



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



130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFGADF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD1SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
10.55.187 - - [07/Jan 18:10:57:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
10.55.187 - - [07/Jan 18:10:57:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"

About Me

▶ Tim Ip

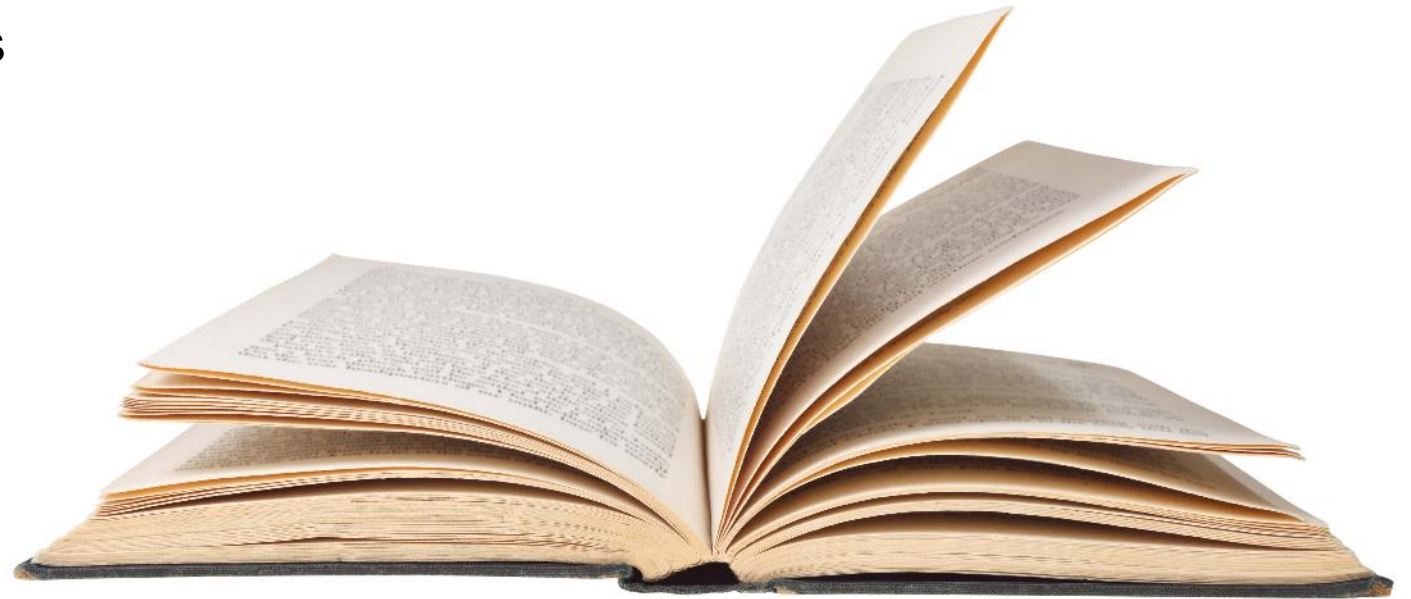
- **Senior Security Engineer**
- Leverages Splunk to automate processes in USF
- From Hong Kong 2 years ago
- 10+ years experience in security industry and 6+ years experience on SIEM development
- Previous worked for a consulting company as a SIEM consultant
- Primary focus on Security monitoring, process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



