.conf2015

How To Use Common Information Model to Gain Security Awareness & Prepare For Enterprise Security

Niklas Blomquist

Senior Sales Engineer SME Security, Splunk

splunk>

Disclaimer

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 the 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.

Personal Introduction

- Niklas Blomquist
- Splunk – Does it need any presentation?
- Senior Sales Engineer/SME Security
  - Lead larger security project
  - How to use Splunk for security
  - 18 Years in security
  - Love my work, cooking (BBQ) and my family

- Fun fact
  - There are no polar bears on the streets in Sweden!!!

Agenda

- What are Common Information Model
- How do I “enable” CIM?
- Technology Add-on
- Dashboards and searches with CIM
- Enterprise Security + CIM

.conf2015

What are the Common Information Model?

splunk>

What are the CIM?

- CIM standardize (normalize) data
- Unified view of data
- Search time schema
- Set of field names and tags
- Does not change raw data

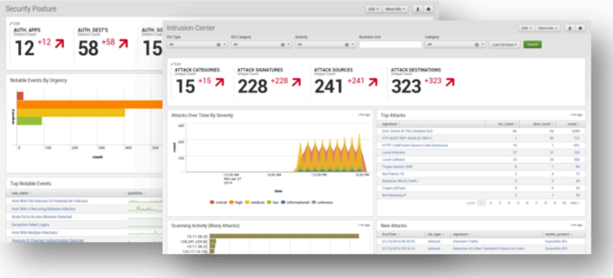
PUBLIC SERVICE ANNOUNCEMENT:
OUR DIFFERENT WAYS OF WRITING DATES AS NUMBERS CAN LEAD TO ONLINE CONFUSION. THAT'S WHY IN 1988 ISO SET A GLOBAL STANDARD NUMERIC DATE FORMAT.
THIS IS THE CORRECT WAY TO WRITE NUMERIC DATES:
2013-02-27
THE FOLLOWING FORMATS ARE THEREFORE DISCOURAGED:
02/27/2013 02/27/13 27/02/2013 27/02/13
20130227 2013.02.27 27.02.13 27-02-13
27.2.13 2013. II. 27. 27⁄2-13 2013.158904109
MMXIII-II-XXVII MMXIII LVII/CCCLXV 1330300800
((3+3)×(111+1)-1)×3/3-1/3³ 2013
10/11011/1101 02/27/20/13 01237
HISSSSS
2-27-13

https://xkcd.com/1179/

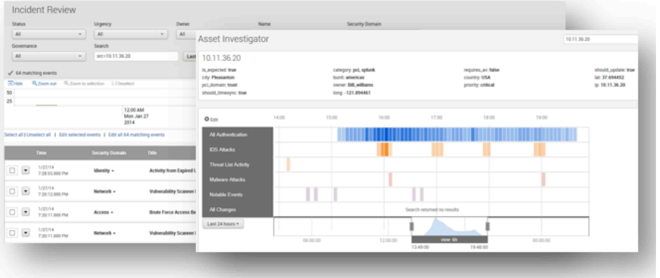
Wow – That's Great! Why do we Need CIM?

To build searches/apps without data knowledge

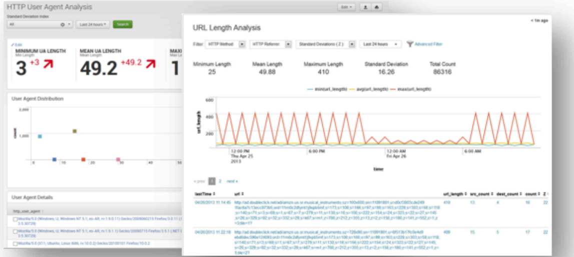
Pre-built searches, alerts, reports, dashboards, workflow



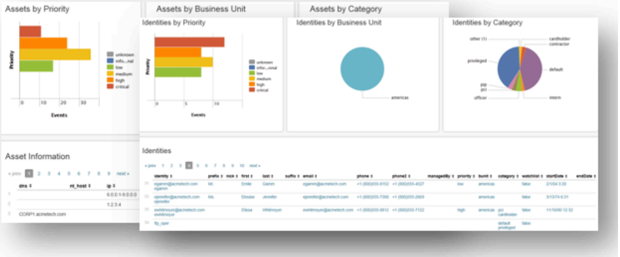
Dashboards and Reports



Incident Investigations & Management



Statistical Outliers



Asset and Identity Aware

Wow – That's Great! Why do we Need CIM?

- Vendor A vs vendor B

Allowed traffic

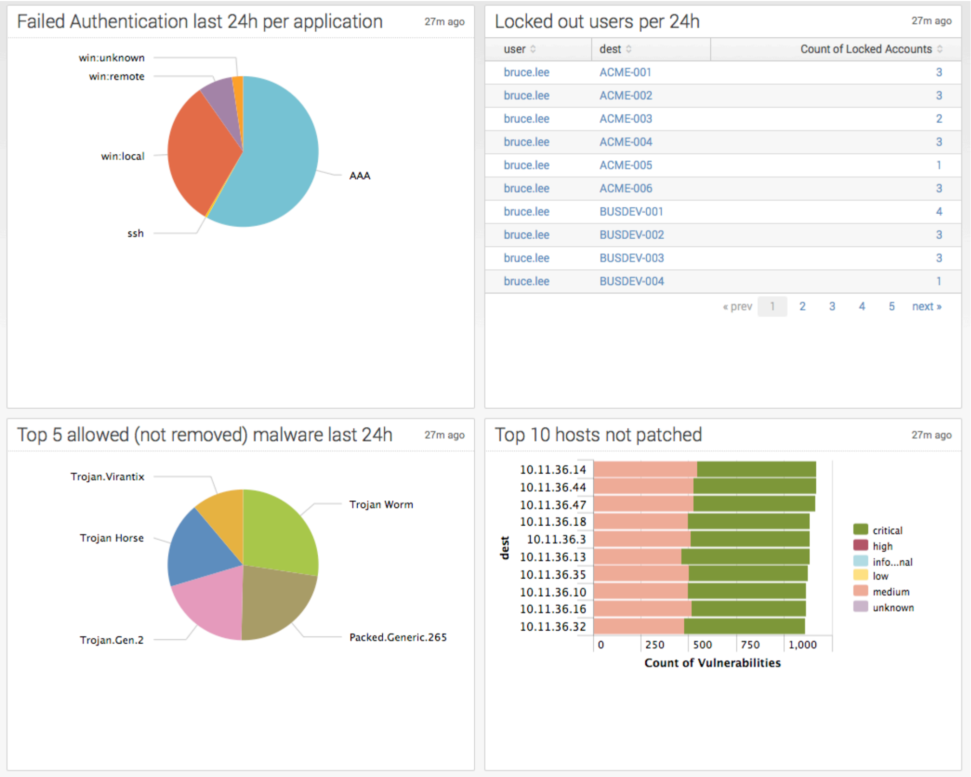
  -
    ```
    Aug  7 15:44:44 10.1.1.99 Aug 07 2007 15:44:44 10.1.1.99 : %ASA-6-302013:
    Built inbound TCP connection 3120386 for outside:192.168.150.85/2309
    (192.168.150.85/2309) to inside:192.168.1.150/80 (192.168.1.150/80)
    ```

  -
    ```
    Feb  4 16:00:01 1,2014/02/04 16:00:01,0009C101998,TR
    1,2014/02/04
    16:00:01,10.75.1.77,167.216.129.11,204.107.141.240,167.2  129.11,RFC19
    18 to
    Internet,,,ssl,vsys1,Trust,Untrust,ae1.902,ae1.1000,Logging oPanorama,
    2014/02/04 16:00:01,1636682,1,52089,443,47241,443,0x4 00000,tcp,allow,
    4442,2350,2092,23,2014/02/04 15:59:19,40,business-and-economy,
    0,4974797752,0x0,10.0.0.0-10.255.255.255,United States,0,13,10
    ```

Allowed traffic

Other Benefits with CIM

- Includes 22 pre-configured data models
- Easier creation of searches/dashboards
- Dashboards/reports from pivot



Failed Authentication last 24h per application 27m ago

Locked out users per 24h 27m ago

user ⇕	dest ⇕	Count of Locked Accounts ⇕
bruce.lee	ACME-001	3
bruce.lee	ACME-002	3
bruce.lee	ACME-003	2
bruce.lee	ACME-004	3
bruce.lee	ACME-005	1
bruce.lee	ACME-006	3
bruce.lee	BUSDEV-001	4
bruce.lee	BUSDEV-002	3
bruce.lee	BUSDEV-003	3
bruce.lee	BUSDEV-004	1

Top 5 allowed (not removed) malware last 24h 27m ago

Top 10 hosts not patched 27m ago

Authentication Datamodel

Field names

- action=success/failure/unknown
- src=src ip
- dest=dest ip
- app=application
- user=user name

Tags

- tag = authentication
- tag = privileged
- tag = default

Example of Failed Authentication

Windows

- LogName=Security EventCode=529 EventType=16 Type=Failure Audit SourceName=Security RecordNumber=725650913 Category=2 CategoryString=Logon/Logoff ComputerName=HOST-001 User=SYSTEM Sid=S-1-5-18 SidType=1 Message=Logon Failure: Reason: Unknown user name or bad password User Name: Hax0r Domain: ACMETECH Logon Type: 2 Logon Process: IAS Authentication Package:

