splunk> .conf2017

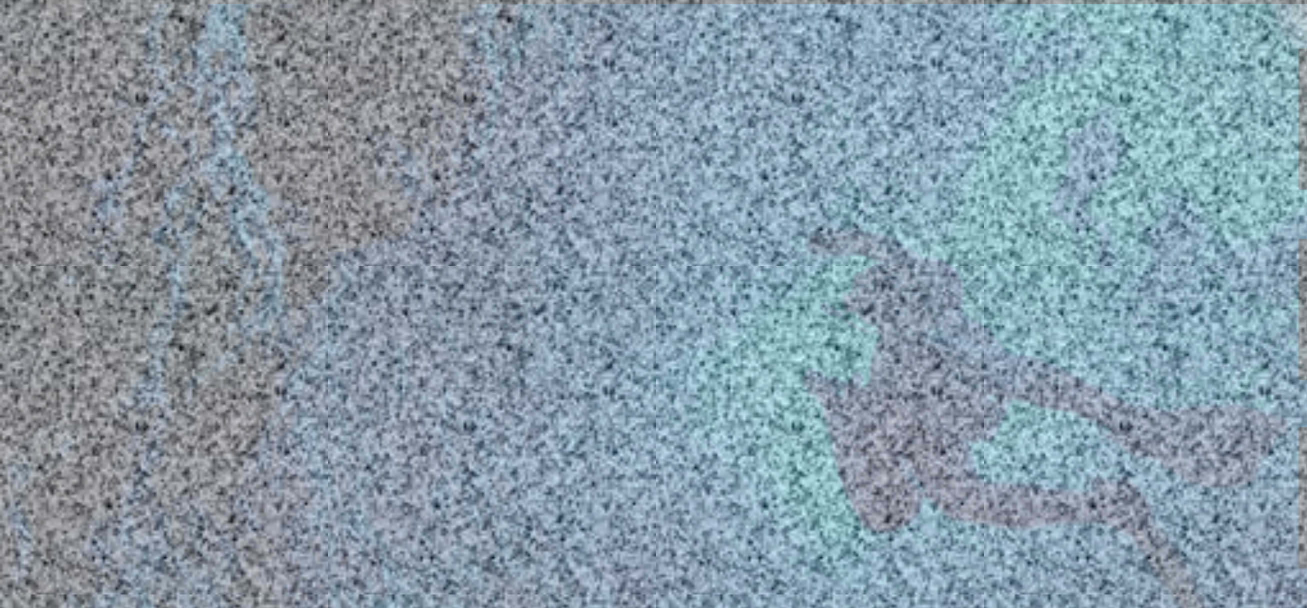
Data Obfuscation and Field Protection in Splunk

Angelo Brancato | Security Specialist
Dirk Nitschke | Senior Sales Engineer

28 September 2017 | Washington, DC

Agenda

Protect Your Machine Data



- The Drivers
- The Solution
- The Demo

Agenda

Protect Your Machine Data

- The Drivers
- The Solution
- The Demo

Who we are

Dirk Nitschke
Senior Sales Engineer

Angelo Brancato
Security Specialist

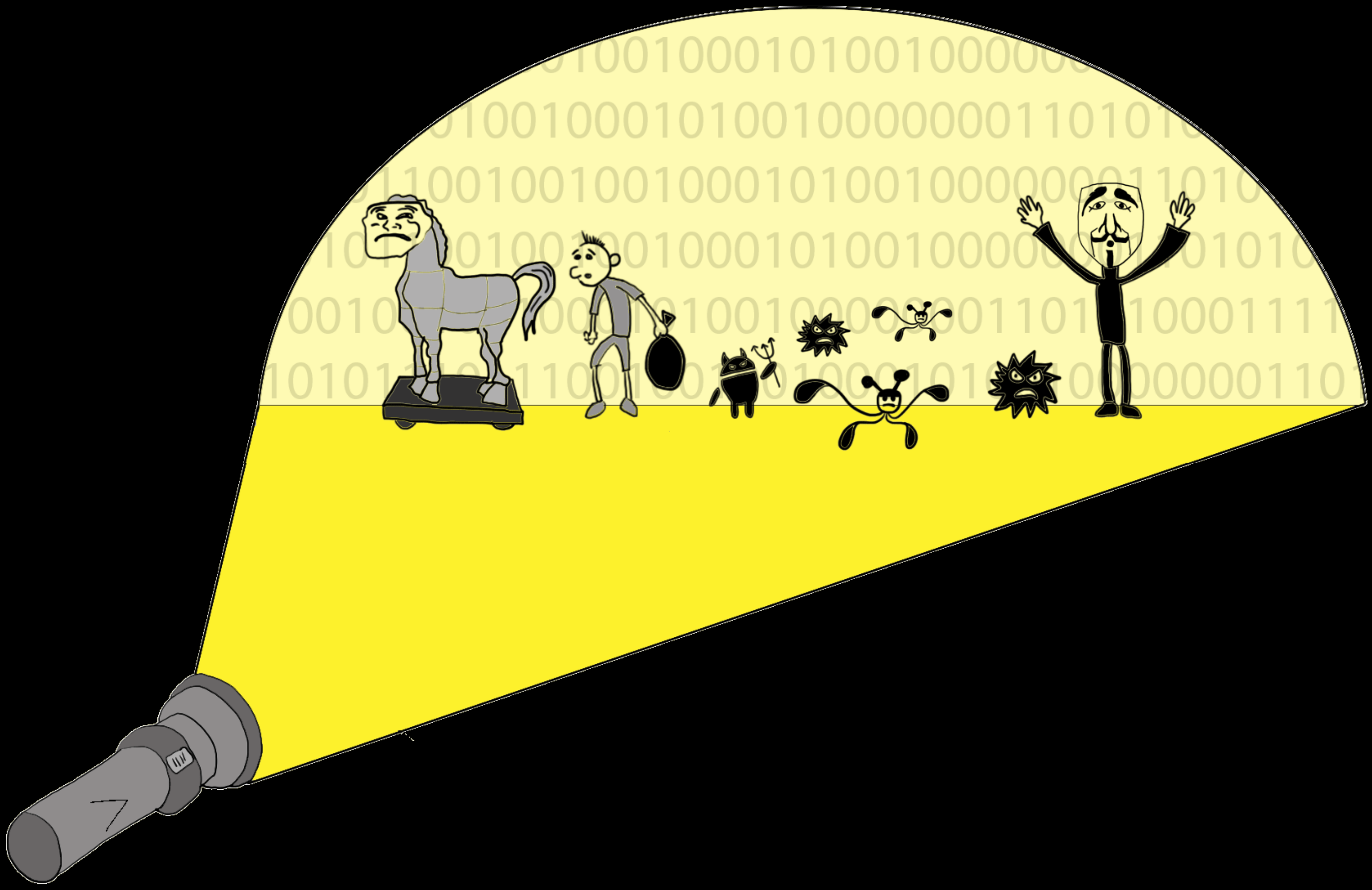
Forward-Looking Statements

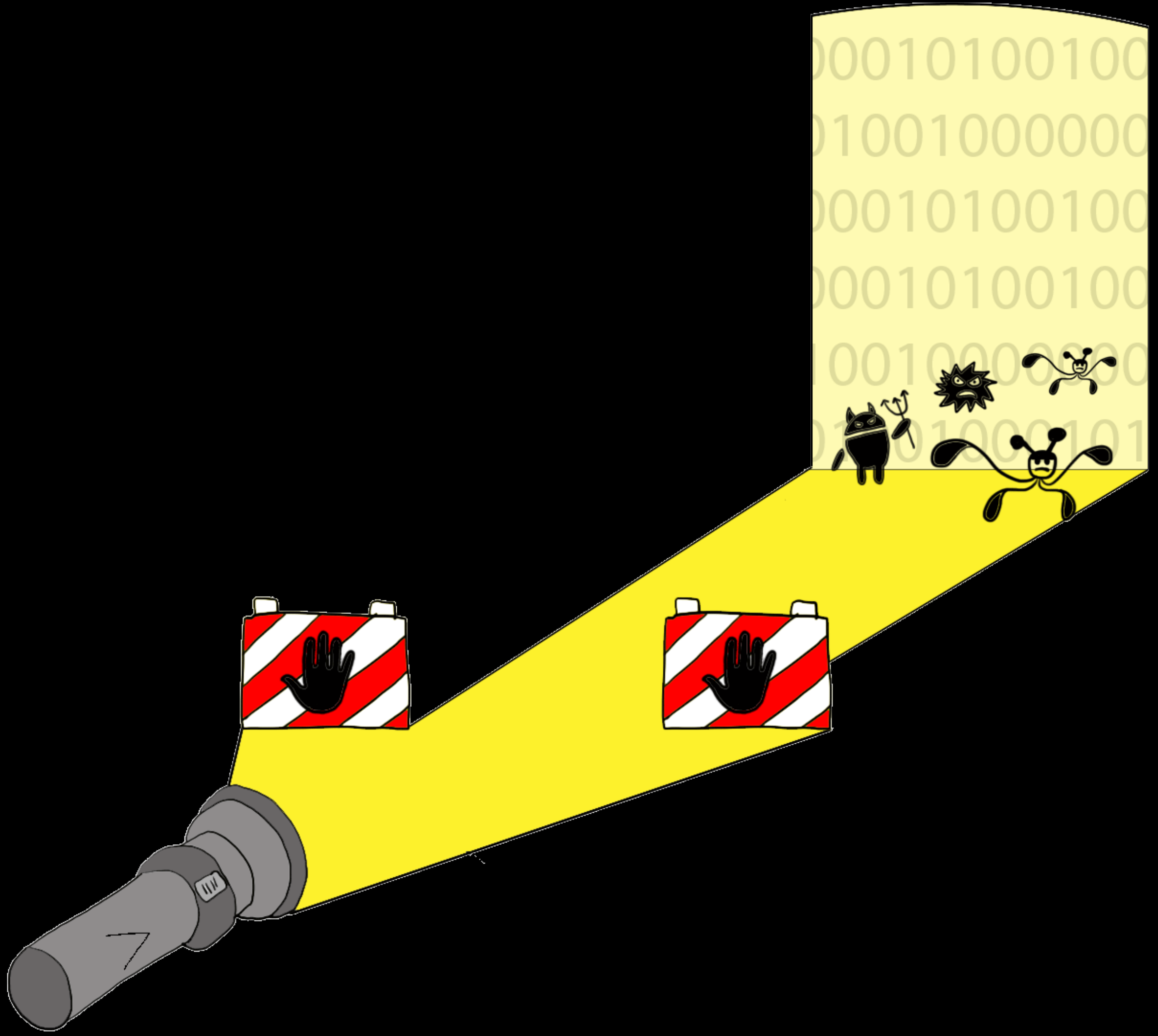
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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.

Why?

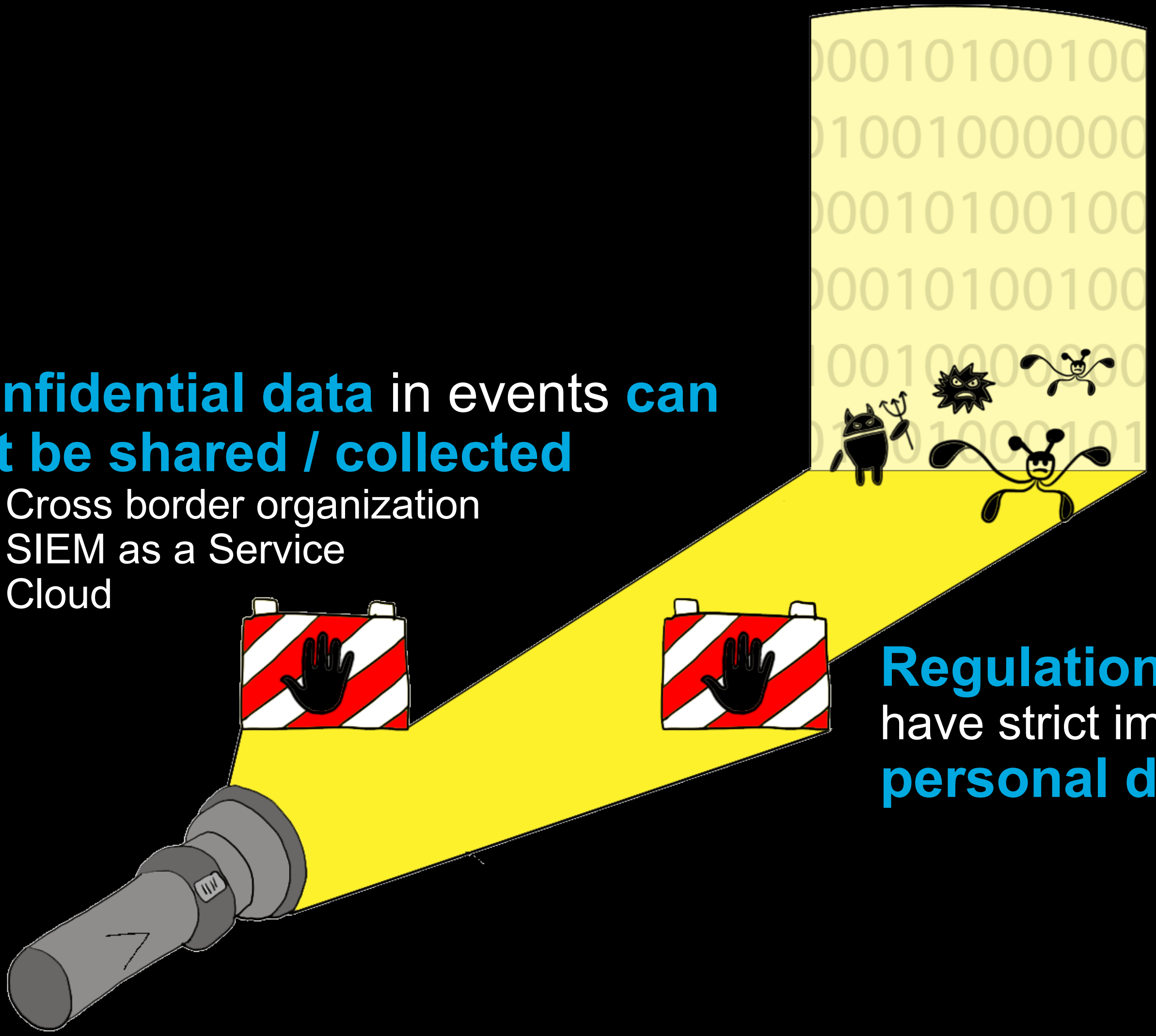
Minimize Risk, Enable Business




00010100100
01001000000
00010100100
00010100100
10010000000
10101000101

Confidential data in events **can not be shared / collected**

- Cross border organization
- SIEM as a Service
- Cloud



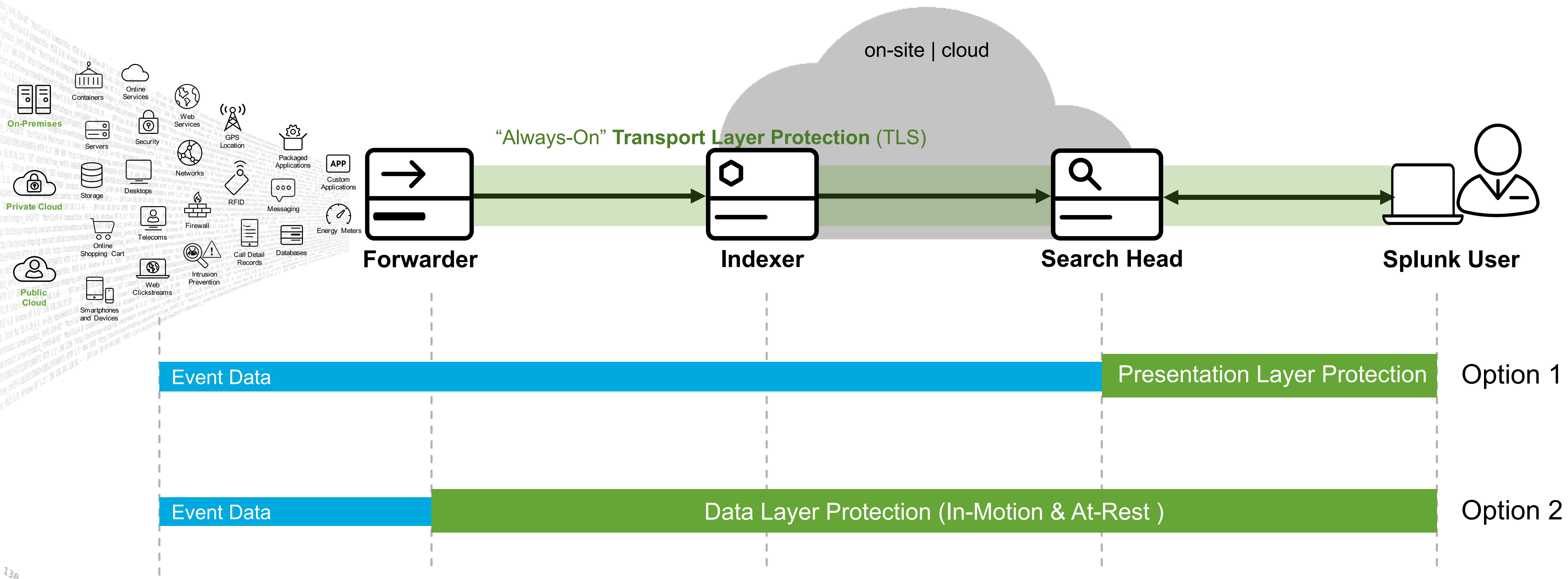
Regulation (like **GDPR, PCI, HIPAA**) have strict imposts on protecting **personal data**

How?