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

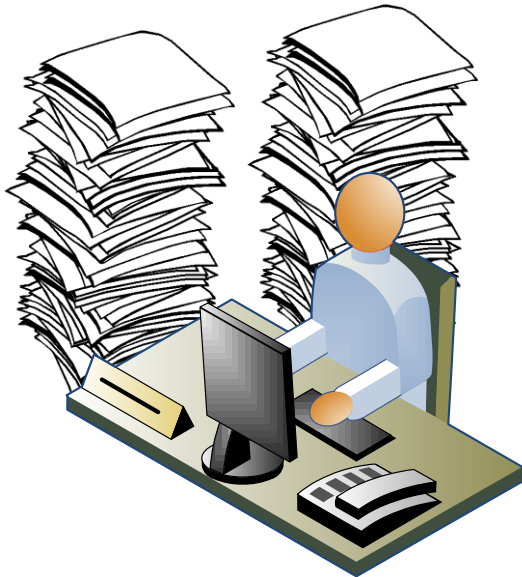
Manual methods to strategic innovations



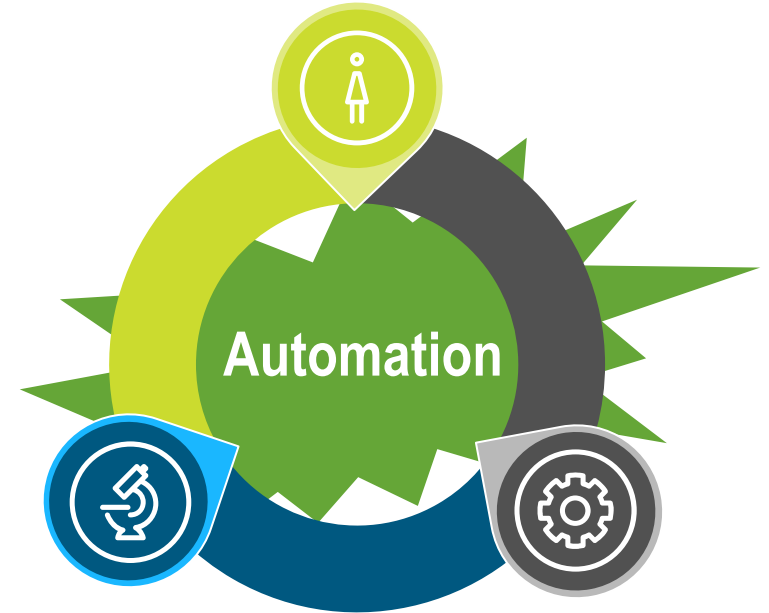
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (C  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Comcast/11.0 (Win  
://buttercup-shopping.com/c?kitemId=EST-16&product_id=RP-LI-02" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
do?action=purchase&itemId=EST-6&product_id=FI-SW-01" 468 125.17 14 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Win  
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Comcast/11.0 (Win
```


Background: Technology Transformation

Manual methods to strategic innovations



**Current State
(2015)**

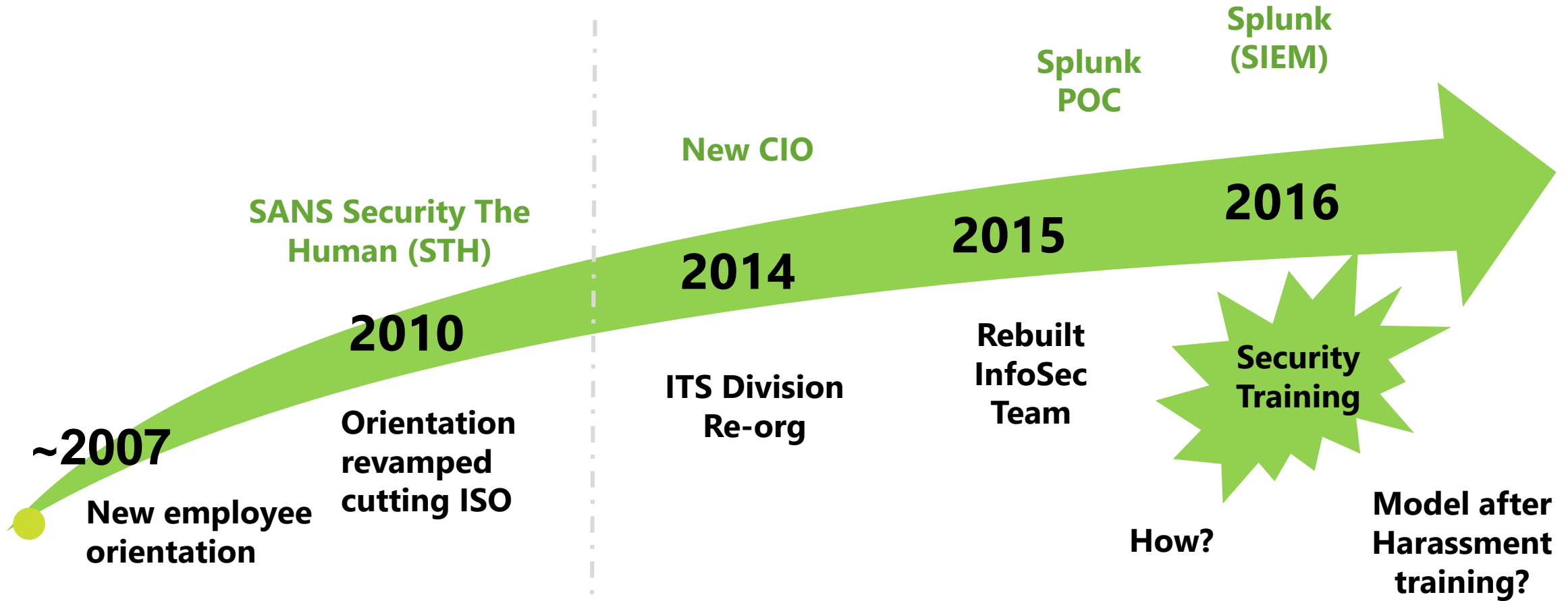


**Future State
(2017)**

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01"

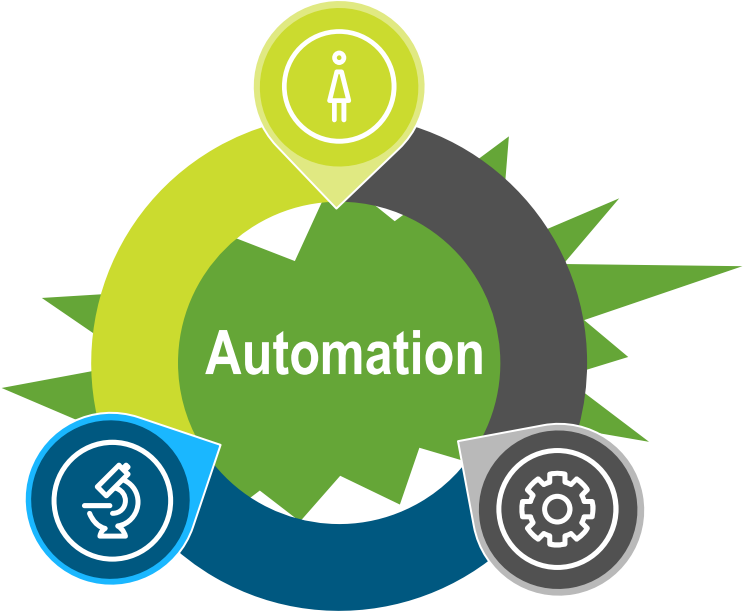
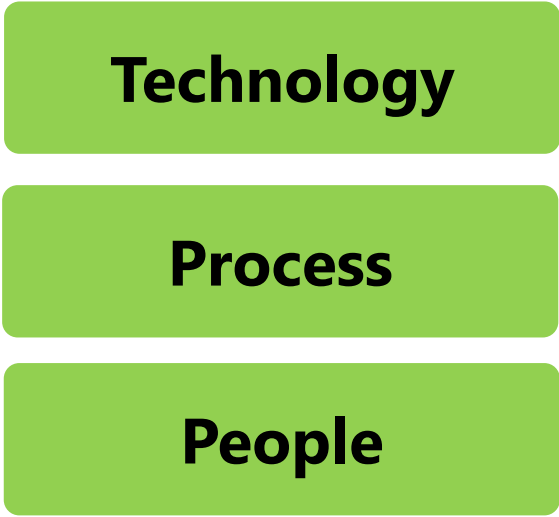
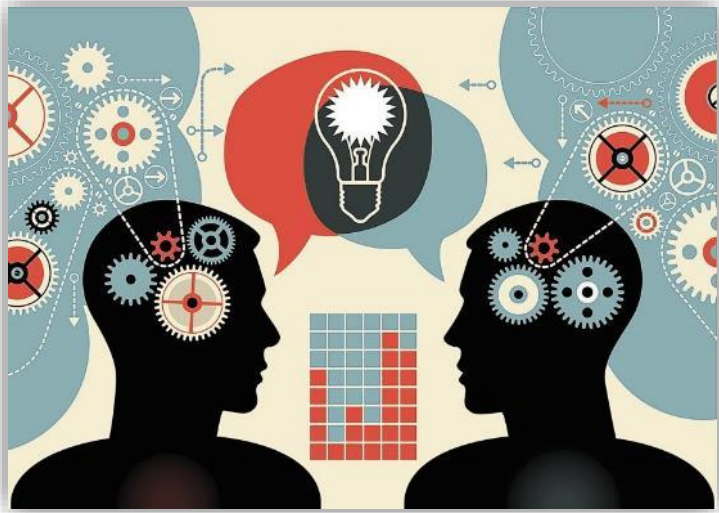
Background: Infosec Training @ USF

Timeline: required security training



Context: Infosec Training @ USF

Conceptual Development



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" ...  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" ...  
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" ...  
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14 ... sscreen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" ...  
buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" ...  
buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" ...
```

InfoSec Course

Context: People, Process and Technology

People:

InfoSec Team



Enrollment (3000 people)
Employee, Faculty & Affiliate

Technology:



Process:

- Enrollment?
- Monitoring progress?
- Encourage completion?

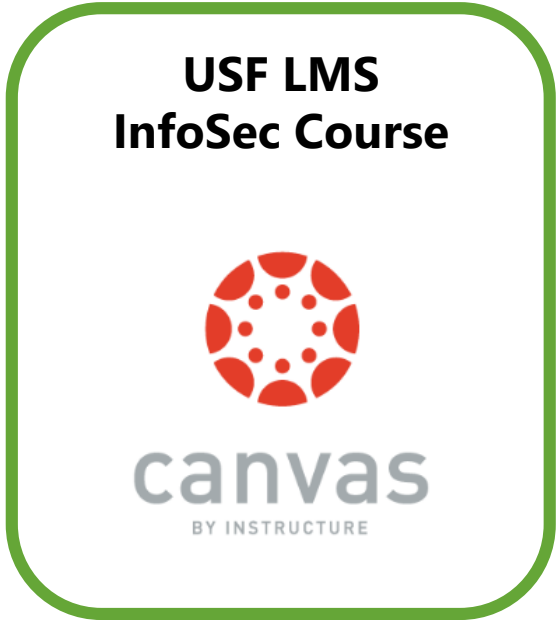


Context: Enrollment

High-level: Leverage Existing Process



HR processes new employee into Banner



130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
 128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 317.27.160.0.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
 ://buttercup-shopping.com/oldlink?item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.1.1.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=FLOWERS-1088"
 ://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
 ://buttercup-shopping.com/oldlink?item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.1.1.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=FLOWERS-1088"

Concept: Auto Alerts

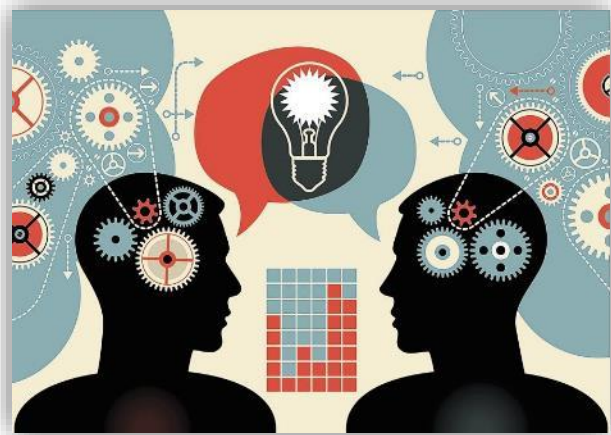
High-level: Inform, Remind, Escalate

Alert #	1	2	3	4	
Email Schedule	<i>Day 1</i>	<i>Day 10</i>	<i>Day 27</i>	<i>Day 31</i>	Monthly
Email Title	<i>Welcome</i>	<i>Courtesy Reminder</i>	<i>Due Date Approaching</i>	<i>Manager Escalation</i>	Executive Status Report
Recipient(s)	<i>1.Employee</i>	<i>1.Employee</i>	<i>1.Employee 2.Supervisor</i>	<i>1.Employee 2.Supervisor 3.Manager</i>	Sent to associated Division/School Leaders