Linux

- Aug 26 15:00:20 acmepayroll sshd[15038]: Failed password for invalid user vpopmail from 10.11.36.11 port 38368 ssh2

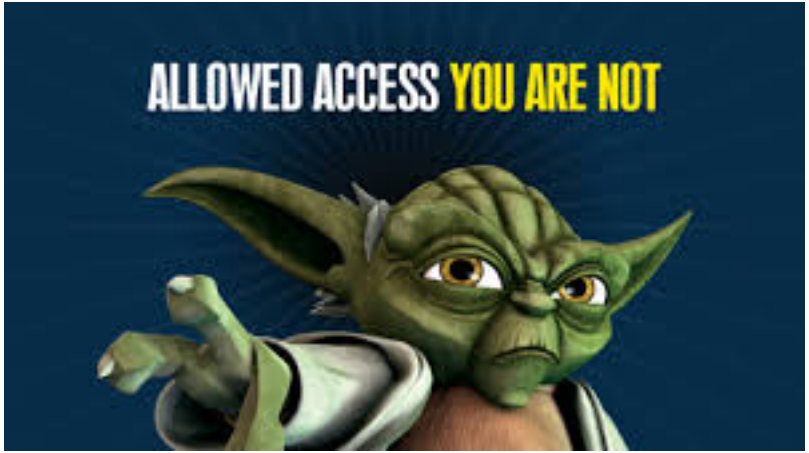
Example of Failed Authentication

Without CIM

- (Sourcetype=WinEventLog:Security (signature_id=4625 OR signature_id=529 OR signature_id=530 OR signature_id=531 OR signature_id=532 OR signature_id=533 OR signature_id=534 OR signature_id=535 OR signature_id=536 OR signature_id=537 OR signature_id=539) OR (sourcetype=linux_secure “Failed password for” OR “Invalid user”) | rename “User Name” AS user, “Source Network Address “ AS src

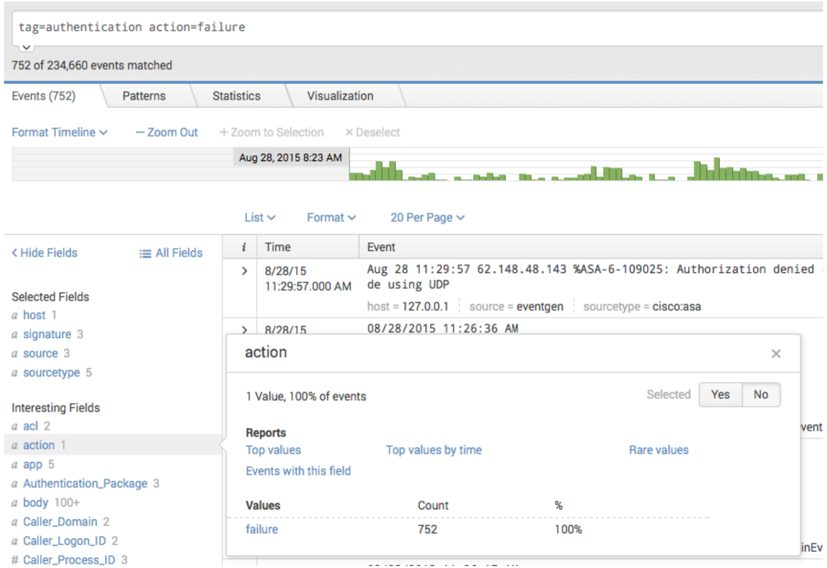
CIM

- tag=authentication action=failure



Searches

- All failed authentication events
  - tag=authentication action=failure
- All privileged authentication events
  - tag=authentication tag=privileged
- All failed authentications for application Oracle
  - tag=authentication action=failed app=oracle



```
tag=authentication action=failure
```

752 of 234,660 events matched

Selected Fields
- a host 1
- a signature 3
- a source 3
- a sourcetype 5

Interesting Fields
- a acl 2
- a action 1
- a app 5
- a Authentication_Package 3
- a body 100+
- a Caller_Domain 2
- a Caller_Logon_ID 2
- # Caller_Process_ID 3

i	Time	Event
>	8/28/15 11:29:57.000 AM	Aug 28 11:29:57 62.148.48.143 %ASA-6-109025: Authorization denied de using UDP host = 127.0.0.1 source = eventgen sourcetype = cisco:asa
>	8/28/15	08/28/2015 11:26:36 AM

action

1 Value, 100% of events

Selected Yes No

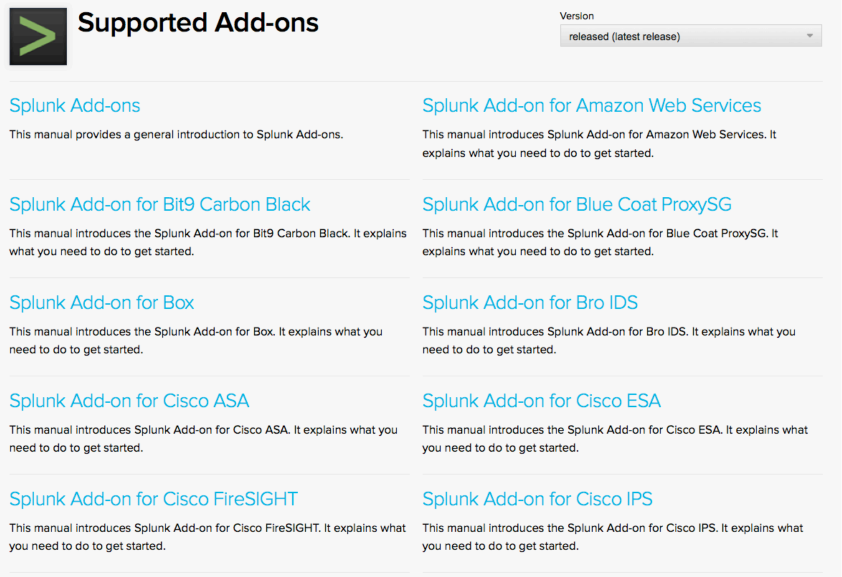
Reports

Values	Count	%
failure	752	100%

How do we do the Normalization?

How do we do the Normalization?

- Technology Add-on (TA's)
- Set of configuration files
  - Correct event breaking
  - Correct field extraction
  - Field rename (if needed)
    - src, dest, user etc
  - Apply context to the data
    - tags
    - fields – action=allow/blocked



Supported Add-ons

Splunk Add-ons
This manual provides a general introduction to Splunk Add-ons.

Splunk Add-on for Amazon Web Services
This manual introduces Splunk Add-on for Amazon Web Services. It explains what you need to do to get started.

Splunk Add-on for Bit9 Carbon Black
This manual introduces the Splunk Add-on for Bit9 Carbon Black. It explains what you need to do to get started.

Splunk Add-on for Blue Coat ProxySG
This manual introduces the Splunk Add-on for Blue Coat ProxySG. It explains what you need to do to get started.

Splunk Add-on for Box
This manual introduces the Splunk Add-on for Box. It explains what you need to do to get started.

Splunk Add-on for Bro IDS
This manual introduces Splunk Add-on for Bro IDS. It explains what you need to do to get started.

Splunk Add-on for Cisco ASA
This manual introduces Splunk Add-on for Cisco ASA. It explains what you need to do to get started.

Splunk Add-on for Cisco ESA
This manual introduces the Splunk Add-on for Cisco ESA. It explains what you need to do to get started.

Splunk Add-on for Cisco FireSIGHT
This manual introduces Splunk Add-on for Cisco FireSIGHT. It explains what you need to do to get started.

Splunk Add-on for Cisco IPS
This manual introduces the Splunk Add-on for Cisco IPS. It explains what you need to do to get started.

- Everything are applied at search time so it can be used with old data!

About TA’s

- Read the documentation!
- OPSEC LEA = OS Dependency
- Correct sourcetype
  - Correct sourcetype are important
  - Every TA are bound to sourcetype/s

- Old data with wrong sourcetype
  - Change sourcetype in TA
  - Export and import data

About TA’s

- Read the documentation!
- Special input requirements
  - Syslog
  - Monitor file
  - DB Connect

