

.conf2014

YOUR DATA ADVENTURE

Vulnerability Management with the Splunk App for Enterprise Security

Randal T. Rioux

Principal Security Strategist and
Minister of Offense

Splunk Inc.

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.

Things We Will Be Discussing

- Field Extractions and Content
- Customizing Views to Help Prioritization
- Available Event Actions
- Managing Vulnerabilities as Notable Events
- Helpful Searches and Procedures
- The Vulnerability Data Model



Things We Will Not Be Discussing

- How to get vulnerability data into Splunk
 - There are lots of ways!
 - Depends heavily on vendor reporting methods
- Details on vendor and scanner products
 - Each has their merit and faults - do your research
 - Examples for this demonstration are not endorsements
- Corporate policies for vulnerability management
 - Everybody has an opinion



.conf2014

YOUR DATA ADVENTURE

Overview of Patch
and Vulnerability
Management

splunk>

What Is Vulnerability Management?

Patch and vulnerability management are one of the most important security programs to implement in an IT infrastructure.

However, surprisingly enough it is also either not a routine process, or it is done in a completely ineffective manner.

Here, I will completely over simplify the technical process, and leave the policy work to you and your organizations to develop.

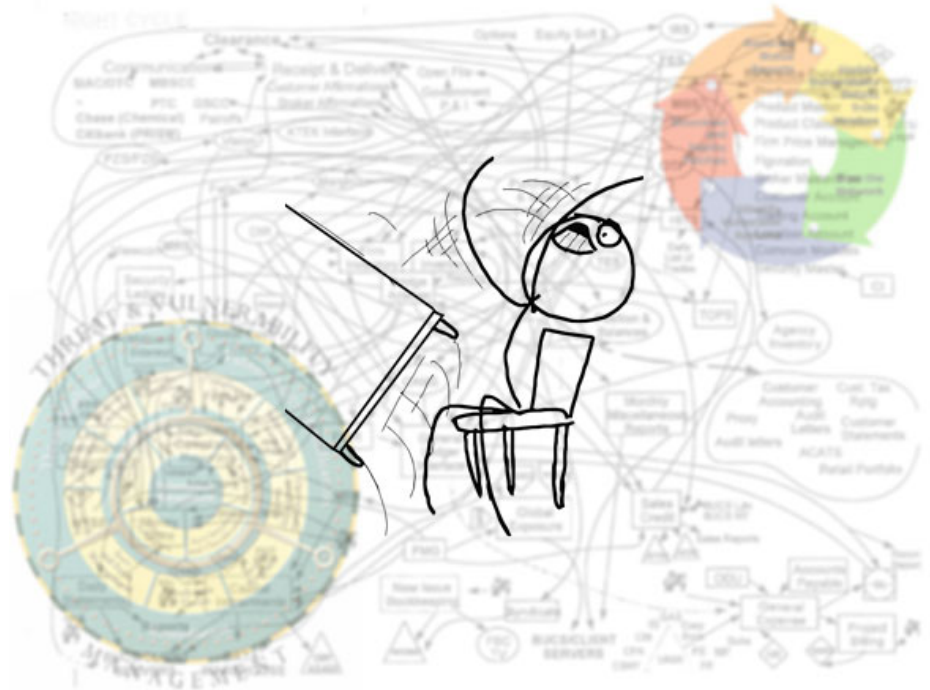
Vulnerability Management Process

This is where most presentations on this subject over complicate things with lifecycle graphics and lengthy procedures.

If you are interested in that sort of thing, take a look at NIST SP 800-40: Creating a Patch and Vulnerability Management Program.

Here's a summary:

1. **DISCOVER**
2. **PRIORITIZE AND ASSIGN**
3. **FIX**



Important Elements of Vulnerability Reports

- Common Vulnerabilities and Exposures (CVE)
 - CVE is a dictionary of publicly known information security vulnerabilities and exposures
 - <https://cve.mitre.org>
- Common Vulnerability Scoring System (CVSS)
 - The CVSS assessment measures three areas of concern:
 - Base Metrics for qualities intrinsic to a vulnerability
 - Temporal Metrics for characteristics that evolve over the lifetime of vulnerability
 - Environmental Metrics for vulnerabilities that depend on a particular implementation or environment
 - These metrics are used to generate a numerical score and a text vector that indicates the severity of the vulnerability, and the way in which it was calculated.



.conf2014

YOUR DATA ADVENTURE

The Splunking...

splunk>

The Anatomy of a Vulnerability Event

Example raw event received from a vulnerability scan:

i	Time	Event
>	9/22/14 7:23:11.000 PM	start_time="Mon Sep 22 17:30:28 2014" end_time="Mon Sep 22 17:31:32 2014" dest_ip="192.168.3.5" os="Linux Kernel 2.6.32-431.20 .3.el6.i686 on Red Hat Enterprise Linux Server release 6.5 (Santiago)" cvss_base_score="9.3" cvss_vector="CVSS2#AV:N/AC:M/Au:N /C:C/I:C/A:C" dest_port_proto="general (0/tcp)" severity_id="3" signature_family="Red Hat Local Security Checks" signature_id= "76515" signature="RHEL 6 : java-1.7.0-openjdk (RHSA-2014:0889)" cve="CVE-2014-2483" cve="CVE-2014-2490" cve="CVE-2014-4209" c ve="CVE-2014-4216" cve="CVE-2014-4218" cve="CVE-2014-4219" cve="CVE-2014-4221" cve="CVE-2014-4223" cve="CVE-2014-4244" cve="CV E-2014-4252" cve="CVE-2014-4262" cve="CVE-2014-4263" cve="CVE-2014-4266" xref="RHSA:2014:0889" xref="IAVA:2014-A-0105" cvss_base_score = 9.3 host = telesto.procyonlabs.com source = /opt/splunk-vm/var/spool/splunk/Full_Scan_-_Linux_6a4gjr.nessus sourcetype = nessus

Splunk takes that event, and at search time (this is an important distinction!) assigns each value a key.

This allows Enterprise Security to start doing what it does best: make it useful!