Context: Infosec Training @ USF

Conceptual formula

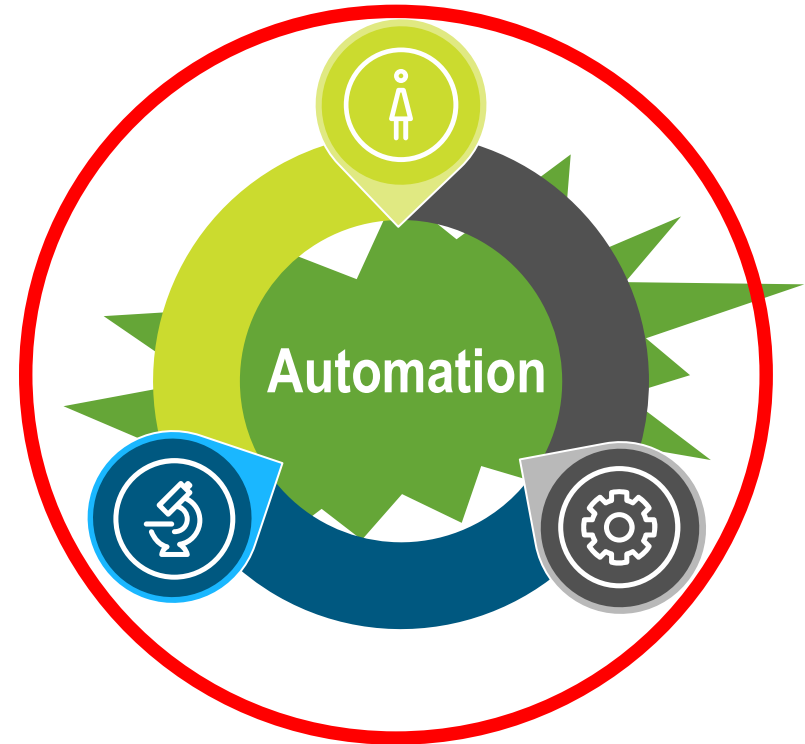
Trusted Partnership



+



=



Business Intel

+

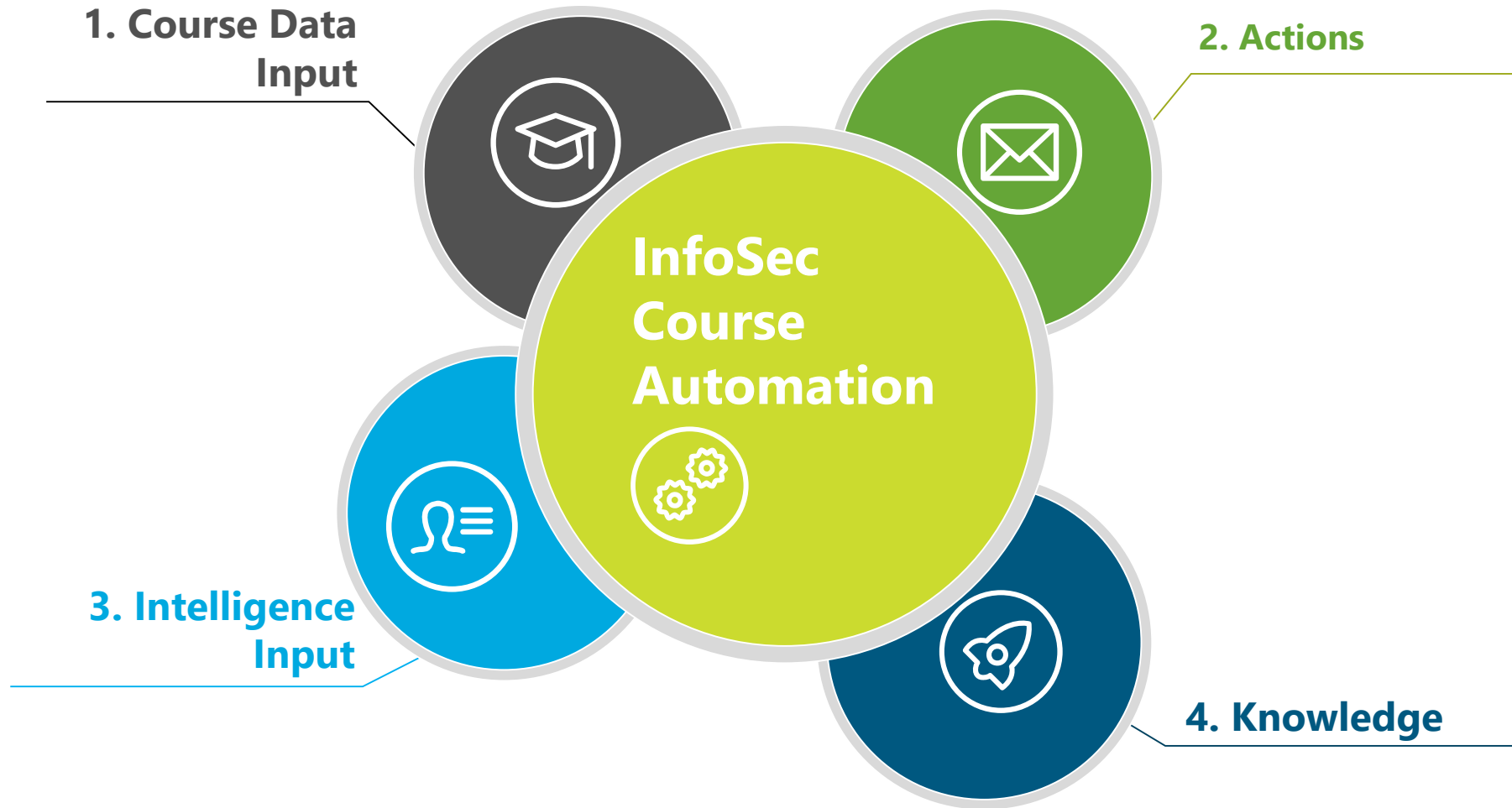
Splunk Ninja 

130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" Moz/1.12.0.0...
 128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Comp/1.1.1.1...
 317.27.160.0.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...
 10.10.1.1 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" Moz/1.12.0.0...

Course Automation

Framework Introduction

Use Case: InfoSec Course Automation



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Comodo Dragon 11.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
10.2.2.100 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0"
```

How to make it happen?



Course Data



Intelligence



Knowledge



Actions



splunk>

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"

```


Splunk@USF

Provides:

- **Filtering**
- **Compression**
- **Encryption**

Data from other systems



Banner



Elucian Ethos Identity

Info

3rd party



canvas

QUALYS



User Endpoints



SplunkCloud >

Splunk Heavy Forwarder

On-Premise

Splunk Heavy Forwarder on AWS


Search Head

Splunk@USF


Provides:

- *Customized Automation*
- *Development Environment*

Data from other systems



Banner



Ellucian Ethos Identity

Infra.



