



Accelerate Incident Investigation With RedSeal and Splunk Adaptive Response Actions

Kurt VanEtten

September 2017 | Washington DC

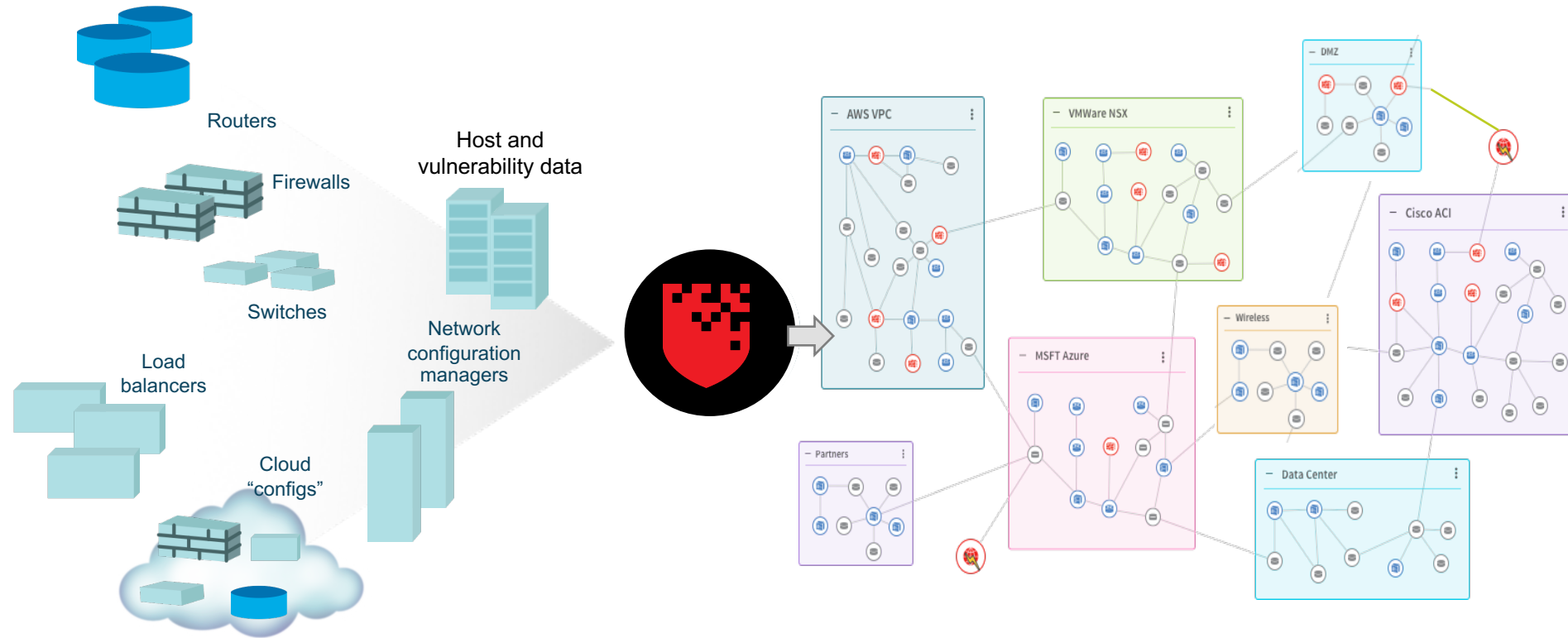
Forward-Looking Statements

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.

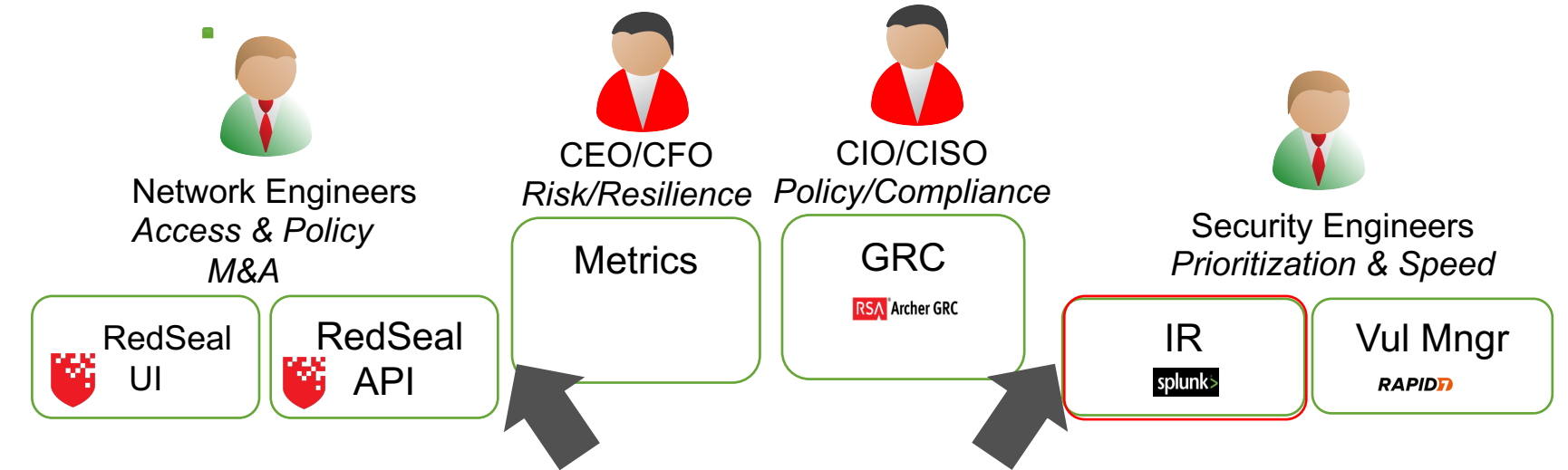
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

RedSeal Creates a Model of Your Network

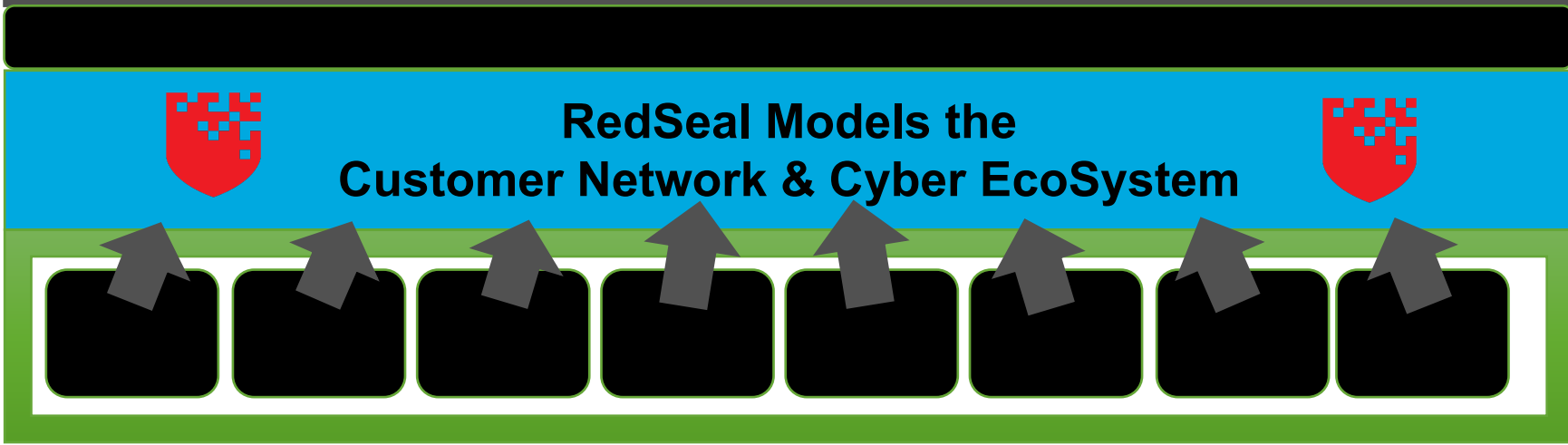


130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885
://buttercup-shopping_id=RP-LI-02" 468 125.17.14.105:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3885

RedSeal Platform: Improves Existing Jobs Across the Enterprise



The right information, in the right place, to the right person, at the right time



```

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-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
125.17.14.189 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
10.0.0.1:5V1: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0"
  
```

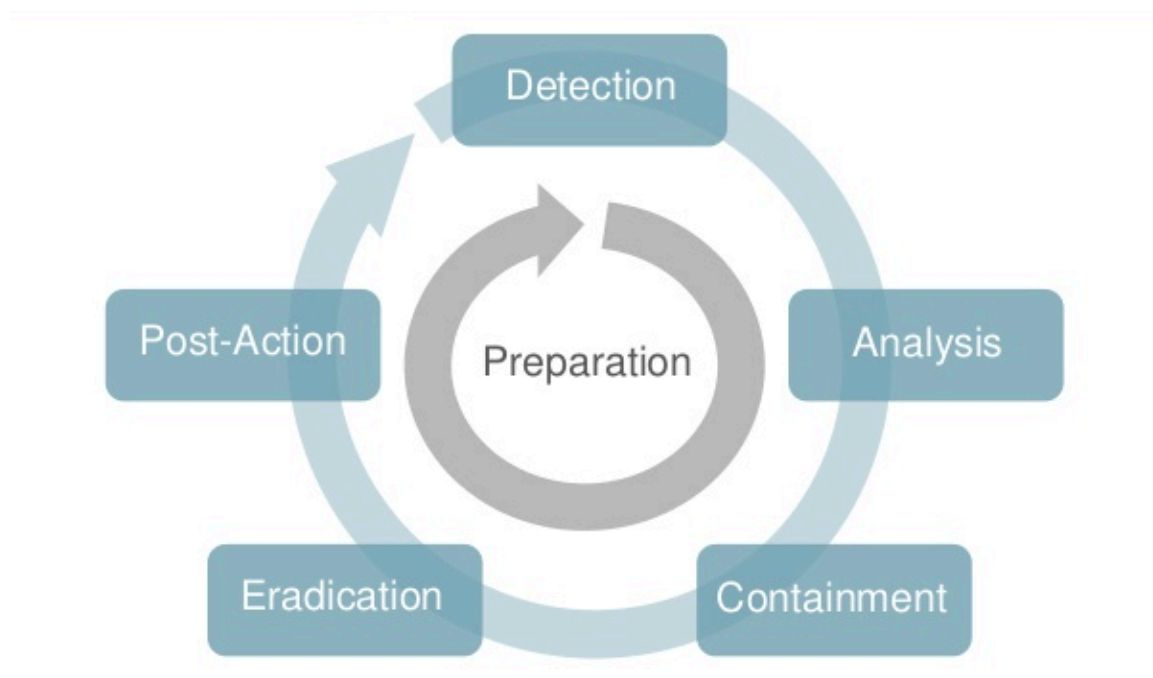
CSO Magazine Network Security Product of the Year