Transport
Presentation &
Data
Layer Protection

On an Event Field Level

Transport, Data, and Presentation Layer Protection



on-site | cloud

"Always-On" **Transport Layer Protection** (TLS)

Forwarder

Indexer

Search Head

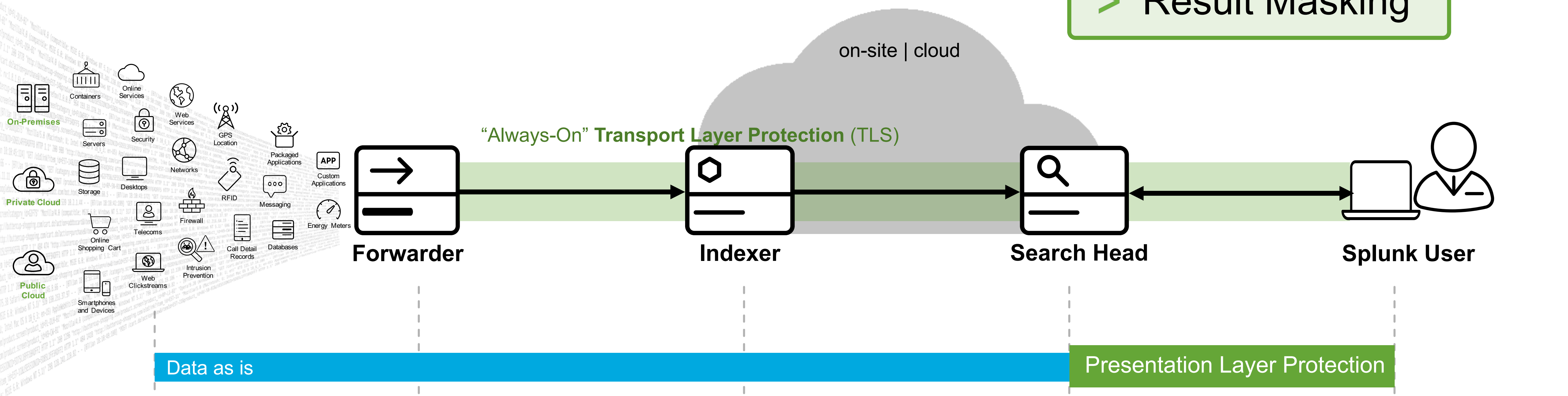
Splunk User

Event Data | Presentation Layer Protection — Option 1

Event Data | Data Layer Protection (In-Motion & At-Rest) — Option 2

Option 1: Presentation Layer Protection

> Result Masking



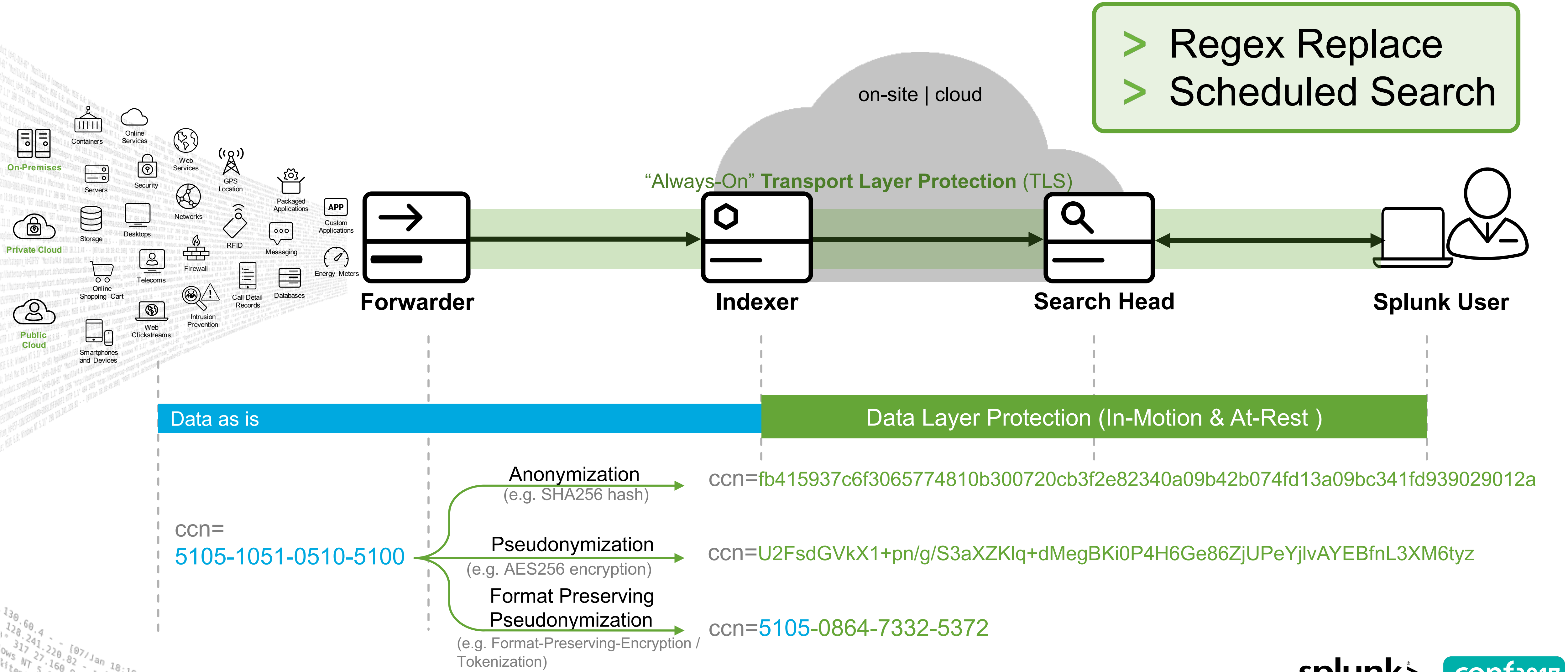
ccn=
5105-1051-0510-5100

Anonymization
(e.g. SHA256 hash)
ccn=fb415937c6f3065774810b300720cb3f2e82340a09b42b074fd13a09bc341fd939029012a

Pseudonymization
(e.g. AES256 encryption)
ccn=U2FsdGVkX1+pn/g/S3aXZKlq+dMegBKi0P4H6Ge86ZjUPeYjlvAYEBfnL3XM6tyz

Format Preserving Pseudonymization
(e.g. Format-Preserving-Encryption / Tokenization)
ccn=5105-0864-7332-5372

Option 2: Data Layer Protection



> Regex Replace
> Scheduled Search

on-site | cloud

“Always-On” **Transport Layer Protection** (TLS)

Forwarder **Indexer** **Search Head** **Splunk User**

Data as is

Data Layer Protection (In-Motion & At-Rest)

ccn=
5105-1051-0510-5100

Anonymization
(e.g. SHA256 hash)

ccn=fb415937c6f3065774810b300720cb3f2e82340a09b42b074fd13a09bc341fd939029012a

Pseudonymization
(e.g. AES256 encryption)

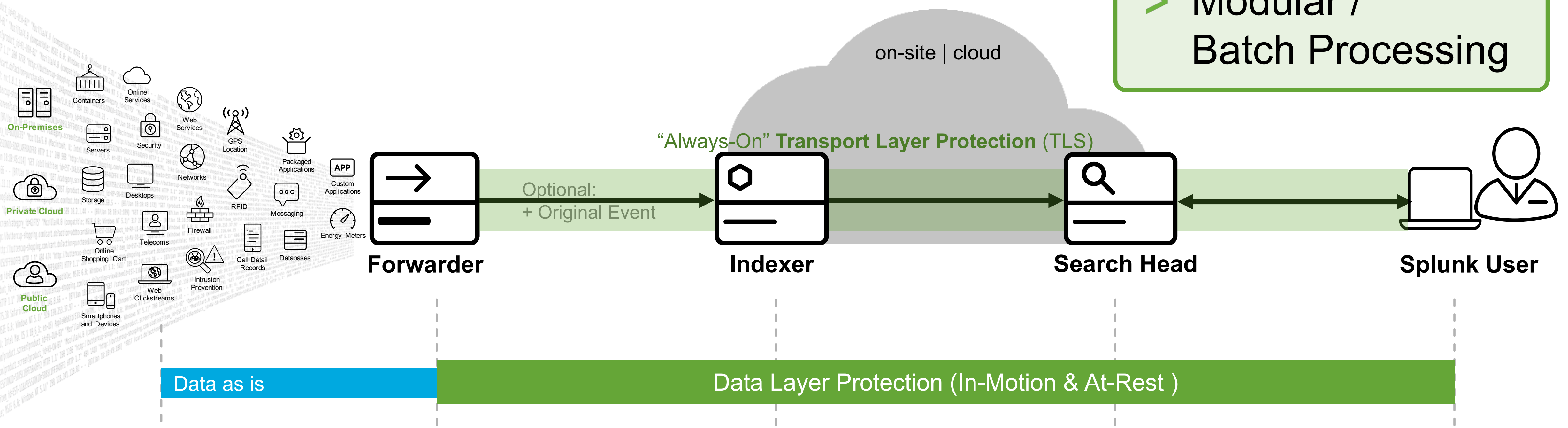
ccn=U2FsdGVkX1+pn/g/S3aXZKlq+dMegBKi0P4H6Ge86ZjUPeYjlvAYEBfnL3XM6tyz

Format Preserving Pseudonymization
(e.g. Format-Preserving-Encryption / Tokenization)

ccn=5105-0864-7332-5372

Option 2: Data Layer Protection

> Modular / Batch Processing



ccn=
5105-1051-0510-5100

Anonymization
(e.g. SHA256 hash)

ccn=fb415937c6f3065774810b300720cb3f2e82340a09b42b074fd13a09bc341fd939029012a

Pseudonymization
(e.g. AES256 encryption)

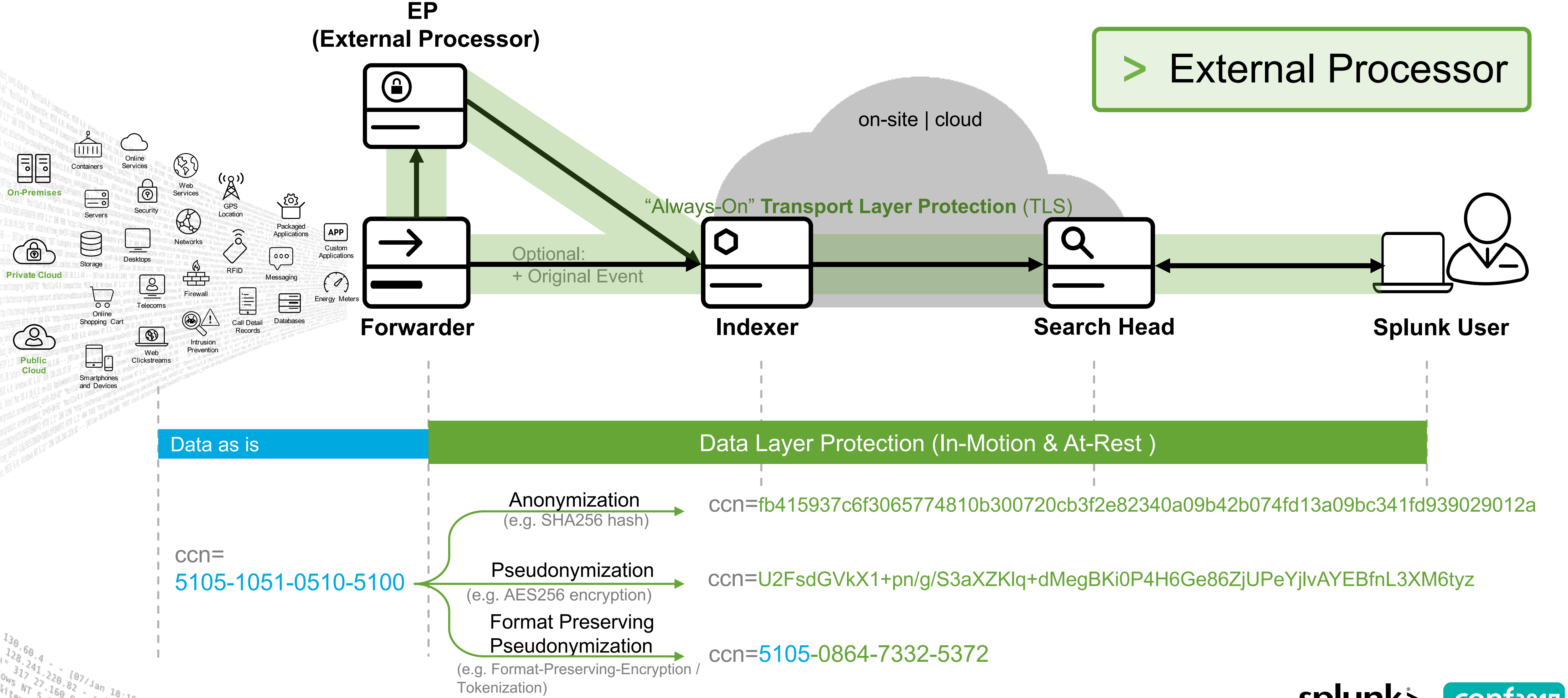
ccn=U2FsdGVkX1+pn/g/S3aXZKlq+dMegBKi0P4H6Ge86ZjUPeYjlvAYEBfnL3XM6tyz