Splunk Cloud

Splunk Heavy Forwarder

On-Premise

Splunk Heavy Forwarder on AWS

Search Head

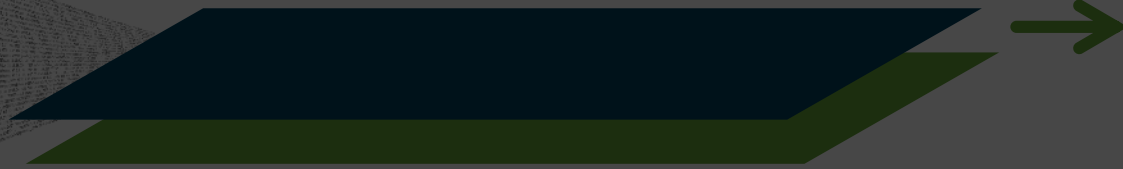
Architecture

 Course Data

 Intelligence

 Knowledge

 Actions



splunk>

1. Course Data Input

For InfoSec Course

Architecture



Course Data



Intelligence



Knowledge



Actions

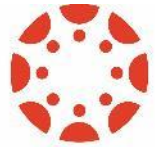
splunk>

splunk>

conf2017

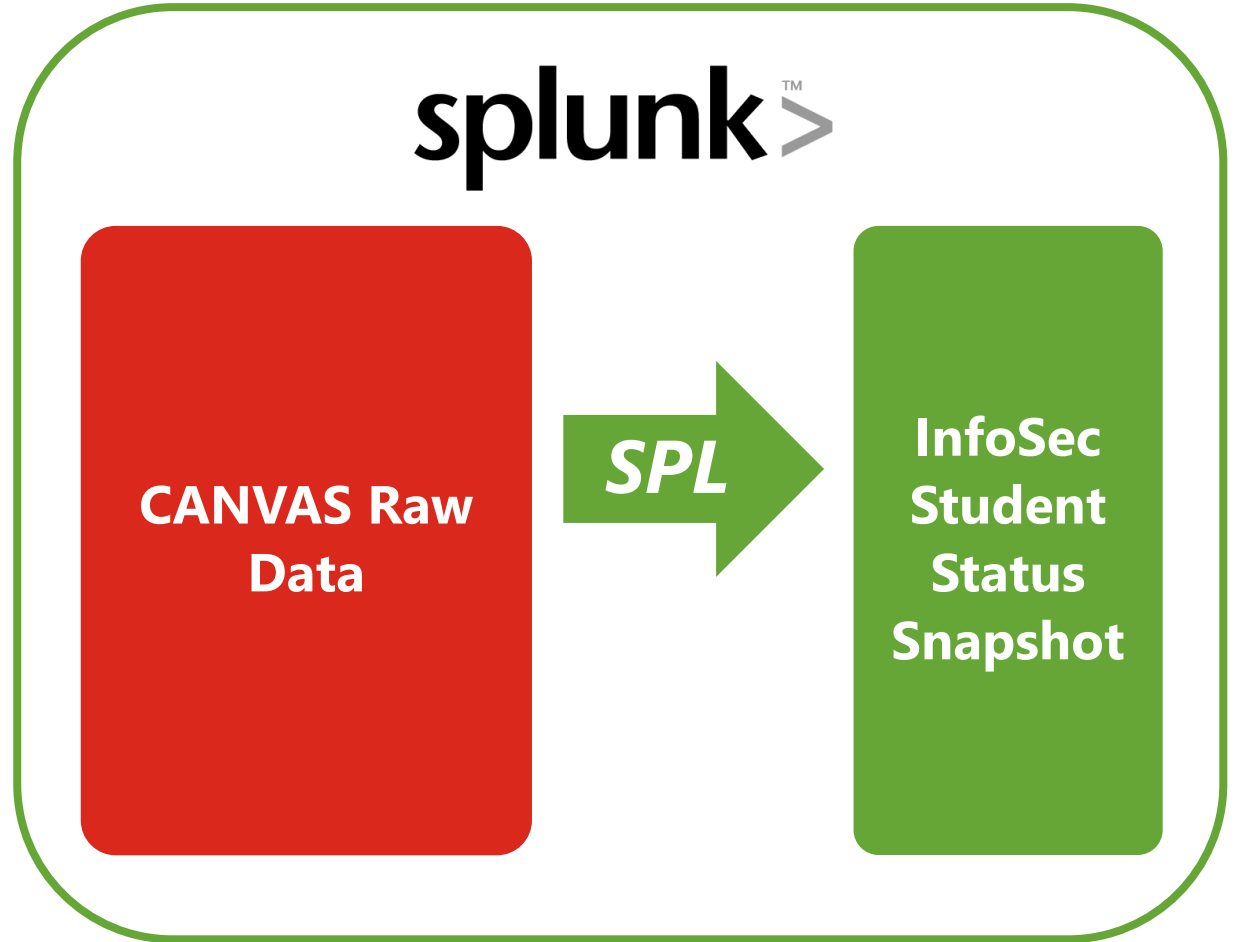


Canvas Integration



canvas

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



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Macintosh; Intel Mac OS X 6_8_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2861.97 Safari/537.36"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2861.97 Safari/537.36"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80 (Macintosh; Intel Mac OS X 6_8_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2861.97 Safari/537.36"
125.17.14 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80 (Macintosh; Intel Mac OS X 6_8_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2861.97 Safari/537.36"
125.17.14 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80 (Macintosh; Intel Mac OS X 6_8_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2861.97 Safari/537.36"
  
```

Canvas Integration

Dashboard



Infosec Course - Monitoring

Select a course: L1PROD: Basic Training - ...
 Select a section: All
 Division: All
 Role: All

Statistics (Click the number to drill down details)

All student (Exists in ServiceNow) 2,803	In Progress / Current 1,231 student(s)	Completed 1,572 student(s) completed the course	Suspicious Enrollment 335 student(s)	Bypass 0 student(s) bypass assignment(s)
-----------------------------------------------------------	------------------------------------------------------------	---------------------------------------------------------------------	----------------------------------------------------------	--------------------------------------------------------------

Hall of Fame

Students who completed last assignment yesterday

name	division	login_id	graded_at
Patri	21-ARTS AND SCIENCES	mur	2017-04-24 21:53:27 PDT
Editr	21-ARTS AND SCIENCES	erbc	2017-04-24 20:10:19 PDT
Daw	25-EDUCATION	dak	2017-04-24 18:32:08 PDT
Jose	21-ARTS AND SCIENCES	jslai	2017-04-24 17:07:09 PDT
Briar	21-ARTS AND SCIENCES	derr	2017-04-24 16:34:51 PDT
Mari	21-ARTS AND SCIENCES	mjc	2017-04-24 12:31:44 PDT

Actionable?



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
    
```


2. Actions

For InfoSec Course

Architecture



Knowledge



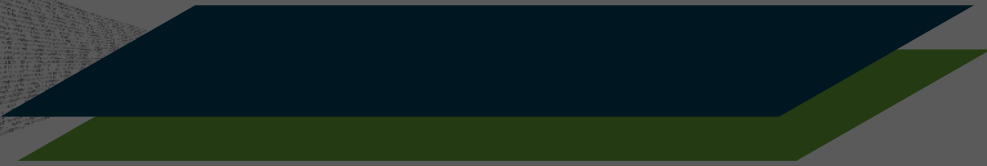
Course Data



Intelligence



Actions



splunk >

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-66&product_id=FI-SW-03" "Opera/9.80...
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "http://buttercup-shopping.com/c...
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADF9" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "http://buttercup-shopping.com/c...
189] "GET /cart.do?action=remove&itemId=EST-SURPRISE&product_id=FLOWERS&JSESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "http://buttercup-shopping.com/c...
100] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-SURPRISE&product_id=FLOWERS&JSESSIONID=SD5SL7FF6ADF9" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "http://buttercup-shopping.com/c..."



Notification

Type of notification

To Students:

- Welcome Email
- Reminder Email
- Overdue Email

To division leads:

- Monthly Report
- Escalation Report



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1"
10.0.2.1 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=LI-02"
10.0.2.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=LI-02"

```




Default Alert Notification

- ▶ Not user friendly
- ▶ Lack of enforcement
- ▶ Not Actionable

Splunk Cloud <alerts@splunkcloud.com> sysadmin@usfca.edu; infosec@usfca.edu 2 Thu 4/6

Splunk Alert: No. Infoblox Recursion Client Quota Used > 4000 (ea_alert_infoblox_highrecursionclient)

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

ea_alert_infoblox_high... 6 KB
ea_alert_infoblox_high... 433 bytes

Splunk detected Infoblox no. of recursion client quota used is larger than 4000. Please check InfoBlox status. Thanks!

Alert: [ea_alert_infoblox_highrecursionclient](#)

Trigger Time: 07:45:04 on April 06, 2017.

[View results in Splunk](#)

host	No of recursion client quota used (5-mins Average)
cache-gridc1.ds.usfca.edu	4243

If you believe you've received this email in error, please see your Splunk > the engine for machine data



USF Canvas <notifications@instructure.com> tip@usfca.edu

Course Invitation

You've been invited to participate in the course, Elevated Access: Information Security Awareness Training. Course role: Teacher

Name: **Tim Ip**
Email: tip@usfca.edu
Username: **tip**

[Get Started](#)

[Click here to view the course page](#) | [Update your notification settings](#)



Customized Email Notifications

Goals

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

The screenshot shows an email header with the USF logo and the text "Information Security and Compliance". Below the header is a green bar with the text "Information Security Awareness Training Course". The main body of the email starts with "Welcome!" and "Dear [redacted]". The text continues: "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." It then states: "For your information, failure to complete this requirement could result suspension of your USF network and email access." A blue link "Click here" is provided to take the course now. Below that, it says: "Rather take the course in a day or two? Add to calendar: [Google Calendar](#) • [Outlook](#)". The email then lists "Additional Information:" and states: "As you may know, awareness of cyber security is one of the most important aspects of 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." It then says: "The following 6 topics will be covered to establish a foundation for our shared responsibilities:" and lists four items: 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

Customized Email Scheduler

Search Head

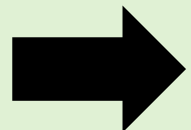
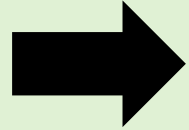
Splunk Query Results

l_c	n_j	n_p	table_html
26	11	5	<tr bgcolor="#EEEEEE"><td>Bill Cartwright</td><td>2016-12-14</td><td>72</td><td>54</td><td>88</td></tr><tr bgcolor="#EEEEEE"><td>Deniz Demirel</td><td>2016-12-14</td><td>72</td><td>0</td><td>0</td></tr><tr bgcolor="#EEEEEE"><td>Jenna Paicelli</td><td>2016-12-14</td>

Email Template

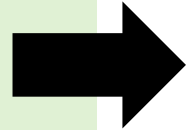
```