“What it does [RedSeal] is act as a ***force multiplier*** for every other security device within a network, finding vulnerabilities and mapping out the dangers in relation to the specific network being protected”

-CSO Magazine
June 2017

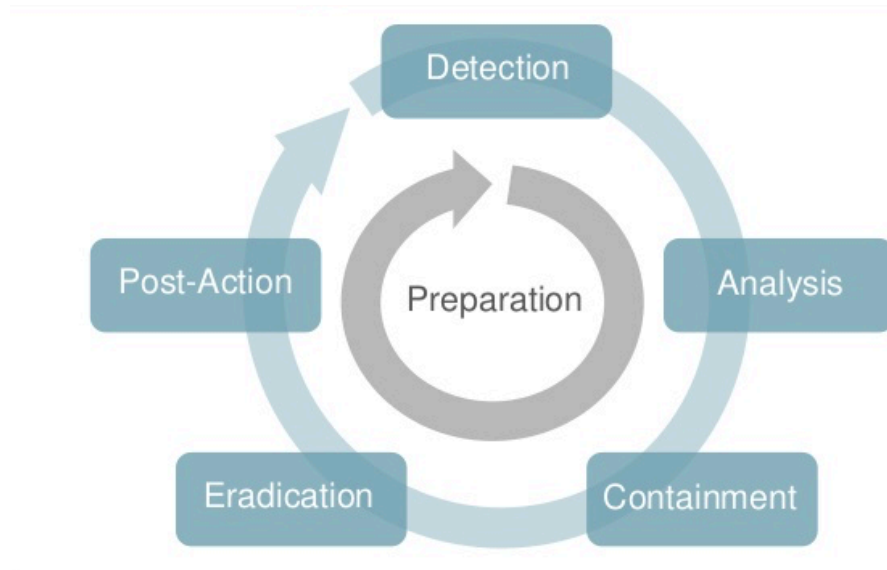
```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14.10.55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
opping.com/purchase&itemId=EST-26&product_id=KQ-CW-01" 468 125.17 14.10.55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
```

Incident Response Process



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=S01SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=S035SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=S05SL9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
10.1.1.1:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
0.0.0.0:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
10.1.1.1:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
10.1.1.1:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
10.1.1.1:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
10.1.1.1:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"  
10.1.1.1:5V1: .NET CLR 1.1.4322) "GET /category.screen?category_id=FLOWERS&JSESSIONID=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL9FFIADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01"
```

Understand the Pain Points- Research Results



Preparation

- Difficult to maintain and tune correlation rules.

Detection

- Far too many Incidents to handle

Analysis

- Inability to locate IoC both logically and physically.
- Extremely tedious and time consuming to find all possible paths to critical assets

Containment

- Inability to execute on containment options because of inability to locate L3 and L2 devices.

Eradication

- Difficult to find all possible malware or access.

Post Action

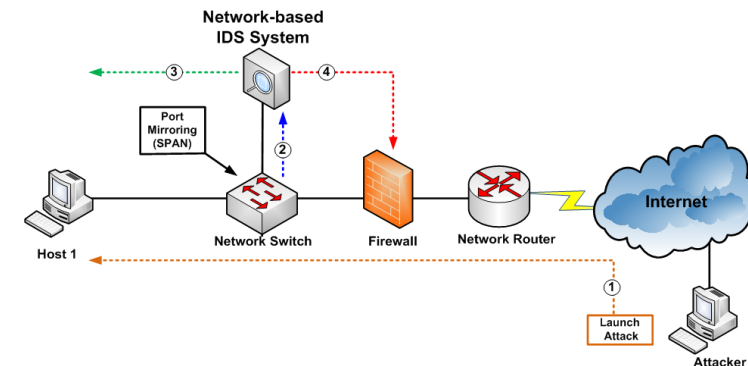
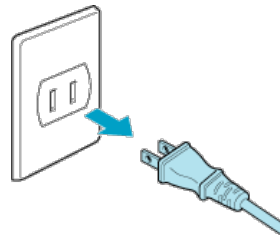
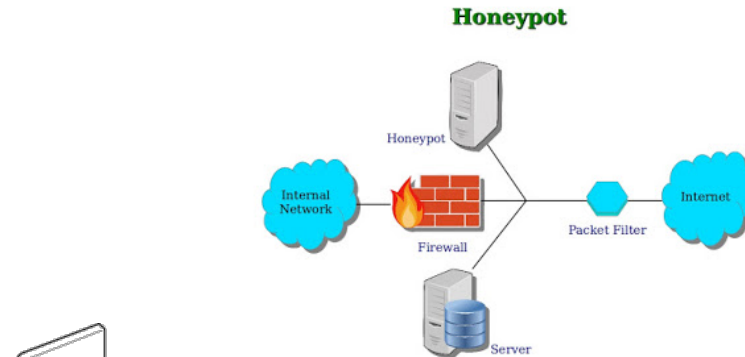
- Difficult to communicate to non tech teams

```

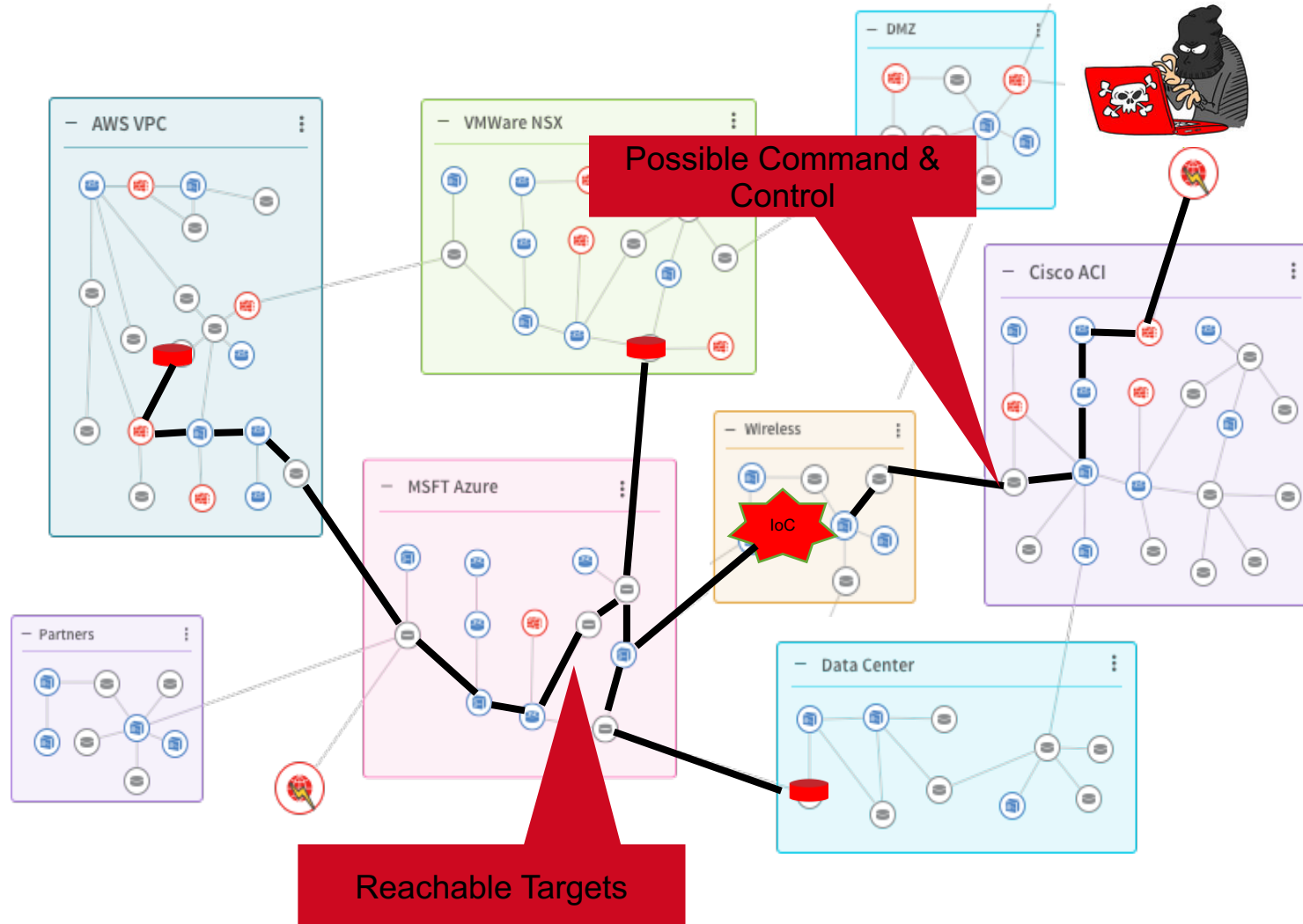
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
10.0.0.1:5V1: - - [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=changequantity&itemId=EST-6&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
  
```


Incident Investigations

- ▶ What is the asset with the indicator of compromise?
- ▶ Where is located logically and physically?
- ▶ Where can the attacker traverse to?
- ▶ How would they get there?
- ▶ What are the options to contain the incident?



Incident Investigations



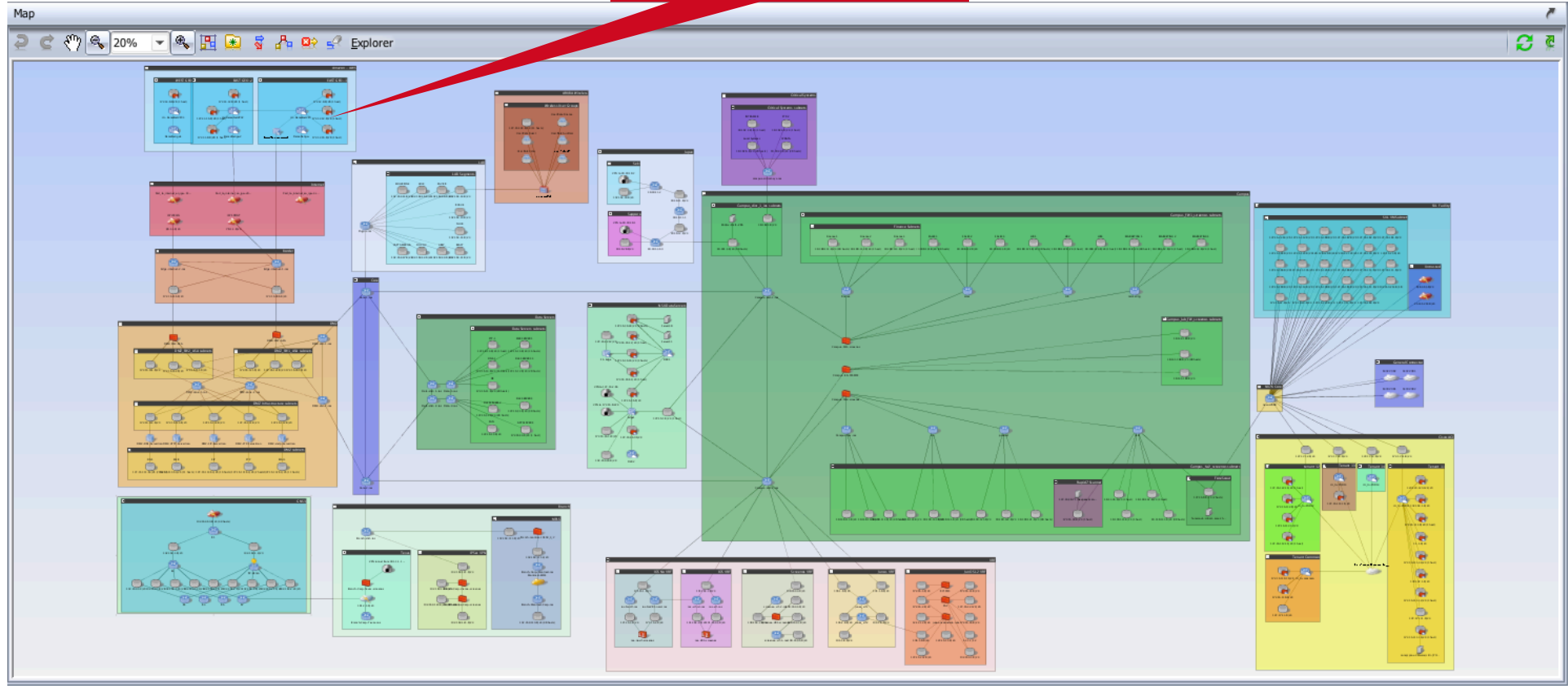
```

