>Progress</th>
<th>No. of Outstanding Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2017-07-14</td>
<td>12</td>
<td>0</td>
<td>0%</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2017-07-14</td>
<td>12</td>
<td>0</td>
<td>0%</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2017-07-14</td>
<td>12</td>
<td>0</td>
<td>0%</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2017-07-14</td>
<td>12</td>
<td>0</td>
<td>0%</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2017-07-14</td>
<td>12</td>
<td>0</td>
<td>0%</td>
<td>8</td>
</tr>
</tbody>
</table>
USER EXPERIENCE

USER FRIENDLY
Ninja Brainstorming
Lack of Enforcement

Will students ignore the notification?

How to influence the action?

Escalate to supervisor!
Hmm... Where can we get the supervisor information?
3. Intelligence Input

For InfoSec Course
Architecture

Course Data

Knowledge

Intelligence

splunk
Banner/ServiceNow – Splunk Integration

- Banner/ServiceNow
- ERP
- ITSM
- Daily Batch Job
- Banner Raw Data
- ServiceNow Raw Data
- Splunk Apps
- User Inventory
- SPL
- Banner Raw Data
## Ingest ERP Data

**Banner: Escalation Data**

<table>
<thead>
<tr>
<th>Employee</th>
<th>Supervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim</td>
<td>Nick</td>
</tr>
<tr>
<td>Vince</td>
<td>Nick</td>
</tr>
<tr>
<td>Nick</td>
<td>Opinder</td>
</tr>
<tr>
<td>Michael</td>
<td>Nick</td>
</tr>
<tr>
<td>Opinder</td>
<td>Paul</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee</th>
<th>Escalation Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim</td>
<td>Tim, Nick, Opinder, Paul</td>
</tr>
<tr>
<td>Vince</td>
<td>Vince, Nick, Opinder, Paul</td>
</tr>
<tr>
<td>Nick</td>
<td>Nick, Opinder, Paul</td>
</tr>
<tr>
<td>Michael</td>
<td>Michael, Nick, Opinder, Paul</td>
</tr>
<tr>
<td>Opinder</td>
<td>Opinder, Paul</td>
</tr>
</tbody>
</table>
# Ingest ITSM data

## ServiceNow: User Profile

- **Roles**
- **Department**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>First name</td>
<td></td>
</tr>
<tr>
<td>Last name</td>
<td></td>
</tr>
<tr>
<td>USF Roles</td>
<td>EMPLOYEE</td>
</tr>
<tr>
<td>Employee</td>
<td>FT_STAFF</td>
</tr>
<tr>
<td>Classification</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>Mobile phone</td>
<td></td>
</tr>
<tr>
<td>Contact Phone</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Lone Mountain North</td>
</tr>
<tr>
<td>Campus Address</td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Cost center</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>ldap</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

**VIP**: 
- **Not Self Service**: checked
- **Locked out**: unchecked
- **Active**: checked

**Email**: auxfca.edu

**Notification**: Email

**Time zone**: System (America/Los_Angeles)

**Updated**: 7-03-2017 05:17:33

**Created**: 7-31-2015 05:22:29
4. Knowledge

For InfoSec Course
Business Logic
From complex business requirements and SPL queries

Day 1
Welcome Email (Employee)

Day 10
Courtesy Reminder (Employee)

Day 27
Course Completed
If user completed the course, they will receive a congratulation email. (Employee)

Day 27
Due Date Approaching (Employee and Supervisor)

Day 30
Manager Escalation (Employee, Supervisor and Manager)
We will listed on department head escalation report.
Knowledge

Ninja Experience/Skills

Business Knowledge

Splunk SPL Query / dashboard/ automation
Results

InfoSec Course
Use Case
For supporting InfoSec Course Automation

1. Machine Data
   - Enrollment
   - Score
   - Assignment

2. Actions
   - Customized Email Notification Scheduler

3. Intelligence
   - ServiceNow: User Inventory
     - Banner: Escalation Path

4. Knowledge
   - Business Logic
   - Splunk Ninja
   - Splunk SPL Query
Normal Notification
Notification vs Completion

Timechart: Email Count and User Completion Count
- Due Date Approaching Overdue
- Due Date Overdue
- Reminder
- Welcome
- Completion_Count

© 2017 SPLUNK INC.
Course Data
Actions
Intelligence
Knowledge

InfoSec Course
Automation
Machine Data
Adaptive Responses
Intelligence
Knowledge

IT InfoSec Course
Automation

© 2017 SPLUNK INC.
USF Automation Framework

**Machine Data**
- OS/Application Log
- App from Splunkbase
- Customized API

**Intelligence**
- CMDB
- User Profile
- Escalation Path

**Knowledge**
- Business Logic
- Splunk Ninja
- Splunk SPL Queries

**Adaptive Responses**
- Self-Service Notification
- ServiceNow Ticket Creation
Intelligence Inputs

External
- Splunkbase
  - e.g.: Splunk Add-on for Facebook ThreatExchange
- Customized Threat Intelligence Download
  - https://github.com/timip/threatintel

Internal
- User Inventory (Human)
- CMDB (Machine)
Adaptive Responses

Human

Severity

Students

Faculty

Customized Email

ServiceNow Ticket

Employee/ Affiliate

Customized Email

ServiceNow Ticket

Slack Channel
Inactive PCI Domain Account

Dear,

Our security intelligence system has detected the following issue(s) with your PCI domain account. Please follow suggested actions below to rectify the issue(s).

If you have any questions, please feel free to contact ITS Helpdesk.

Sincerely,
Information Security and Compliance (ISC)

Issues

Your PCI Account is inactive for more than 90 days

Action: Please logon to a designated PCI Point of Sale laptop to retain access to your PCI account. If your job function has changed and you no longer require your PCI account, please:
- Contact by email and request your account to be decommissioned
- (ITS staff only) Obtain documented approval from department director, then submit a ServiceNow ID removal request ticket to DE Team

Your PCI account password has not been changed for more than 90 days

Action: Please login to a designated PCI Point of Sale laptop and reset your password. If you need assistance, please contact ITS Help Desk.
Adaptive Responses
Next Step: Human + Machine

Students
- Customized Email
- ServiceNow Ticket

Faculty
- Customized Email
- ServiceNow Ticket
- Slack Channel

Employee/ Affiliate
- Customized Email
- ServiceNow Ticket

Machine
- Trigger Antivirus Full Scan
- Apply new IP blocking firewall rule
- And more…
Knowledge

Ninja Experience

Business Requirements

Splunk SPL Query
Expanding Use Cases
Increase automation to IT

Machine Data Input
- InfoSec Course Automation: Canvas
- PCI Password Expired Notification: Domain Controller User List
- PCI Anti-Virus Problem Notification: Sophos Log

Intelligence Input
- Banner / ServiceNow

Adaptive Response
- Email

Knowledge
- Email
- Email / ServiceNow Ticket
- Splunk Ninja + Business Intel

Splunk Staffing
- ServiceNow User Profile
- ServiceNow CMDB

ServiceNow Staffing
- ServiceNow User Profile
- ServiceNow CMDB
- ServiceNow Ticket
- Splunk Ninja + Business Intel
Key Takeaways

People:
• Trusted partnership - business intel/company culture & Splunk Ninja skills

Technology
• Splunk - reuse valuable data for various use cases – security, IT operations, beyond

Process
• Transition data/business intelligence in to queries/actions

Automation: Turn data/intelligence into answers and/or actions
Thank You

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