- Version dependency's

Blue Coat

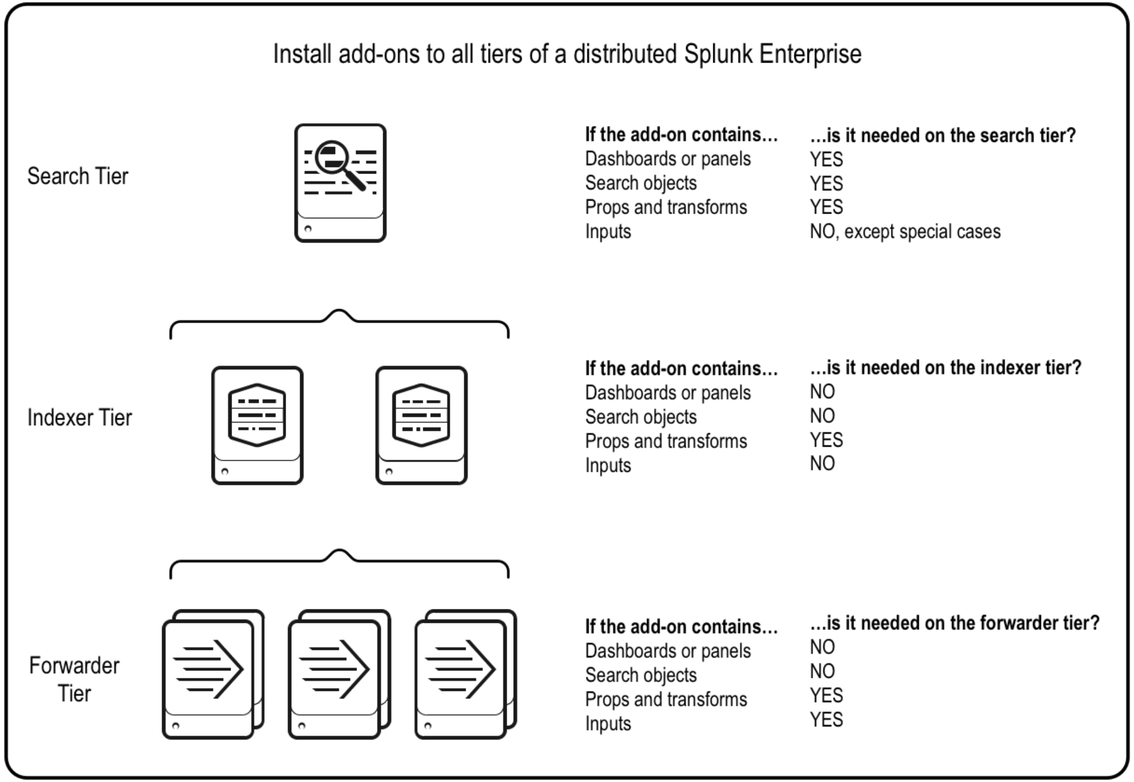
About Syslog

- Different type on same port will not work
- Unless they are written to support it
  - Cisco ASA – PIX – FWSM

- Different ports – different TA's/sourcetype

- Best Practice:
  - Syslog-NG/Rsyslog writes into a file
  - Splunk Universal Forwarder monitors file

Where to Apply the TA’s



Install add-ons to all tiers of a distributed Splunk Enterprise

Search Tier

If the add-on contains...	...is it needed on the search tier?
Dashboards or panels	YES
Search objects	YES
Props and transforms	YES
Inputs	NO, except special cases

Indexer Tier

If the add-on contains...	...is it needed on the indexer tier?
Dashboards or panels	NO
Search objects	NO
Props and transforms	YES
Inputs	NO

Forwarder Tier

If the add-on contains...	...is it needed on the forwarder tier?
Dashboards or panels	NO
Search objects	NO
Props and transforms	YES
Inputs	YES

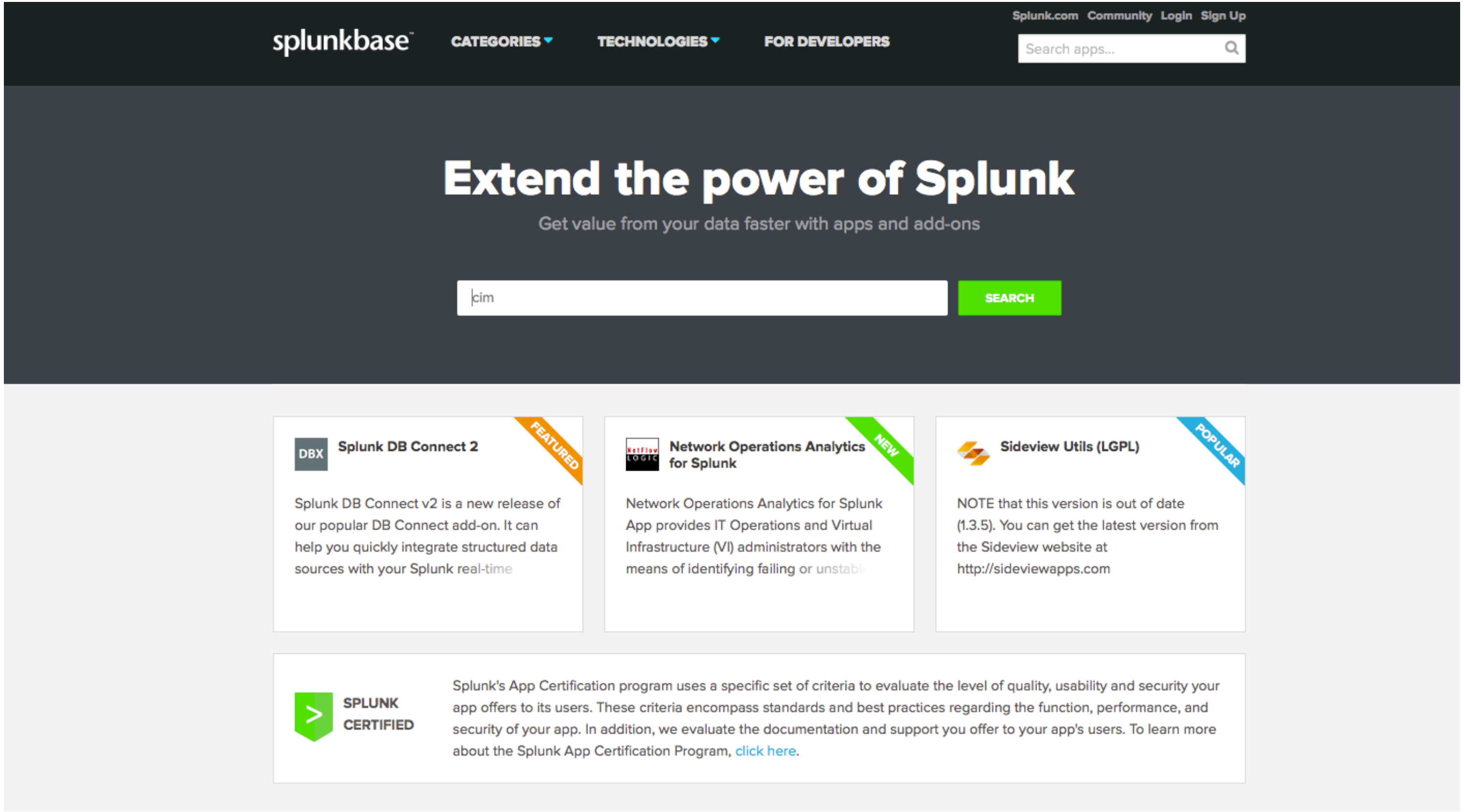
Some Troubleshooting Tips

- Check the documentation
- Do you get data in at all?
- Is the input working (port, file monitor etc)?
- Correct sourcetype
- Correct inputtype
- Have you restarted Splunk?
- Version dependency's

Some Troubleshooting Tips

- Access to the index
- Default search for the index
- Missing fields – correct data sent?
- Permissions correctly on knowledge objects?
  - Global, App, Private
- Verify all fields and tags

Nice – Where can I Download This???



Extend the power of Splunk

Get value from your data faster with apps and add-ons

cim

SEARCH

Splunk DB Connect 2

Splunk DB Connect v2 is a new release of our popular DB Connect add-on. It can help you quickly integrate structured data sources with your Splunk real-time

Network Operations Analytics for Splunk

Network Operations Analytics for Splunk App provides IT Operations and Virtual Infrastructure (VI) administrators with the means of identifying failing or unstabl

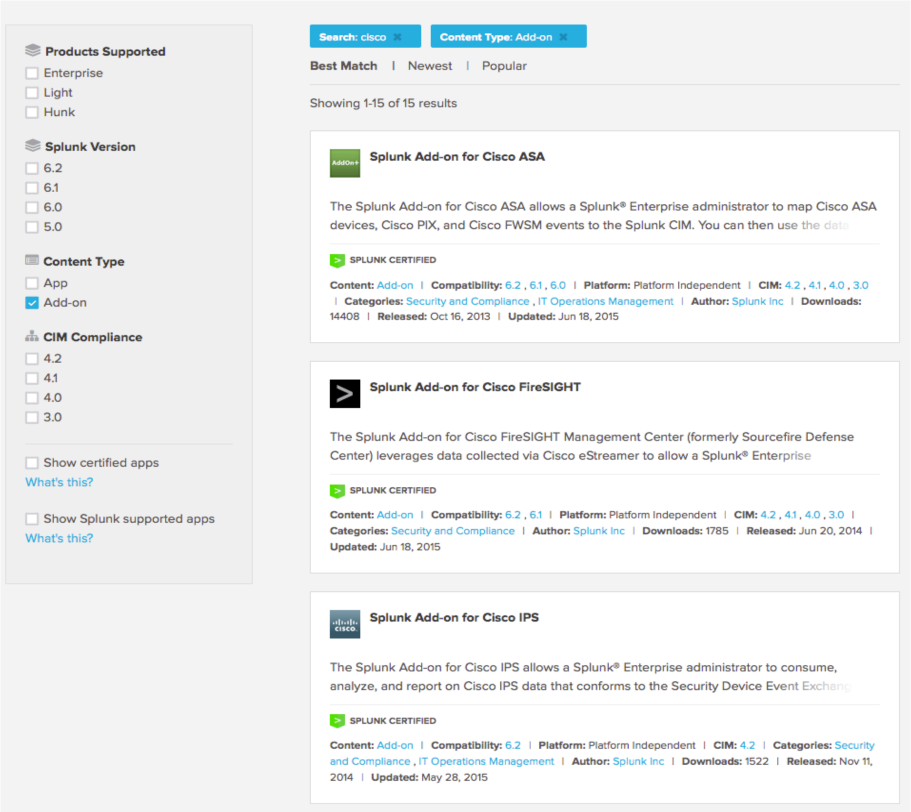
Sideview Utils (LGPL)

NOTE that this version is out of date (1.3.5). You can get the latest version from the Sideview website at http://sideviewapps.com

SPLUNK CERTIFIED

Splunk's App Certification program uses a specific set of criteria to evaluate the level of quality, usability and security your app offers to its users. These criteria encompass standards and best practices regarding the function, performance, and security of your app. In addition, we evaluate the documentation and support you offer to your app's users. To learn more about the Splunk App Certification Program, click here.