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=S01SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-268&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
: //buttercup-shopping.com/ol - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-268&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1"
do?action=purchase-shopping_id=RP-LI-02" 468 125.17 14 - [07/Jan 18:10:55:187] "GET /cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1" 200 3557 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
shopping.com/cart.do?action=purchase-shopping_id=RP-LI-02" 468 125.17 14 - [07/Jan 18:10:55:187] "GET /cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1" 200 3557 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
shopping.com/cart.do?action=purchase-shopping_id=RP-LI-02" 468 125.17 14 - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=S035L7FF6ADFF9 HTTP 1.1" 200 3557 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"

```

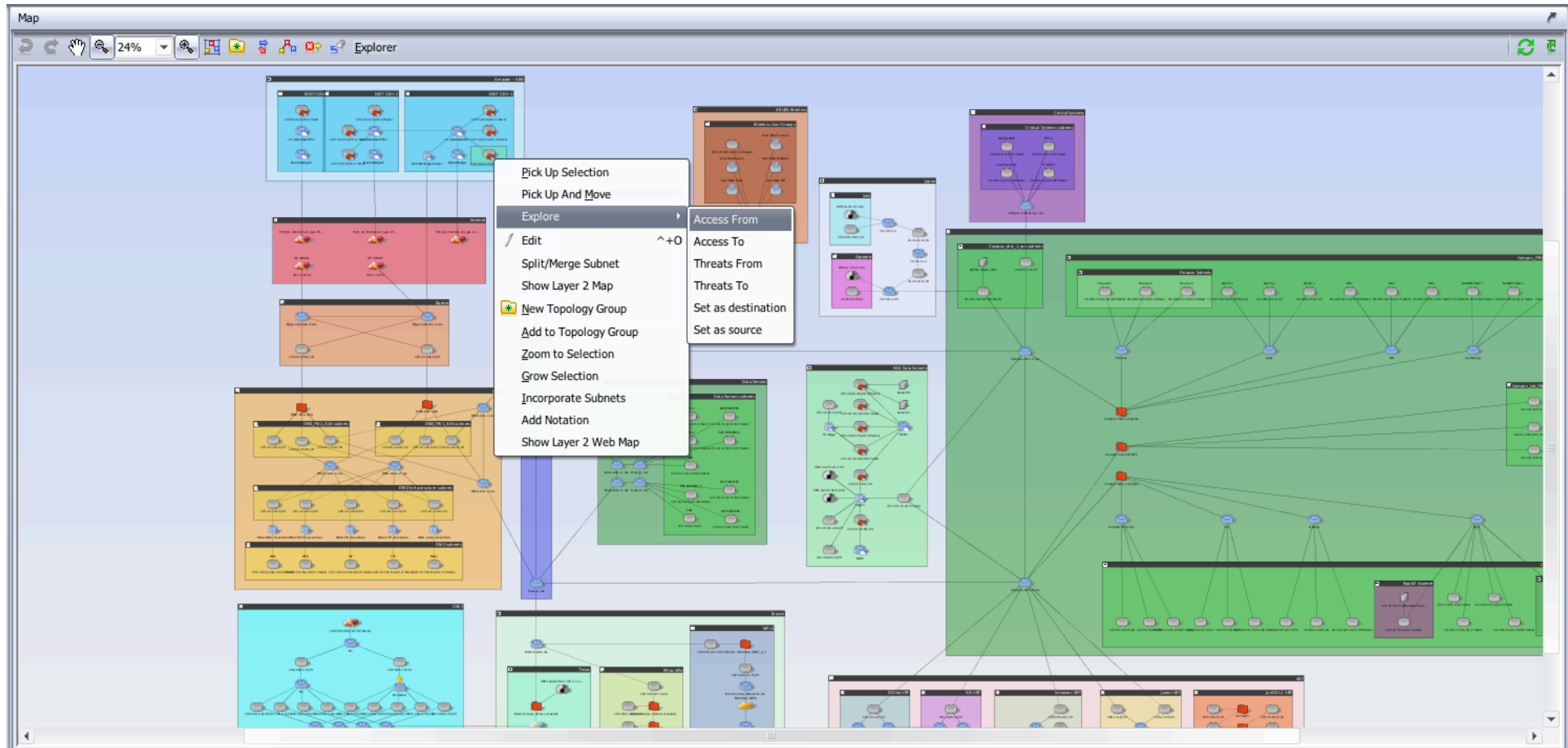
Incident Investigations- Understanding Access Policy

Indicator of
Compromise



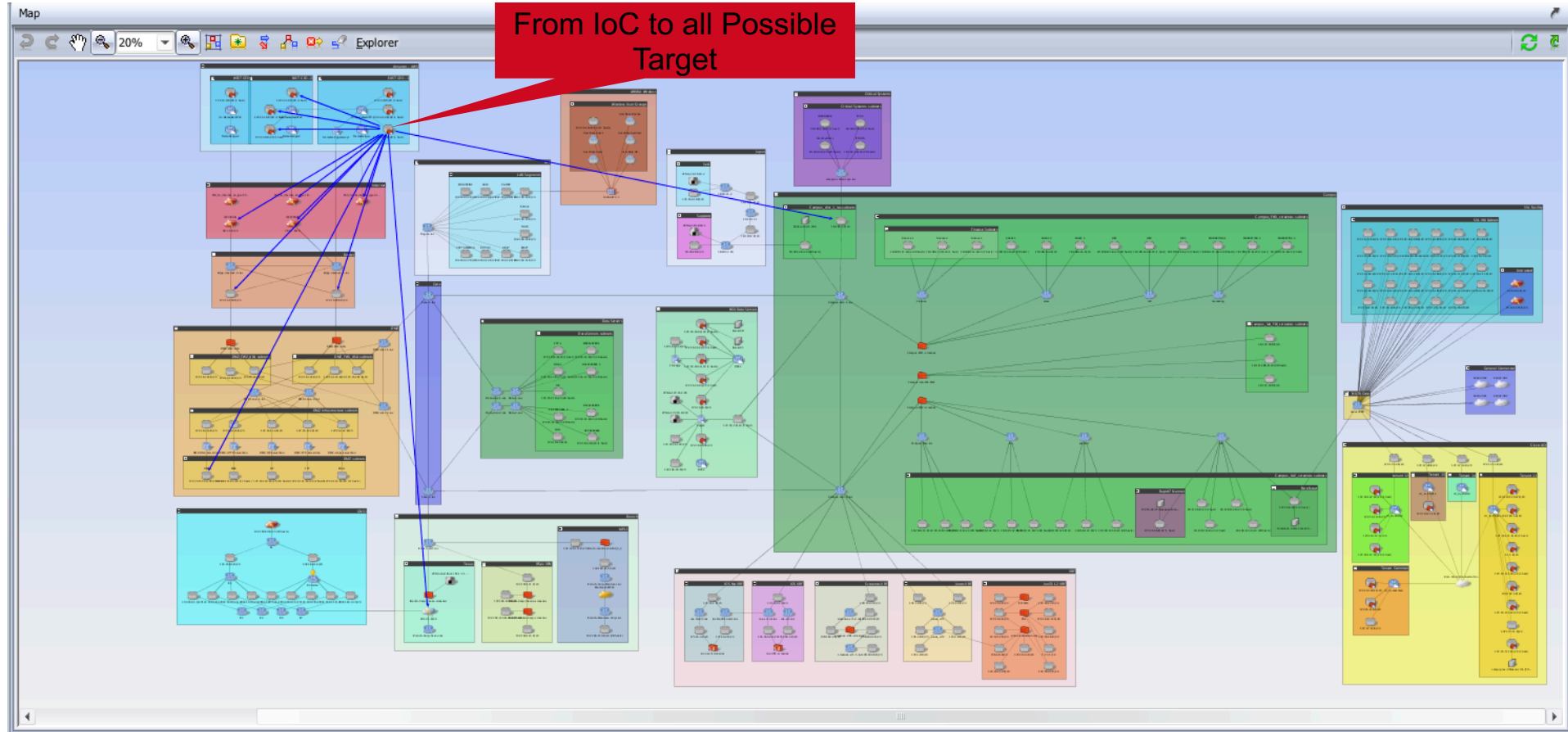
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"
192.168.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3"

Incident Investigations- Understanding Access Policy



130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD51LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD51LAF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD51LAF10ADFF10 HTTP 1.1"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD51LAF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" 468 125.17 14 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD51LAF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" 468 125.17 14 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD51LAF10ADFF10 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"

Incident Investigations-All Possible Access Paths



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-03"
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/category.screen?category_id=GIFTS"
317.27.160.0 - - [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=purchase&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD55L9FF1ADFF3"
125.17.14 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"
10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"
10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"
10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"
10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"
10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"
10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3"

Incident Investigations- Understanding Access Policy

The screenshot displays the Splunk Network Investigator interface. On the left, a 'Map' view shows a network topology with various nodes and connections. The central pane is titled 'Detailed Path Summary' and shows a path of 8 hops. The 'Paths Found' section contains a table with the following data:

Hop	Flow	Element
		172.32.16.0/20
1		vpc-062c2963 DMZ-FW1-ASA
2		rtr-DemoNetVPC
3		DemoNetvpgateway1
4		Edge-internet-1-ios
5		DMZ-FW1-ASA or DMZ-FW1-ASA
6		DMZ-dist-1-ios
7		Core-1-ios
8		Campus-dist-1-ios
		10.102.1.0/24 (connected to Campus-dist-1-ios)

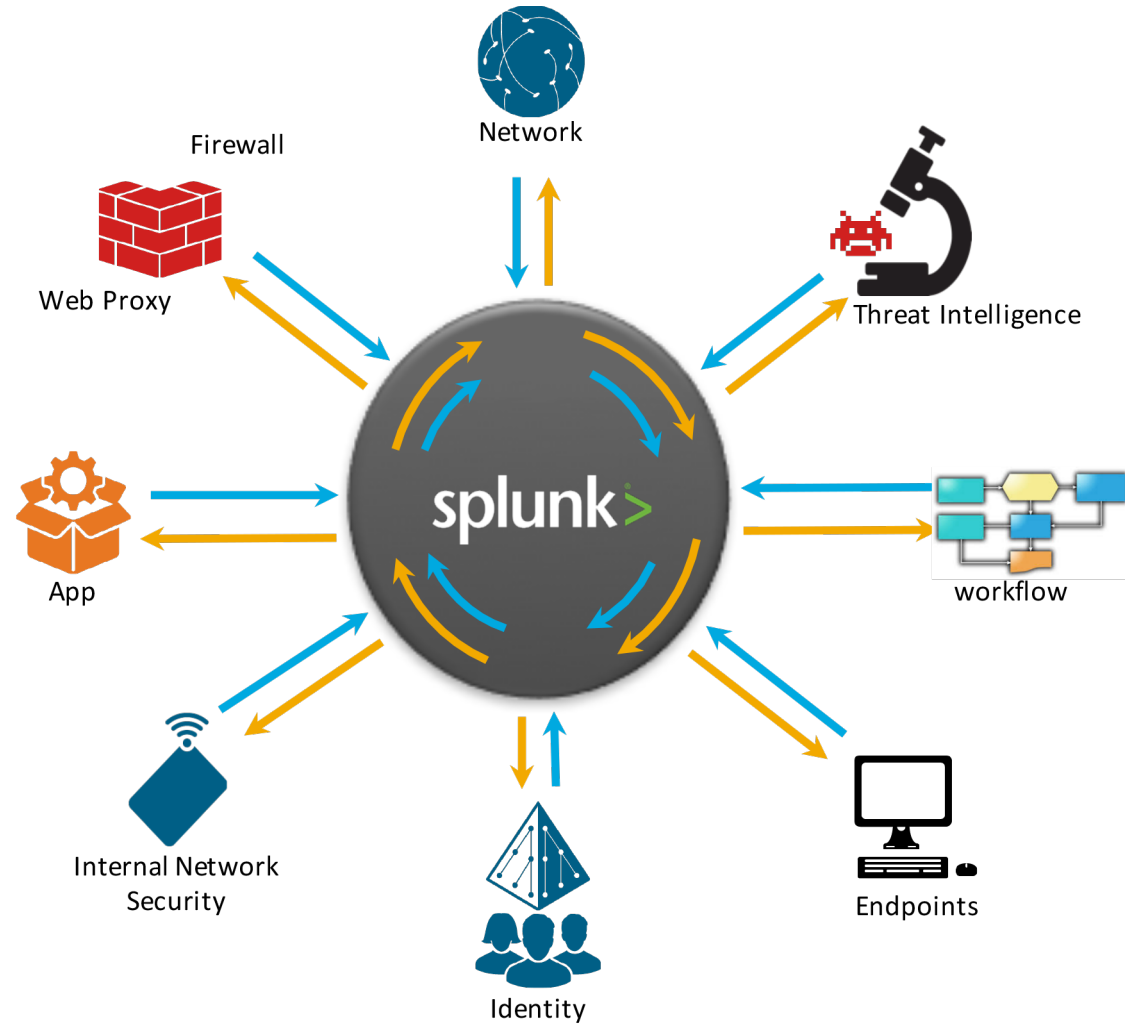
On the right, a configuration window for 'DMZ-FW1-ASA' is open, showing a list of inbound filters. The first line is highlighted:

Device	Type	First Line/Description
DMZ-FW1-ASA	Inbound Filter	(config:125) access-list Outside-IN extended permit tcp host 172.32.22.167 host 10.102.1.20 eq 22
DMZ-FW1-ASA	Inbound Filter	(implicit) deny all

Two red callout boxes are present: one at the top right pointing to the configuration window with the text 'Line Allowing Traffic', and another in the center pointing to the path table with the text 'Path across Cloud, SDN, and on prem'. The background map shows a complex network structure with nodes representing different network segments and their interconnections.

