.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 vender 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

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.

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	cvss_base_score	9.3	
	host	telesto.procyonlabs.com	
	source	/opt/splunk-vm/var/spool/splunk/Full_Scan_-_Linux_6a4gjr.nessus	
	sourcetype	nessus	
Event	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	
	cvss_vector	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	
	dest	192.168.3.5	
	dest_asset_id	ab55803d42d270e688c6d82e3fc0da4bf3abef01	
	dest_asset_tag	should_update	
		iso27001	
		should_timesync	
		americas	
	host_is_expected	false	
	host_pci_domain	untrust	
	host_requires_av	false	
	host_should_timesync	false	
	host_should_update	false	
	idm_flags	001000	
	index	main	
	linecount	1	
	os	Linux Kernel 2.6.32-431.20.3.el6.i686 on Red Hat Enterprise Linux Server release 6.5 (Santiago)	
	product	Nessus	
	severity	high	
	severity_id	3	
	signature	RHEL 6 : java-1.7.0-openjdk (RHSA-2014:0889)	
	signature_family	Red Hat Local Security Checks	
	signature_id	76515	
	splunk_server	telesto.procyonlabs.com	
	start_time	Mon Sep 22 17:30:28 2014	
	tag	inventory	
		network	
		os	
		report	
		should_timesync	
		should_update	
		system	
		version	
		vulnerability	
	timestamp	none	
	transport	tcp	
	vendor	Tenable	
	xref	RHSA:2014:0889	

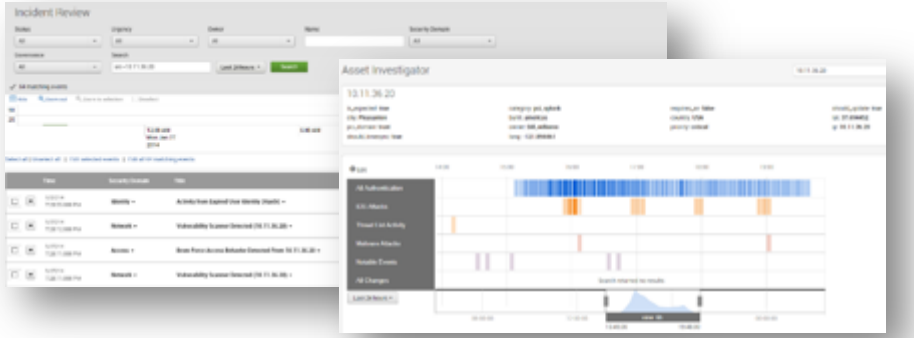
VM - The Splunk App for Enterprise Security Way