TA’s on Splunkbase



Products Supported

- □ Enterprise
- □ Light
- □ Hunk

Splunk Version

- □ 6.2
- □ 6.1
- □ 6.0
- □ 5.0

Content Type

- □ App
- ☑ Add-on

CIM Compliance

- □ 4.2
- □ 4.1
- □ 4.0
- □ 3.0

□ Show certified apps
What's this?

□ Show Splunk supported apps
What's this?

Showing 1-15 of 15 results

Splunk Add-on for Cisco ASA

The Splunk Add-on for Cisco ASA allows a Splunk® Enterprise administrator to map Cisco ASA devices, Cisco PIX, and Cisco FWSM events to the Splunk CIM. You can then use the data

SPLUNK CERTIFIED

Content: Add-on | **Compatibility:** 6.2 , 6.1 , 6.0 | **Platform:** Platform Independent | **CIM:** 4.2 , 4.1 , 4.0 , 3.0 | **Categories:** Security and Compliance , IT Operations Management | **Author:** Splunk Inc | **Downloads:** 14408 | **Released:** Oct 16, 2013 | **Updated:** Jun 18, 2015

Splunk Add-on for Cisco FireSIGHT

The Splunk Add-on for Cisco FireSIGHT Management Center (formerly Sourcefire Defense Center) leverages data collected via Cisco eStreamer to allow a Splunk® Enterprise

SPLUNK CERTIFIED

Content: Add-on | **Compatibility:** 6.2 , 6.1 | **Platform:** Platform Independent | **CIM:** 4.2 , 4.1 , 4.0 , 3.0 | **Categories:** Security and Compliance | **Author:** Splunk Inc | **Downloads:** 1785 | **Released:** Jun 20, 2014 | **Updated:** Jun 18, 2015

Splunk Add-on for Cisco IPS

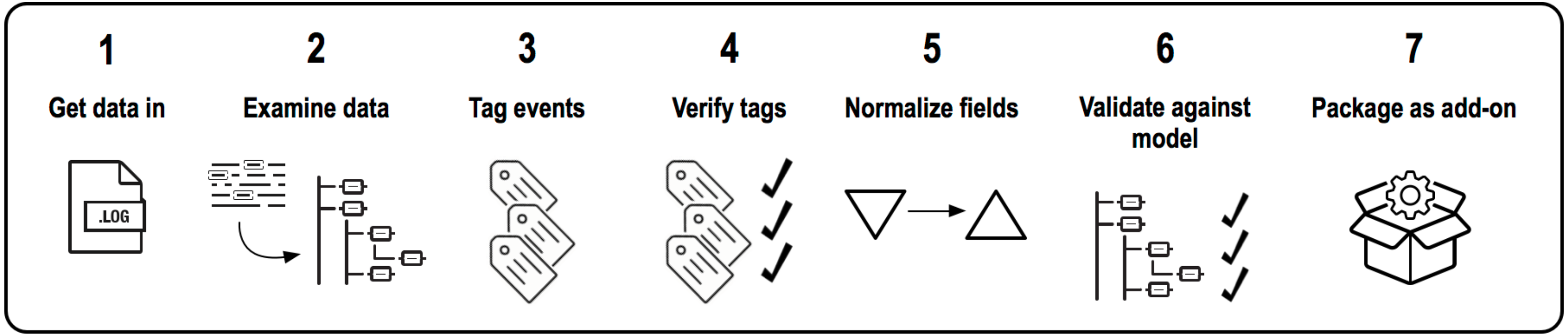
The Splunk Add-on for Cisco IPS allows a Splunk® Enterprise administrator to consume, analyze, and report on Cisco IPS data that conforms to the Security Device Event Exchang

SPLUNK CERTIFIED

Content: Add-on | **Compatibility:** 6.2 | **Platform:** Platform Independent | **CIM:** 4.2 | **Categories:** Security and Compliance , IT Operations Management | **Author:** Splunk Inc | **Downloads:** 1522 | **Released:** Nov 11, 2014 | **Updated:** May 28, 2015

What do I do if There is no TA’s for my Stuff?

- TA’s Can be created by the customer, our partners or via Splunk PS
- Everything you need are documented on docs.splunk.com



.conf2015

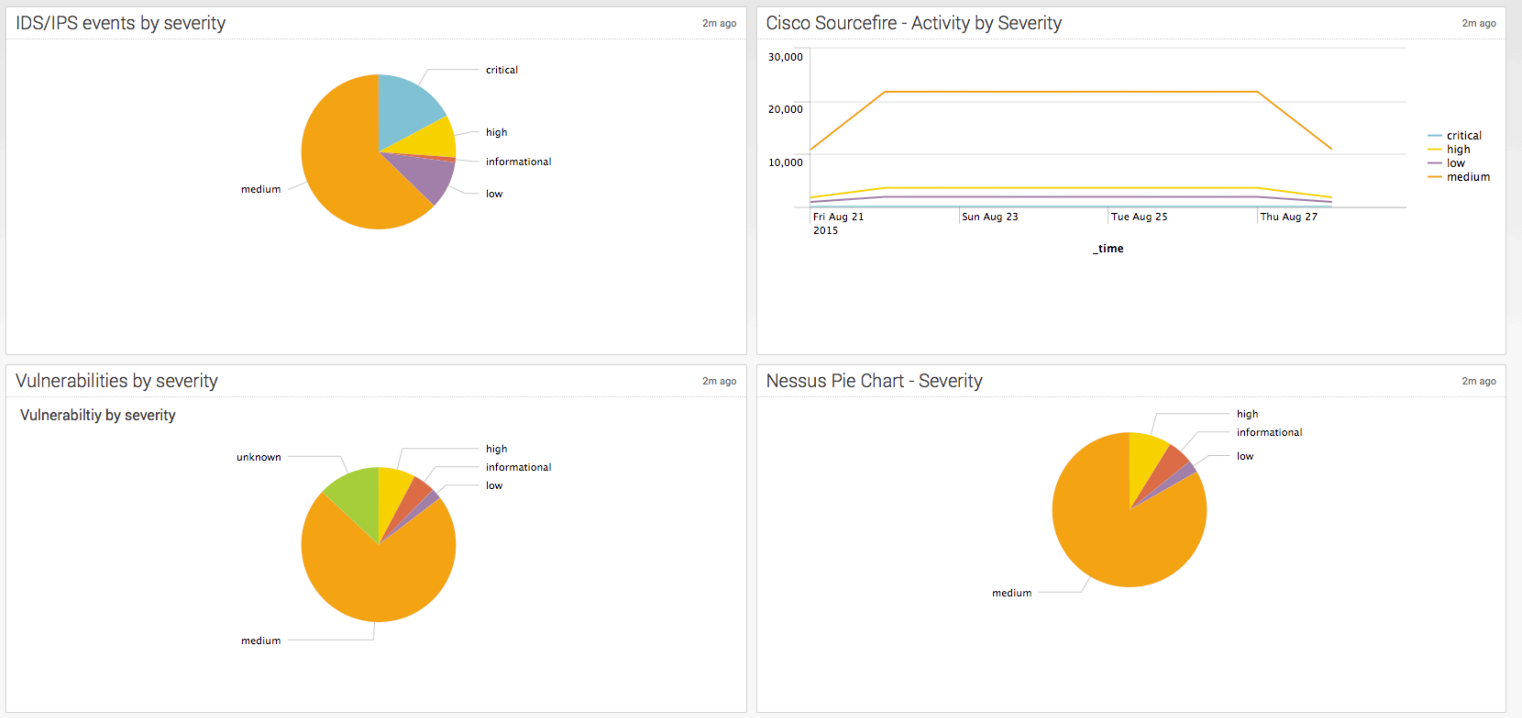
How to Create Dashboards and Reports From Data Models

splunk>

Panels from Pivot vs Premade Panels?