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-6&product_id=FI-SW-03"
128.241.220.82... [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FFGADF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-208product_id=KQ-CB-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14... [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FFGADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SLFFPAD111A"
to?action=purchase&product_id=RP-LI-02" 468 125.17 14... [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FLOWERS&JSESSIONID=SD5SLFFPAD111A"
opping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SLFFPAD111A HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FLOWERS&JSESSIONID=SD5SLFFPAD111A"
to?action=remove&itemId=EST-11&product_id=FLOWERS&JSESSIONID=SD5SLFFPAD111A HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=FLOWERS&JSESSIONID=SD5SLFFPAD111A"

Splunk Enterprise Security Adaptive Response



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"

Splunk ES RedSeal Adaptive Response

splunk> App: Enterprise Security

Administrator Messages Settings Activity Help Find

Security Posture Incident Review My Investigations Glass Tables Security Intelligence Security Domains Audit Search Configure Enterprise Security

Incident Review

Urgency

- CRITICAL 5
- HIGH 119
- MEDIUM 556
- LOW 0
- INFO 0

Status: Name:

Owner: Search:

Security Domain: Time: Last 24 hours

Tag:

680 events (2/3/17 12:00:00 PM to 2/4/17 12:23:08 PM)

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

Edit Selected | Edit All 680 Matching Events | Add Selected to Investigation

#	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	2/4/17 12:10:47.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.95.233.119	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.90.65.167	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.90.249.242	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.89.108.98	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.171.18.43	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.165.74.249	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.163.243.2	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP GET Request Events By 10.123.125.160	Medium	New	unassigned	⌵
>	2/4/17 12:10:42.000 PM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.50	Medium	New	unassigned	⌵
>	2/4/17 11:10:32.000 AM	Network	Abnormally High Number of HTTP CONNECT Request Events By 192.168.3.153	High	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.9.131.94	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP GET Request Events By 10.88.35.78	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP GET Request Events By 10.85.157.9	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP GET Request Events By 10.84.159.171	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.44.36.165	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP POST Request Events By 10.44.13.99	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.3.205.25	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.19.241.41	Medium	New	unassigned	⌵
>	2/4/17 11:10:29.000 AM	Network	Abnormally High Number of HTTP GET Request Events By 10.187.155.143	Medium	New	unassigned	⌵

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 318 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FI-SW-03"
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&item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1"
ows NT 5.1; SV: .NET CLR 1.1.4322" 468 125.17 14...srreen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-1408"
toaction=purchase&item_id=RP-LI-02"
shopping.com/purchase&item_id=RP-LI-02"