Format Preserving
Pseudonymization
(e.g. Format-Preserving-Encryption /
Tokenization)

ccn=5105-0864-7332-5372

Option 2: Data Layer Protection

> External Processor



EP
(External Processor)

on-site | cloud

"Always-On" **Transport Layer Protection** (TLS)

Optional:
+ Original Event

Forwarder

Indexer

Search Head

Splunk User

Data as is

Data Layer Protection (In-Motion & At-Rest)

ccn=
5105-1051-0510-5100

Anonymization
(e.g. SHA256 hash)

ccn=fb415937c6f3065774810b300720cb3f2e82340a09b42b074fd13a09bc341fd939029012a

Pseudonymization
(e.g. AES256 encryption)

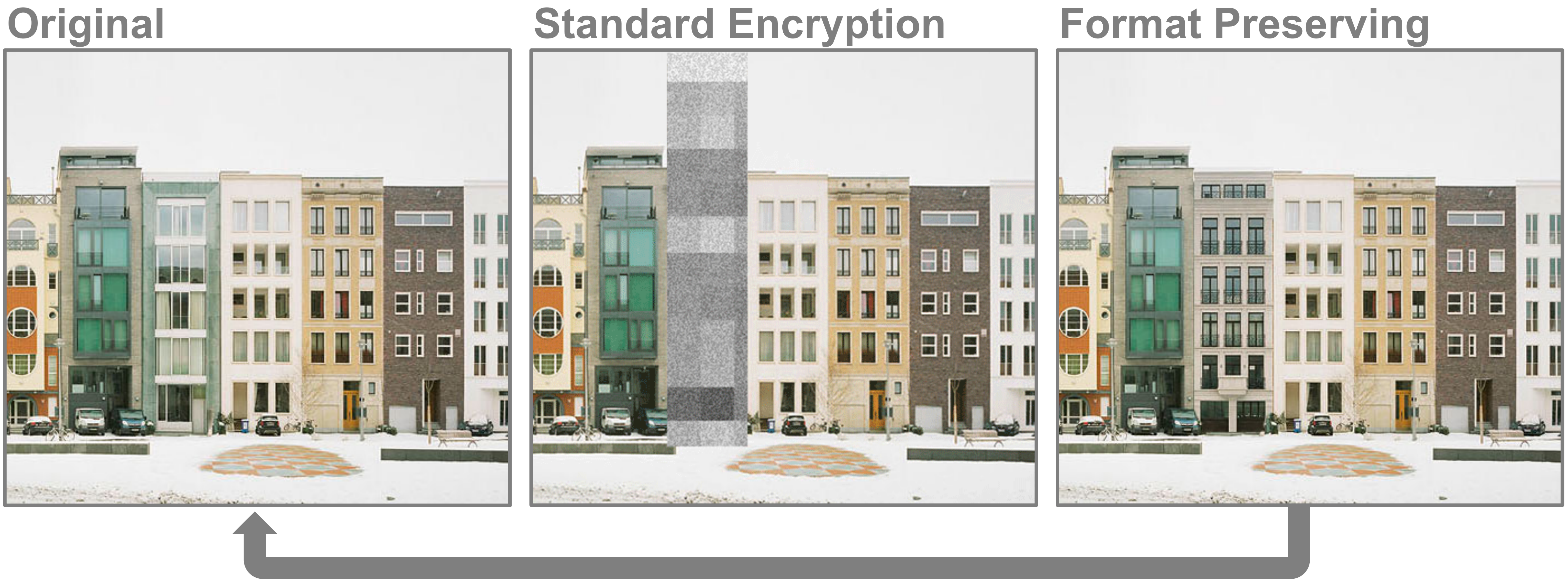
ccn=U2FsdGVkX1+pn/g/S3aXZKlq+dMegBKi0P4H6Ge86ZjUPeYjlvAYEBfnL3XM6tyz

Format Preserving
Pseudonymization
(e.g. Format-Preserving-Encryption / Tokenization)

ccn=5105-0864-7332-5372

What is Format Preserving Encryption?

An Analogy…



Original

Standard Encryption

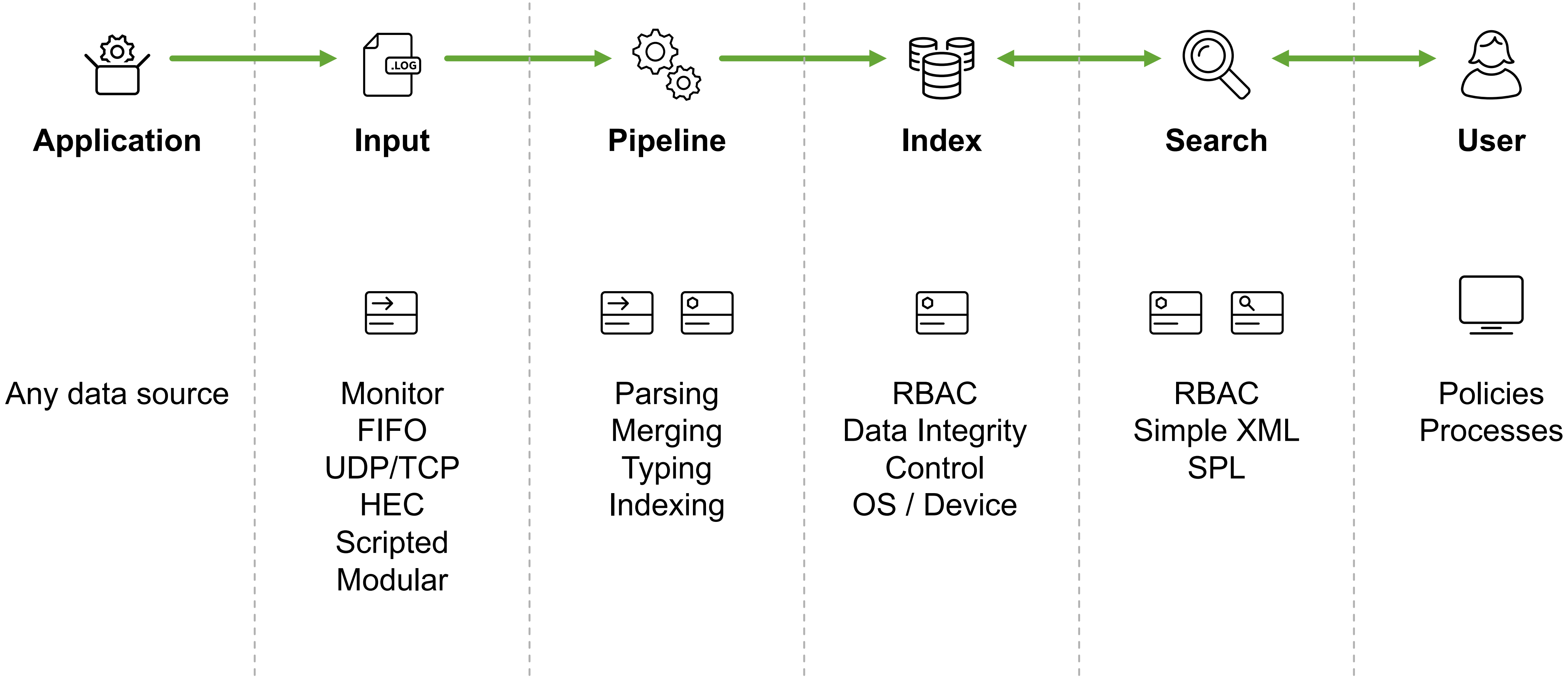
Format Preserving

What?

Various Options to Protect Event Fields

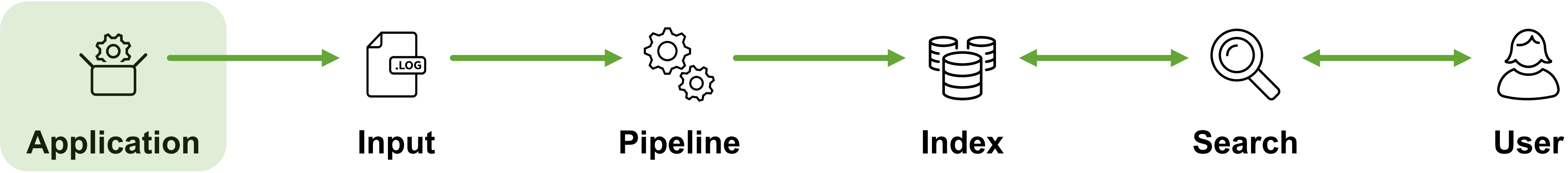
Protect Field Values

Data Flow



Application	Input	Pipeline	Index	Search	User
Any data source	Monitor FIFO UDP/TCP HEC Scripted Modular	Parsing Merging Typing Indexing	RBAC Data Integrity Control OS / Device	RBAC Simple XML SPL	Policies Processes

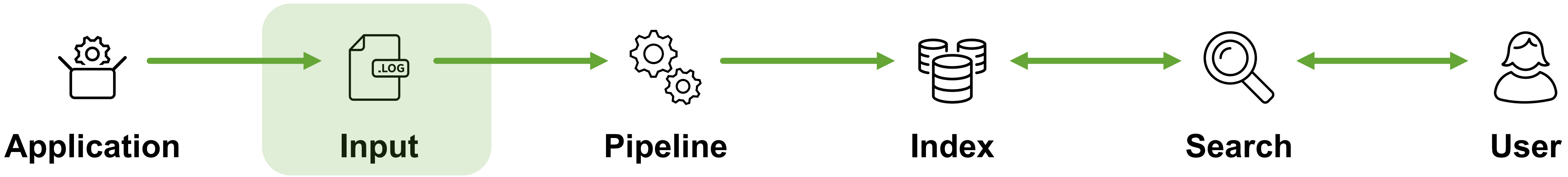
Data Source Layer – Application



- Protect data at earliest stage in the process
- Data source owner is responsible

- Application support
- May need a means to decode data again

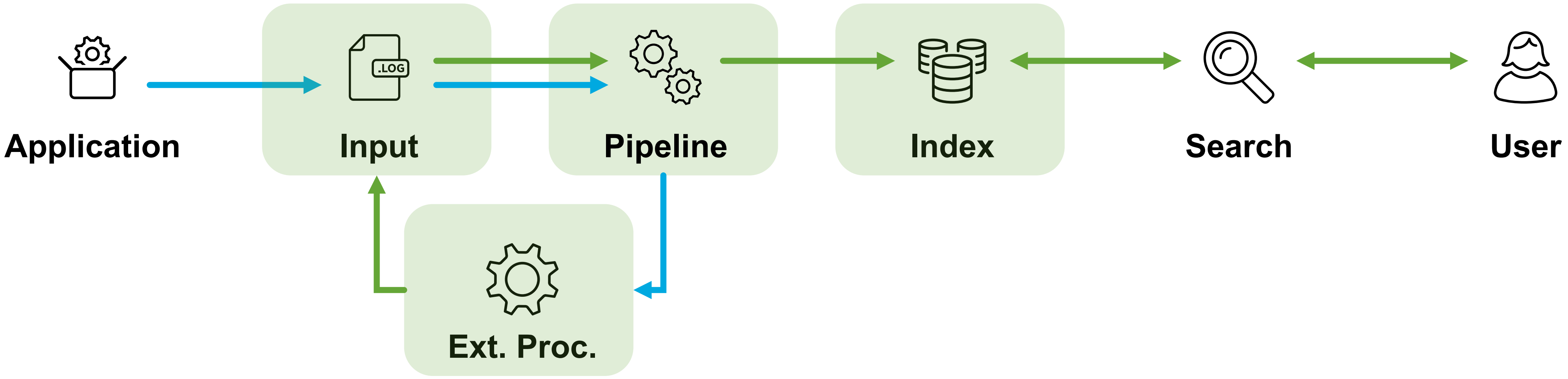
Input Layer – Modular / Batch Processing



- Pre-process data
- Create your own data input capabilities using a modular input

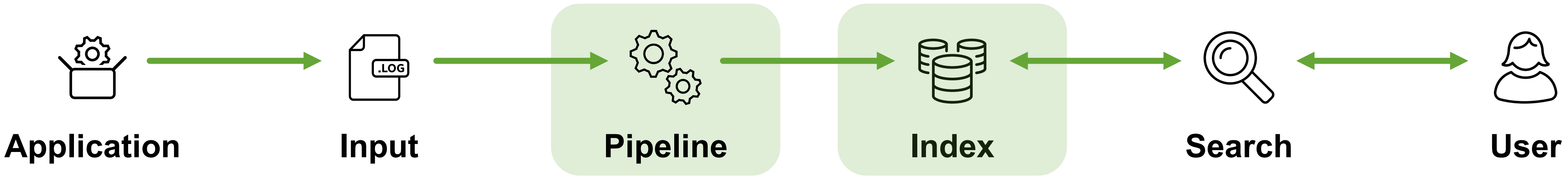
- Very flexible
- Requires scripting, programming

External Processor



- Forward raw data plus meta data to external processing engine
- Output of external processor is an input for Splunk again
- Very flexible but also complex

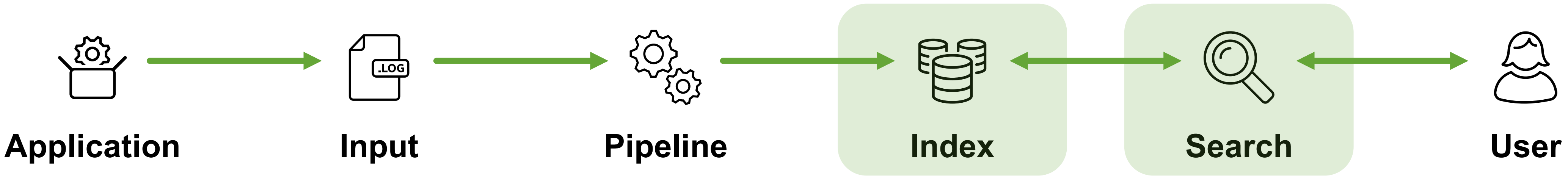
Built-In at Indexing Time – Regex Replace



- Typing pipeline / regex replacement processor
- Uses SEDCMD or TRANSFORMS to modify data at indexing time

- Easy to implement
- Limited flexibility, mainly anonymization

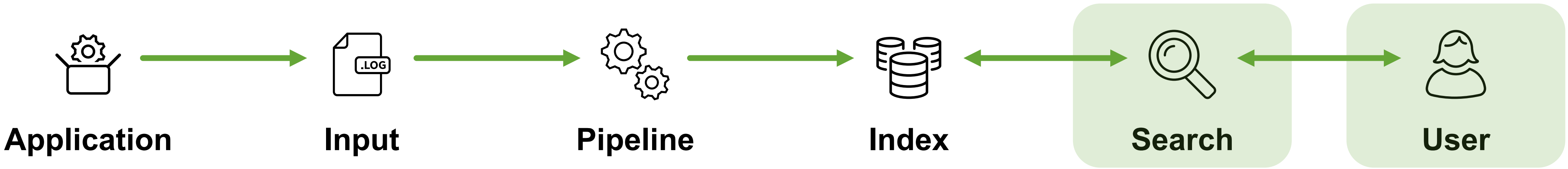
Copy Events – Scheduled Search



- Scheduled search selects and transforms the data
  - SPL and custom search commands if needed
- Send modified events to a different index
  - Think about collect, cefout, or a custom search command

- Modified events are delayed because of scheduling
- Preservation of event metadata