Panels from Pivot

Panels from TA’s



IDS/IPS events by severity

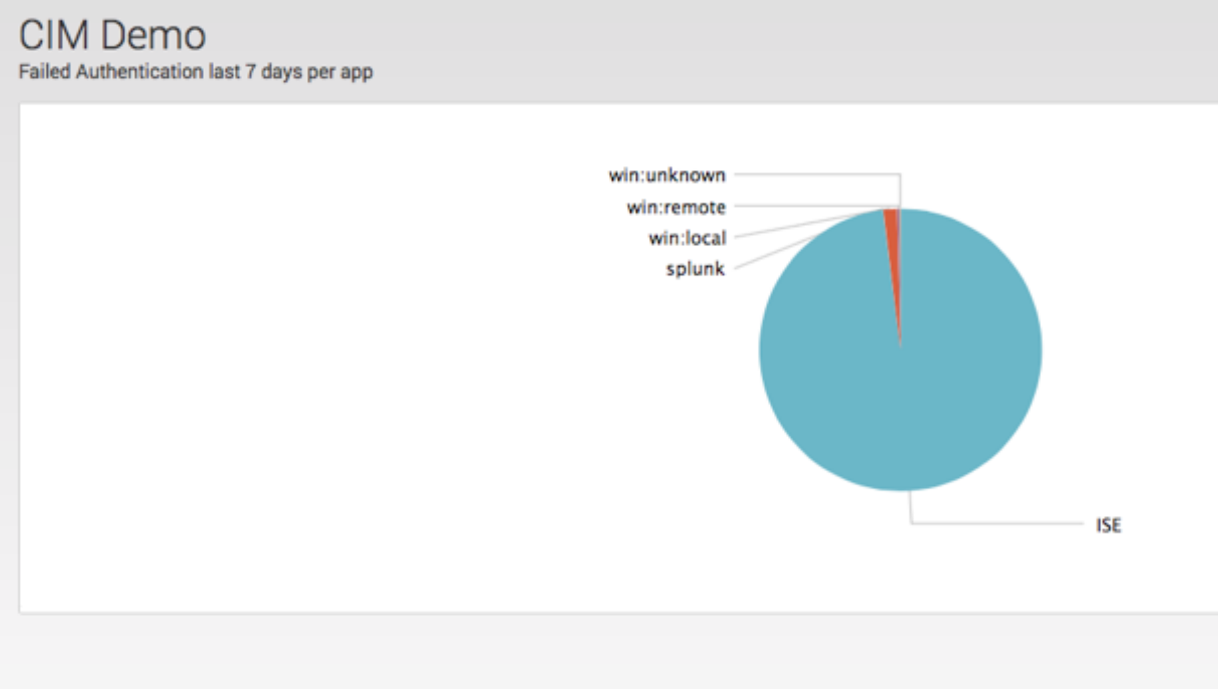
Cisco Sourcefire - Activity by Severity

Vulnerabilities by severity

Vulnerabiltiy by severity

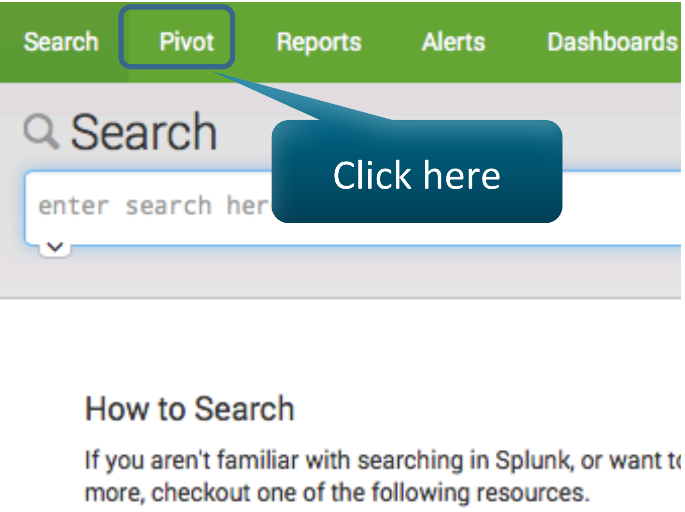
Nessus Pie Chart - Severity

Nr of Failed Authentication Last 7 days per App



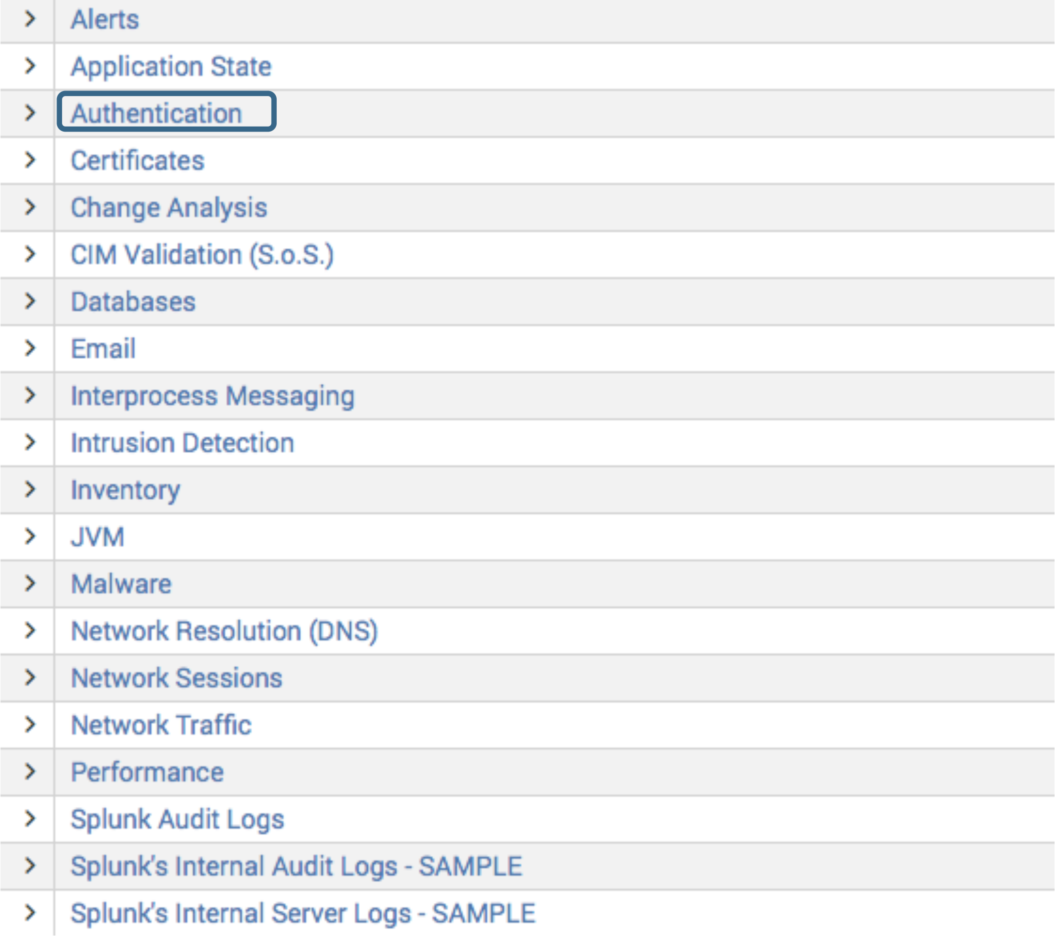
CIM Demo

Failed Authentication last 7 days per app

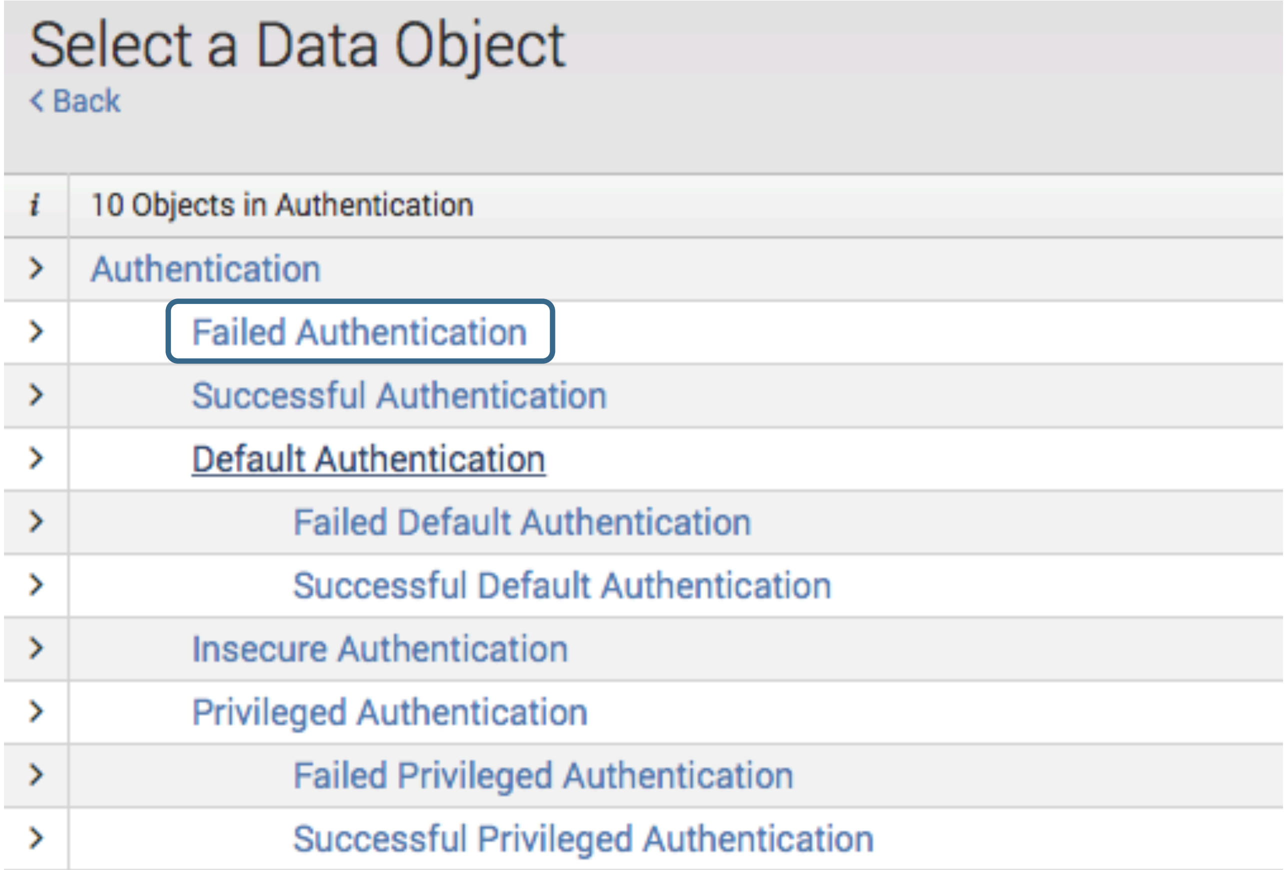


How to Search

If you aren't familiar with searching in Splunk, or want t
more, checkout one of the following resources.



- Alerts
- Application State
- Authentication
- Certificates
- Change Analysis
- CIM Validation (S.o.S.)
- Databases
- Email
- Interprocess Messaging
- Intrusion Detection
- Inventory
- JVM
- Malware
- Network Resolution (DNS)
- Network Sessions
- Network Traffic
- Performance
- Splunk Audit Logs