```


Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk Enterprise Security (ES) Incident Review interface. At the top, the navigation bar includes 'Security Posture', 'Incident Review', 'My Investigations', 'Glass Tables', 'Security Intelligence', 'Security Domains', 'Audit', 'Search', and 'Configure'. The main header shows 'Enterprise Security'.

The 'Incident Review' section is active, displaying a summary of incident counts by urgency:

- CRITICAL: 5
- HIGH: 119
- MEDIUM: 556
- LOW: 0
- INFO: 0

Search filters include Status (All), Owner (All), Security Domain (All), and Time (Last 24 hours). A 'Submit' button is present.

A timeline chart shows 680 events from 2/3/17 12:00:00 PM to 2/4/17 12:23:08 PM. The chart shows a significant spike in activity around 6:00 PM on Friday, February 3, 2017.

The event list below the chart shows a selected event at 2/3/17 9:10:52.00 PM, categorized as 'Network' with the title 'Abnormally High Number of HTTP Method Events By Src - Rule'. The event's urgency is 'Critical', status is 'New', and owner is 'unassigned'. A red callout box labeled 'IoC IP Address' points to the source IP '10.11.36.20' in the event details.

The event description states: 'A system (10.11.36.20) was detected as generating an abnormally high number of CONNECT request events...'. The 'Additional Fields' section lists various attributes for the source system, such as 'Source IP Address: 10.11.36.20' and 'Source Country: USA'. The 'Action' column shows a dropdown menu for each field.

The 'History' section includes a link to 'View all review activity for this Notable Event'. The 'Contributing Events' section lists related events. The 'Adaptive Responses' section shows a table of responses:

Response	Mode	Time	User	Status
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

The 'Next Steps' section contains a text input field.

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-5W-03" Moz11/2.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 404 322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CB-01" Moz11/2.0
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF0" Moz11/2.0
10.11.36.20 - - [07/Jan 18:10:52:000] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" Moz11/2.0
10.11.36.20 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" Moz11/2.0
10.11.36.20 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" Moz11/2.0

Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk ES Incident Review interface. On the left, there are filters for Urgency (CRITICAL: 5, HIGH: 119, MEDIUM: 556, LOW: 0, INFO: 0), Status (All), Owner (All), Security Domain (All), and Time (Last 24 hours). A central bar chart shows 680 events from 2/3/17 12:00:00 PM to 2/4/17 12:23:08 PM. Below the chart is a table of events. The selected event is titled "Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20".

Time	Security Domain	Title
2/3/17 9:10:52.000 PM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20

Description:
A system (10.11.36.20) was detected as generating an abnormally high number of CONNECT request events.

Additional Fields	Value
HTTP Method	CONNECT
Source	10.11.36.20 240
Source Business Unit	americas
Source Category	pcl
	splunk
Source City	Pleasanton
Source Country	USA
Source IP Address	10.11.36.20
Source Expected	true
Source Latitude	37.694452
Source Longitude	-121.894461
Source Owner	Bill Williams
Source PCI Domain	trust
Source Requires Antivirus	false
Source Should Time Synchronize	true
Source Should Update	true

Adaptive Response Actions

- Add Event to Investigation
- Create notable event
- Build Event Type
- Extract Fields
- Run Adaptive Response Actions
- Share Notable Event
- Suppress Notable Events
- Show Source

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

130.60.4... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FI-SW-03" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-18" 200 3855

Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk ES RedSeal Adaptive Response interface. The main window is titled "Incident Review" and shows a summary of incident counts by urgency: CRITICAL (5), HIGH (119), MEDIUM (556), LOW (0), and INFO (0). Below this, there are filters for Status, Owner, Security Domain, and Tag. A table of incident events is visible, with the selected event having a time of 2/3/17 9:10:52:00 PM and a security domain of Network. The description of the incident states: "A system (10.11.36.20) was detected as generating an abnormally high number of CON...".

An "Adaptive Response Actions" dialog box is open, allowing the user to select actions to run. The dialog includes a search bar and a checkbox for "Show only recommended actions". The following actions are listed:

- RedSeal : Display Source Details**
View L2 and other details
Category: Information Gathering | Task: scan | Subject: endpoint | Vendor: RedSeal
- RedSeal : List Top Reachable Groups**
Reachable groups prioritized by network access risk
Category: Information Gathering | Task: scan | Subject: endpoint | Vendor: RedSeal
- RedSeal : View Detailed Path**
View access path details
Category: Information Gathering | Task: scan | Subject: network | Vendor: RedSeal
- Stream Capture**
Creates stream capture
Category: Information Gathering | Task: create | Subject: network.capture | Vendor: RedSeal
- Nbtstat**
Runs the nbtstat command

A red arrow points from the text "RedSeal Adaptive Response Actions" to the dialog box. Below the dialog, a table shows the status of the response actions:

Response	Mode	Time	User	Status
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

The interface also includes a "Contributing Events" section with a link to "View Web Activity on 10.11.36.20" and a table for "Adaptive Responses".

Splunk ES RedSeal Adaptive Response

Incident Review

Urgency: CRITICAL 5, HIGH 119, MEDIUM 556, LOW 0, INFO 0

Status: All, Owner: All, Security Domain: All, Tag: [Submit]

Description: A system (10.11.36.20) was detected as generating an abnormally high number of connections...

Additional Fields

Field	Value
HTTP Method	CONNECT
Source	10.11.36.20
Source Business Unit	americas
Source Category	pci
Source City	splunk
Source Country	Pleasanton
Source IP Address	USA
Source Expected	10.11.36.20
Source Latitude	true
Source Longitude	37.694452
Source Owner	-121.894461
Source PCI Domain	Bill Williams
Source Requires Antivirus	trust
Source Should Time Synchronize	false
Source Should Update	true
	true

Adaptive Response Actions

Select actions to run.

+ Add New Response Action

- RedSeal: Display Source Details
 - Source: [Input Field]
 - Leave it blank to use the 'src' field from the incident

[Run]

Adaptive Responses

Response	Mode	Time	User	Status
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF10 HTTP 1.1" 404 720
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D95L7FF6ADF0 HTTP 1.1" 404 3322
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318
 10.11.36.20 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865
 10.11.36.20 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865

Splunk ES RedSeal Adaptive Response

splunk > App: Enterprise Security

Administrator 3 Messages Settings Activity Help Find

Security Posture Incident Review My Investigations Glass Tables Security Intelligence

Enterprise Security

Incident Review

Urgency

CRITICAL	5
HIGH	119
MEDIUM	556
LOW	0
INFO	0

Status: Name:

Owner: Search:

Security Domain: Time:

Tag:

Edit Selected | Edit All 680 Matching Events | Add Selected to Investigation

<input type="checkbox"/>	<input type="text" value="Time"/>	<input type="text" value="Security Domain"/>
<input checked="" type="checkbox"/>	2/3/17 9:10:52:00 PM	Network

Description:
A system (10.11.36.20) was detected as generating an abnormally high number of CON

Additional Fields

Field	Value
HTTP Method	CONNECT
Source	10.11.36.20
Source Business Unit	americas
Source Category	pci
Source City	splunk
Source Country	Pleasanton
Source IP Address	USA
Source Expected	10.11.36.20
Source Latitude	37.694452
Source Longitude	-121.894461
Source Owner	Bill Williams
Source PCI Domain	trust
Source Requires Antivirus	false
Source Should Time Synchronize	true
Source Should Update	true

Adaptive Response Actions

RedSeal · Display Source Details has been dispatched. Check the status of the action in the notable event details.

Select actions to run.

[+ Add New Response Action](#)

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

[View Adaptive Response Invocations](#)

Next Steps:

1 hour per column

Feb 4

Urgency Status Owner Actions

Critical New unassigned

1 2 3 4 5 6 7 8 9 10 next

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" Moz/1.17.0 "COMPACT" 20
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01" Moz/1.17.0 "COMPACT" 20
 317.27.160.0 - - [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=KQ-CB-01" Moz/1.17.0 "COMPACT" 20
 125.17.14.105:1871 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01" Moz/1.17.0 "COMPACT" 20
 125.17.14.105:1871 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01" Moz/1.17.0 "COMPACT" 20
 125.17.14.105:1871 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01" Moz/1.17.0 "COMPACT" 20

Splunk ES RedSeal Adaptive Response

splunk> App: Enterprise Security

Administrator Messages Settings Activity Help Find

Security Posture Incident Review My Investigations Glass Tables Security Intelligence

Enterprise Security

Incident Review

Urgency: CRITICAL 5, HIGH 124, MEDIUM 550, LOW 0, INFO 0

Status: All, Owner: All, Security Domain: All, Tag: []

2/3/17 9:10:52:00 PM Network

Description: A system (10.11.35.20) was detected as generating an abnormally high number of CON

Additional Fields:

Field	Value
HTTP Method	CONNECT
Source	10.11.35.20
Source Business Unit	americas
Source Category	pci
Source City	splunk
Source Country	Pleasanton
Source IP Address	10.11.35.20
Source Expected	true
Source Latitude	37.694452
Source Longitude	-121.894461
Source Owner	Bill.Williams
Source PCI Domain	trust
Source Requires Antivirus	false
Source Should Time Synchronize	true
Source Should Update	true

Adaptive Response Actions

RedSeal : Display Source Details' has been dispatched. Check the status of the action in the notable event details.

Select actions to run.

+ Add New Response Action

Category: All

Show only recommended actions

- RedSeal : Display Source Details
View L2 and other details
Category: Information Gathering | Task: scan | Subject: endpoint | Vendor: RedSeal
- RedSeal : List Top Reachable Groups
Reachable groups prioritized by network access risk
Category: Information Gathering | Task: scan | Subject: endpoint | Vendor: RedSeal
- RedSeal : View Detailed Path
View access path details
Category: Information Gathering | Task: scan | Subject: network | Vendor: RedSeal
- Stream Capture
Creates stream capture
Category: Information Gathering | Task: create | Subject: network.capture | Vendor: Splunk
- Nbtstat
Runs the nbtstat command

Run

Adaptive Responses:

Response	Mode	Time	User	Status
RedSeal : Display Source Details	adhoc	2017-02-04T12:24:02-0800	system	success
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

View Adaptive Response Invocations

Next Steps:

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?product_id=FL-DSH-01&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-26&SESSIONID=5D55L9FF1ADFF3" screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3

128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?product_id=FL-DSH-01&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-26&SESSIONID=5D55L9FF1ADFF3" screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3

317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?category_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-26&SESSIONID=5D55L9FF1ADFF3" screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3

125.17.14.10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-26&SESSIONID=5D55L9FF1ADFF3" screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3

Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk Enterprise Security interface. The main view is an 'Incident Review' for a critical incident. The incident details include:

- Urgency:** CRITICAL (5), HIGH (124), MEDIUM (550), LOW (0), INFO (0)
- Status:** All
- Owner:** All
- Security Domain:** All
- Tag:** (empty)

The incident description states: "A system (10.11.36.20) was detected as generating an abnormally high number of CON...". The 'Additional Fields' table shows the following data:

Additional Fields	Value
HTTP Method	CONNECT
Source	10.11.36.20
Source Business Unit	americas
Source Category	pci
Source City	splunk
Source Country	Pleasanton
Source IP Address	USA
Source Latitude	10.11.36.20
Source Longitude	true
Source Owner	37.694452
Source PCI Domain	-121.894461
Source Requires Antivirus	Bill_williams
Source Should Time Synchronize	trust
Source Should Update	false
	true
	true

An 'Adaptive Response Actions' dialog box is open, showing that the action 'RedSeal : Display Source Details' has been dispatched. Below, a list of actions to run is shown:

- RedSeal : List Top Reachable Groups**
 - Source:
 - Leave it blank to use the 'src' field from the incident.