Presentation Layer – Result Masking



- Hide data at presentation layer
- <your_search> | eval user=sha256(user) or your own custom search command
- Optionally: user lockdown
  - Pre-defined app with dashboard access only
  - No search app, no raw search, no raw event drill down

- May be good enough

Overview – All Options

No scientific research

Option	Layer	Latency	Security	Complexity	Usability
Application	Data Source	Low	Very High	Medium (decoding)	Medium (decoding)
Modular / Batch	Data	Medium (API calls)	High	High	High
External Processor	Data	Medium (API calls)	High	High	High
Regex Replace	Data	Medium	High (anonymization)	Low	Low (anonymization)
Scheduled Search	Data	Very High (schedule)	Low	Medium	Medium (due to latency)
Result Masking	Presentation	Medium	Low (need-to-know)	Low	High

Summing Up

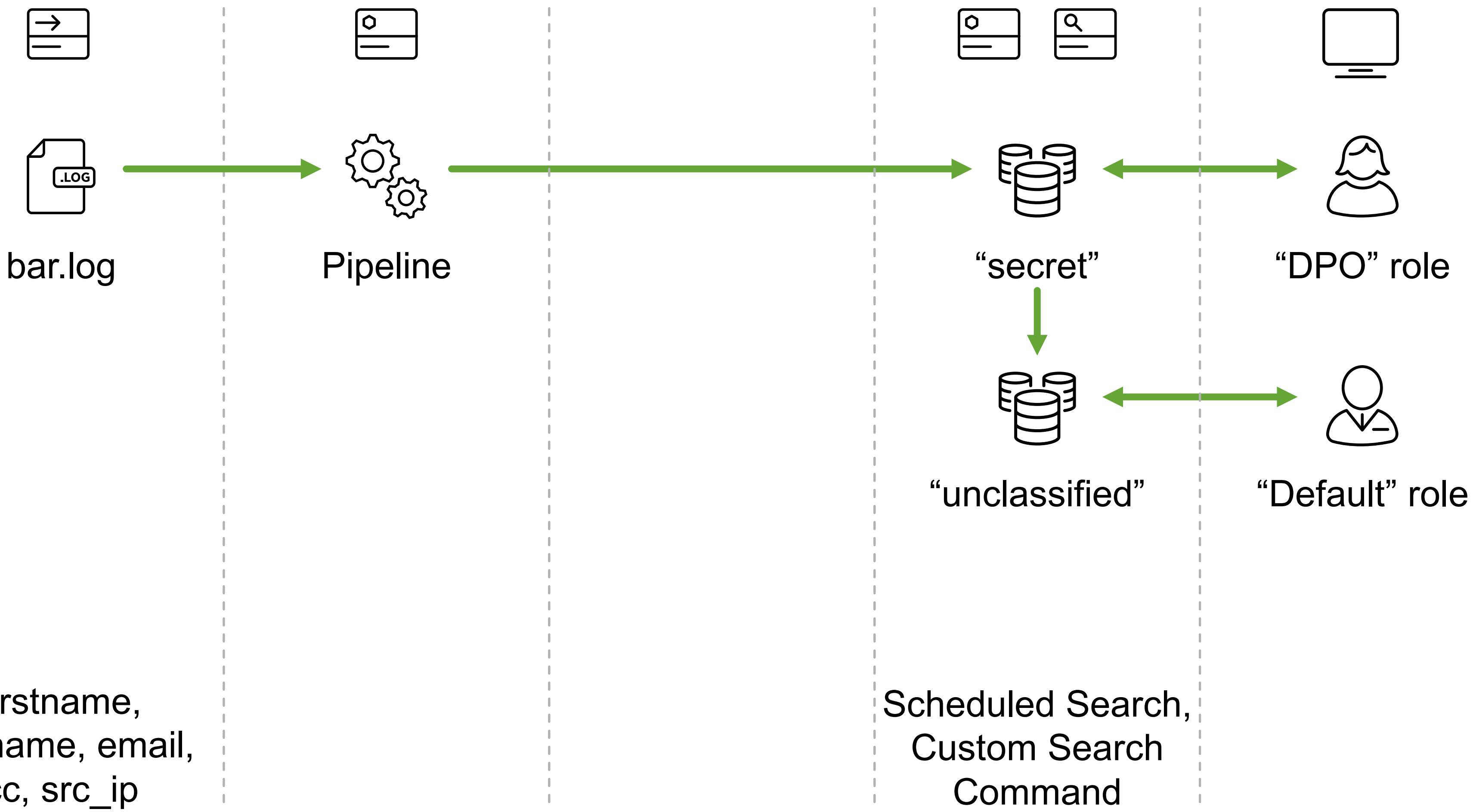
1. Many possible ways – each has pros and cons
2. Qualify – what are the requirements and boundary conditions
3. Data obfuscation requires a proper concept and careful planning
4. Choose and mix – and keep it simple

How?

Demo

Just a Demo – Your Mileage Will Vary

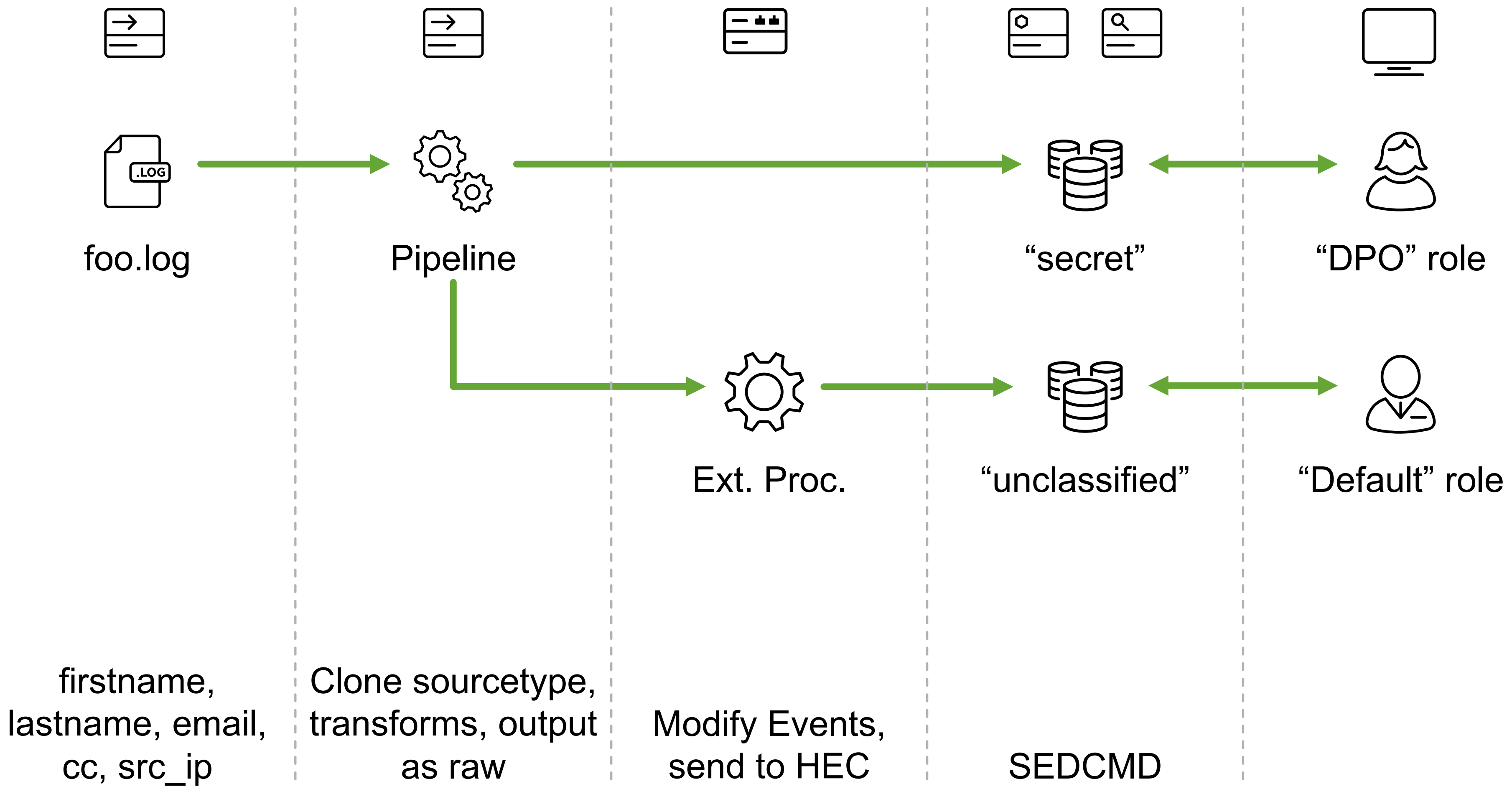
Demo Setup



firstname, lastname, email, cc, src_ip

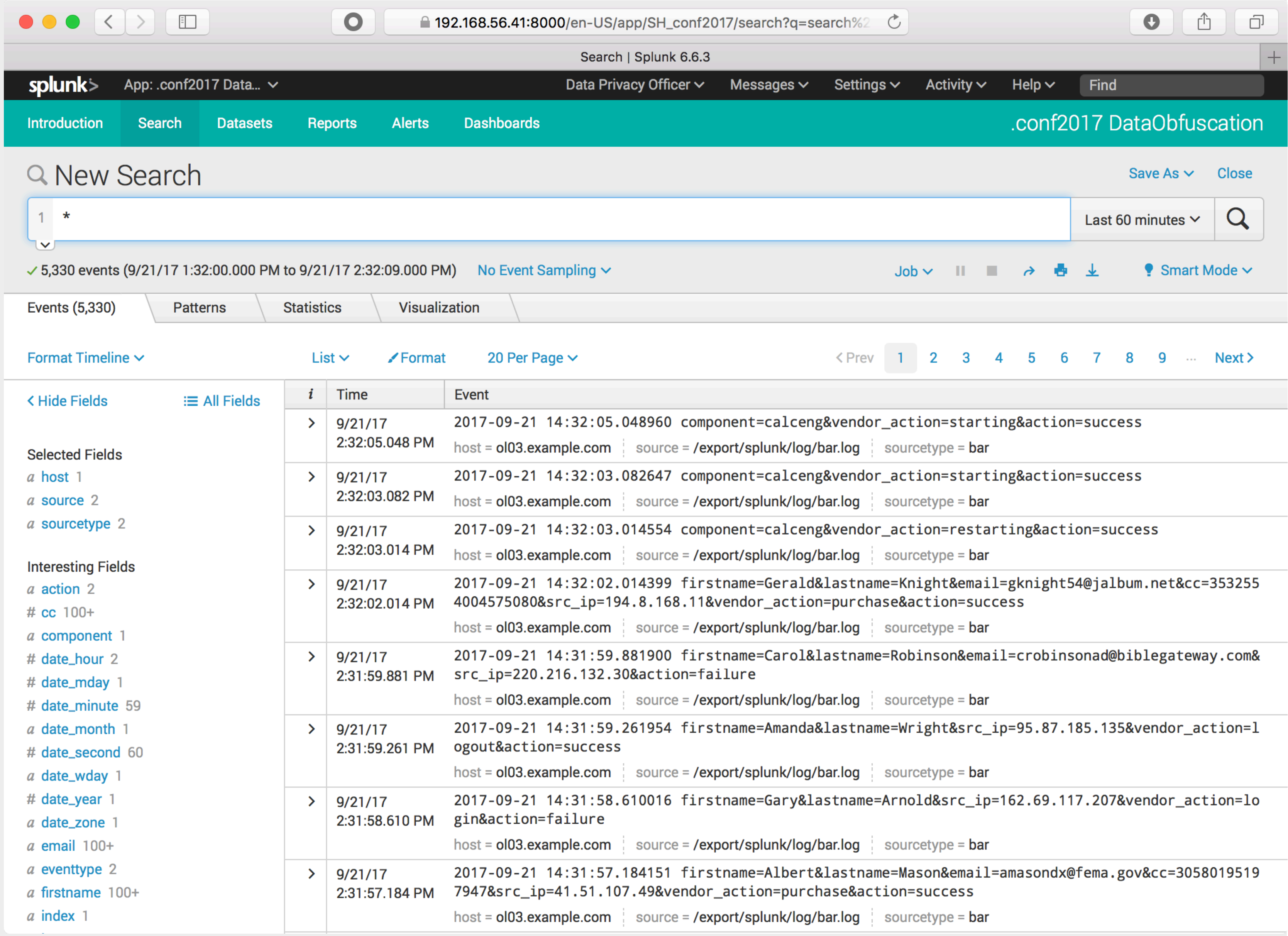
Scheduled Search, Custom Search Command

Demo Setup



foo.log
Pipeline
"secret"
"DPO" role
Ext. Proc.
"unclassified"
"Default" role
firstname, lastname, email, cc, src_ip
Clone sourcetype, transforms, output as raw
Modify Events, send to HEC
SEDCMD

Original Events



New Search

```
1  *
```

Last 60 minutes

✓ 5,330 events (9/21/17 1:32:00.000 PM to 9/21/17 2:32:09.000 PM)   No Event Sampling

Selected Fields

- a host 1
- a source 2
- a sourcetype 2

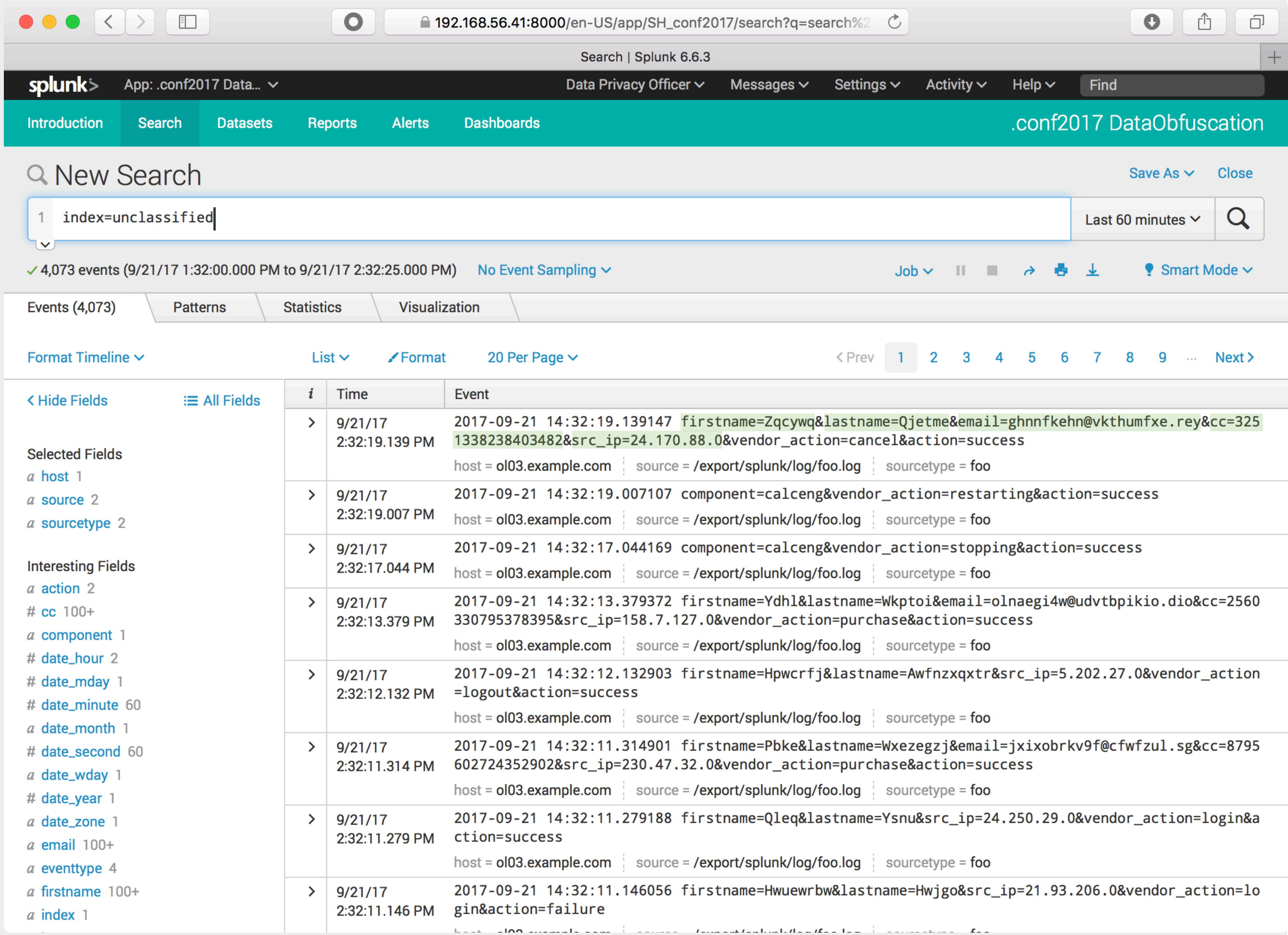
Interesting Fields

- a action 2
- # cc 100+
- a component 1
- # date_hour 2
- # date_mday 1
- # date_minute 59
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- a date_zone 1
- a email 100+
- a eventtype 2
- a firstname 100+
- a index 1