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> cvss_base_score ▾	9.3	▾
	<input checked="" type="checkbox"/> host ▾	telesto.procyonlabs.com	▾
	<input checked="" type="checkbox"/> source ▾	/opt/splunk-vm/var/spool/splunk/Full_Scan_-_Linux_6a4gjr.nessus	▾
	<input checked="" type="checkbox"/> sourcetype ▾	nessus	
Event	<input type="checkbox"/> cve ▾	CVE-2014-2483	
		CVE-2014-2490	
		CVE-2014-4209	
		CVE-2014-4216	
		CVE-2014-4218	
		CVE-2014-4219	
		CVE-2014-4221	
		CVE-2014-4223	
		CVE-2014-4244	
		CVE-2014-4252	
		CVE-2014-4262	
		CVE-2014-4263	
		CVE-2014-4266	
	<input type="checkbox"/> cvss_vector ▾	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	
	<input type="checkbox"/> dest ▾	192.168.3.5	
	<input type="checkbox"/> dest_asset_id ▾	ab55803d42d270e688c6d82e3fc0da4bf3abef01	
	<input type="checkbox"/> dest_asset_tag ▾	should_update	
		iso27002	
		should_timesync	
		americas	
	<input type="checkbox"/> host_is_expected ▾	false	▾
	<input type="checkbox"/> host_pci_domain ▾	untrust	▾
	<input type="checkbox"/> host_requires_av ▾	false	▾
	<input type="checkbox"/> host_should_timesync ▾	false	▾
	<input type="checkbox"/> host_should_update ▾	false	▾
	<input type="checkbox"/> idm_flags ▾	001000	▾
	<input type="checkbox"/> index ▾	main	▾
	<input type="checkbox"/> linecount ▾	1	▾
	<input type="checkbox"/> os ▾	Linux Kernel 2.6.32-431.20.3.el6.i686 on Red Hat Enterprise Linux Server release 6.5 (Santiago)	▾
	<input type="checkbox"/> product ▾	Nessus	▾
	<input type="checkbox"/> severity ▾	high	▾
	<input type="checkbox"/> severity_id ▾	3	▾
	<input type="checkbox"/> signature ▾	RHEL 6 : java-1.7.0-openjdk (RHSA-2014:0889)	▾
	<input type="checkbox"/> signature_family ▾	Red Hat Local Security Checks	▾
	<input type="checkbox"/> signature_id ▾	76515	▾
	<input type="checkbox"/> splunk_server ▾	telesto.procyonlabs.com	▾
	<input type="checkbox"/> start_time ▾	Mon Sep 22 17:30:28 2014	▾
	<input type="checkbox"/> tag ▾	inventory	▾
		network	▾
		os	▾
		report	▾
		should_timesync	▾
		should_update	▾
		system	▾
		version	▾
		vulnerability	▾
	<input type="checkbox"/> timestamp ▾	none	▾
	<input type="checkbox"/> transport ▾	tcp	▾
	<input type="checkbox"/> vendor ▾	Tenable	▾
	<input type="checkbox"/> xref ▾	RHSA:2014:0889	▾



.conf2014

YOUR DATA ADVENTURE

VM - The Splunk
App for Enterprise
Security Way

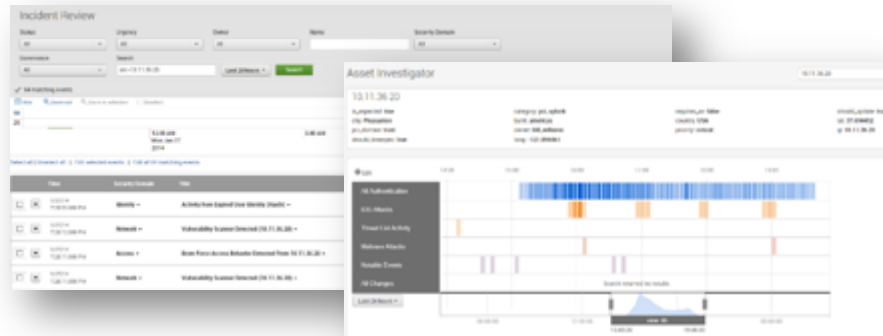
splunk>

Splunk App for Enterprise Security

Pre-built searches, alerts, reports, dashboards, threat intel feeds, workflow



Dashboards and Reports



Incident Investigations & Management



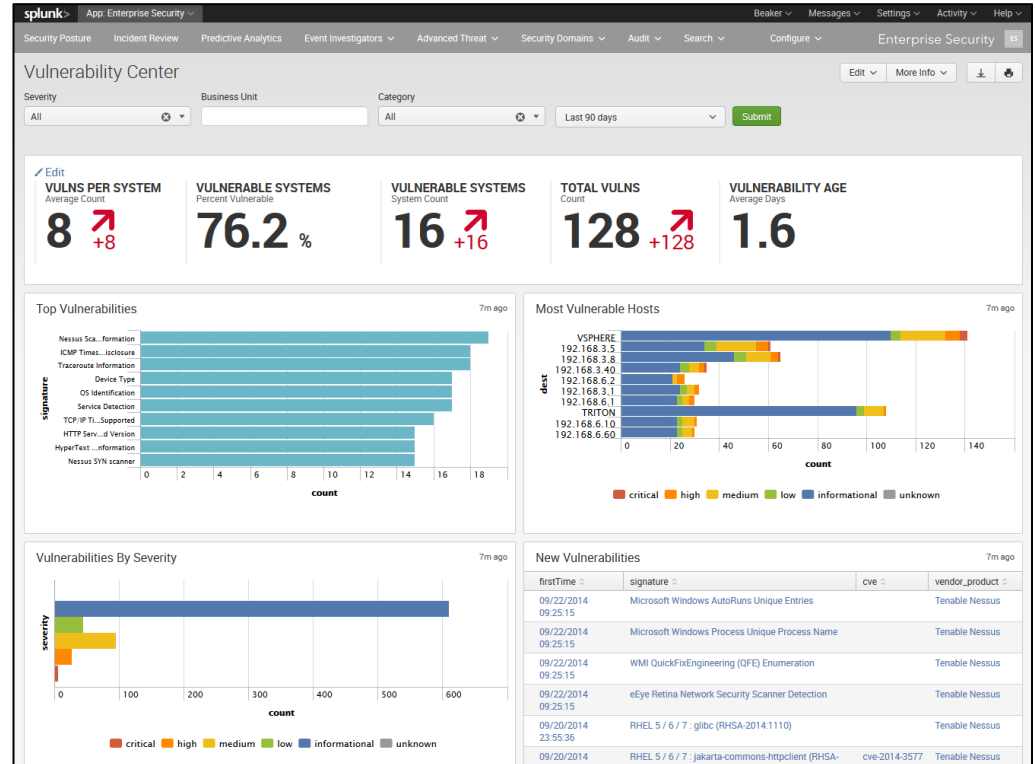
Statistical Outliers



Asset and Identity Aware

Splunk App for Enterprise Security

- The Splunk App for Enterprise Security is designed to be generic enough for immediate value, with the power to be customized according to your organization's monitoring and workflow needs.
- Splunk itself is a framework, and ES follows that flexibility by enabling customization for all views via the GUI, or for more advanced users, the application code beneath it.