"#8C898A">$header$</font>
  <div style="
    <table border="1" style="width:100%; border-collapse: collapse;">
      <tr text-align="center" style="background-color:#f2f2f2;">
        <td>Name</td>
        <td>Created</td>
        <td>Last Modified</td>
        <td>Status</td>
      </tr>
      <tr>
        <td>Dear $first_name$ $last_name$,</td>
      </tr>
      <tr>
        <td>This is a second course</td>
      </tr>
    </table>
  </div>
  
```



Email Scheduler

- Expanding results
- Replace tokens with query results
- Loop
- Send out email



130.60.4 - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01" Moz/11.0.0...
 128.241.220.82 - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Mozilla/5.0...
 317.27.160.0.0 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Mozilla/5.0...
 130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01" Moz/11.0.0...
 128.241.220.82 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Mozilla/5.0...
 317.27.160.0.0 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Mozilla/5.0...
 130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01" Moz/11.0.0...
 128.241.220.82 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Mozilla/5.0...
 317.27.160.0.0 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Mozilla/5.0...

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



Information Security Awareness Training Course

Due Date Approaching Overdue

Dear [REDACTED],

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.

Customized Email Notification For Executive

- ▶ Executive Report
 - Statistics by role
 - Overview and details



Information Security Awareness Training Course

Monthly Executive Escalation Status Report

Dear [REDACTED],

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

	Completion Percentage	No. of Past Due People
Affiliate	62%	12
Employee_FT	100%	0
Employee_PT	100%	0
Faculty_PT	58%	4

Customized Email Notification

For Executive

- ▶ Executive Report
 - Statistics by role
 - Overview and details

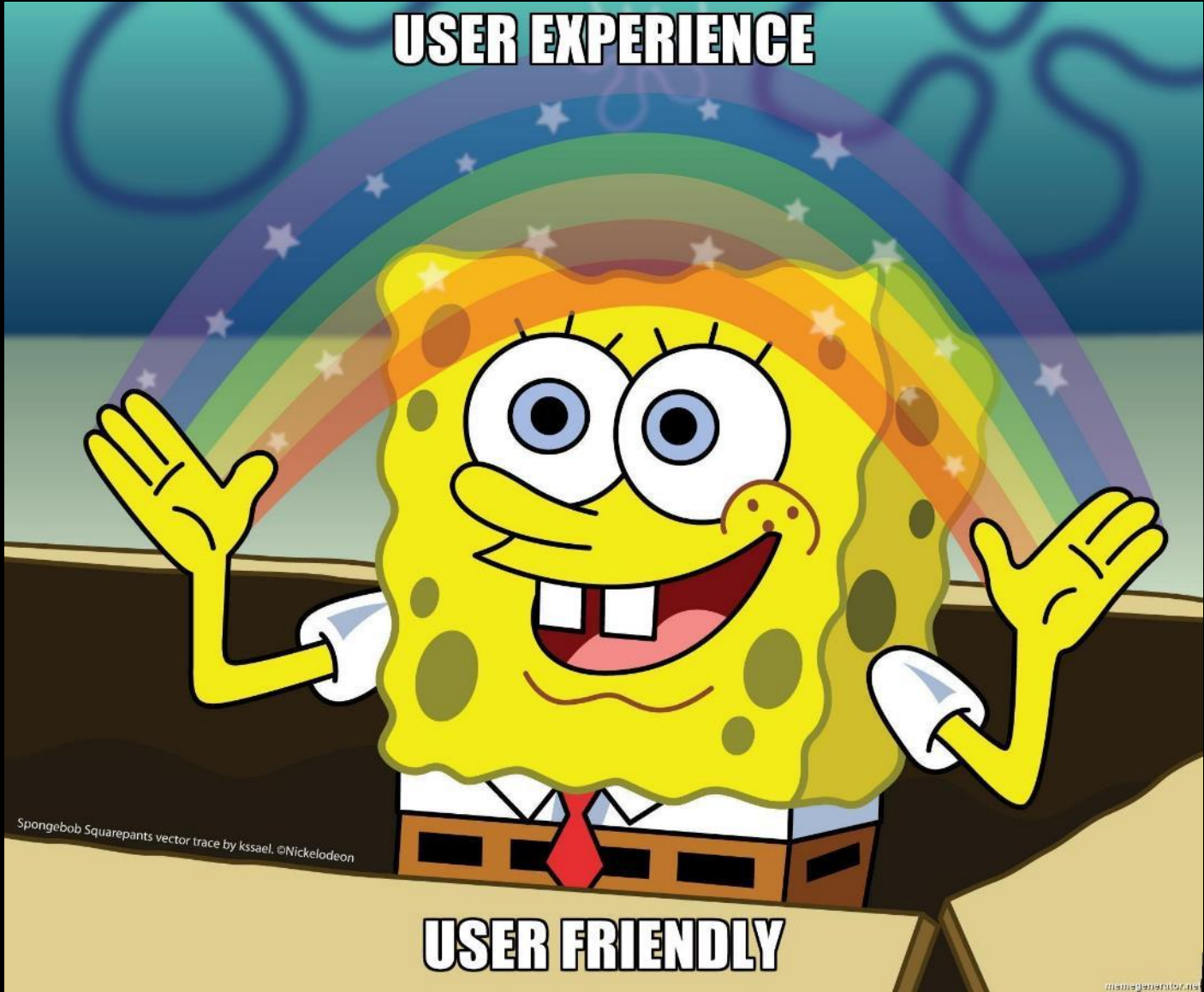
Affiliate Details

Statistics

Total Number	Completed	In Progress	Past Due
50	31	19	12

List of Past Due People

Name	Enrollment Date	No. of business day from first enrollment	Total Activity Time (Minutes)	Progress	No. of Outstanding Assignment
[Redacted] (Sponsor: [Redacted])	2017-07-14	12	0	0%	8
[Redacted] (Sponsor: [Redacted])	2017-07-14	12	0	0%	8
[Redacted] (Sponsor: [Redacted])	2017-07-14	12	0	0%	8
[Redacted] (Sponsor: [Redacted])	2017-07-14	12	0	0%	8
[Redacted] (Sponsor: [Redacted])	2017-07-14	12	0	0%	8



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?*

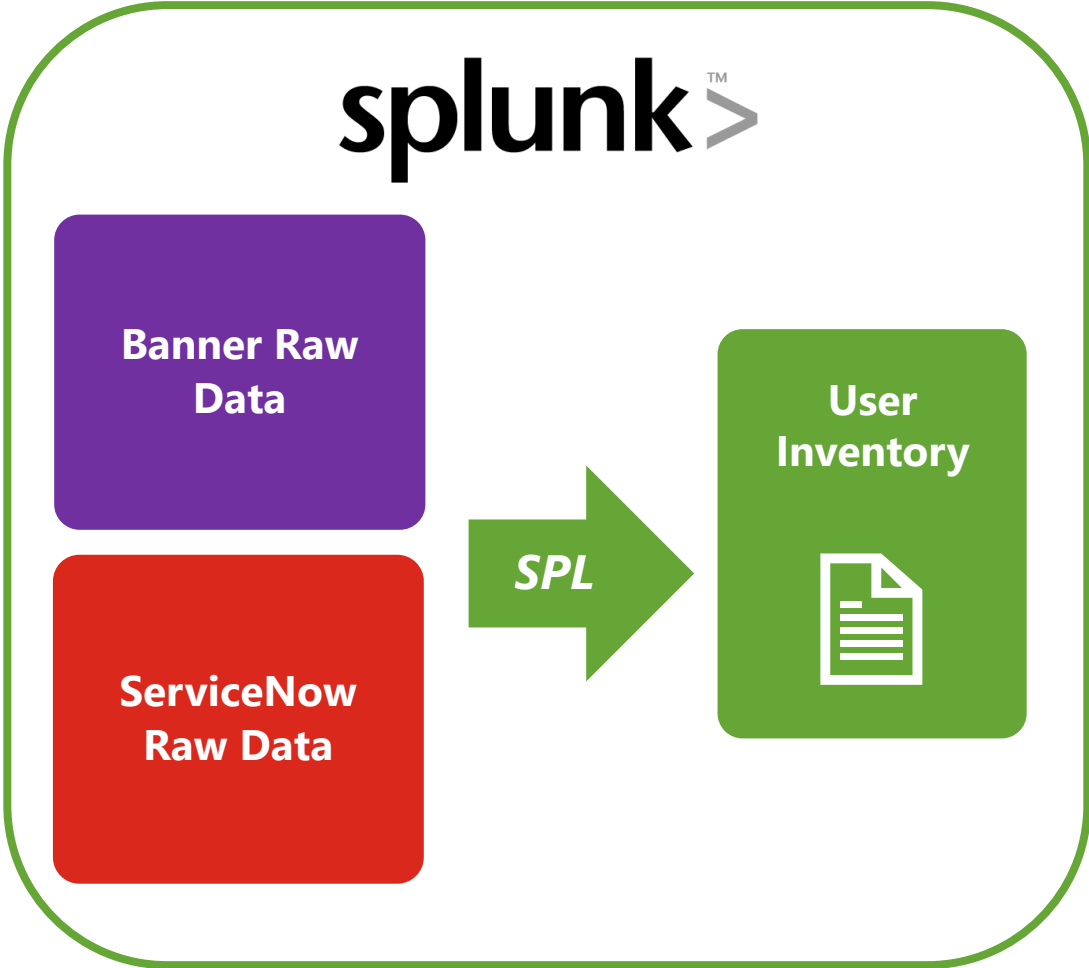
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80.2013.10.0; Linux x86_64; rv:15.0 Gecko/20100827 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100827 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 468 125.17.14.108 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100827 Firefox/53.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80.2013.10.0; Linux x86_64; rv:15.0 Gecko/20100827 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100827 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 468 125.17.14.108 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100827 Firefox/53.0"
```