splunk>

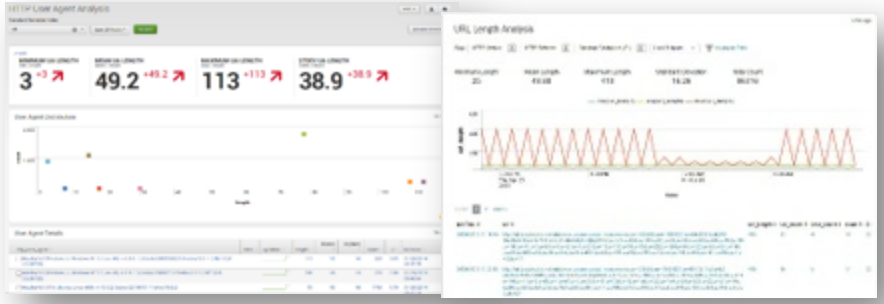
Splunk App for Enterprise Security

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

Dashboards and Reports



Incident Investigations & Management

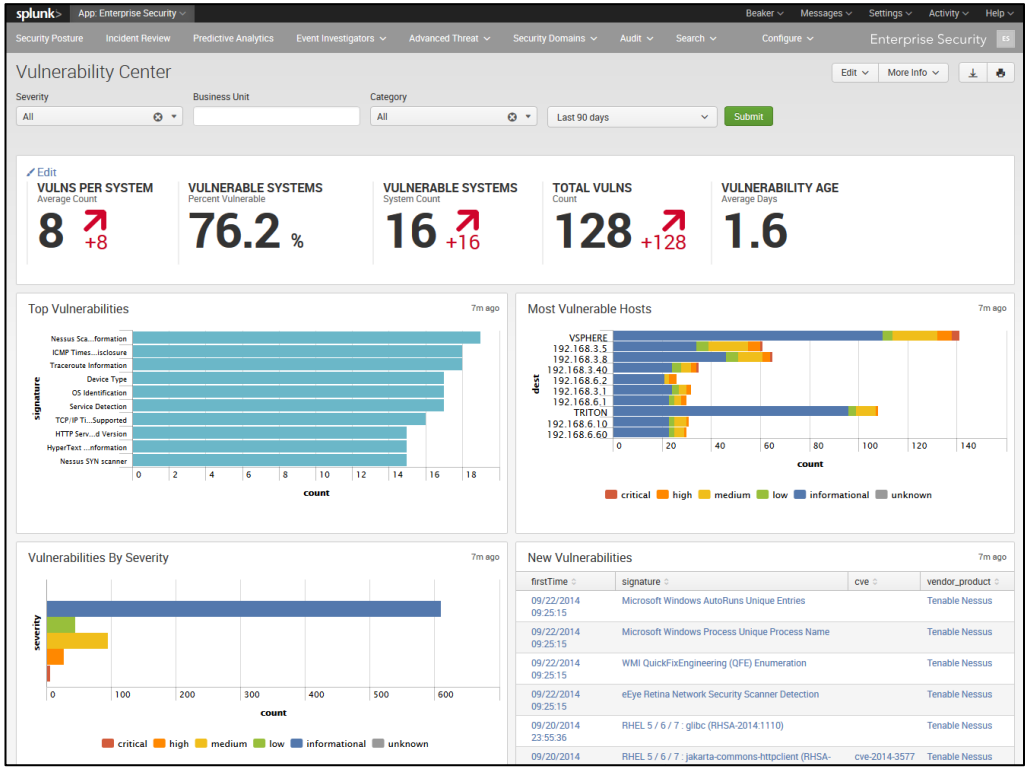


Statistical Outliers

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.