.conf2014

YOUR DATA ADVENTURE

Use and
Customization

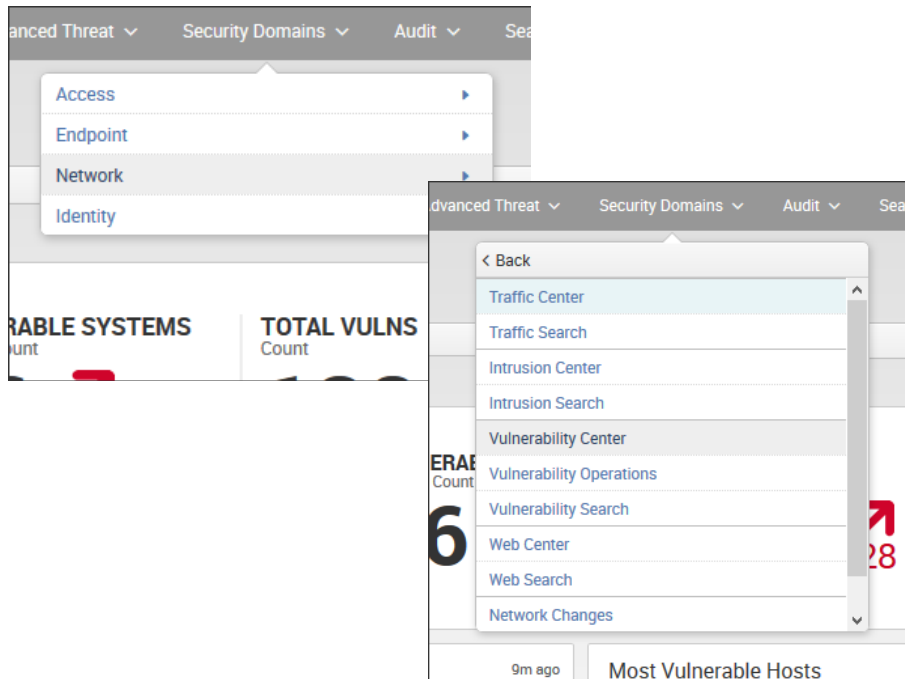
splunk>

Use and Customization

Security Domain: Network

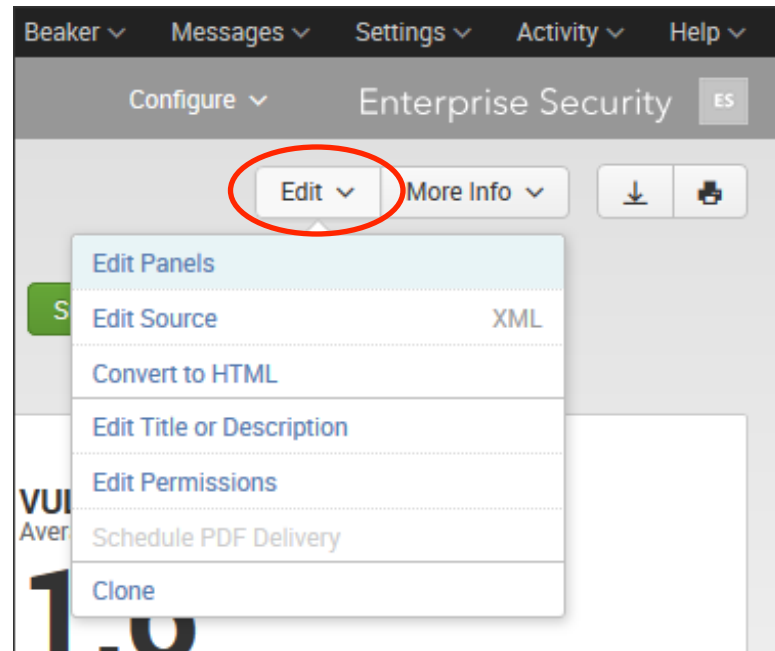
ES contains many areas of focus. For vulnerability management, we want to use the views and tools associated with the “Security Domains” drop down “Network,” which includes:

- Vulnerability Center
- Vulnerability Operations
- Vulnerability Search



Use and Customization

- All security domain “views” have the option to edit what you see
- The defaults are helpful, but adding, removing and editing panels specific to the things you care about is vital to enhancing your work flow

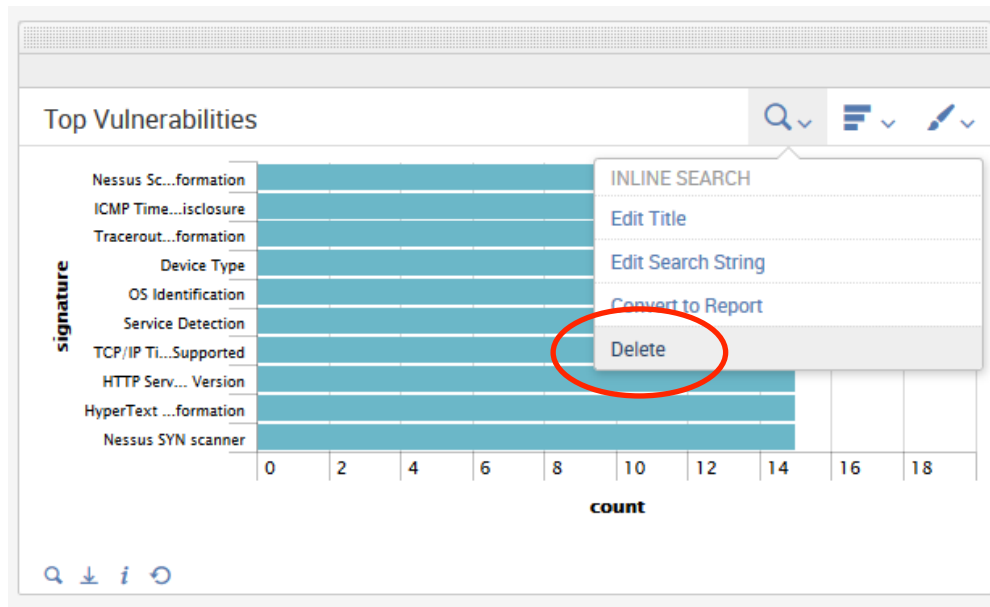




Let me show you how it's done...