3. Intelligence Input

For InfoSec Course



Banner/ServiceNow – Splunk Integration



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CU-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L7FF6ADFF9"
do?buttercup-shopping_id=RP-LI-02" 468 125.17 14 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
317 27.160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CU-01"
item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" 468 125.17 14 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CU-01"

```



Ingest ERP Data

Banner: Escalation Data

Employee	Supervisor
Tim	Nick
Vince	Nick
Nick	Opinder
Michael	Nick
Opinder	Paul



Employee	Escalation Path
Tim	Tim, Nick, Opinder, Paul
Vince	Vince, Nick, Opinder, Paul
Nick	Nick, Opinder, Paul
Michael	Michael, Nick, Opinder, Paul
Opinder	Opinder, Paul

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3"
10.2.1.1 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18"
  
```



Ingest ITSM data

ServiceNow: User Profile

- ▶ Roles
- ▶ Department

Username	[Redacted]
First name	[Redacted]
Last name	[Redacted]
USF Roles	EMPLOYEE
Employee Classification	FT_STAFF
Phone	[Redacted]
Mobile phone	[Redacted]
Contact Phone	[Redacted]
Location	Lone Mountain North
Campus Address	[Redacted]
Department	[Redacted]
Cost center	[Redacted]
Title	[Redacted]
Source	ldap
Password	[Redacted]
See User Notes	<input type="checkbox"/>

VIP	<input type="checkbox"/>
Not Self Service	<input checked="" type="checkbox"/>
Locked out	<input type="checkbox"/>
Active	<input checked="" type="checkbox"/>
Email	[Redacted]@usfca.edu
Notification	Email
Time zone	System (America/Los_Angeles)
Campus	[Redacted]
College	[Redacted]
Degree	[Redacted]
Major	[Redacted]
Program	[Redacted]
Updated	7-03-2017 05:17:33
Updated by	system
Created	7-31-2015 05:22:20
Created by	system

4. Knowledge

For InfoSec Course

Architecture



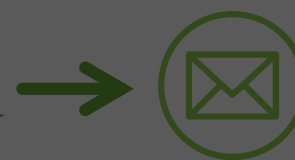
Knowledge



Course Data



Intelligence



Actions

splunk>



Business Logic

From complex business requirements and SPL queries



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
10.2.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"