i	Time	Event
>	9/21/17 2:32:05.048 PM	2017-09-21 14:32:05.048960 component=calceng&vendor_action=starting&action=success host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:32:03.082 PM	2017-09-21 14:32:03.082647 component=calceng&vendor_action=starting&action=success host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:32:03.014 PM	2017-09-21 14:32:03.014554 component=calceng&vendor_action=restarting&action=success host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:32:02.014 PM	2017-09-21 14:32:02.014399 firstname=Gerald&lastname=Knight&email=gknight54@jalbum.net&cc=3532554004575080&src_ip=194.8.168.11&vendor_action=purchase&action=success host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:31:59.881 PM	2017-09-21 14:31:59.881900 firstname=Carol&lastname=Robinson&email=crobinsonad@biblegateway.com&src_ip=220.216.132.30&action=failure host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:31:59.261 PM	2017-09-21 14:31:59.261954 firstname=Amanda&lastname=Wright&src_ip=95.87.185.135&vendor_action=logout&action=success host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:31:58.610 PM	2017-09-21 14:31:58.610016 firstname=Gary&lastname=Arnold&src_ip=162.69.117.207&vendor_action=login&action=failure host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar
>	9/21/17 2:31:57.184 PM	2017-09-21 14:31:57.184151 firstname=Albert&lastname=Mason&email=amasondx@fema.gov&cc=30580195197947&src_ip=41.51.107.49&vendor_action=purchase&action=success host = ol03.example.com source = /export/splunk/log/bar.log sourcetype = bar

Processed Events

Masked critical data



```
1  index=unclassified
```

✓ 4,073 events (9/21/17 1:32:00.000 PM to 9/21/17 2:32:25.000 PM)

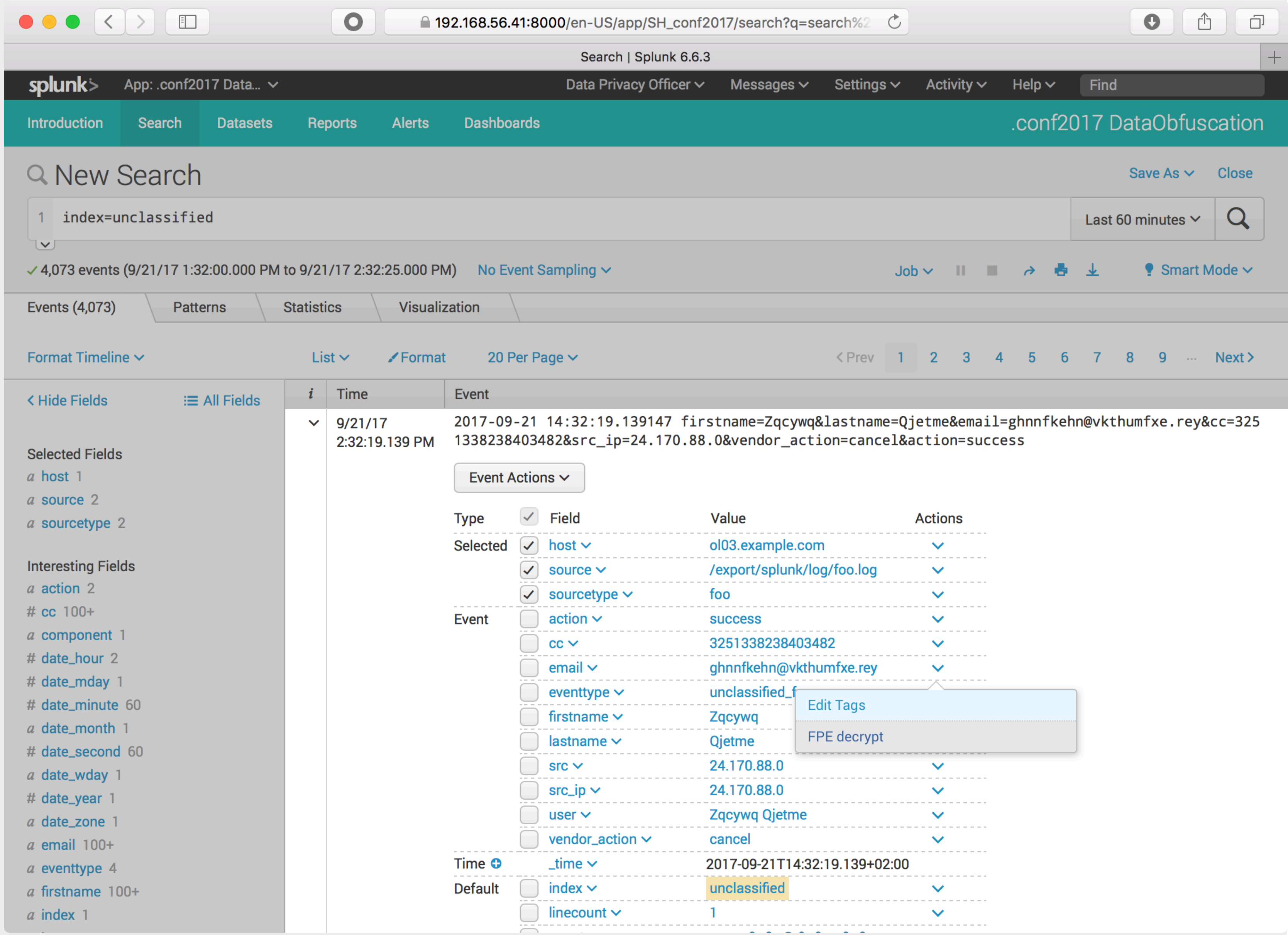
Selected Fields
- a host 1
- a source 2
- a sourcetype 2

Interesting Fields
- a action 2
- # cc 100+
- a component 1
- # date_hour 2
- # date_mday 1
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- a date_zone 1
- a email 100+
- a eventtype 4
- a firstname 100+
- a index 1

i	Time	Event
>	9/21/17 2:32:19.139 PM	2017-09-21 14:32:19.139147 firstname=Zqcywq&lastname=Qjetme&email=ghnnfkehn@vkthumfxe.rey&cc=3251338238403482&src_ip=24.170.88.0&vendor_action=cancel&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:19.007 PM	2017-09-21 14:32:19.007107 component=calceng&vendor_action=restarting&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:17.044 PM	2017-09-21 14:32:17.044169 component=calceng&vendor_action=stopping&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:13.379 PM	2017-09-21 14:32:13.379372 firstname=Ydhl&lastname=Wkptoi&email=olnaegi4w@udvtbpikio.dio&cc=2560330795378395&src_ip=158.7.127.0&vendor_action=purchase&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:12.132 PM	2017-09-21 14:32:12.132903 firstname=Hpwcrfj&lastname=Awfnzxqxtr&src_ip=5.202.27.0&vendor_action=logout&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:11.314 PM	2017-09-21 14:32:11.314901 firstname=Pbke&lastname=Wxezegzj&email=jxixobrkv9f@cfwfzul.sg&cc=8795602724352902&src_ip=230.47.32.0&vendor_action=purchase&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:11.279 PM	2017-09-21 14:32:11.279188 firstname=Qleq&lastname=Ysnu&src_ip=24.250.29.0&vendor_action=login&action=success host = ol03.example.com source = /export/splunk/log/foo.log sourcetype = foo
>	9/21/17 2:32:11.146 PM	2017-09-21 14:32:11.146056 firstname=Hwuewrbw&lastname=Hwjgo&src_ip=21.93.206.0&vendor_action=login&action=failure

Workflow Action

Decode field values from the UI



```
1  index=unclassified
```

✓ 4,073 events (9/21/17 1:32:00.000 PM to 9/21/17 2:32:25.000 PM)

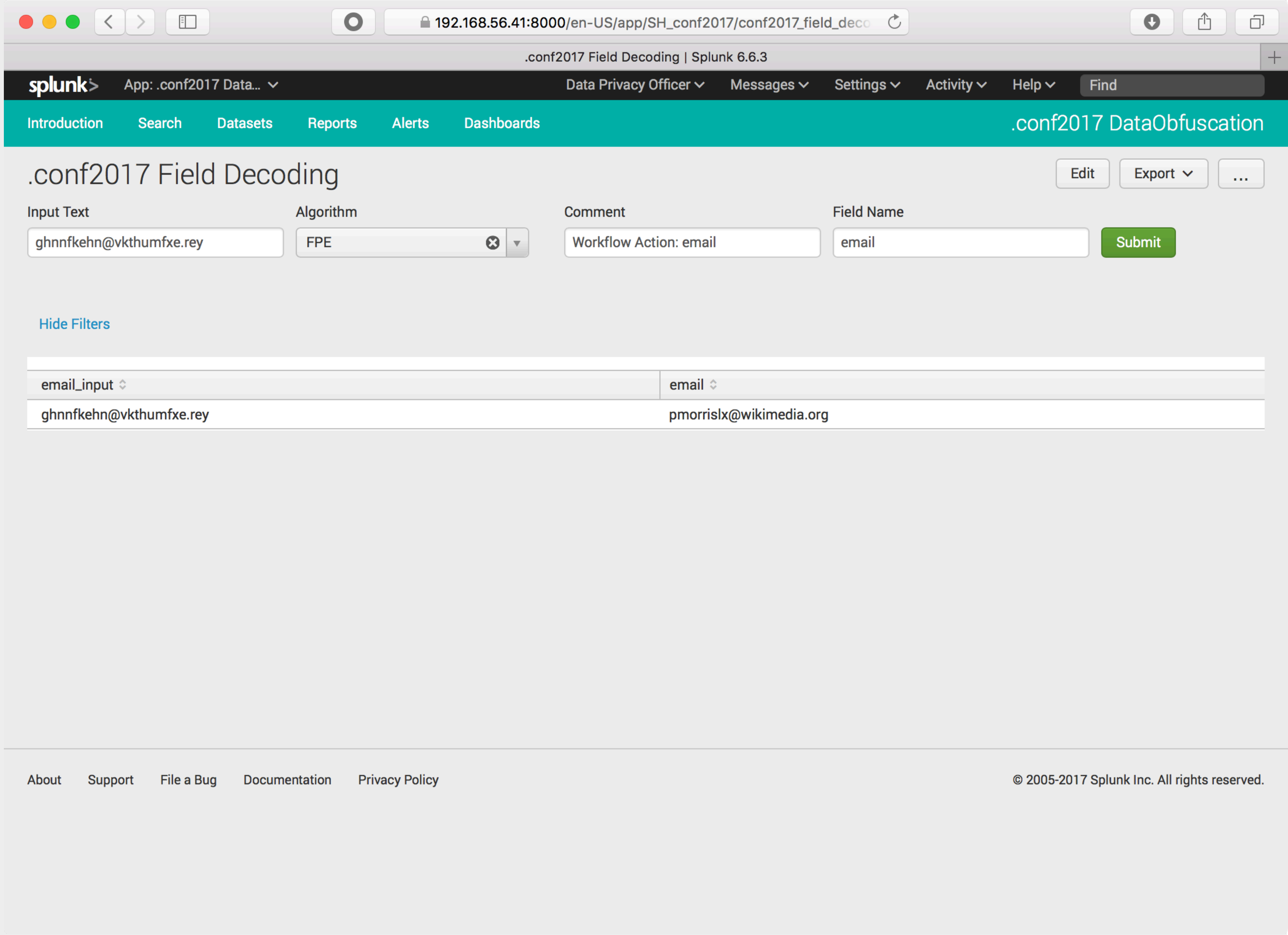
Selected Fields
- a host 1
- a source 2
- a sourcetype 2

Interesting Fields
- a action 2
- # cc 100+
- a component 1
- # date_hour 2
- # date_mday 1
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- a date_zone 1
- a email 100+
- a eventtype 4
- a firstname 100+
- a index 1

i	Time	Event
	9/21/17 2:32:19.139 PM	2017-09-21 14:32:19.139147 firstname=Zqcywq&lastname=Qjetme&email=ghnnfkehn@vkthumfxe.rey&cc=3251338238403482&src_ip=24.170.88.0&vendor_action=cancel&action=success

Type	✓	Field	Value	Actions
Selected	☑	host	ol03.example.com	
	☑	source	/export/splunk/log/foo.log	
	☑	sourcetype	foo	
Event	☐	action	success	
	☐	cc	3251338238403482	
	☐	email	ghnnfkehn@vkthumfxe.rey	
	☐	eventtype	unclassified_f	
	☐	firstname	Zqcywq	
	☐	lastname	Qjetme	
	☐	src	24.170.88.0	
	☐	src_ip	24.170.88.0	
	☐	user	Zqcywq Qjetme	
	☐	vendor_action	cancel	
Time		_time	2017-09-21T14:32:19.139+02:00	
Default	☐	index	unclassified	
	☐	linecount	1	