Panel Editing

- First, let's delete the "Top Vulnerabilities" panel. We don't really care about that stuff anyway
- This frees up some precious real estate for the dashboard

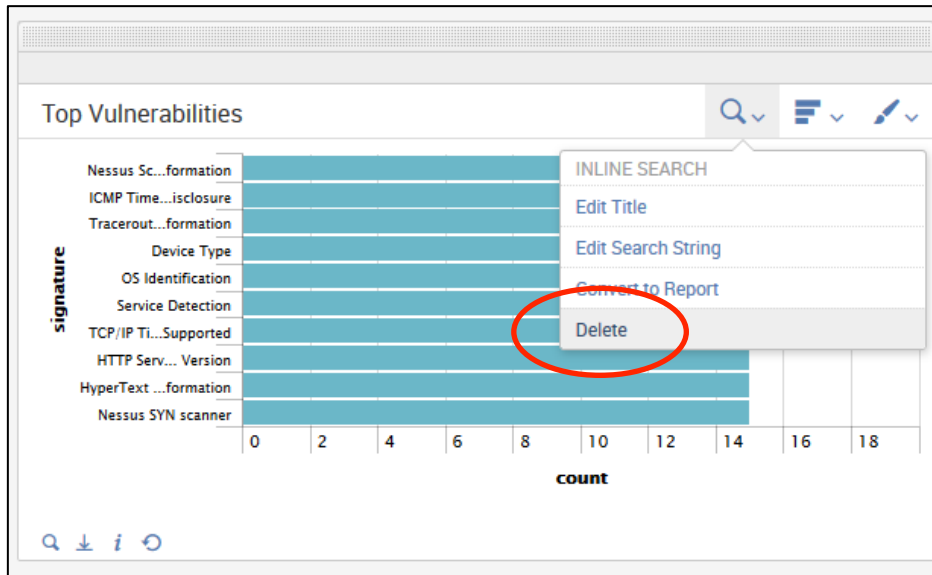
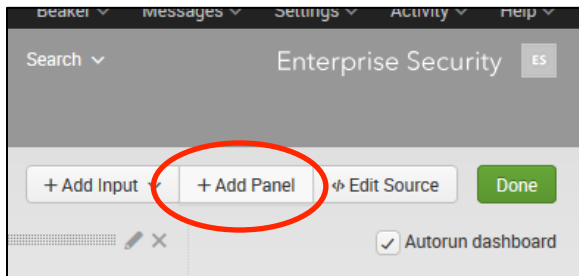




Let me show you how it's done...

Panel Editing

- First, let's delete the "Top Vulnerabilities" panel. We don't really care about that stuff anyway, and it frees up some precious real estate for the dashboard
- Next, click on "+ Add Panel"





Let me show you how it's done...

Panel Editing

- Title the panel “Systems w/ CVSS > 7”
- Use the following Search String:
`tag=vulnerability cvss_base_score>7 | top dest_ip`
- Time Range Scope should be “Shared Time Picker (global)”
 - This uses the time selection set for the entire view in the header/search area
- Click Save
- It is now added to the bottom of the page, using the default bar chart display. Drag the panel up to where the deleted one was

Add Panel

Content Title: Systems w/ CVSS > 7

Content Type: [Search] [Refresh] [Copy]

Search String: tag=vulnerability cvss_base_score>7 | top dest_ip

Run Search

Time Range Scope: Shared Time Picker (global) v

- ✓ Shared Time Picker (global)
- Explicit Selection
- Tokens

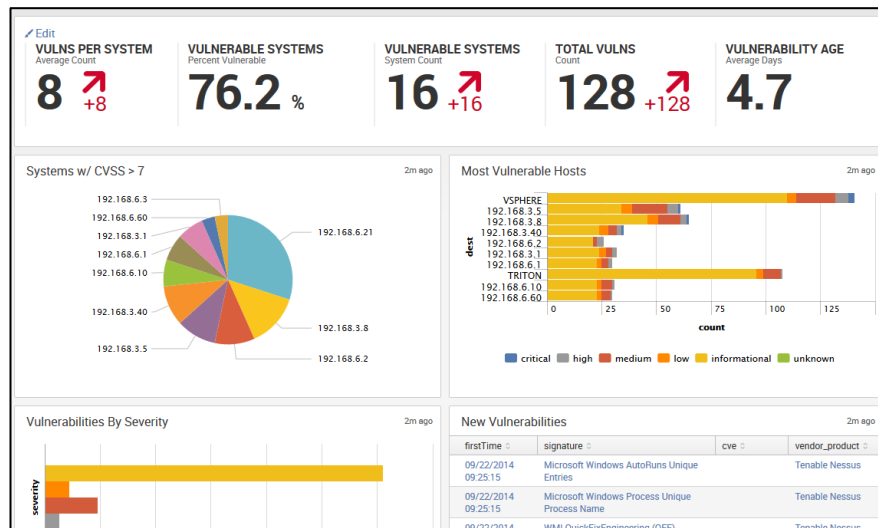
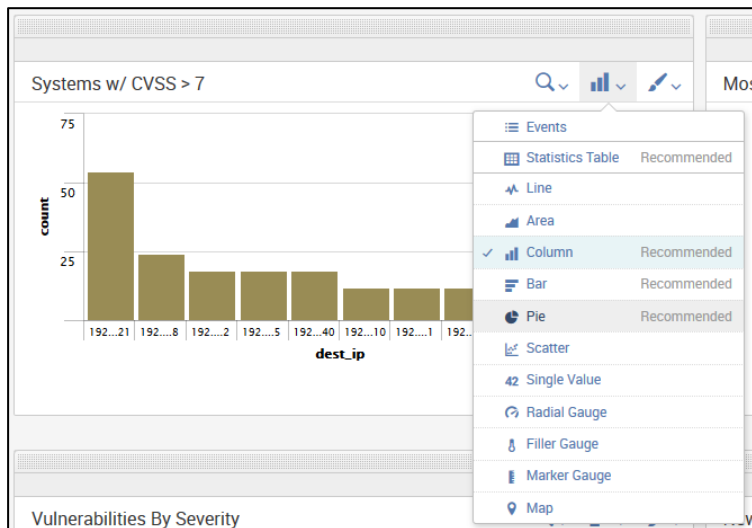
Cancel



Let me show you how it's done...