Knowledge

Ninja
Experience/Skills



Business
Knowledge

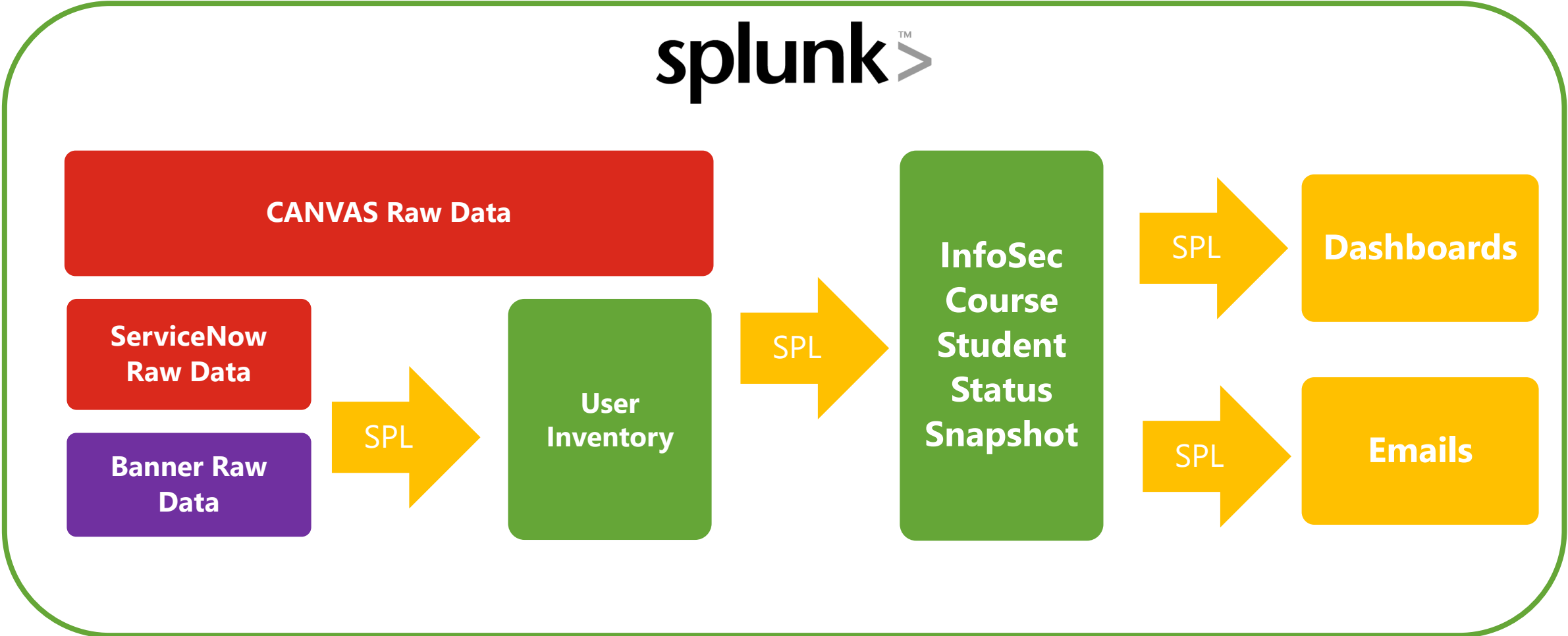


Splunk SPL
Query /
dashboard/
automation

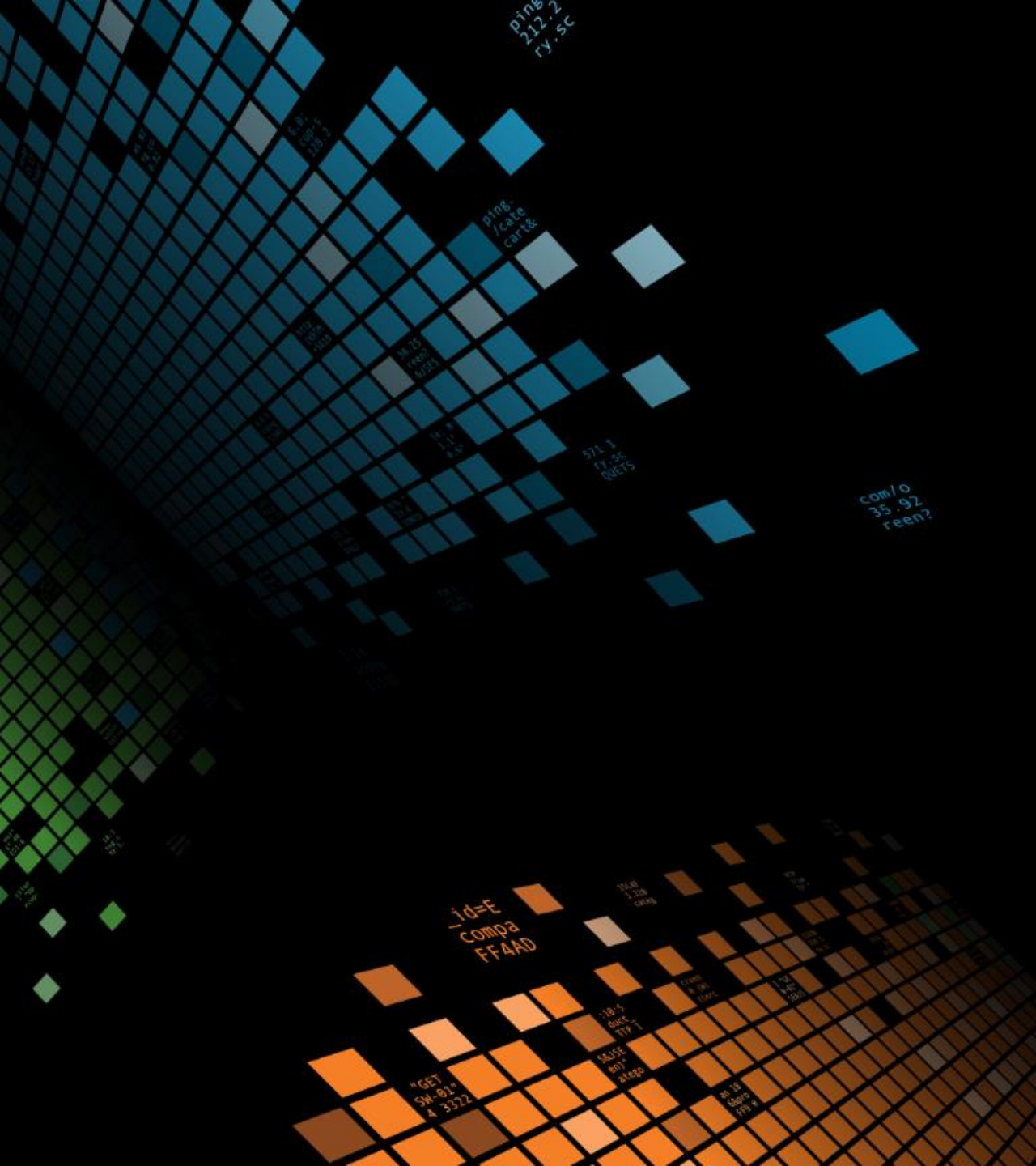
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80.2013.10474;O; Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD95L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD95L7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
10.20.20.20 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 468 125.17.14.11 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" "Opera/9.80.2013.10474;O; Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
10.20.20.20 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD95L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
10.20.20.20 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD95L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
10.20.20.20 - - [07/Jan 18:10:56:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD95L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
```



SPL Queries



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0.0.0.0" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0.0.0.0" 130.60.4 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD1SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0.0.0.0" 130.60.4 - - [07/Jan 18:10:57:189] "GET /cart.do?action=remove&itemId=EST-1 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0.0.0.0" 130.60.4 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0.0.0.0" 130.60.4 - - [07/Jan 18:10:57:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0.0.0.0"



Results

InfoSec Course

Use Case

For supporting InfoSec Course Automation



1. Machine Data

- Enrollment
- Score
- Assignment



2. Actions

- Customized Email Notification Scheduler



InfoSec Course Automation

3. Intelligence

- ServiceNow: User Inventory
- Banner: Escalation Path



4. Knowledge

- Business Logic
- Splunk Ninja
- Splunk SPL Query



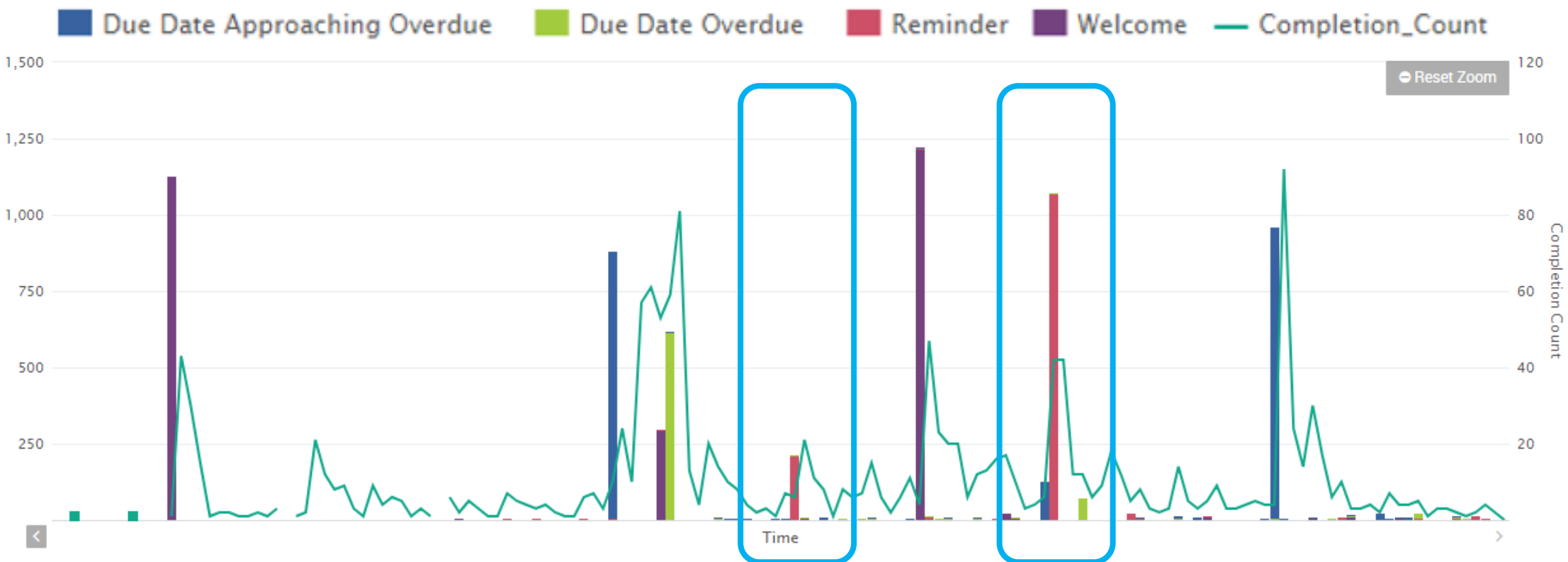
130.60.4... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" Mozzi11740 "Opera/9.80... 20...
128.241.220.82... [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Compa11111...
317.27.160.0.0... [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Compa11111...
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14... sscreen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Compa11111...
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14... sscreen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Compa11111...
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14... sscreen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" Compa11111...



Normal Notification

Notification vs Completion

Timechart: Email Count and User Completion Count

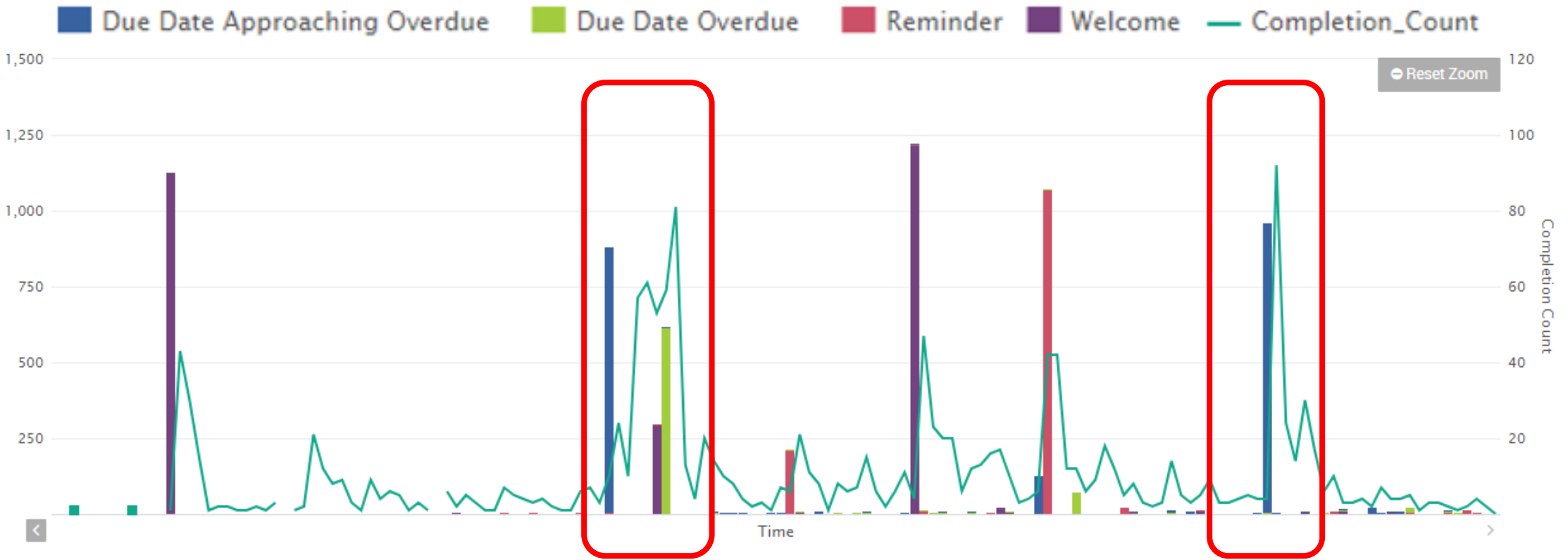