The 'Run' button is visible at the bottom right of the dialog. Below the dialog, the 'Adaptive Responses' table shows the following entries:

Response	Mode	Time	User	Status
RedSeal : Display Source Details	adhoc	2017-02-04T12:24:02-0800	system	success
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

The background interface shows a bar chart and a table with columns for Urgency, Status, Owner, and Actions. The Urgency is set to Critical, Status to New, and Owner to unassigned.

Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk Enterprise Security interface. The main window shows an incident review for a system (10.11.35.20) detected as generating an abnormally high number of connections. A modal window titled "Adaptive Response Actions" is open, showing two actions that have been dispatched:

- RedSeal : Display Source Details* has been dispatched. Check the status of the action in the notable event details.
- RedSeal : List Top Reachable Groups* has been dispatched. Check the status of the action in the notable event details.

Below the actions, there is a section for "Select actions to run" with a "+ Add New Response Action" button. A red arrow points from the modal to a red box containing the text "RedSeal Adaptive Response actions executed successfully".

In the background, the incident review shows a table of additional fields:

Additional Fields	Value
HTTP Method	CONNECT
Source	10.11.35.20
Source Business Unit	americas
Source Category	pci
Source City	splunk
Source Country	Pleasanton
Source IP Address	10.11.35.20
Source Expected	true
Source Latitude	37.694452
Source Longitude	-121.894461
Source Owner	Bill Williams
Source PCI Domain	trust
Source Requires Antivirus	false
Source Should Time Synchronize	true
Source Should Update	true

At the bottom of the interface, there is a table showing the status of the response actions:

Response	Mode	Time	User	Status
RedSeal : Display Source Details	adhoc	2017-02-04T12:24:02-0800	system	success
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk Enterprise Security incident review interface. At the top, there are navigation tabs for 'Security Posture', 'Incident Review', 'My Investigations', 'Glass Tables', 'Security Intelligence', 'Security Domains', 'Audit', 'Search', and 'Configure'. The 'Incident Review' section is active, showing a list of incidents with filters for 'Urgency', 'Status', 'Owner', 'Security Domain', and 'Tag'. A bar chart shows the number of events over time, with a significant spike on Friday, February 3, 2017, at 6:00 PM. The selected incident is titled 'Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20'. The description states: 'A system (10.11.36.20) was detected as generating an abnormally high number of CONNECT request events.' The 'Additional Fields' table lists various attributes of the source system, including IP address, location, and owner. The 'Adaptive Response' table shows the following actions:

Response	Mode	Time	User	Status
RedSeal : List Top Reachable Groups	adhoc	2017-02-04T13:43:32-0800	system	success
RedSeal : Display Source Details	adhoc	2017-02-04T12:24:02-0800	system	success
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

The interface also includes a search bar, a 'Submit' button, and a table of incident details with columns for Time, Security Domain, Title, Status, Owner, and Actions. A red callout box with the text 'RedSeal Adaptive Response Results' points to the Adaptive Response table.

```

130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01"
128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADF9 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-268product_id=KQ-CU-01"
317.27.160.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD18SL8FF2ADF9"
130.60.4 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=FLOWERS&JSESSIONID=SD55L9FF1ADF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&JSESSIONID=SD55L9FF1ADF3"
130.60.4 - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-26&JSESSIONID=SD55L9FF1ADF3"
    
```

Splunk ES RedSeal Adaptive Response

The screenshot shows the Splunk ES interface with a search query: `tag=modaction_result orig_sid=scheduler__admin_REEtRVNTLU5ldHdvcmTQcm90ZWNoaW9u__RMD55df51155da61e965_at_1486185000_7294 orig_rid=0 orig_action_name=get_host_metrics`. The search results show one event from 2/4/17 12:19:02.000 PM to 2/4/17 12:29:02.000 PM. The event details are expanded to show a table with columns for Time and Event. The event occurred at 2/4/17 12:24:04.000 PM and contains host details for `Mac-00:10:11:36:00:20` and `host = localhost`. A red arrow points from the event details to a red box labeled "Host Details".

f	Time	Event
>	2/4/17 12:24:04.000 PM	Name=MinSrv-Test4-20, PrimaryService=HTTP, OS=Linux, AttackDepth=2, VulnerabilityCount=50, AccessibleFromUntrusted=False, HasAccessToCritical=False, Applications=None, IpAddress=10.11.36.20, Subnet=None, Mac=00:10:11:36:00:20, ConnectedSwitch=test-1136-sw1 (null), ConnectedPort=test-1136-sw1 (null) host = localhost

Selected Fields: host 1

Interesting Fields: AccessibleFromUntrusted 1, Applications 1, AttackDepth 1, ConnectedPort 1, ConnectedSwitch 1, eventtype 3, HasAccessToCritical 1, Index 1, IpAddress 1, Linecount 1, Mac 1, Name 1, orig_action_name 1, orig_rid 1, orig_sid 1, OS 1, PrimaryService 1, source 1, sourcetype 1, splunk_server 1, Subnet 1, tag 1, tag_eventtype 1, timestamp 1

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5L9FFIADPF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FI-SW-01" Moz/1.12.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5L9FFIADPF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&SESSIONID=SD5L9FFIADPF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&product_id=RP-LI-02" Moz/1.12.0
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&SESSIONID=SD5L9FFIADPF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&product_id=RP-LI-02" Moz/1.12.0
buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&product_id=RP-LI-02" Moz/1.12.0

Splunk ES RedSeal Adaptive Response

✓ 1 event (2/4/17 12:19:02.000 PM to 2/4/17 12:29:02.000 PM) No Event Sampling

Events (1) | Patterns | Statistics | Visualization

Format Timeline | **Zoom Out** | + Zoom to Selection | × Deselect | 1 minute per column

List | ✓ Format | 50 Per Page

< Hide Fields | All Fields

Selected Fields

- host 1

Interesting Fields

- AccessibleFromUntrusted 1
- Applications 1
- AttackDepth 1
- ConnectedPort 1
- ConnectedSwitch 1
- eventtype 3
- HasAccessToCritical 1
- index 1
- IpAddress 1
- linecount 1
- Mac 1
- OS 1
- Name 1
- ong_action_name 1
- orig_rid 1
- orig_sid 1
- OS 1
- PrimaryService 1
- source 1
- sourcetype 1
- splunk_server 1
- Subnet 1
- tag 1
- tag:eventtype 1
- timestamp 1
- VulnerabilityCount 1

+ Extract New Fields

Type	Field	Value	Actions
Selected	host ✓	localhost	
Event	AccessibleFromUntrusted	False	
	Applications	None	
	AttackDepth	2	
	ConnectedPort	test-1136-sw1	
	ConnectedSwitch	test-1136-sw1 (null)	
	HasAccessToCritical	False	
	IpAddress	10.11.36.20	
	Mac	00:10:11:36:00:20	
	Name	WinSrv-Test4-20	
	OS	Linux	
	PrimaryService	HTTP	
	Subnet	None	
	VulnerabilityCount	50	
	eventtype	get_detailed_path_modaction_result (n)	
	orig_action_name	get_host_metrics	
	orig_rid	0	
	orig_sid	scheduler_admin_REEBRVNTLU5dHdvcmtGcm9QZWN0aW9u_RMD55df51155da61e965_at_1486185000_7294	
	tag	modaction_result	
	timestamp	none	
Time	time	2017-02-04T12:24:04.000-08:00	
Default	index	main	
	linecount	1	
	source	localhost	
	sourcetype	redseal_data	
	splunk_server	pm-splunk-1	

**Host Details:
Attack Depth
Port ,Switch,
Access to Critical Assets**

130.60.4... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2703.84 Safari/537.36" [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF10ADF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF10ADF10" [07/Jan 18:10:56:156] "GET /oldlink?product_id=FL-DSH-01&JSESSIONID=5D55L9FF10ADF10 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?product_id=FL-DSH-01&JSESSIONID=5D55L9FF10ADF10" [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF10ADF10 HTTP 1.1" 200 385 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF10ADF10" [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF10ADF10 HTTP 1.1" 200 385 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF10ADF10"

Splunk ES RedSeal Adaptive Response

splunk App: Enterprise Security Administrator 3 Messages Settings Activity Help Find

Security Posture Incident Review My Investigations Glass Tables Security Intelligence Security Domains Audit Search Configure Enterprise Security

Incident Review

Urgency

CRITICAL	5
HIGH	124
MEDIUM	550
LOW	0
INFO	0

Status: Name:

Owner: Search:

Security Domain: Time: Last 24 hours

Tag:

679 events (2/3/17 1:00:00:00 PM to 2/4/17 1:30:54:00 PM)

Edit Selected | Edit All 679 Matching Events | Add Selected to Investigation

#	Time	Security Domain	Title	Urgency	Status	Owner	Actions
1	2/3/17 9:10:52:00 PM	Network	Abnormally High Number of HTTP CONNECT Request Events By 10.11.36.20	Critical	New	unassigned	

Description:
A system (10.11.36.20) was detected as generating an abnormally high number of CONNECT request events.