Panel Editing

- The bar chart is ugly for this one. Click on the bar chart icon, and you have a bunch of choices
- Click on “Pie”. I like pie. Now click the Done button on the top of the page, and admire your work



.conf2014

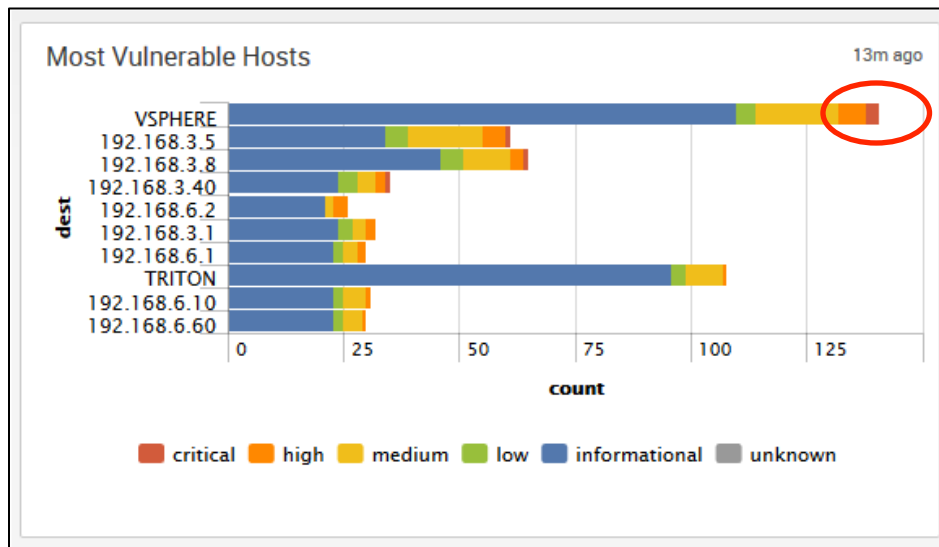
YOUR DATA ADVENTURE

Working With and
Alerting On Events

splunk>

Managing Scanned Discoveries

- Most everything you see by default is drill-downable. That is a word, I assure you
- The panel on the right has a listing of hosts we should probably pay attention to
- Let's click on the red part of the bar for the VSPHERE host to see what is going on there



Managing Scanned Discoveries

Creating Alerts from Vulnerabilities



Managing Scanned Discoveries

This Windows system (named “VSPHERE”) is running a VMware vCenter server, and it hasn’t been tended to in quite a while. Let’s click on the first item listed.

Vulnerability Search

Severity: critical

Destination: VSPHERE

Submit

_time	category	severity	signature	cve	dest	count
2014-09-22 19:23:13	unknown	critical	Microsoft SQL Server Unsupported Version Detection		VSPHERE	3
2014-09-22 19:23:13	unknown	critical	VMware Security Updates for vCenter Server (VMSA-2014-0008)	cve-2013-4322 cve-2013-4590 cve-2013-6629 cve-2013-6954 cve-2014-0050 cve-2014-0114 cve-2014-0429 cve-2014-0432 cve-2014-0446	VSPHERE	3

Managing Scanned Discoveries

New Search

```
| `datamodel("Vulnerabilities", "Vulnerabilities")` | search Vulnerabilities.signature="Microsoft SQL Server Unsupported Version Detection" Vulnerabilities.dest="VSPHERE" | `drop_dm_object_name("Vulnerabilities")`
```

3 events (6/25/14 12:00:00.000 AM to 9/23/14 1:57:37.000 AM)

Events (3) | Statistics | Visualization

Format Timeline | - Zoom Out | + Zoom to Selection | x Deselect

1 day per column

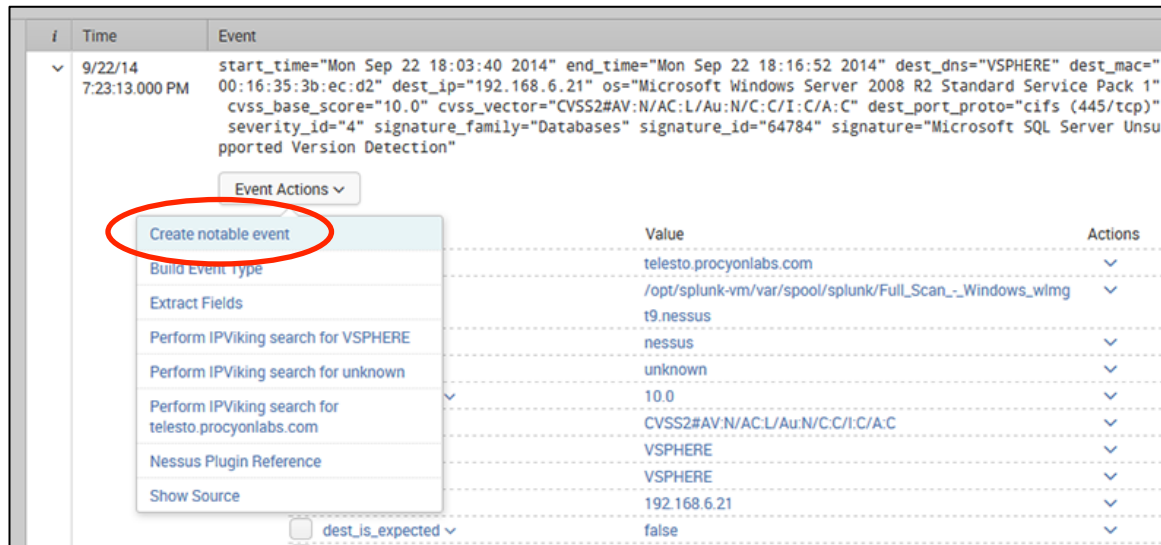
Click to Expand

	List	Format	20 Per Page
< Hide Fields	≡ All Fields		
Selected Fields			
a host 1			
a source 3			
a sourcetype 1			
Interesting Fields			
a category 1			
# cvss_base_score 1			