Decoding Dashboard



.conf2017 Field Decoding

Input Text: ghnnfkehn@vkthumfxe.rey

Algorithm: FPE

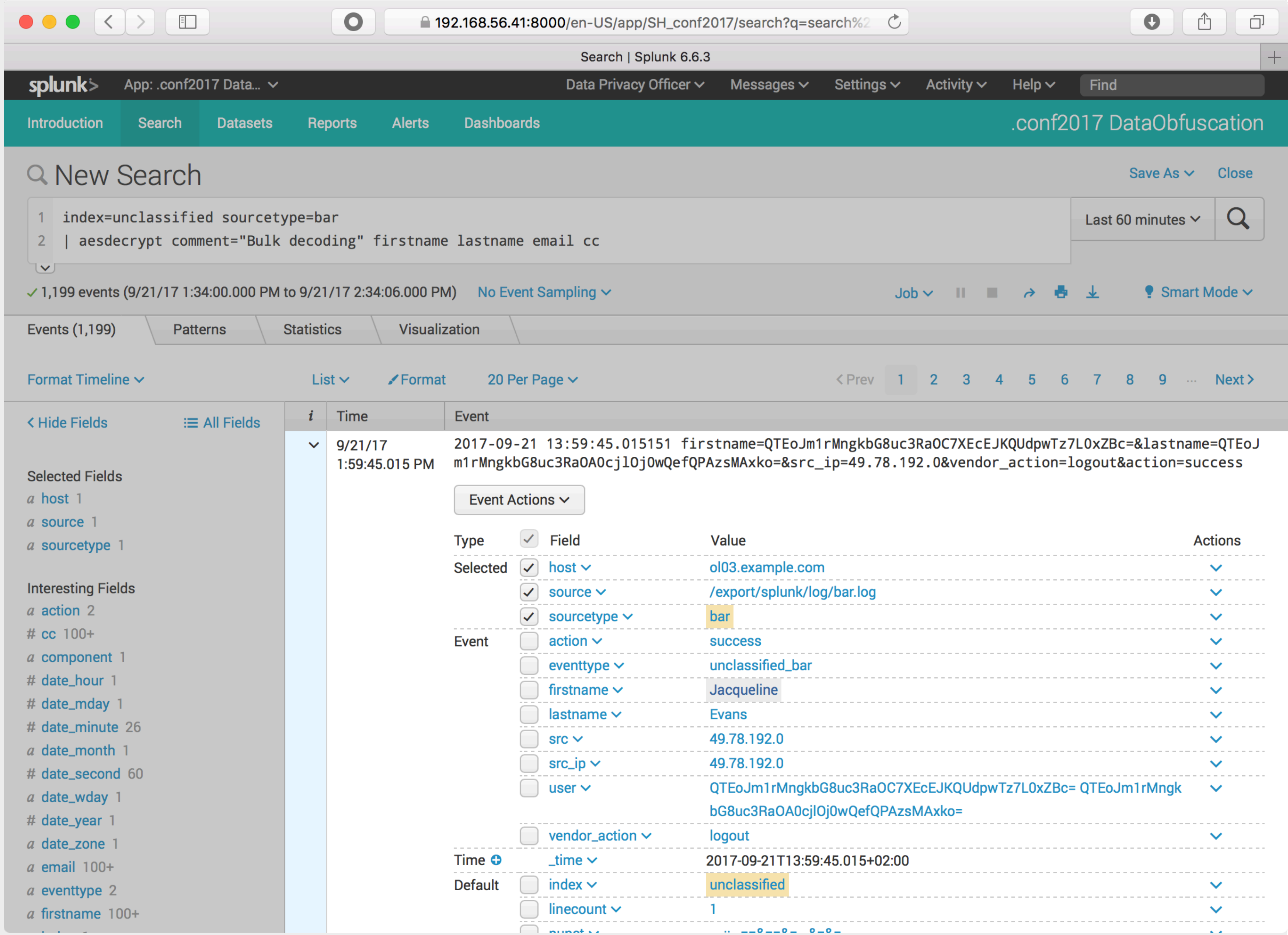
Comment: Workflow Action: email

Field Name: email

email_input	email
ghnnfkehn@vkthumfxe.rey	pmorrislx@wikimedia.org

Custom Search Command

Encoding and decoding



```
index=unclassified sourcetype=bar
| aesdecrypt comment="Bulk decoding" firstname lastname email cc
```

✓ 1,199 events (9/21/17 1:34:00.000 PM to 9/21/17 2:34:06.000 PM)

Selected Fields

- a host 1
- a source 1
- a sourcetype 1

Interesting Fields

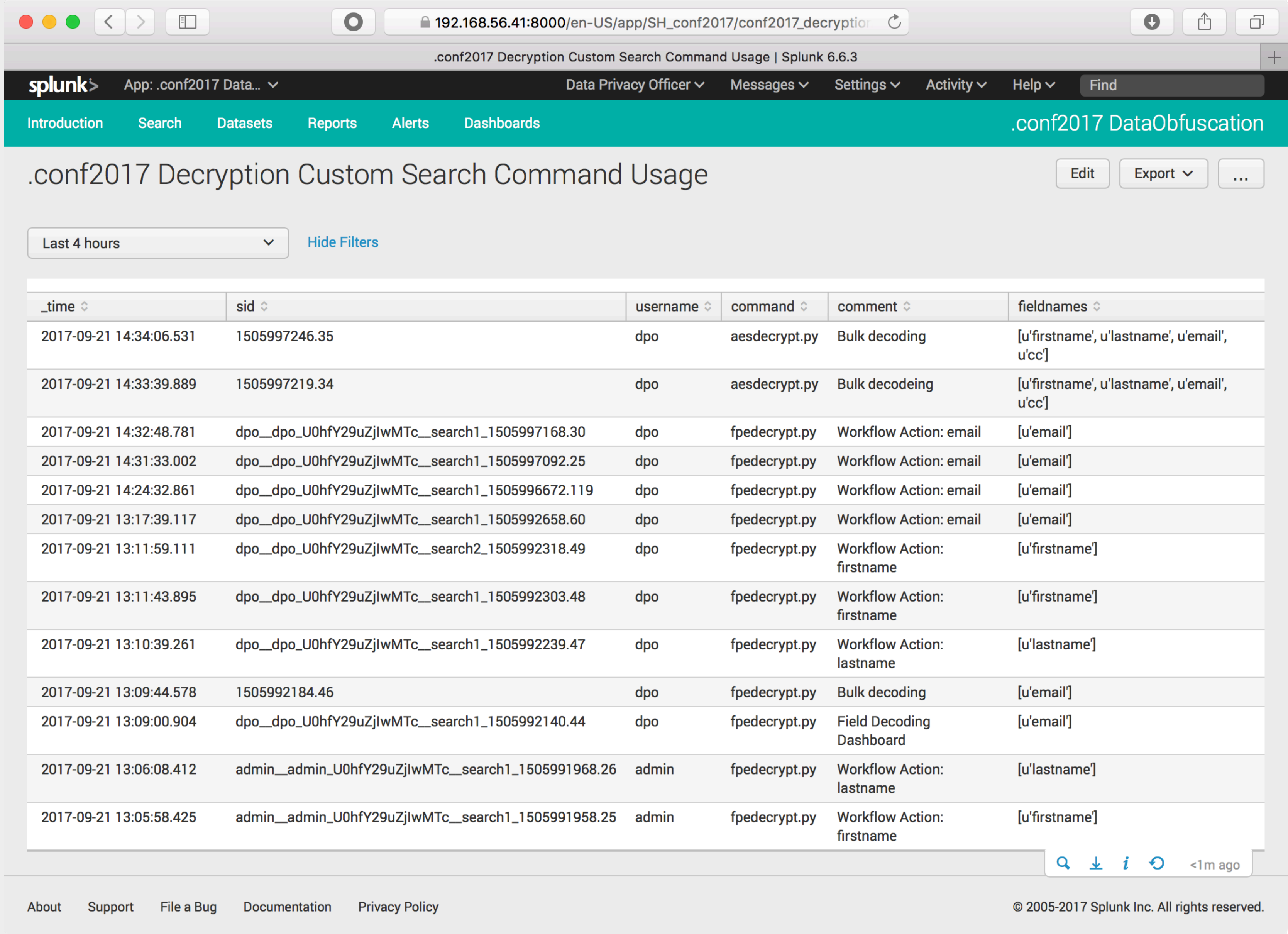
- a action 2
- # cc 100+
- a component 1
- # date_hour 1
- # date_mday 1
- # date_minute 26
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- a date_zone 1
- a email 100+
- a eventtype 2
- a firstname 100+

i	Time	Event
	9/21/17 1:59:45.015 PM	2017-09-21 13:59:45.015151 firstname=QTEoJm1rMngkbG8uc3RaOC7XEcEJKQUdpwTz7L0xZBc=&lastname=QTEoJm1rMngkbG8uc3RaOA0cjlOj0wQefQPAzsMAxko=&src_ip=49.78.192.0&vendor_action=logout&action=success

Type	✓	Field	Value	Actions
Selected	☑	host	ol03.example.com	
	☑	source	/export/splunk/log/bar.log	
	☑	sourcetype	bar	
Event	□	action	success	
	□	eventtype	unclassified_bar	
	□	firstname	Jacqueline	
	□	lastname	Evans	
	□	src	49.78.192.0	
	□	src_ip	49.78.192.0	
	□	user	QTEoJm1rMngkbG8uc3RaOC7XEcEJKQUdpwTz7L0xZBc= QTEoJm1rMngkbG8uc3RaOA0cjlOj0wQefQPAzsMAxko=	
	□	vendor_action	logout	
Time		_time	2017-09-21T13:59:45.015+02:00	
Default	□	index	unclassified	
	□	linecount	1	

Decryption Command Usage

Track usage of critical commands

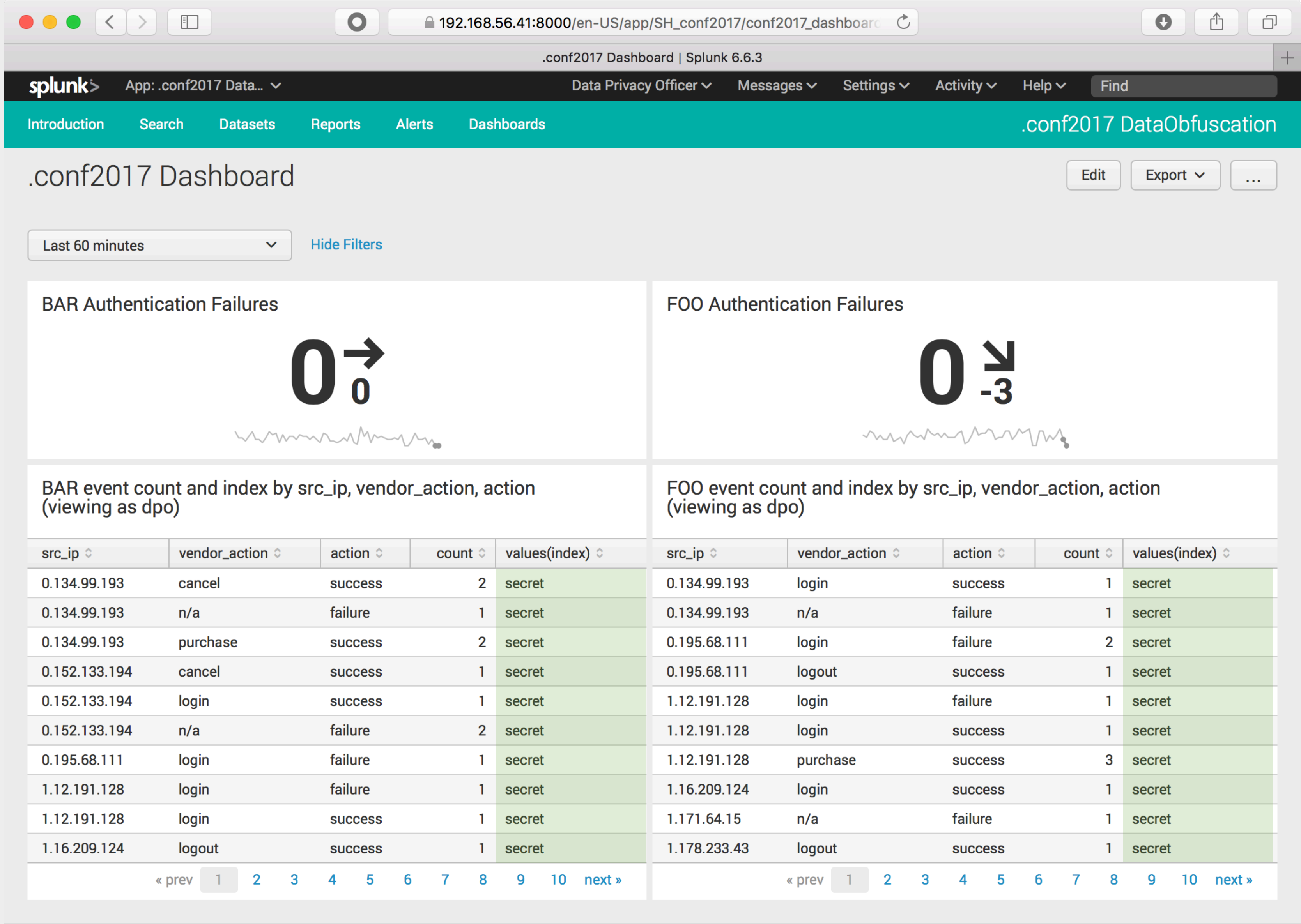


.conf2017 Decryption Custom Search Command Usage

_time	sid	username	command	comment	fieldnames
2017-09-21 14:34:06.531	1505997246.35	dpo	aesdecrypt.py	Bulk decoding	[u'firstname', u'lastname', u'email', u'cc']
2017-09-21 14:33:39.889	1505997219.34	dpo	aesdecrypt.py	Bulk decodeing	[u'firstname', u'lastname', u'email', u'cc']
2017-09-21 14:32:48.781	dpo__dpo_U0hfY29uZjIwMTc__search1_1505997168.30	dpo	fpedecrypt.py	Workflow Action: email	[u'email']
2017-09-21 14:31:33.002	dpo__dpo_U0hfY29uZjIwMTc__search1_1505997092.25	dpo	fpedecrypt.py	Workflow Action: email	[u'email']
2017-09-21 14:24:32.861	dpo__dpo_U0hfY29uZjIwMTc__search1_1505996672.119	dpo	fpedecrypt.py	Workflow Action: email	[u'email']
2017-09-21 13:17:39.117	dpo__dpo_U0hfY29uZjIwMTc__search1_1505992658.60	dpo	fpedecrypt.py	Workflow Action: email	[u'email']
2017-09-21 13:11:59.111	dpo__dpo_U0hfY29uZjIwMTc__search2_1505992318.49	dpo	fpedecrypt.py	Workflow Action: firstname	[u'firstname']
2017-09-21 13:11:43.895	dpo__dpo_U0hfY29uZjIwMTc__search1_1505992303.48	dpo	fpedecrypt.py	Workflow Action: firstname	[u'firstname']
2017-09-21 13:10:39.261	dpo__dpo_U0hfY29uZjIwMTc__search1_1505992239.47	dpo	fpedecrypt.py	Workflow Action: lastname	[u'lastname']
2017-09-21 13:09:44.578	1505992184.46	dpo	fpedecrypt.py	Bulk decoding	[u'email']
2017-09-21 13:09:00.904	dpo__dpo_U0hfY29uZjIwMTc__search1_1505992140.44	dpo	fpedecrypt.py	Field Decoding Dashboard	[u'email']
2017-09-21 13:06:08.412	admin__admin_U0hfY29uZjIwMTc__search1_1505991968.26	admin	fpedecrypt.py	Workflow Action: lastname	[u'lastname']
2017-09-21 13:05:58.425	admin__admin_U0hfY29uZjIwMTc__search1_1505991958.25	admin	fpedecrypt.py	Workflow Action: firstname	[u'firstname']

Common Dashboard

Privileged view



.conf2017 Dashboard

BAR Authentication Failures

0 → 0

FOO Authentication Failures

0 ↘ -3

BAR event count and index by src_ip, vendor_action, action (viewing as dpo)

src_ip	vendor_action	action	count	values(index)
0.134.99.193	cancel	success	2	secret
0.134.99.193	n/a	failure	1	secret
0.134.99.193	purchase	success	2	secret
0.152.133.194	cancel	success	1	secret
0.152.133.194	login	success	1	secret
0.152.133.194	n/a	failure	2	secret
0.195.68.111	login	failure	1	secret
1.12.191.128	login	failure	1	secret
1.12.191.128	login	success	1	secret
1.16.209.124	logout	success	1	secret