- Splunk's Internal Audit Logs - SAMPLE
- Splunk's Internal Server Logs - SAMPLE

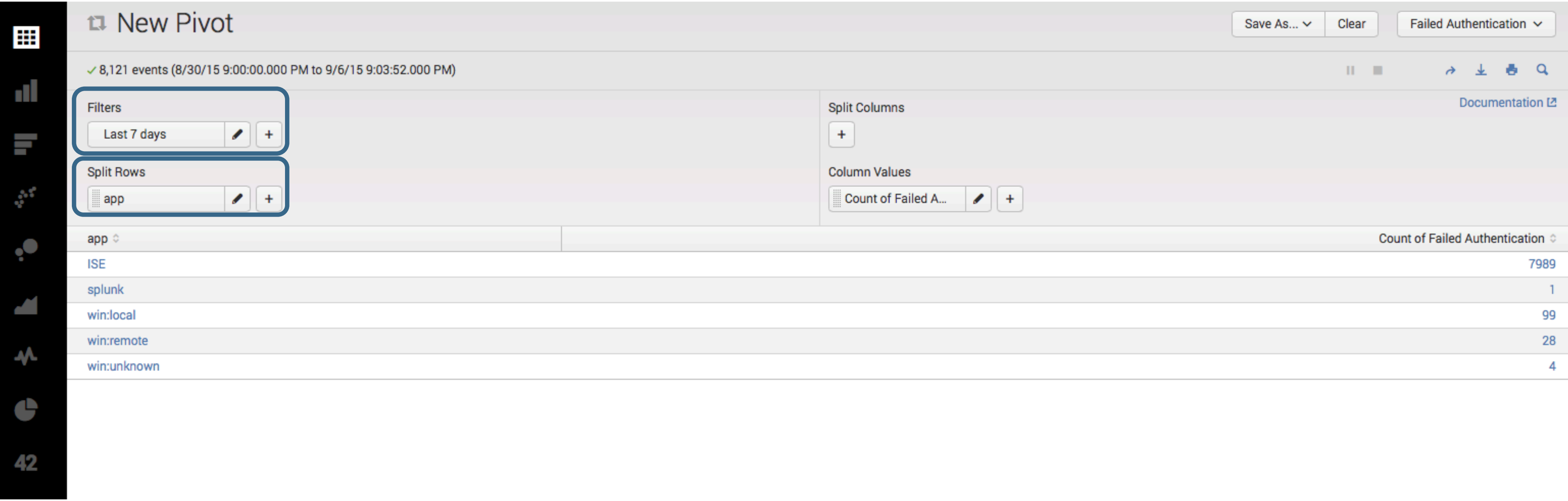


Select a Data Object

‹ Back

i 10 Objects in Authentication

- › Authentication
  - › Failed Authentication
  - › Successful Authentication
  - › Default Authentication
    - › Failed Default Authentication
    - › Successful Default Authentication
  - › Insecure Authentication
  - › Privileged Authentication
    - › Failed Privileged Authentication
    - › Successful Privileged Authentication



✓ 8,121 events (8/30/15 9:00:00.000 PM to 9/6/15 9:03:52.000 PM)

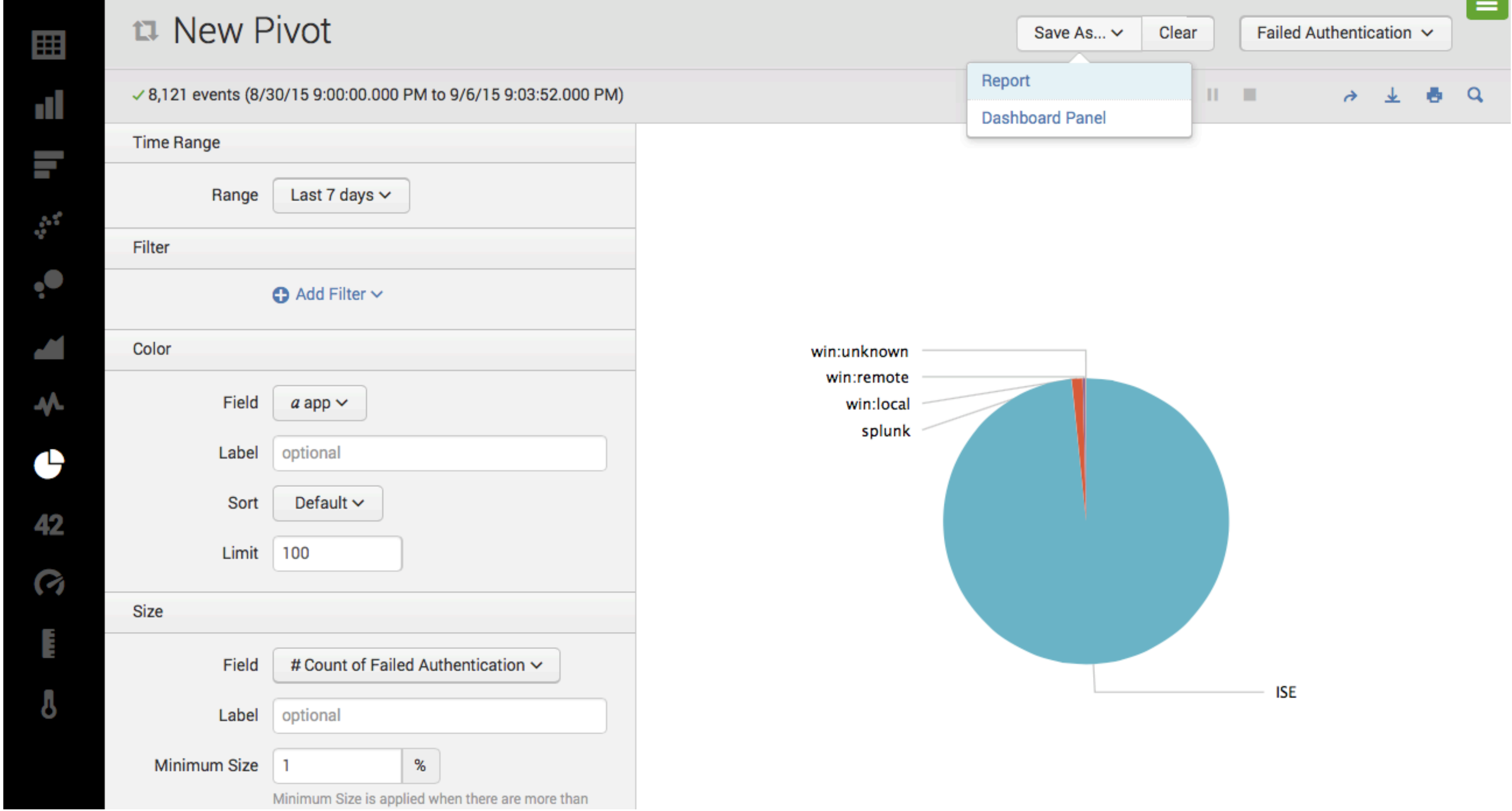
Filters: Last 7 days

Split Rows: app

Split Columns: +

Column Values: Count of Failed A...

app	Count of Failed Authentication
ISE	7989
splunk	1
win:local	99
win:remote	28
win:unknown	4



New Pivot

✓8,121 events (8/30/15 9:00:00.000 PM to 9/6/15 9:03:52.000 PM)