	Time	Event
>	9/22/14 7:23:13.000 PM	start_time="Mon Sep 22 18:03:40 2014" end_time="Mon Sep 22 18:16:52 2014" dest_dns="VSPHERE" dest_mac="00:16:35:3b:ec:d2" dest_ip="192.168.6.21" os="Microsoft Windows Server 2008 R2 Standard Service Pack 1" cvss_base_score="10.0" cvss_vector="CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C" dest_port_proto="cifs (445/tcp)" severity_id="4" signature_family="Databases" signature_id="64784" signature="Microsoft SQL Server Unsupported Version Detection" host = telesto.procyonlabs.com ; source = /opt/splunk-vm/var/spool/splunk/Full_Scan_-_Windows_wimgt9.nessus ; sourcetype = nessus
>	9/22/14 9:25:15.000 AM	start_time="Sun Sep 21 22:05:54 2014" end_time="Sun Sep 21 22:20:02 2014" dest_dns="VSPHERE" dest_mac="00:16:35:3b:ec:d2" dest_ip="192.168.6.21" os="Microsoft Windows Server 2008 R2 Standard Service Pack 1" cvss_base_score="10.0" cvss_vector="CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C" dest_port_proto="cifs (445/tcp)"

Managing Scanned Discoveries

- Now we have access to the “Event Actions” contextual menu. This has a default list of actions we can take on the current event. To manage the vulnerability, and start the process of assignment and mitigation, we will select “Create notable event”
- Note that this is the manual process. To automate this kind of activity, correlation rules can be leveraged. We’ll review that later in this presentation



The screenshot displays a Splunk event in a table. The event details are as follows:

i	Time	Event
✓	9/22/14 7:23:13.000 PM	start_time="Mon Sep 22 18:03:40 2014" end_time="Mon Sep 22 18:16:52 2014" dest_dns="VSPHERE" dest_mac="00:16:35:3b:ec:d2" dest_ip="192.168.6.21" os="Microsoft Windows Server 2008 R2 Standard Service Pack 1" cvss_base_score="10.0" cvss_vector="CVSS2#AV:N/AC:L/Au:N/C:I/C/A:C" dest_port_proto="cifs (445/tcp)" severity_id="4" signature_family="Databases" signature_id="64784" signature="Microsoft SQL Server Unsupported Version Detection"

Below the event details, an "Event Actions" dropdown menu is open, with "Create notable event" highlighted by a red circle. The menu items are:

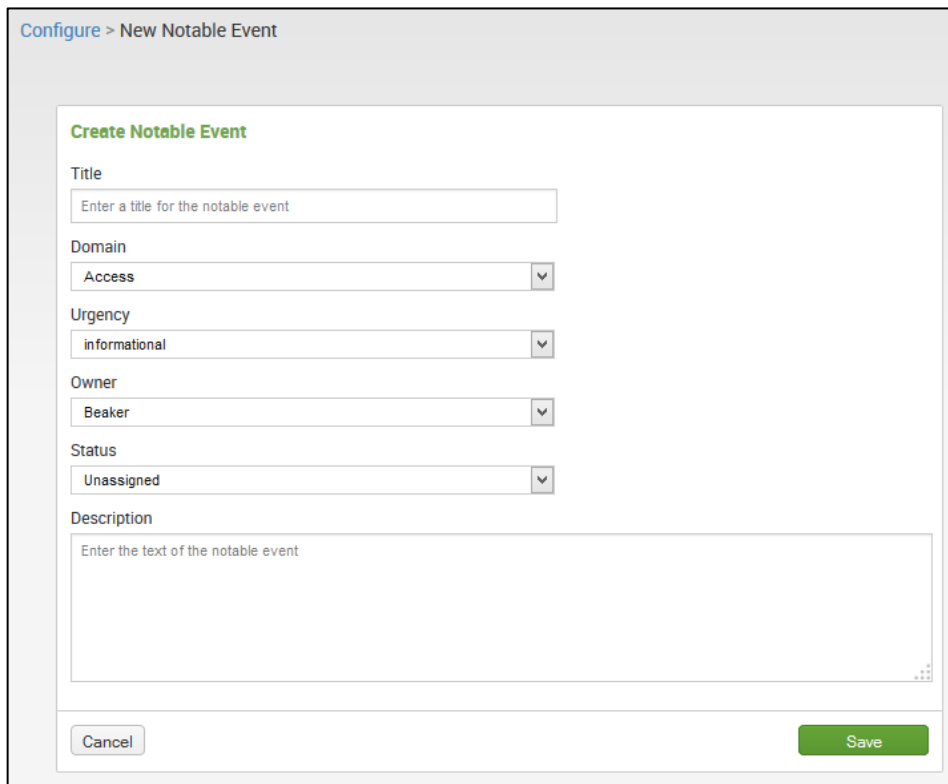
- Create notable event
- Build Event type
- Extract Fields
- Perform IPViking search for VSPHERE
- Perform IPViking search for unknown
- Perform IPViking search for telesto.procyonlabs.com
- Nessus Plugin Reference
- Show Source

At the bottom of the event details, there is a checkbox for "dest_is_expected" which is currently unchecked.

Value	Actions
telesto.procyonlabs.com	▼
/opt/splunk-vm/var/spool/splunk/Full_Scan_-_Windows_wimg	▼
t9.nessus	▼
nessus	▼
unknown	▼
10.0	▼
CVSS2#AV:N/AC:L/Au:N/C:I/C/A:C	▼
VSPHERE	▼
VSPHERE	▼
192.168.6.21	▼
false	▼

Managing Scanned Discoveries

This is where we begin to define properties to help us track the progress of this event.



The screenshot shows the 'Configure > New Notable Event' interface. It features a form titled 'Create Notable Event' with the following fields:

- Title:** A text input field with the placeholder text 'Enter a title for the notable event'.
- Domain:** A dropdown menu currently set to 'Access'.
- Urgency:** A dropdown menu currently set to 'informational'.
- Owner:** A dropdown menu currently set to 'Beaker'.
- Status:** A dropdown menu currently set to 'Unassigned'.
- Description:** A large text area with the placeholder text 'Enter the text of the notable event'.

At the bottom of the form, there are two buttons: 'Cancel' on the left and 'Save' on the right.

Managing Scanned Discoveries

Here we have done the following to create this event:

- Helpful title
- Specify domain
(ES treats vulnerability data by default as part of the “Network” domain. Yes, you can change this!)
- Select urgency
- Assign an owner
- Provide current status
- Add description of what you are doing.
This is time stamped and records the name of the editor

The screenshot shows the 'Configure > New Notable Event' interface. The form is titled 'Create Notable Event' and contains the following fields:

- Title:** Upgrade SQL Server on this machine!
- Domain:** Network (dropdown menu)
- Urgency:** high (dropdown menu)
- Owner:** Beaker (dropdown menu)
- Status:** In Progress (dropdown menu)
- Description:** Passed to Beaker for mitigation. (text area)

At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

Managing Scanned Discoveries

Once saved, we are immediately redirected to the Incident Review part of ES. Let's expand this event by clicking the > symbol on the left of it.