```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/4.0" "Completion_Count"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
10.1.1.1: SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD19SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
0.1.1.1: SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD19SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
0.1.1.1: SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD19SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
0.1.1.1: SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD19SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
0.1.1.1: SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD19SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0" "Completion_Count"
```

Management Escalation

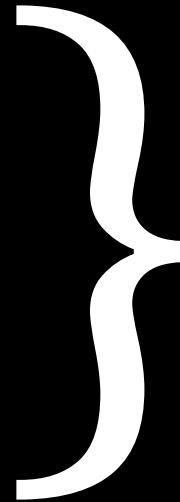
Notification vs Completion

Timechart: Email Count and User Completion Count



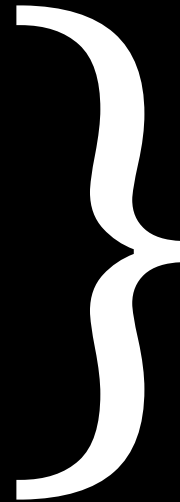
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
125.17.14. - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
125.17.14. - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
125.17.14. - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"

Course Data
Actions
Intelligence
Knowledge



InfoSec Course
Automation

Machine Data
Adaptive Responses
Intelligence
Knowledge



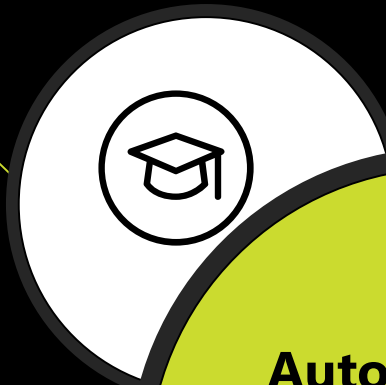
IT ~~InfoSec Course~~
Automation

IT Automation

USF Automation Framework

Machine Data

- OS/Application Log
- App from Splunkbase
- Customized API



Adaptive Responses

- Self-Service Notification
- ServiceNow Ticket Creation



Automation Framework



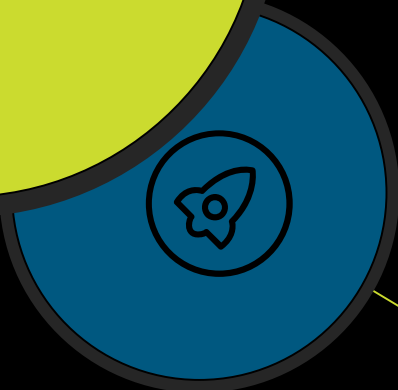
Intelligence

- Cmdb
- User Profile
- Escalation Path



Knowledge

- Business Logic
- Splunk Ninja
- Splunk SPL Queries



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD95L9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Compa
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17.10.10 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF2 HTTP/1.1" 200 2423 "http://buttercup-shoppin
item_id=EST-16&product_id=RP-LI-02" "Opera/9.80.
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=FL-SW-01" "Opera/9.80.
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=FL-SW-01" "Opera/9.80.
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=FL-SW-01" "Opera/9.80.

```



Intelligence Inputs

External

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

FBTX Splunk Add-on for Facebook ThreatExchange

★★★★★ 1 rating

Splunk Built

Internal

- ▶ User Inventory (Human)
- ▶ CMDDB (Machine)

Name	URL	Category	sev
emerging_threats_compromised_ip_blocklist	http://rules.emergingthreats.net/blockrules/compromised-ips.txt	ip	H:Compromised_IP
palevo_ip_blocklist	https://palevotracker.abuse.ch/blocklists.php?download=ipblocklist	ip	H:C&C
iblocklist_web_attacker	http://list.iblocklist.com/?list=ghlztqxncvtvjjwwag	range	H:AttackerIP
zeus_bad_ip_blocklist	https://zeustracker.abuse.ch/blocklist.php?download=badips	ip	H:C&C
emerging_threats_ip_blocklist	http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	ip	M:Blocklist
sans	http://isc.sans.edu/block.txt	col	M:Blocklist
zeus_standard_ip_blocklist	https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist	ip	M:Blocklist
malc0de.com	http://malc0de.com/bl/IP_Blacklist.txt	ip	M:Blocklist
iblocklist_proxy	http://list.iblocklist.com/?list=xoebmyexwuiogmbyprb	range	L:TOR
iblocklist_spyware	http://list.iblocklist.com/?list=bt_spyware	range	H:Spyware
iblocklist_tor	http://list.iblocklist.com/?list=tor	range	L:TOR



Adaptive Responses

Human

Severity



Severity	
<p>Students</p>	<p>Faculty</p>
<p>Customized Email</p>	<p>ServiceNow Ticket</p>
<p>Employee/ Affiliate</p>	<p>Customized Email</p>
	<p>ServiceNow Ticket</p>
	<p>Slack Channel</p>

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" Opera/9.80
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD95L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100826 Firefox/3.0
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100826 Firefox/3.0
10.55.187 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD218FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100826 Firefox/3.0
10.55.108 - - [07/Jan 18:10:55:108] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD218FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100826 Firefox/3.0
  
```



Adaptive Response

Self Service Notification

Information Security Notification

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 [\[redacted\]](#) by email and request your account to be decommissioned [OR](#)
- (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



Faculty



Customized Email

ServiceNow Ticket

Employee/ Affiliate

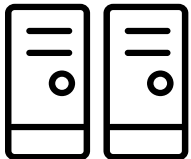


Customized Email

ServiceNow Ticket

Slack Channel

Machine



Trigger Antivirus Full Scan

Apply new IP blocking firewall rule

And more...



Expanding Use Cases

Increase automation to IT



Machine Data Input



Intelligence Input



Adaptive Response



Knowledge

InfoSec Course Automation

Canvas

Banner / ServiceNow

Email

Splunk Ninja + Business Intel

PCI Password Expired Notification

Domain Controller User List

ServiceNow User Profile

Email

Splunk Ninja + Business Intel

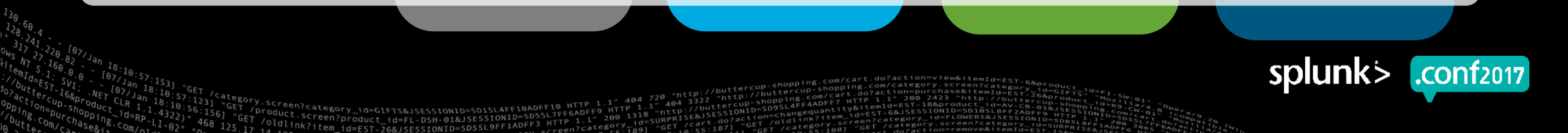
PCI Anti-Virus Problem Notification

Sophos Log

ServiceNow CMDB

Email / 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**

Q&A

Tim Ip | Senior Security Engineer
Nicholas Recchia | Director & Information Security Office

Thank You

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

splunk> **.conf2017**