Use and Customization

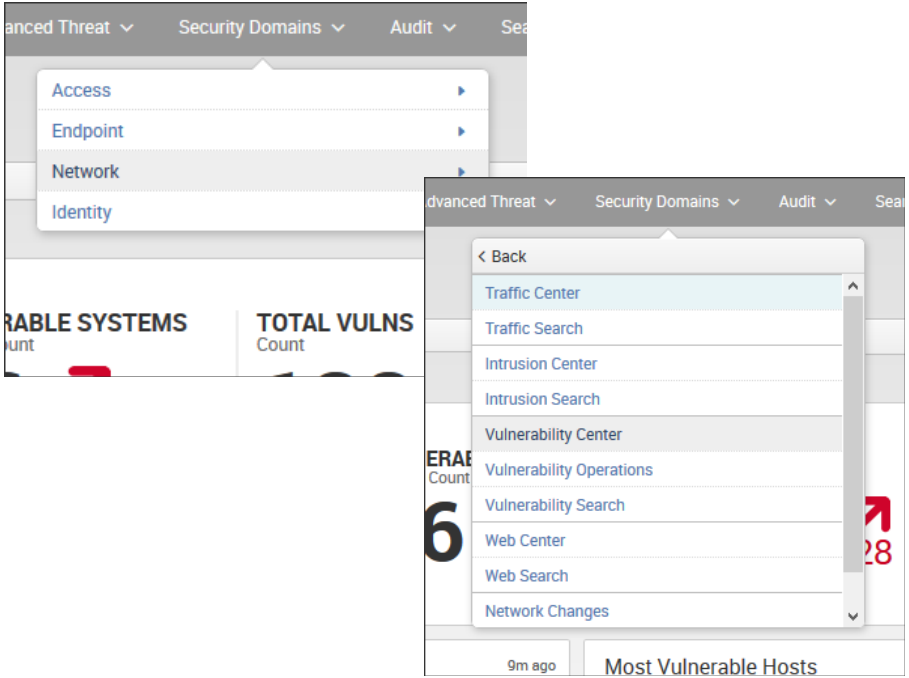
splunk>

Use and Customization

Security Domain: Network

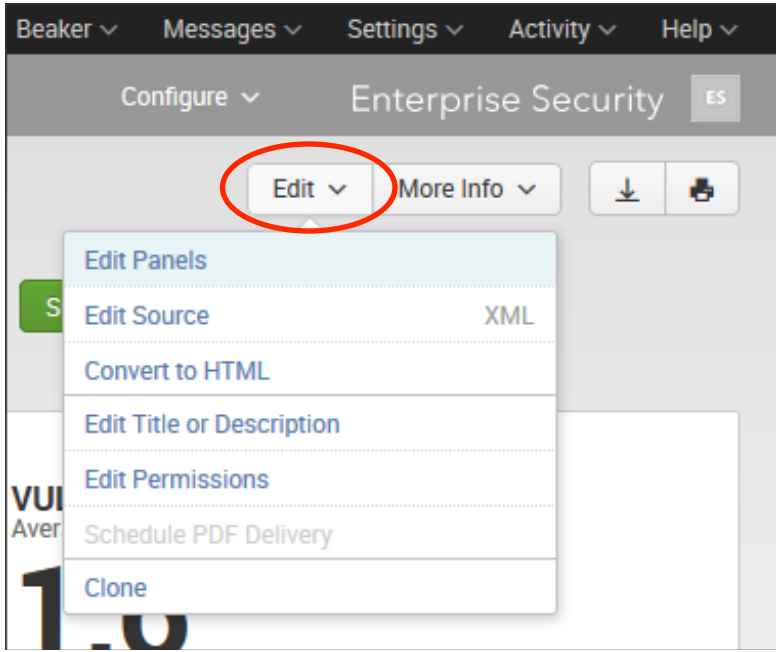
ES contains many areas of focus. For vulnerability management, we want to use the views and tools associated with the “Security Domains” drop down “Network,” which includes:

- Vulnerability Center
- Vulnerability Operations
- Vulnerability Search



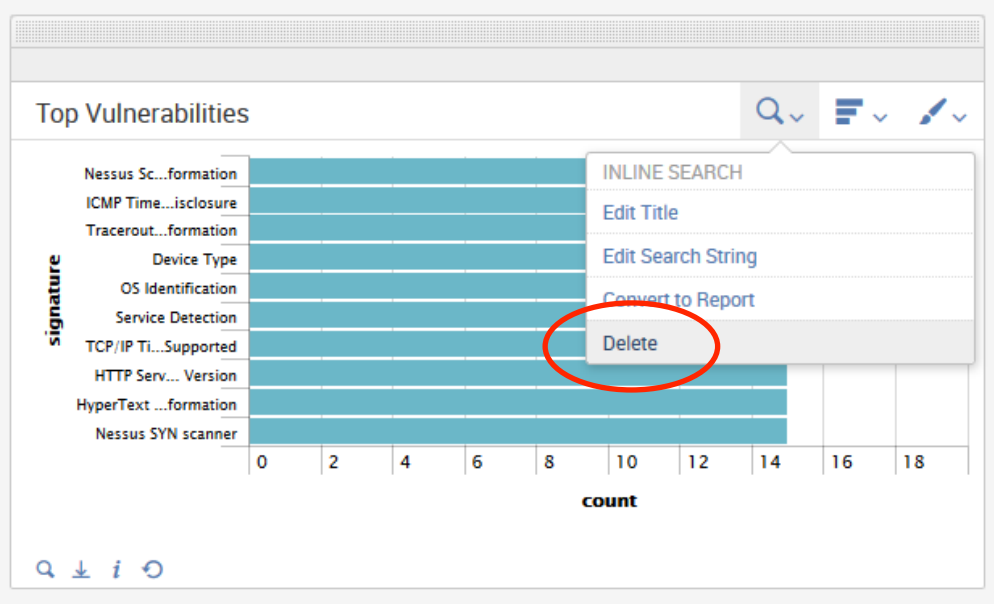
Use and Customization

- 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



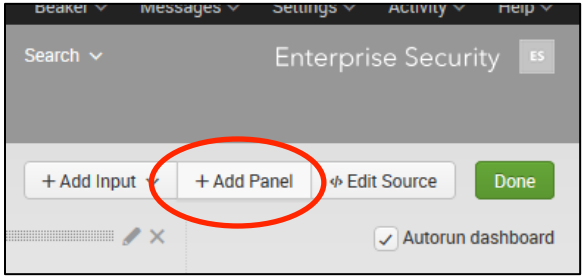
Panel Editing

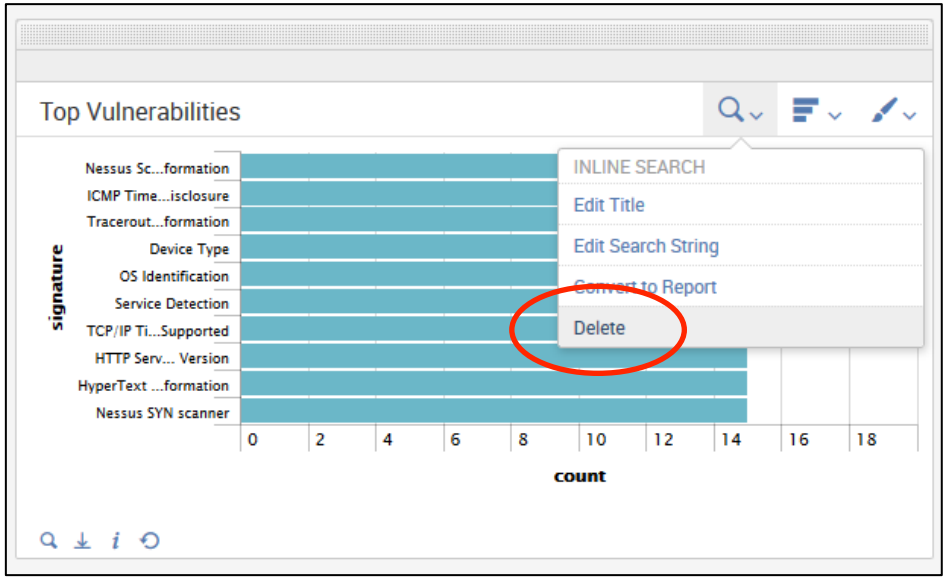
- First, let's delete the "Top Vulnerabilities" panel. We don't really care about that stuff anyway
- This frees up some precious real estate for the dashboard



Panel Editing

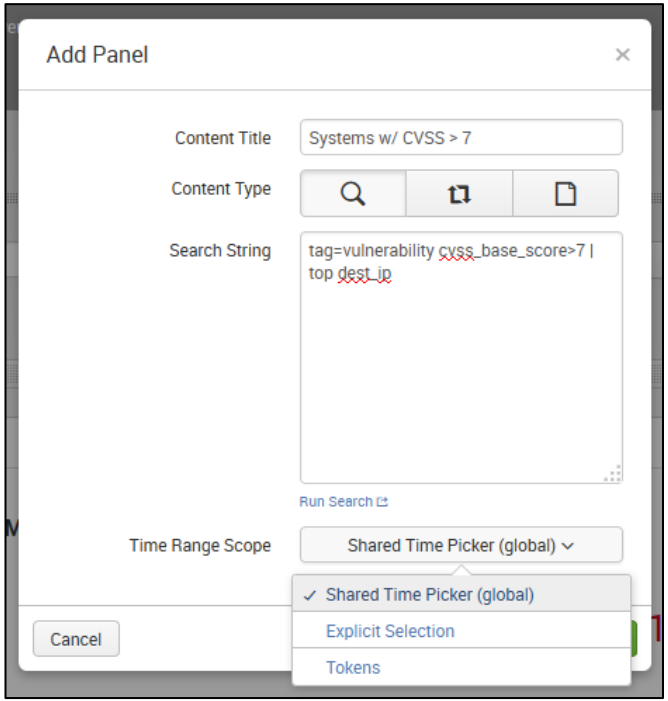
- First, let's delete the "Top Vulnerabilities" panel. We don't really care about that stuff anyway, and it frees up some precious real estate for the dashboard
- Next, click on "+ Add Panel"