Additional Fields

Field	Value
HTTP Method	CONNECT
Source	10.11.36.20 240
Source Business Unit	americas
Source Category	pci
Source City	splunk
Source Country	Pleasanton
Source IP Address	USA
Source Latitude	10.11.36.20
Source Longitude	true
Source Owner	37.694452
Source PCI Domain	-121.894461
Source Requires Antivirus	BILL WILLIAMS
Source Should Time Synchronize	trust
Source Should Update	false
	true

Correlation Search:
Web - Abnormally High Number of HTTP Method Events By Src - Rule

History:
[View all review activity for this Notable Event](#)

Contributing Events:
[View Web Activity on 10.11.36.20](#)

Adaptive Responses:

Response	Mode	Time	User	Status
RedSeal : List Top Reachable Groups	adhoc	2017-02-04T13:43:32-0800	system	success
RedSeal : Display Source Details	adhoc	2017-02-04T12:24:02-0800	system	success
Notable	saved	2017-02-03T21:10:52-0800	admin	success
Risk Analysis	saved	2017-02-03T21:10:52-0800	admin	success

Next Steps:

130.60.4... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"...

Splunk ES RedSeal Adaptive Response

splunk> App: Enterprise Security Administrator 3 Messages Settings Activity Help Find

Security Posture Incident Review My Investigations Glass Tables Security Intelligence Security Domains Audit Search Configure Enterprise Security

Q New Search Save As Close

tag=modaction_result orig_sid=scheduler__admin_REEtRVNTLU5ldHdvcm90Zm9uRMD55df51155da61e965_at_1486185000_7294 orig_rid=0 orig_action_name=get_incident_response Date time range

✓ 1 event (2/4/17 1:38:32.000 PM to 2/4/17 1:48:32.000 PM) No Event Sampling Job Visualization Smart Mode

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

f	Time	Event
>	2/4/17 1:43:35.000 PM	Source=10.11.36.20 ReachableGroups="Critical Systems subnets (95),DMZ subnets (14),Data Servers subnets (10),NSX Data Servers (9),Wireless User Groups (7),Campus_dist_1_ios subnets (5),MPLS (5),Campus_FW1_screens subnets (5),Finance Subnets (5),Campus_fw2_screens subnets (0)" rsServer=pm-rsa-1.lab.redseal.net rsPort=443 rsUri=/redseal/a/incidentResponse/queryResult?source=10.11.36.20 ReachableGroups = Critical Systems subnets (95),DMZ subnets (14),Data Servers subnets (10),NSX Data Server... Source = 10.11.36.20 host = localhost

Selected Fields
a host 1
a ReachableGroups 1
a Source 1

Interesting Fields
a eventtype 4
a index 1
linecount 1
a orig_action_name 1
orig_rid 1
orig_sid 1
rsPort 1
a rsServer 1
a rsUri 1
a source 1
a sourcetype 1
a splunk_server 1
a tag 2
a tag:eventtype 2
a timestamp 1

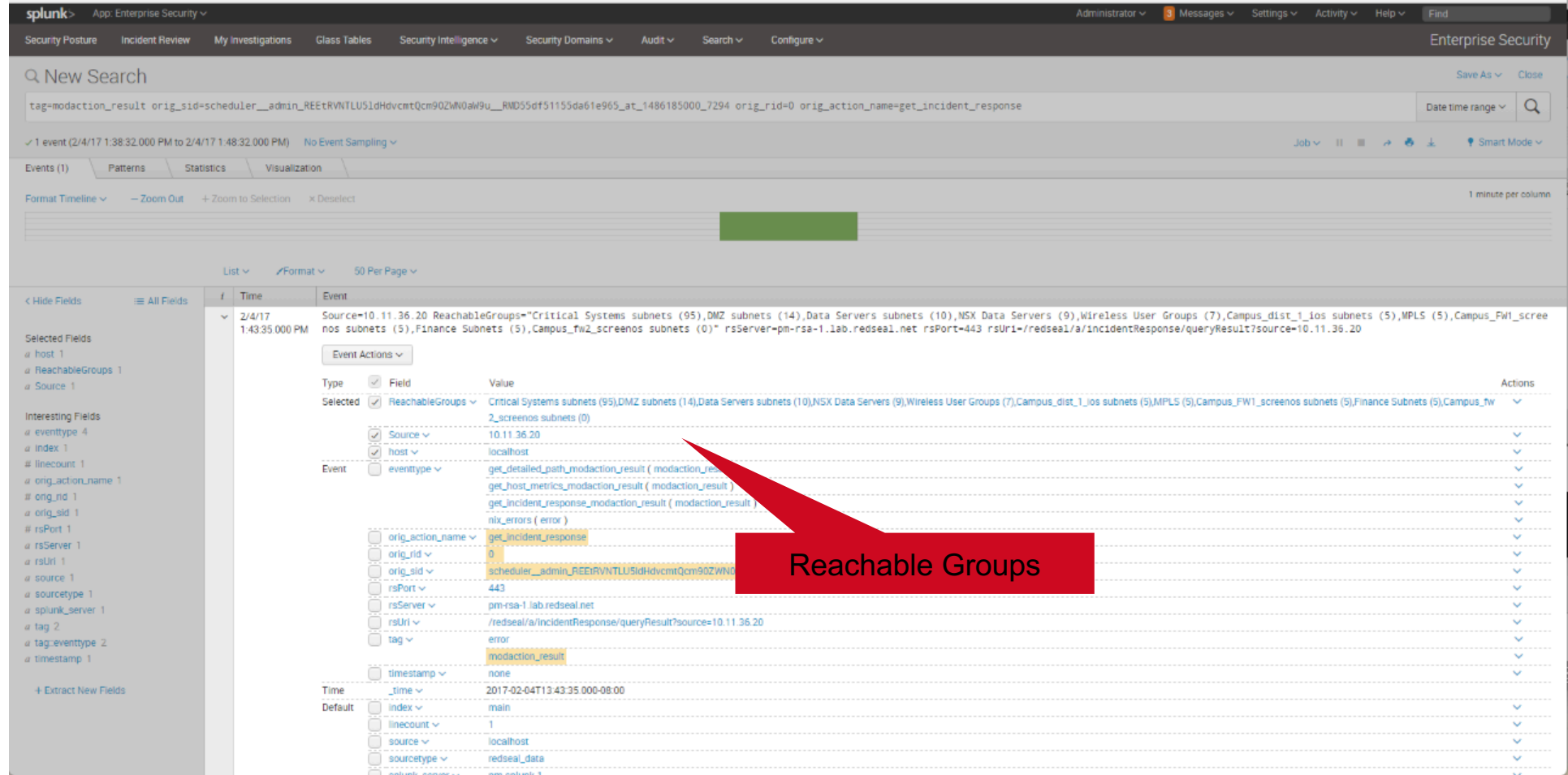
+ Extract New Fields

About Support File a Bug Documentation Privacy Policy © 2005-2017 Splunk Inc. All rights reserved.

Reachable Groups from IoC

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" Moz/1.1.0.0 "00000000-0000-0000-0000-000000000000"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CB-01" Moz/1.1.0.0 "00000000-0000-0000-0000-000000000000"
 1317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" Moz/1.1.0.0 "00000000-0000-0000-0000-000000000000"
 10.11.36.20 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" Moz/1.1.0.0 "00000000-0000-0000-0000-000000000000"
 10.11.36.20 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" Moz/1.1.0.0 "00000000-0000-0000-0000-000000000000"

Splunk ES RedSeal Adaptive Response



The screenshot shows the Splunk Enterprise Security interface. At the top, there's a search bar with a query: `tag=modaction_result orig_sid=scheduler__admin_REEtrVNTLUSIdHdvcmQcm90ZmW0aW9u_RmD55df51155da61e965_at_1486185000_7294 orig_rid=0 orig_action_name=get_incident_response`. Below this, a list of events is shown, with one event selected from 2/4/17 at 1:43:35 PM. The event details pane on the right shows the following fields:

Type	Field	Value	Actions
Selected	ReachableGroups	Critical Systems subnets (95),DMZ subnets (14),Data Servers subnets (10),NSX Data Servers (9),Wireless User Groups (7),Campus_dist_1_ios subnets (5),MPLS (5),Campus_FW1_screensubnets (5),Finance Subnets (5),Campus_tw2_screensubnets (0)	
	Source	10.11.36.20	
	host	localhost	
Event	eventtype	get_detailed_path_modaction_result (modaction_result) get_host_metrics_modaction_result (modaction_result) get_incident_response_modaction_result (modaction_result) nix_errors (error)	
	orig_action_name	get_incident_response	
	orig_rid	0	
	orig_sid	scheduler__admin_REEtrVNTLUSIdHdvcmQcm90ZmW0aW9u_RmD55df51155da61e965_at_1486185000_7294	
	rsPort	443	
	rsServer	pm-rsa-1.lab.redseal.net	
	rsUri	/redseal/a/incidentResponse/queryResult?source=10.11.36.20	
	tag	error	
	modaction_result		
	timestamp	none	
Time	time	2017-02-04T13:43:35.000-08:00	

A red arrow points from the text 'Reachable Groups' to the 'ReachableGroups' field in the event details pane. In the background, a network diagram is visible with a green box highlighting a specific host.