Incident Review

Urgency

- CRITICAL 0
- HIGH 1
- MEDIUM 0
- LOW 0
- INFO 0

Status: All

Name:

Owner: All

Security Domain: All

Time: Last 24 hours

Submit

1 event (9/22/14 2:00:00.000 AM to 9/23/14 2:18:27.000 AM)

Format Timeline | Zoom Out | Zoom to Selection

x Deselect | 1 hour per column

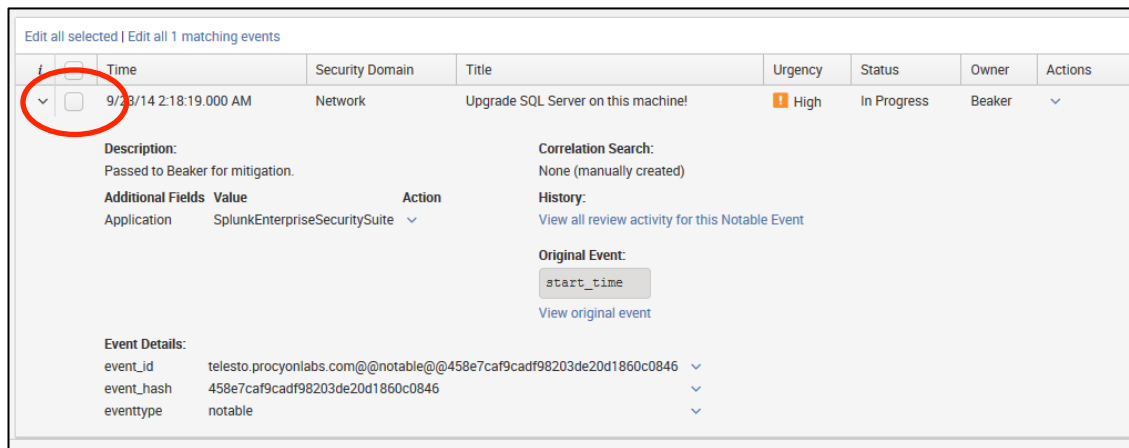
i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	9/23/14 2:18:19.000 AM	Network	Upgrade SQL Server on this machine!	High	In Progress	Beaker	▼

Managing Scanned Discoveries

Here, we have even more options.

Checking the edit box, and then clicking “Edit all selected” for this event allows us to perform more actions.

For example, once I receive verification that SQL Server was indeed upgraded, I can close out the case as shown on the next slide.



The screenshot shows a table with columns: i, Time, Security Domain, Title, Urgency, Status, Owner, and Actions. The first row is selected, and a red circle highlights the edit box (checkbox) in the 'i' column. Below the table, there are sections for Description, Correlation Search, Additional Fields, History, Original Event, and Event Details.

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
<input type="checkbox"/>	9/23/14 2:18:19.000 AM	Network	Upgrade SQL Server on this machine!	High	In Progress	Beaker	▼

Description:
Passed to Beaker for mitigation.

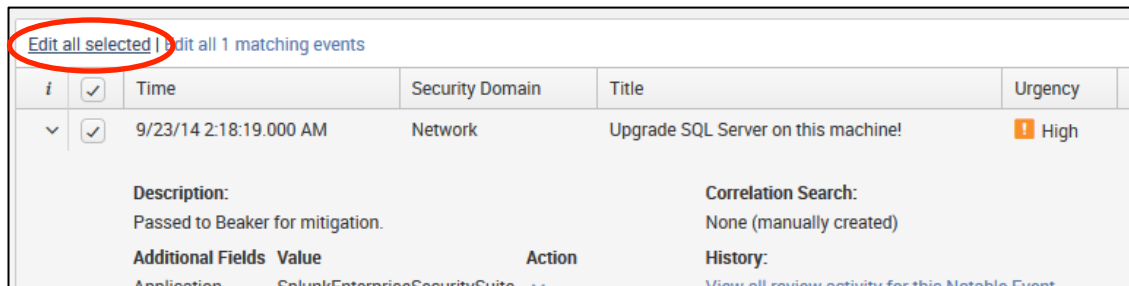
Correlation Search:
None (manually created)

Additional Fields

Value	Action
SplunkEnterpriseSecuritySuite	▼

Event Details:

event_id	telesto.procyonlabs.com@@notable@@458e7caf9cadf98203de20d1860c0846
event_hash	458e7caf9cadf98203de20d1860c0846
eventtype	notable



The screenshot shows the same table as the previous slide, but the edit box in the 'i' column is now checked. A red circle highlights the 'Edit all selected' link in the top left corner of the table.

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
<input checked="" type="checkbox"/>	9/23/14 2:18:19.000 AM	Network	Upgrade SQL Server on this machine!	High	In Progress	Beaker	▼

Description:
Passed to Beaker for mitigation.

Correlation Search:
None (manually created)

Additional Fields

Value	Action
SplunkEnterpriseSecuritySuite	▼

Event Details:

event_id	telesto.procyonlabs.com@@notable@@458e7caf9cadf98203de20d1860c0846
event_hash	458e7caf9cadf98203de20d1860c0846
eventtype	notable

Managing Scanned Discoveries

Edit Events

Status: Closed

Urgency:

Owner: Beaker

Comment: This has been fixed. We are now safe. Hurray!

Cancel Save changes

Once saved, the event is now closed.

It is important to note that ES is not currently designed to replace a dedicated issue tracking system. Splunk does interface with many popular applications, however.

Most of these solutions allow REST/API communications as well – simplifying the integration process.

Edit all selected | Edit all 1 matching events

<i>i</i>	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	9/23/14 2:18:19.000 AM	Network	Upgrade SQL Server on this machine!	High	Closed	Beaker	▼

Automating the Process

- Correlation Searches (rules) are awesome
- When a search correlates with parameters for time and throttling, a Notable Event can be automatically created
- Be aware that a poorly written one can rain havoc on your system and human resources – test, monitor and constantly evaluate your creations!





Let me show you how it's done...