« prev 1 2 3 4 5 6 7 8 9 10 next »

FOO event count and index by src_ip, vendor_action, action (viewing as dpo)

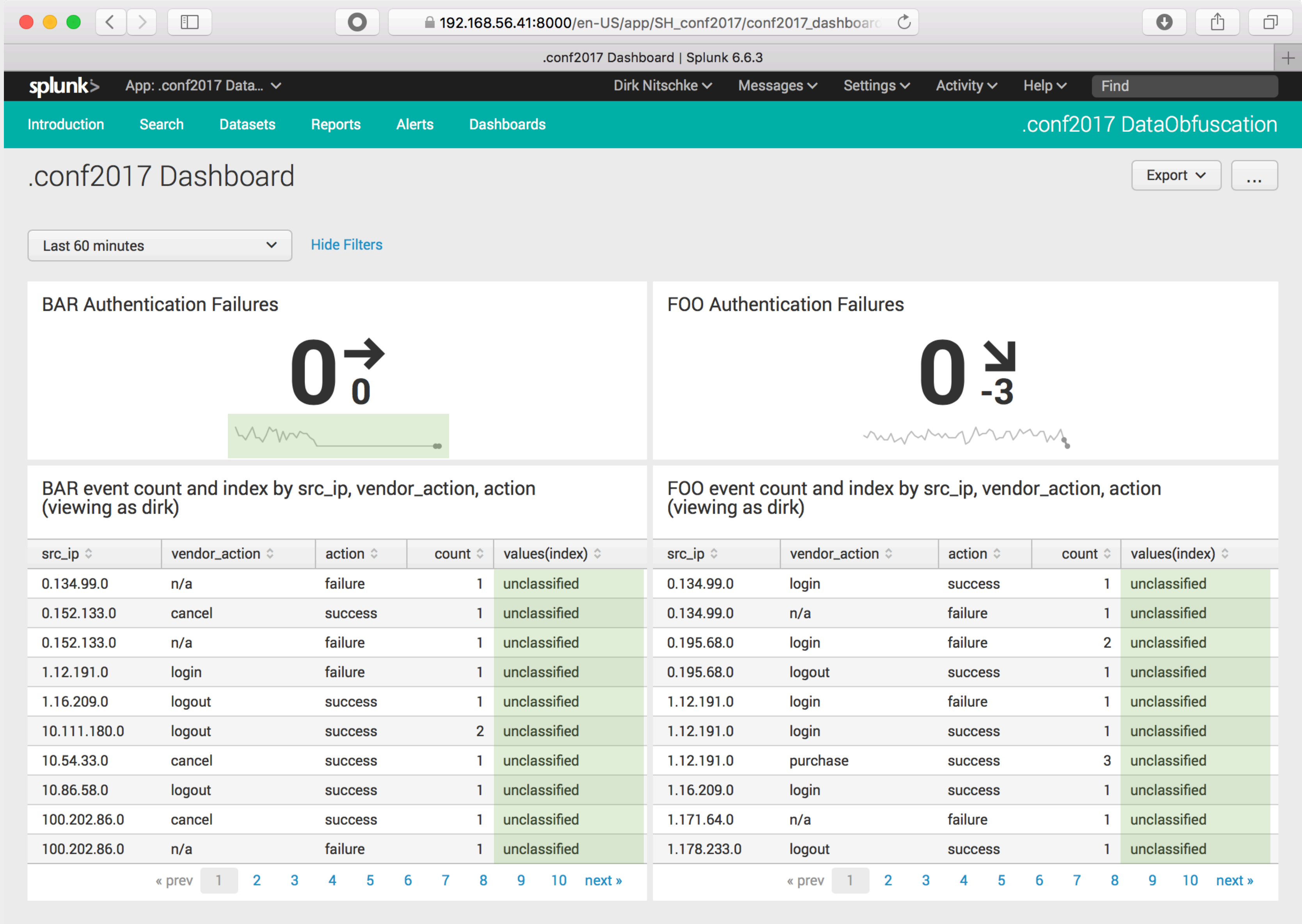
src_ip	vendor_action	action	count	values(index)
0.134.99.193	login	success	1	secret
0.134.99.193	n/a	failure	1	secret
0.195.68.111	login	failure	2	secret
0.195.68.111	logout	success	1	secret
1.12.191.128	login	failure	1	secret
1.12.191.128	login	success	1	secret
1.12.191.128	purchase	success	3	secret
1.16.209.124	login	success	1	secret
1.171.64.15	n/a	failure	1	secret
1.178.233.43	logout	success	1	secret

« prev 1 2 3 4 5 6 7 8 9 10 next »

splunk> .conf2017

Common Dashboard

Normal view



.conf2017 Dashboard

BAR Authentication Failures

0 → 0

FOO Authentication Failures

0 ↘ -3

BAR event count and index by src_ip, vendor_action, action (viewing as dirk)

src_ip	vendor_action	action	count	values(index)
0.134.99.0	n/a	failure	1	unclassified
0.152.133.0	cancel	success	1	unclassified
0.152.133.0	n/a	failure	1	unclassified
1.12.191.0	login	failure	1	unclassified
1.16.209.0	logout	success	1	unclassified
10.111.180.0	logout	success	2	unclassified
10.54.33.0	cancel	success	1	unclassified
10.86.58.0	logout	success	1	unclassified
100.202.86.0	cancel	success	1	unclassified
100.202.86.0	n/a	failure	1	unclassified

« prev 1 2 3 4 5 6 7 8 9 10 next »

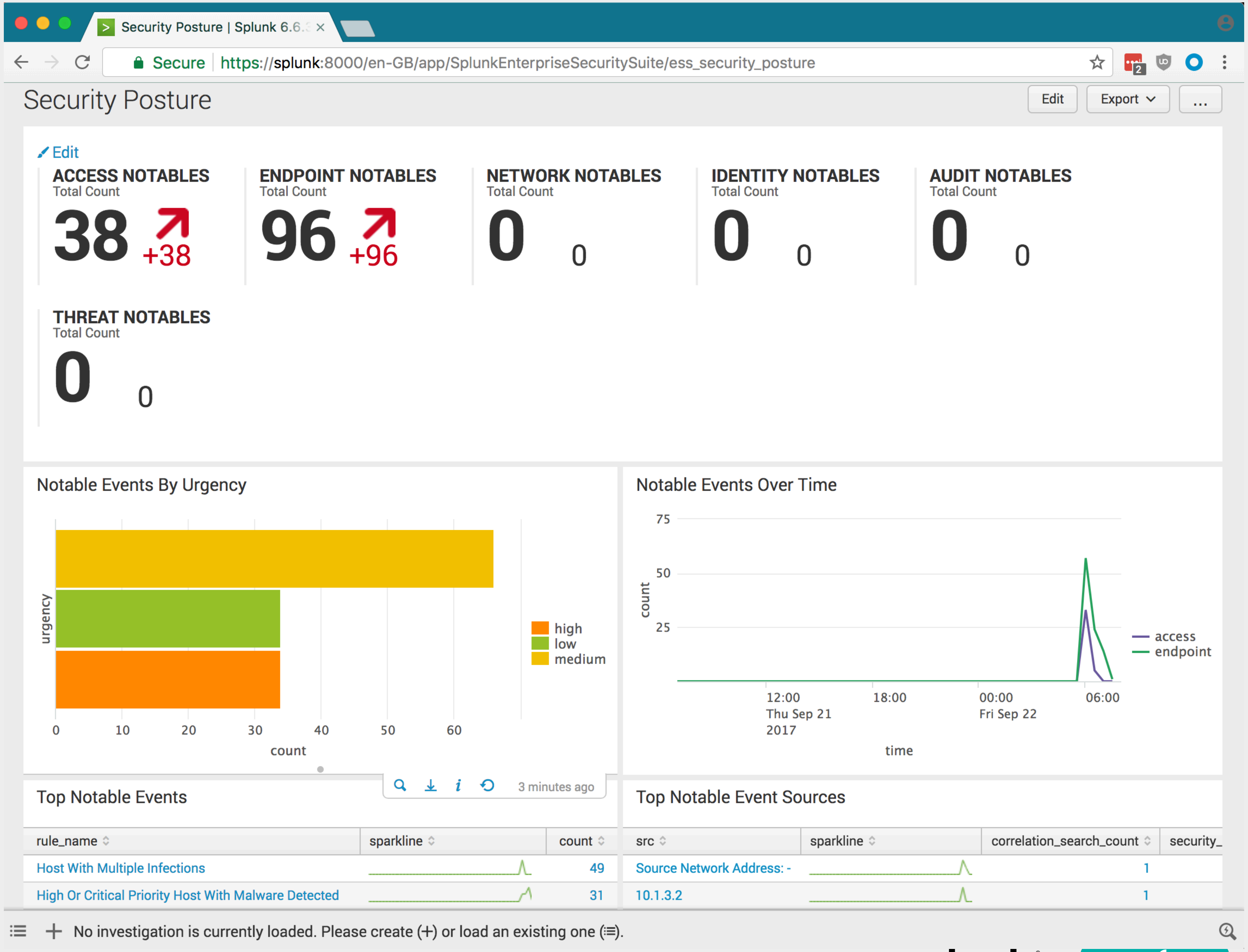
FOO event count and index by src_ip, vendor_action, action (viewing as dirk)

src_ip	vendor_action	action	count	values(index)
0.134.99.0	login	success	1	unclassified
0.134.99.0	n/a	failure	1	unclassified
0.195.68.0	login	failure	2	unclassified
0.195.68.0	logout	success	1	unclassified
1.12.191.0	login	failure	1	unclassified
1.12.191.0	login	success	1	unclassified
1.12.191.0	purchase	success	3	unclassified
1.16.209.0	login	success	1	unclassified
1.171.64.0	n/a	failure	1	unclassified
1.178.233.0	logout	success	1	unclassified

« prev 1 2 3 4 5 6 7 8 9 10 next »

Enterprise Security

Normal view



Security Posture | Splunk 6.6.
Secure
https://splunk:8000/en-GB/app/SplunkEnterpriseSecuritySuite/ess_security_posture
Edit
Export
...

Security Posture

Edit

ACCESS NOTABLES Total Count 38 +38

ENDPOINT NOTABLES Total Count 96 +96

NETWORK NOTABLES Total Count 0 0

IDENTITY NOTABLES Total Count 0 0

AUDIT NOTABLES Total Count 0 0

THREAT NOTABLES Total Count 0 0

Notable Events By Urgency

Notable Events Over Time

Top Notable Events

rule_name	sparkline	count
Host With Multiple Infections		49
High Or Critical Priority Host With Malware Detected		31

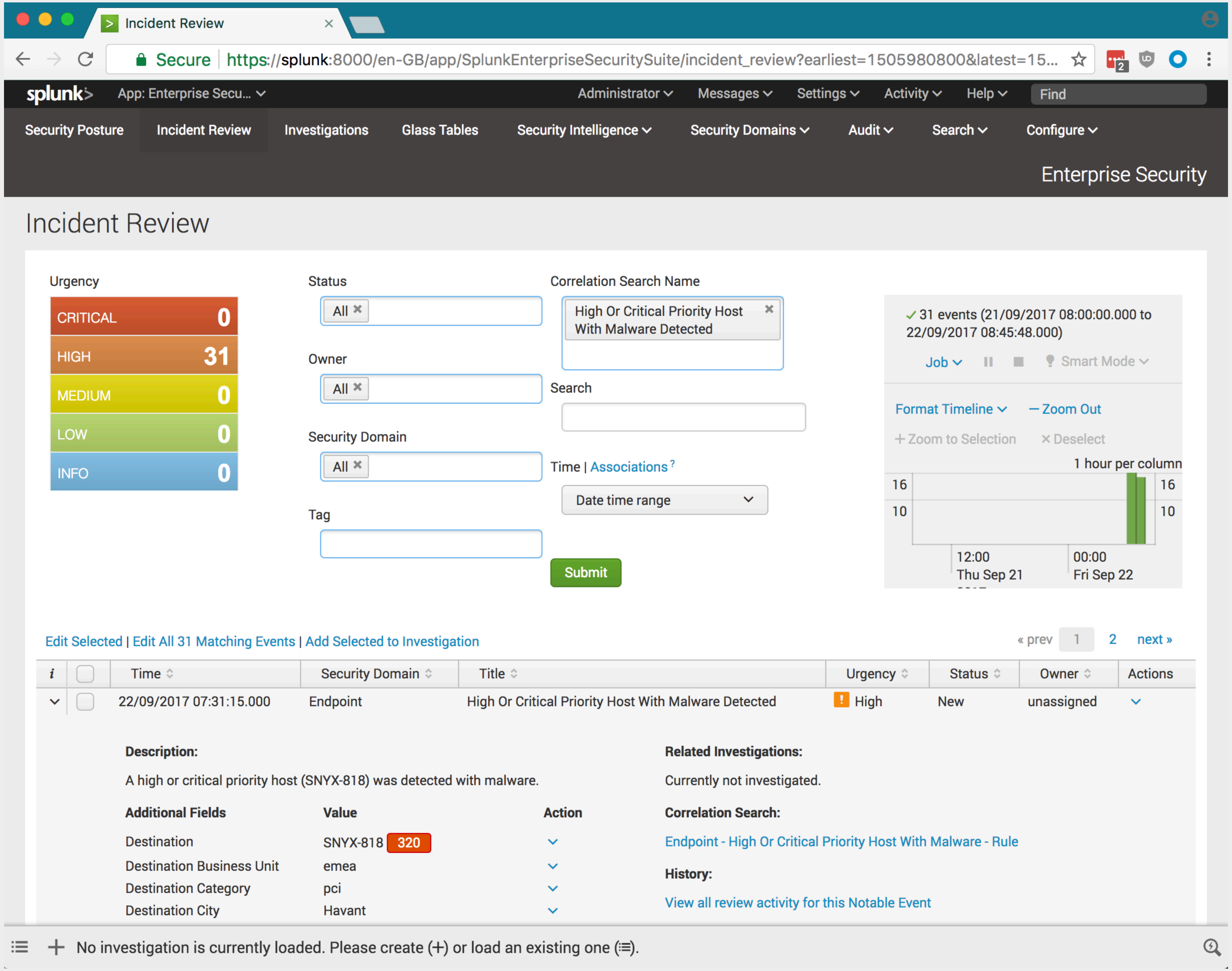
Top Notable Event Sources

src	sparkline	correlation_search_count	security_
Source Network Address: -		1	
10.1.3.2		1	

No investigation is currently loaded. Please create (+) or load an existing one (☰).

Enterprise Security

Normal view



Incident Review

Urgency

CRITICAL	0
HIGH	31
MEDIUM	0
LOW	0
INFO	0

Status: All ×

Owner: All ×

Security Domain: All ×

Tag:

Correlation Search Name: High Or Critical Priority Host With Malware Detected ×

Search:

Time | Associations ?

Date time range

Submit

✓ 31 events (21/09/2017 08:00:00.000 to 22/09/2017 08:45:48.000)

Edit Selected | Edit All 31 Matching Events | Add Selected to Investigation

« prev 1 2 next »

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
⌄	□	22/09/2017 07:31:15.000	Endpoint	High Or Critical Priority Host With Malware Detected	! High	New	unassigned	⌄

Description:

A high or critical priority host (SNYX-818) was detected with malware.