130.60.4
128.241.220.82
317 27.160.0.0
itemId=EST-16&product_id=RP-LI-02
purchase_id=EST-16&product_id=RP-LI-02
purchase_id=EST-16&product_id=RP-LI-02

Splunk ES RedSeal Adaptive Response

The screenshot displays the Splunk Enterprise Security interface. At the top, the search bar contains the query: `tag=modaction_result orig_sid=scheduler__admin_REEtRVNTLU5ldHdvcmrQcm90ZW0aW9u__RMD55df51155da61e965_at_1486185000_7294 orig_rid=0 orig_action_name=get_incident_response`. Below the search bar, a single event is shown with a time range of 2/4/17 1:38:32.000 PM to 2/4/17 1:48:32.000 PM. The event details are as follows:

Time	Event
2/4/17 1:43:35.000 PM	Source=10.11.36.20 ReachableGroups="Critical Systems subnets (95),DMZ subnets (14),Data Servers subnets (10),NSX Data Servers (9),Wireless User Groups (7),Campus_dist_1_ios subnets (5),MPLS (5),Campus_FW1_screens subnets (5),Finance Subnets (5),Campus_fw2_screens subnets (0)" rsServer=pm-rsa-1.lab.redseal.net rsPort=443 rsUri=/redseal/a/incidentResponse/queryResult?source=10.11.36.20

An 'Event Actions' menu is open over the event, with 'Launch RedSeal' highlighted. A red arrow points from this menu to a red box containing the text 'Launch RedSeal'. The event's field values are listed below:

Field	Value
orig_rid	0
orig_sid	scheduler__admin_REEtRVNTLU5ldHdvcmrQcm90ZW0aW9u__RMD55df51155da61e965_at_1486185000_7294
rsPort	443
rsServer	pm-rsa-1.lab.redseal.net
rsUri	/redseal/a/incidentResponse/queryResult?source=10.11.36.20
tag	error
modaction_result	
timestamp	none
Time	time 2017-02-04T13:43:35.000-08:00
Default	index main
linecount	1
source	localhost
sourcetype	redseal_data

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "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)" 468 125.17 14.10.18.108

Splunk ES RedSeal Adaptive Response

The screenshot displays the RedSeal interface with the following sections:

- Control Center:** Network Map, Network Access, Threats, Vulnerabilities, Configuration Issues, Security Impact, Detailed Path, Incident Response.
- Find Threat Source:** 10.11.36.20
- Threat Source Overview:**
 - Host Information:** Name: 10.11.36.20, Operating System: Linux, Applications: HTTPD, OpenSSH, rquotad, vsFTPD.
 - Groups:** Policy Groups: Trusted, Campus_fw2_screensos subnets; Topology Groups: IP Address: 10.11.36.20, Subnet: 10.11.36.0/24; Layer 2 Location: MAC Address: 00:10:11:36:00:20, Connected Switch: test-1136-sw1 (null), Connected Port: GigabitEthernet0/20.
- Reachable Groups:**

Group	Value
Data Servers subnets	95
NSX Data Servers	14
Wireless User Groups	10
Campus_dist_1_ios subnets	9
MPLS	7
Campus_fw1_screensos subnets	6
Finance Subnets	5
Campus_fw2_screensos subnets	5
Campus_fw2_screensos subnets	0
- Reachable Targets:** (Empty)
- Reachable Target Overview:** (Empty)

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.11.187] "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-CB-01"
://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" 404 125.17 14.11.187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

```


Splunk ES RedSeal Adaptive Response

REDSEAL
Launch Java App Help Logged in as: uiadmin

Control Center Network Map Network Access Threats Vulnerabilities Configuration Issues Security Impact Detailed Path Incident Response

Find Threat Source

Threat Source Overview		Reachable Groups		Reachable Targets		Reachable Target Overview	
Host Information		Group		Name			
Name	10.11.36.20	Group	Value	Name	Value		
Operating System	Linux	Critical Systems subnets	95	crit-web-svr-70	100		
Applications	HTTPD OpenSSH rquotad vsFTpd		14	crit-sys-sql-srv-120	95		
Groups		Data Servers subnets	10	crit-sys-sql-srv-119	95		
Policy Groups	Trusted	NSX Data Servers	9	crit-sys-sql-srv-118	95		
	Campus_fw2_screensos subnets	Wireless User Groups	7	crit-sys-sql-srv-117	95		
Topology Groups		Campus_dist_1_los subnets	5	crit-sys-sql-srv-116	95		
Topology	0	MPLS	5	crit-sys-sql-srv-115	95		
IP Address	10.11.36.20	Campus_FW1_screensos subnets	5	crit-sys-sql-srv-114	95		
Subnet	10.11.36.0/24			crit-sys-sql-srv-113	95		
Layer 2 Location				crit-sys-sql-srv-112	95		
MAC Address	00:10:11:36:00:20			crit-sys-sql-srv-111	95		
Connected Switch	test-1136-sw1 (null)			crit-sys-sql-srv-110	95		
Connected Port	GigabitEthernet0/20			crit-sys-sql-srv-109	95		

What is it?

Where is it?

```

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-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FF6ADF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=SD1S5LFF2ADF0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD1S5LFF2ADF0 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
  
```


Splunk ES RedSeal Adaptive Response

REDSEAL Launch Java App Help Logged in as: uiaadmin

Control Center Network Map Network Access Threats Vulnerabilities Configuration Issues Security Impact Detailed Path Incident Response

Find Threat Source: 10.11.36.20 Selected Target: crit-web-svr-70 Detailed Path Set As Source

Threat Source Overview

Host Information

- Name: 10.11.36.20
- Operating System: Linux
- Applications: HTTPD, OpenSSH, rquotad, vsFTPD

Groups

- Policy Groups: Trusted
- Topology Groups: Campus_fw2_screens subnets

Topology

- IP Address: 10.11.36.20
- Subnet: 10.11.36.0/24

Layer 2 Location

- MAC Address: 00:10:11:36:00:20
- Connected Switch: test-1136-sw1 (null)
- Connected Port: GigabitEthernet0/20

Reachable Groups

Group	Value
Critical Systems subnets	95
DMZ subnets	14
Data Servers subnets	10
NSX Data Servers	9
Wireless User Groups	7
Campus_dist_1_los subnets	5
MPLS	5
Campus_FW1_screens subnets	5
Finance Subnets	5
Campus_fw2_screens subnets	0

Reachable Targets

show 100 targets/page Page: 1

Name	Value
crit-web-svr-70	100
crit-sys-sql-srv-120	95
crit-sys-sql-srv-119	95
crit-sys-sql-srv-118	95
crit-sys-sql-srv-117	95
crit-sys-sql-srv-116	95
crit-sys-sql-srv-115	95
crit-sys-sql-srv-114	95
crit-sys-sql-srv-113	95
crit-sys-sql-srv-112	95
crit-sys-sql-srv-111	95
crit-sys-sql-srv-110	95
crit-sys-sql-srv-109	95
crit-sys-sql-srv-108	95
crit-sys-sql-srv-107	95
crit-sys-sql-srv-106	95
crit-sys-sql-srv-105	95
crit-sys-sql-srv-104	95
crit-sys-sql-srv-103	95
crit-sys-sql-srv-102	95
crit-sys-sql-srv-101	95
crit-sys-nfs-srv-120	95

Reachable Target Overview

Host Information

- Name: crit-web-svr-70
- Operating System: Windows
- Applications: SSL
- Value: 100

Groups

- Policy Groups: Trusted
- Critical Systems subnets

Topology Groups

- IP Address: 10.102.3.70
- Subnet: INTRA WEB

Layer 2 Location

- MAC Address: 10:10:20:03:00:70
- Connected Switch: campus-critical-3-sw1 (null)
- Connected Port: GigabitEthernet0/1

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=FI-SW-03"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADF3"
125.17.14 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15LAF10ADF10 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

```

Splunk ES RedSeal Adaptive Response

REDSEAL Launch Java App Help Logged in as: uiadmin

Control Center | Network Map | Network Access | Threats | Vulnerabilities | Configuration Issues | Security Impact | Detailed Path | Incident Response

Detailed Path Query

Sources: Destinations: Protocols: Ports:

Exhaustive Query

DETAILED PATH RESULT Tools

Fully Open Path →

1 Path(s) Discovered:

Result	Hops	Start	Finish
Not Filtered	5	10.11.36.0/24 (connected to test4)	10.102.3.0/24 INTRA WEB

Individual path with 5 hop(s)

How would they get there?

Access	Device	Interface	VRF Table	Protocol	Source IP	Source Port	Destination IP	Destination Port
	10.11.36.0/24							
	test							
	Campus-fw2-screensos							
	Campus-dist-2-ios							
	Campus-dist-1-ios							
	campus-critical-sys-ios							
	INTRA WEB							

Path Details

Access Details

Access	Device	Interface	VRF Table	Protocol	Source IP	Source Port	Destination IP	Destination Port

Splunk ES RedSeal Adaptive Response

REDSEAL
Launch Java App Help Logged in as: uiadmin

Control Center Network Map Network Access Threats Vulnerabilities Configuration Issues Security Impact Detailed Path Incident Response

Detailed Path Query

Sources: Destinations: Protocols: Ports:

Exhaustive Query

Individual path with 5 hop(s)

Honeypot

Network-based IDS System

Hop Details: Cam

Access	De
Input	Ca
Output	Ca

Filter/NAT Rules and Routes

Row count: 2

Device	Type	Config	First Line
Campus-fw2-screens	Filter Rule	set policy id 3 from "Test" to "dist" "Any" "Any" "Any" permit	config:111
Campus-fw2-screens	Filter Rule	(implicit) deny all	

Source Port	Destination IP	Destination Port
any	10.102.3.70	any
any	10.102.3.70	any

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"

317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3"

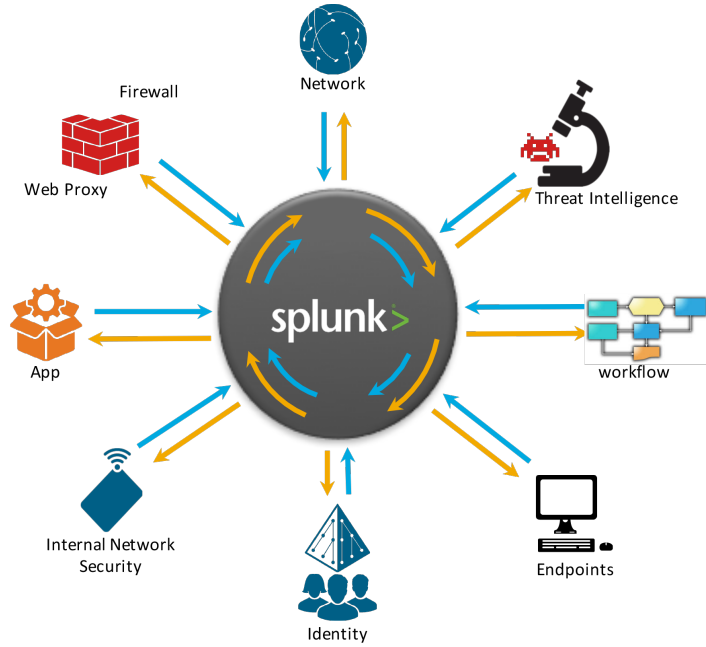
10.11.36.20 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3"

10.11.36.20 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3"

10.11.36.20 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3"

10.11.36.20 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3"

Splunk ES RedSeal Adaptive Response



REDSEAL

```
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-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
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-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
468 125.17 14.11.11.11 [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=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
10.10.10.10 [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=remove&itemId=EST-1" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
```




Thank you.



Q&A

Thank You

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

splunk> .conf2017