Time Range

Range: Last 7 days

Filter

Add Filter

Color

Field: a app

Label: optional

Sort: Default

Limit: 100

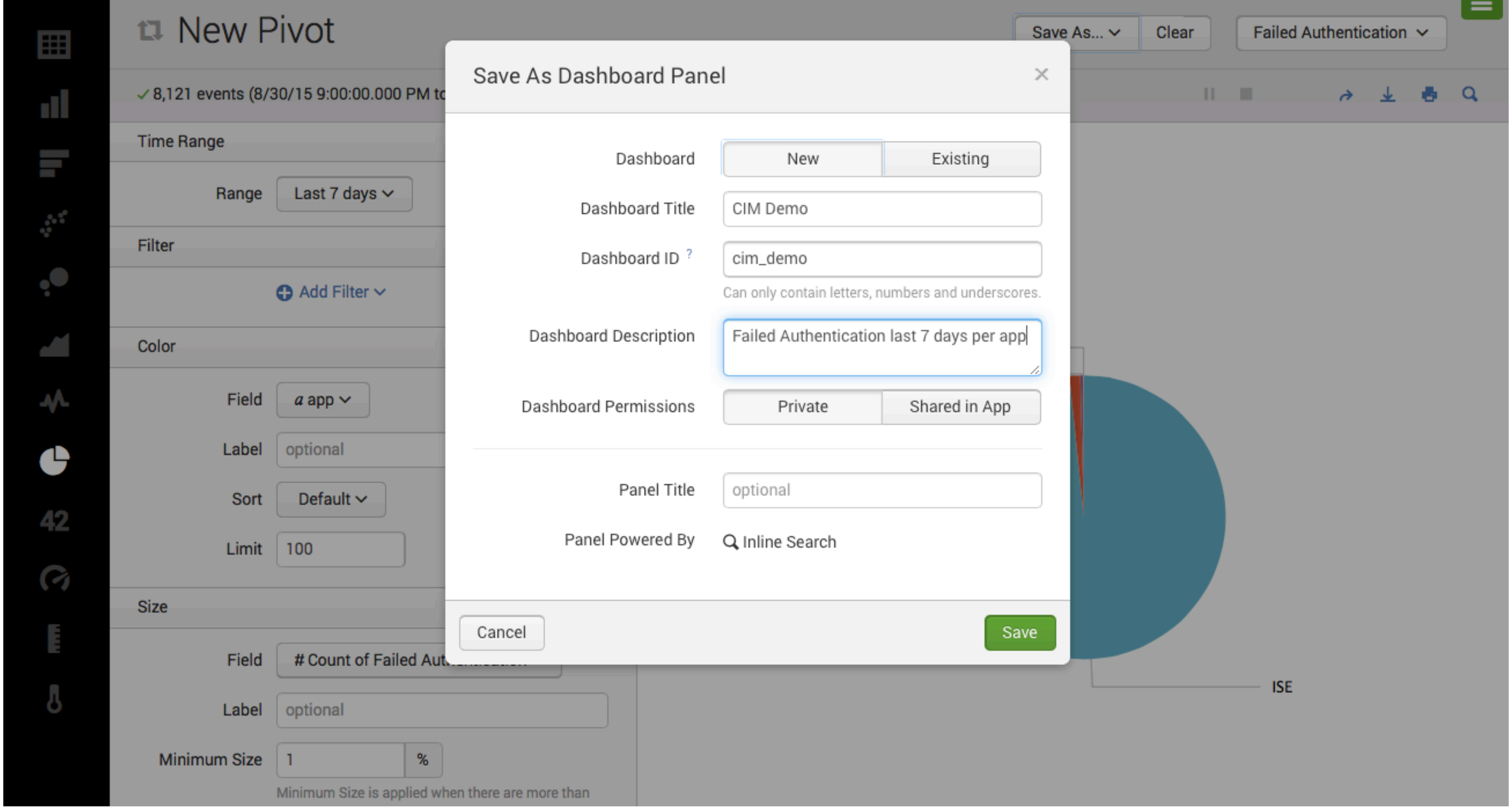
Size

Field: # Count of Failed Authentication

Label: optional

Minimum Size: 1 %

Minimum Size is applied when there are more than



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: CIM Demo

Dashboard ID ?: cim_demo

Can only contain letters, numbers and underscores.

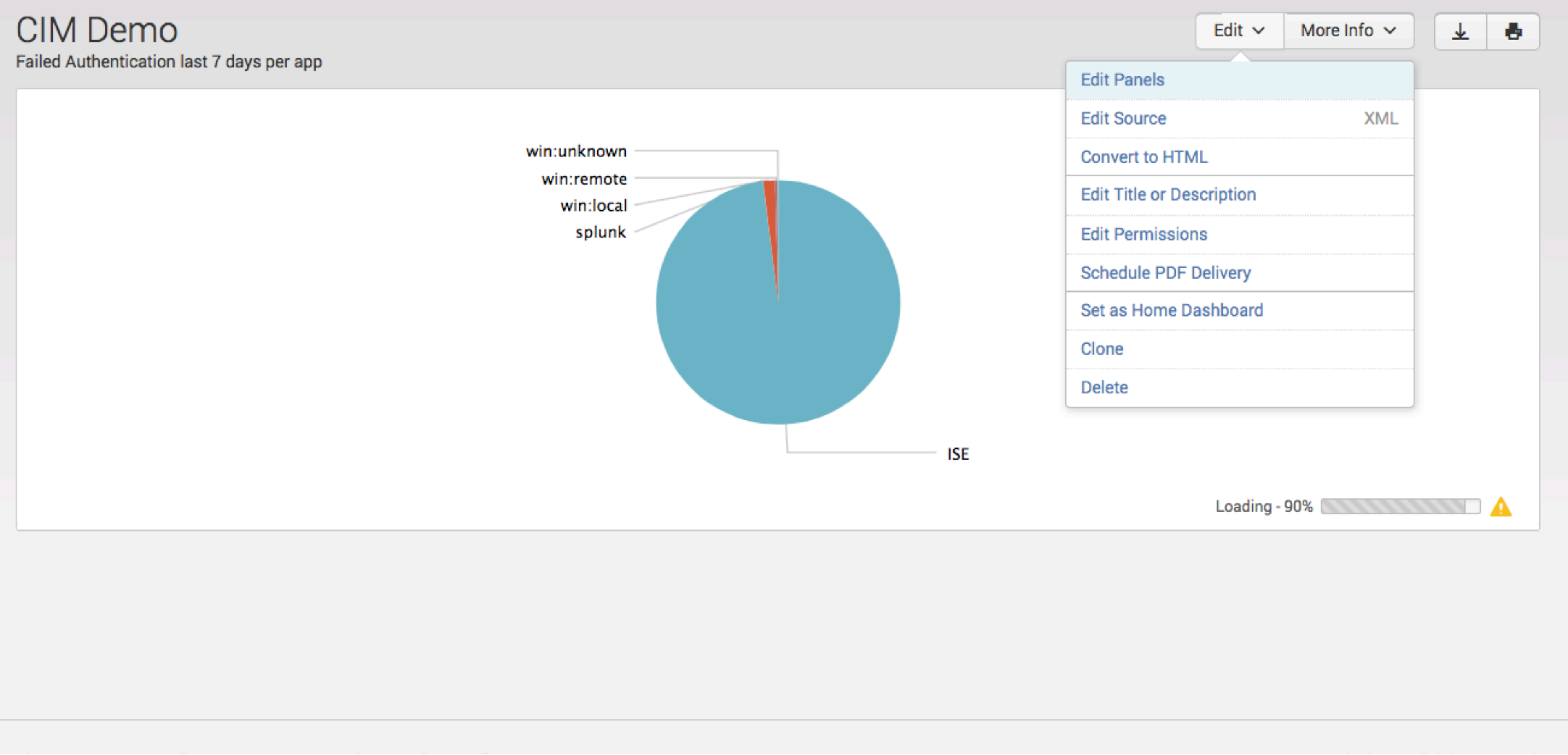
Dashboard Description: Failed Authentication last 7 days per app