Additional Fields	**Value**	**Action**
Destination	SNYX-818 320	⌄
Destination Business Unit	emea	⌄
Destination Category	pci	⌄
Destination City	Havant	⌄

Related Investigations:

Currently not investigated.

Correlation Search:

Endpoint - High Or Critical Priority Host With Malware - Rule

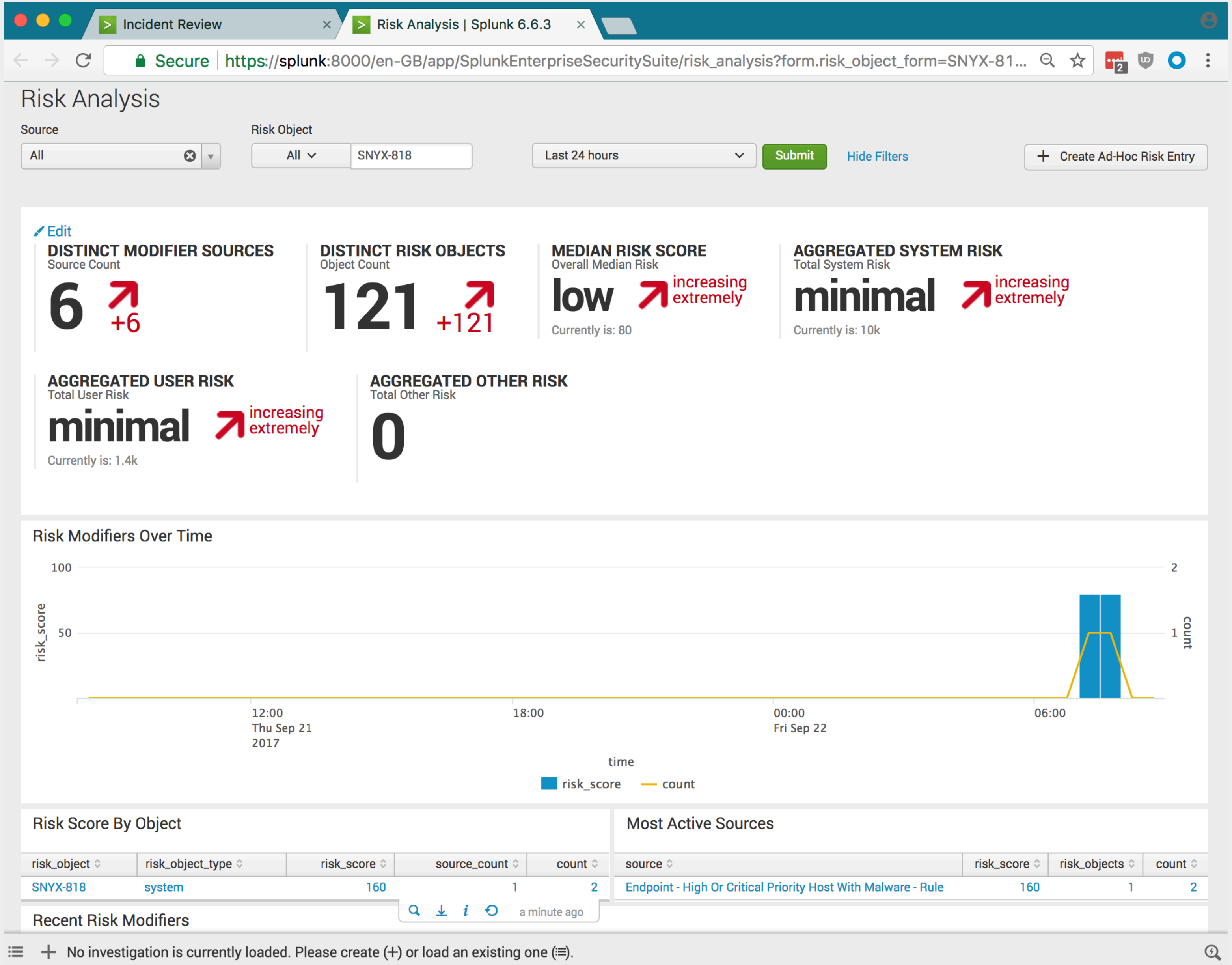
History:

View all review activity for this Notable Event

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Enterprise Security

Normal view



https://splunk:8000/en-GB/app/SplunkEnterpriseSecuritySuite/risk_analysis?form.risk_object_form=SNYX-81...

Risk Analysis

Source: All

Risk Object: All SNYX-818

Last 24 hours

DISTINCT MODIFIER SOURCES
Source Count
6 +6

DISTINCT RISK OBJECTS
Object Count
121 +121

MEDIAN RISK SCORE
Overall Median Risk
low increasing extremely
Currently is: 80

AGGREGATED SYSTEM RISK
Total System Risk
minimal increasing extremely
Currently is: 10k

AGGREGATED USER RISK
Total User Risk
minimal increasing extremely
Currently is: 1.4k

AGGREGATED OTHER RISK
Total Other Risk
0

Risk Modifiers Over Time

Risk Score By Object

risk_object	risk_object_type	risk_score	source_count	count
SNYX-818	system	160	1	2

Most Active Sources

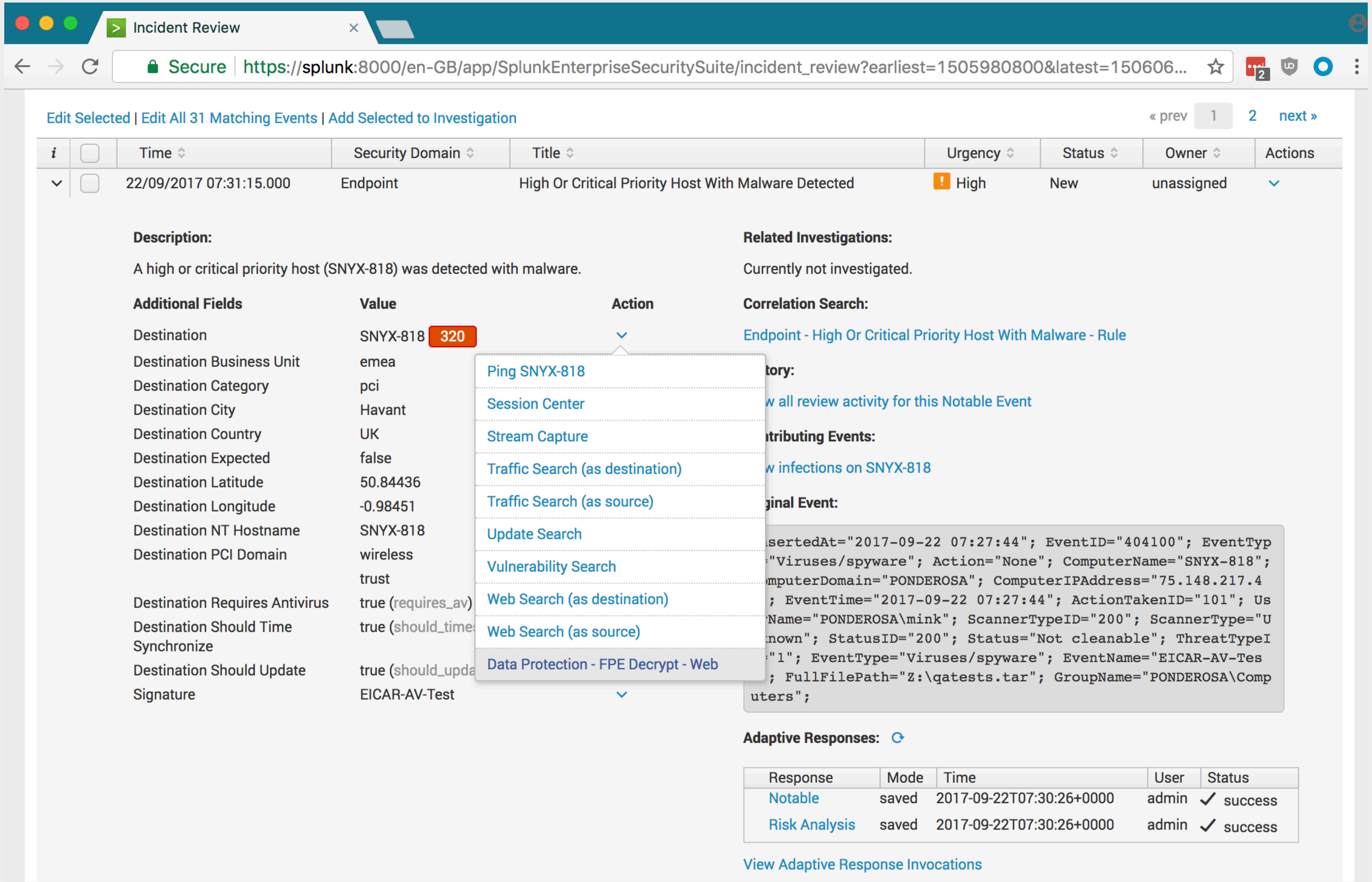
source	risk_score	risk_objects	count
Endpoint - High Or Critical Priority Host With Malware - Rule	160	1	2

Recent Risk Modifiers

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Enterprise Security

Normal view



Incident Review
Secure
https://splunk:8000/en-GB/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=1505980800&latest=150606...

Edit Selected | Edit All 31 Matching Events | Add Selected to Investigation

« prev 1 2 next »

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
⌄	□	22/09/2017 07:31:15.000	Endpoint	High Or Critical Priority Host With Malware Detected	! High	New	unassigned	⌄

Description:

A high or critical priority host (SNYX-818) was detected with malware.

Additional Fields	Value	Action
Destination	SNYX-818 320	⌄
Destination Business Unit	emea	
Destination Category	pci	
Destination City	Havant	
Destination Country	UK	
Destination Expected	false	
Destination Latitude	50.84436	
Destination Longitude	-0.98451	
Destination NT Hostname	SNYX-818	
Destination PCI Domain	wireless trust	
Destination Requires Antivirus	true (requires_av)	
Destination Should Time Synchronize	true (should_time	
Destination Should Update	true (should_upda	
Signature	EICAR-AV-Test	⌄

Ping SNYX-818
Session Center
Stream Capture
Traffic Search (as destination)
Traffic Search (as source)
Update Search
Vulnerability Search
Web Search (as destination)
Web Search (as source)
Data Protection - FPE Decrypt - Web

Related Investigations:

Currently not investigated.

Correlation Search:

Endpoint - High Or Critical Priority Host With Malware - Rule

tory:

w all review activity for this Notable Event

tributing Events:

w infections on SNYX-818

ginal Event:

```
sertedAt="2017-09-22 07:27:44"; EventID="404100"; EventTyp
"Viruses/spyware"; Action="None"; ComputerName="SNYX-818";
mputerDomain="PONDEROSA"; ComputerIPAddress="75.148.217.4
; EventTime="2017-09-22 07:27:44"; ActionTakenID="101"; Us
Name="PONDEROSA\mink"; ScannerTypeID="200"; ScannerType="U
nown"; StatusID="200"; Status="Not cleanable"; ThreatTypeI
"1"; EventType="Viruses/spyware"; EventName="EICAR-AV-Tes
; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Comp
uters";
```

Adaptive Responses:

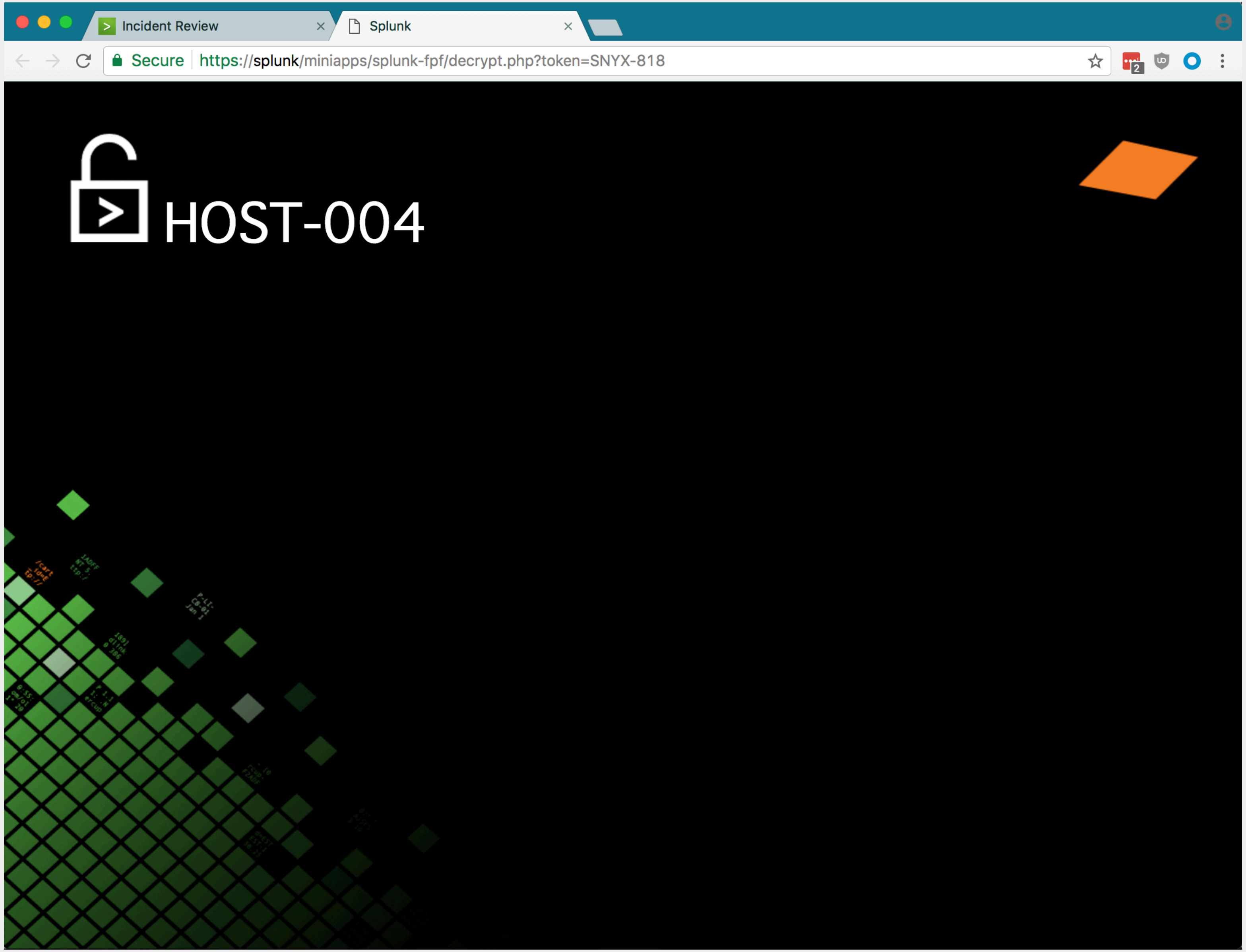
Response	Mode	Time	User	Status
Notable	saved	2017-09-22T07:30:26+0000	admin	✓ success
Risk Analysis	saved	2017-09-22T07:30:26+0000	admin	✓ success

View Adaptive Response Invocations

splunk> .conf2017

Enterprise Security

Normal view



Incident Review

Splunk

Secure https://splunk/miniapps/splunk-fpf/decrypt.php?token=SNYX-818

Q&A

Angelo Brancato | Security Specialist

Dirk Nitschke | Senior Sales Engineer

Thank You

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

splunk> .conf2017