Creating a Correlation Search

- If you are not watching this presentation at .conf2014, these slides will be your guide
- If you are at this talk, I will now switch to a live demonstration



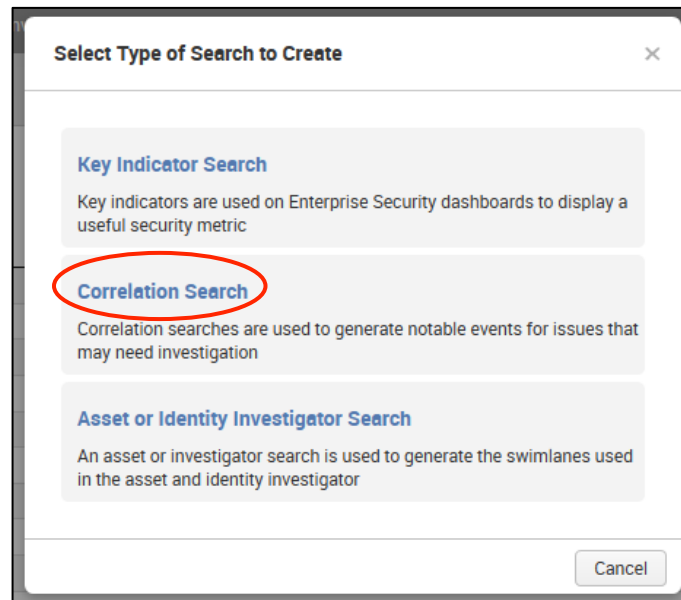
Let me show you how it's done...



Creating a Correlation Search

- From within the ES App, click on the Configure drop-down:
- Select General -> Custom Searches
- Click the green New button:
- When the pop-up for search types appears, select Correlation Search

Configure ▾



Let me show you how it's done...



Creating a Correlation Search

- For this example, we want to create a Notable Event from a Correlation Search that looks specifically for the following:
 - ✓ Vulnerability has a CVSS score of greater than 6
 - ✓ Host is our public Web server (192.168.3.5)
 - ✓ Check every hour for this occurrence
- When an event matching these parameters is detected, perform the following:
 - ✓ Create a Notable Event
 - ✓ Send email to responsible party

For more information:

<http://docs.splunk.com/Documentation/ES/latest/User/CreateCorrelationSearches>

Let me show you how it's done...



Creating a Correlation Search

Complete the form page like so (fields not used are omitted here) and save it. Also, the action to send an email upon a positive match is a good idea. System administrators love getting automated emails. Known fact.

Search Name: High CVSS Vulnerability on Public Server

Application Context: SA-NetworkProtection (the ES Security Domain for Vulnerabilities)

Search: tag=vulnerability cvss_base_score>6 dest_ip="192.168.3.5"

> NOTE: There is a "guided mode" to create the search, and it helps a lot!

Cron Schedule: 0 * * * *

> NOTE: Cron format is slightly cryptic. The style is: *minute hour day month day-of-week*

So, "0 * * * *" is every hour. The "0" means at the top of the hour. The asterisk in the hour field means every single hour.

In other words, every hour, on the hour.

Notable Event: Check the box (new fields appear)

Title: CVSS \$cvss_base_score\$ Vulnerability on \$dest_ip\$

Description: A vulnerability scan of the public Web server \$dest_ip\$ reported a CVSS \$cvss_base_score\$ vulnerability: \$signature\$

Security Domain: Network

Severity: high

Default Owner: Whoever the responsible person is

Default Status: New

.conf2014

YOUR DATA ADVENTURE

The Vulnerability
Data Model

splunk>

Data Model Overview

A data model in Splunk is a hierarchically structured, search-time mapping of semantic knowledge about one or more datasets that encode the domain knowledge necessary to generate specialized searches of those datasets. Splunk Enterprise uses these specialized searches to generate reports for Pivot users.

They enable users of Pivot to realize compelling reports and dashboards without having to write the searches that generate them. Data models are typically designed by Splunk Enterprise knowledge managers who understand the format and semantics of their data and the manner in which their Pivot users expect to work with that data.

Data models are constructed in the Data Model Editor. They are composed of hierarchies of data model objects.

They can use data model acceleration to improve the speed of the searches that drive the generation of Pivot tables and charts.

The Vulnerability Data Model

Objects	Vulnerabilities	
	Vulnerabilities	
EVENTS	CONSTRAINTS	
Vulnerabilities	tag=vulnerability tag=report	Constraint
- High Or Critical Vulnerabilities		
- Medium Vulnerabilities		
- Low Or Informational Vulnerabilities		
- Missing Extractions (S.o.S)		
SEARCHES	INHERITED	
Untagged Vulnerabilities (S.o.S)	<input type="checkbox"/> _time	Time
	<input type="checkbox"/> host	String
	<input type="checkbox"/> source	String
	<input type="checkbox"/> sourcetype	String
	EXTRACTED	
	<input type="checkbox"/> dest_bunit	String
	<input type="checkbox"/> dest_category	String
	<input type="checkbox"/> dest_priority	String
	<input type="checkbox"/> dvc_bunit	String
	<input type="checkbox"/> dvc_category	String
	<input type="checkbox"/> dvc_priority	String
	<input type="checkbox"/> tag	String
	<input type="checkbox"/> user	String
	<input type="checkbox"/> user_bunit	String

The Vulnerability Data Model

<input type="checkbox"/>	user_bunit	String	
<input type="checkbox"/>	user_category	String	
<input type="checkbox"/>	user_priority	String	
CALCULATED			
<input type="checkbox"/>	bugtraq	String	Eval Expression
<input type="checkbox"/>	category	String	Eval Expression
<input type="checkbox"/>	cert	String	Eval Expression
<input type="checkbox"/>	cve	String	Eval Expression
<input type="checkbox"/>	dest	String	Eval Expression
<input type="checkbox"/>	dvc	String	Eval Expression
<input type="checkbox"/>	msft	String	Eval Expression
<input type="checkbox"/>	mskb	String	Eval Expression
<input type="checkbox"/>	severity	String	Eval Expression
<input type="checkbox"/>	signature	String	Eval Expression
<input type="checkbox"/>	vendor_product	String	Eval Expression
<input type="checkbox"/>	xref	String	Eval Expression

Calculated attributes are processed in the order above, so ensure any dependent attributes are defined first. Drag to rearrange.

Questions?



.conf2014

YOUR DATA ADVENTURE

THANK YOU



beaker@splunk.com

splunk >