Dashboard Permissions: Private | Shared in App

Panel Title: optional

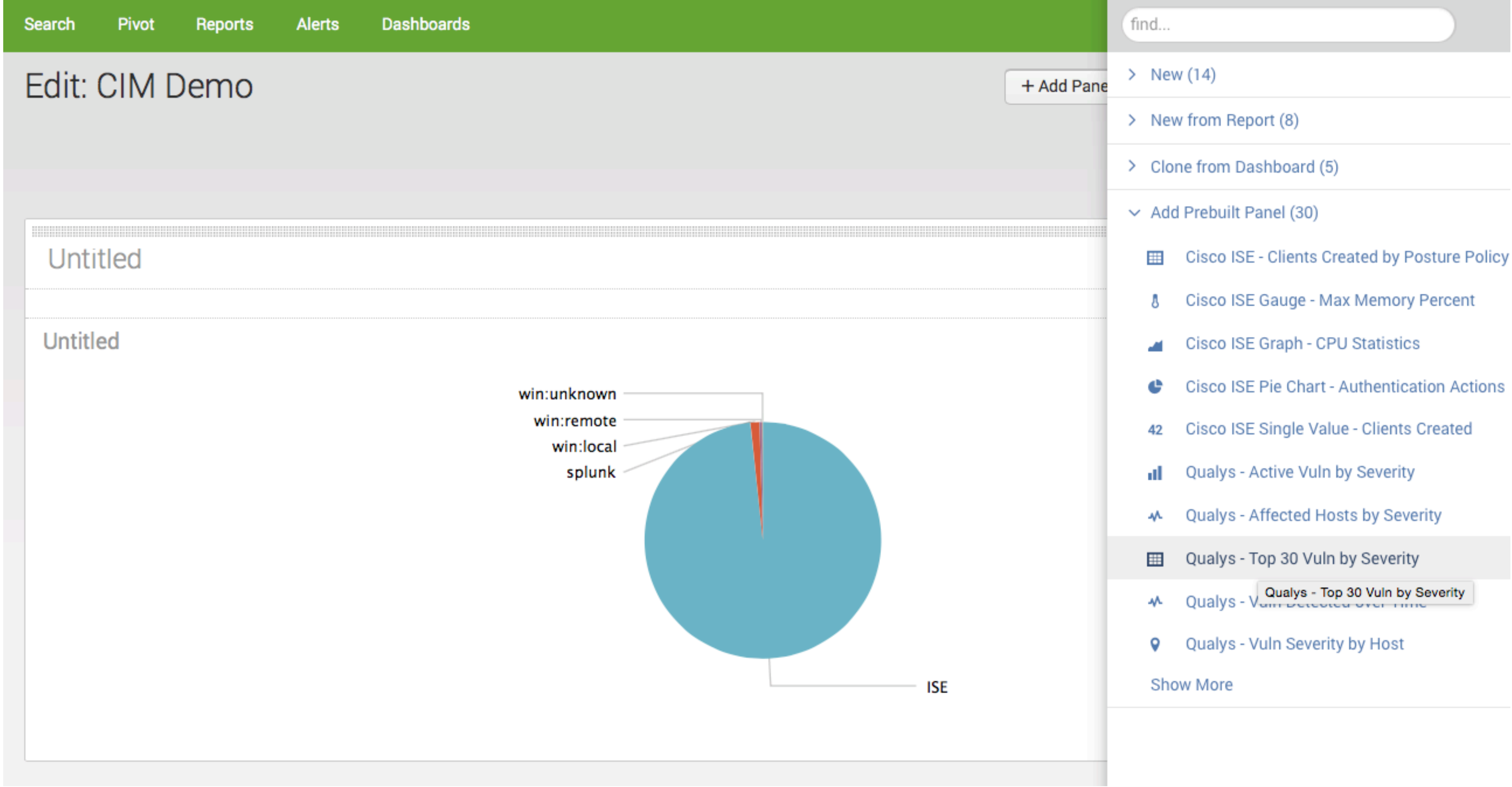
Panel Powered By: Inline Search

Cancel | Save



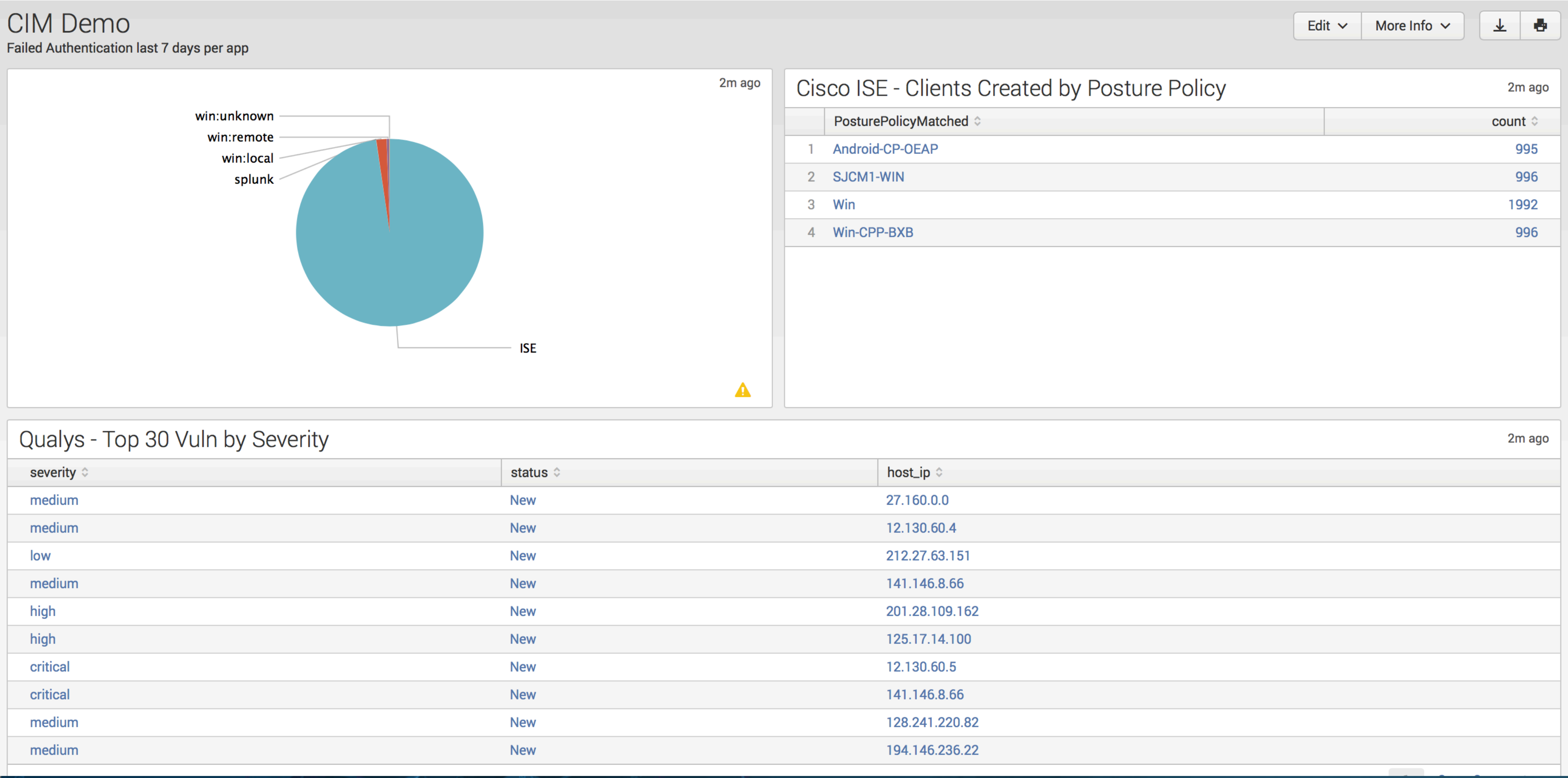
CIM Demo

Failed Authentication last 7 days per app



Edit: CIM Demo

Search
Pivot
Reports
Alerts
Dashboards
+ Add Pane
Untitled
Untitled
win:unknown
win:remote
win:local
splunk
ISE
find...
New (14)
New from Report (8)
Clone from Dashboard (5)
Add Prebuilt Panel (30)
Cisco ISE - Clients Created by Posture Policy
Cisco ISE Gauge - Max Memory Percent
Cisco ISE Graph - CPU Statistics
Cisco ISE Pie Chart - Authentication Actions
42
Cisco ISE Single Value - Clients Created
Qualys - Active Vuln by Severity
Qualys - Affected Hosts by Severity
Qualys - Top 30 Vuln by Severity
Qualys - Top 30 Vuln by Severity
Qualys - Vuln Detected over Time
Qualys - Vuln Severity by Host
Show More



CIM Demo

Failed Authentication last 7 days per app

Cisco ISE - Clients Created by Posture Policy

2m ago

	PosturePolicyMatched	count
1	Android-CP-OEAP	995
2	SJCM1-WIN	996
3	Win	1992
4	Win-CPP-BXB	996

Qualys - Top 30 Vuln by Severity

2m ago

severity	status	host_ip
medium	New	27.160.0.0
medium	New	12.130.60.4
low	New	212.27.63.151
medium	New	141.146.8.66
high	New	201.28.109.162
high	New	125.17.14.100
critical	New	12.130.60.5
critical	New	141.146.8.66
medium	New	128.241.220.82
medium	New	194.146.236.22

.conf2015

Enterprise Security – How Will CIM Prepare For that?

splunk>

Enterprise Security – How will CIM Prepare for that?

- Most work are with getting data in
- Create new TA's will be a part of that
- All data = CIM = ready to go!

What do I Need to do more?

- Install Enterprise Security app
- Create asset.csv and identity.csv
- Edit other lookups/lists
- Enable relevant correlation searches
- Tune correlation searches
- Add more correlation searches for specific use-cases

Recap

- CIM Are used to normalize the data
- Unified view of data
- Prepare for Enterprise Security
- Provides 22 data models
- Easy to create searches and dashboards
- TA’s Are used to normalized data
- Uses tagging and specific field names
- Both CIM and TA’s are available at Splunkbase

What Questions do you Have?

.conf2015

THANK YOU

splunk>

Appendix

Links

- CIM APP: https://splunkbase.splunk.com/app/1621/
- Documentation: http://docs.splunk.com/Documentation/CIM/latest/User/Overview
- How to create TA's: http://docs.splunk.com/Documentation/CIM/latest/User/UsetheCIMtonormalizedataatsearchtime