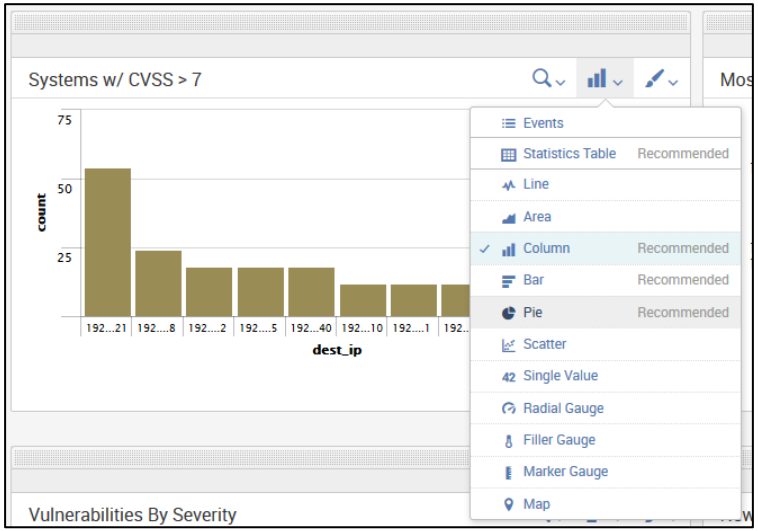
Panel Editing

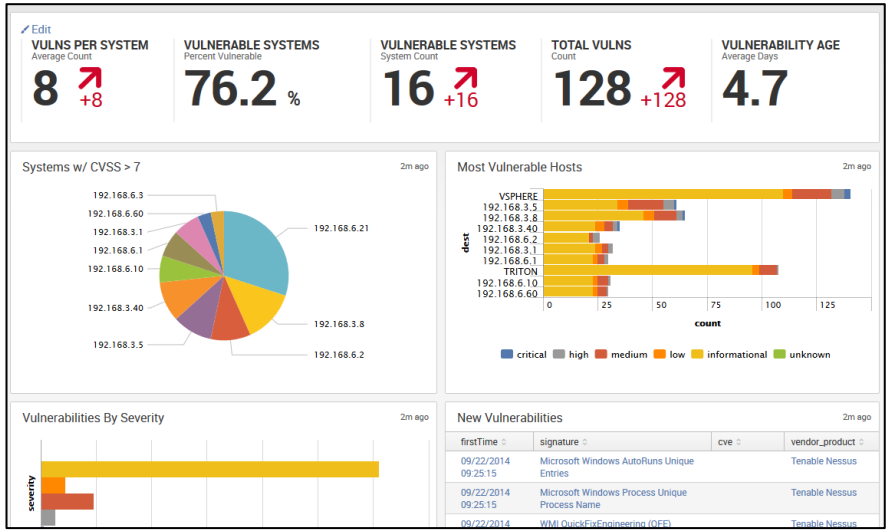
- Title the panel “Systems w/ CVSS > 7”
- Use the following Search String:
  `tag=vulnerability cvss_base_score>7 | top dest_ip`
- Time Range Scope should be “Shared Time Picker (global)”
  - This uses the time selection set for the entire view in the header/search area
- Click Save
- It is now added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



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



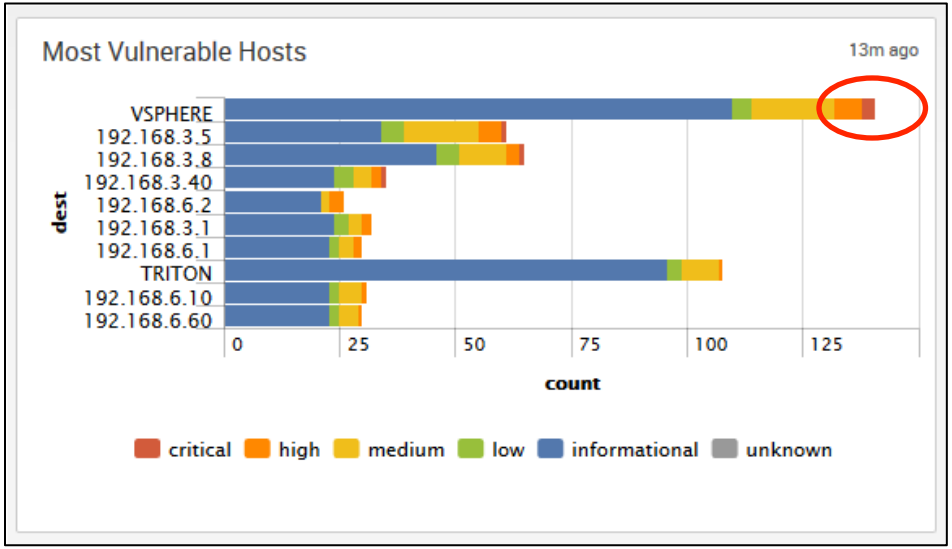


Working With and Alerting On Events

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

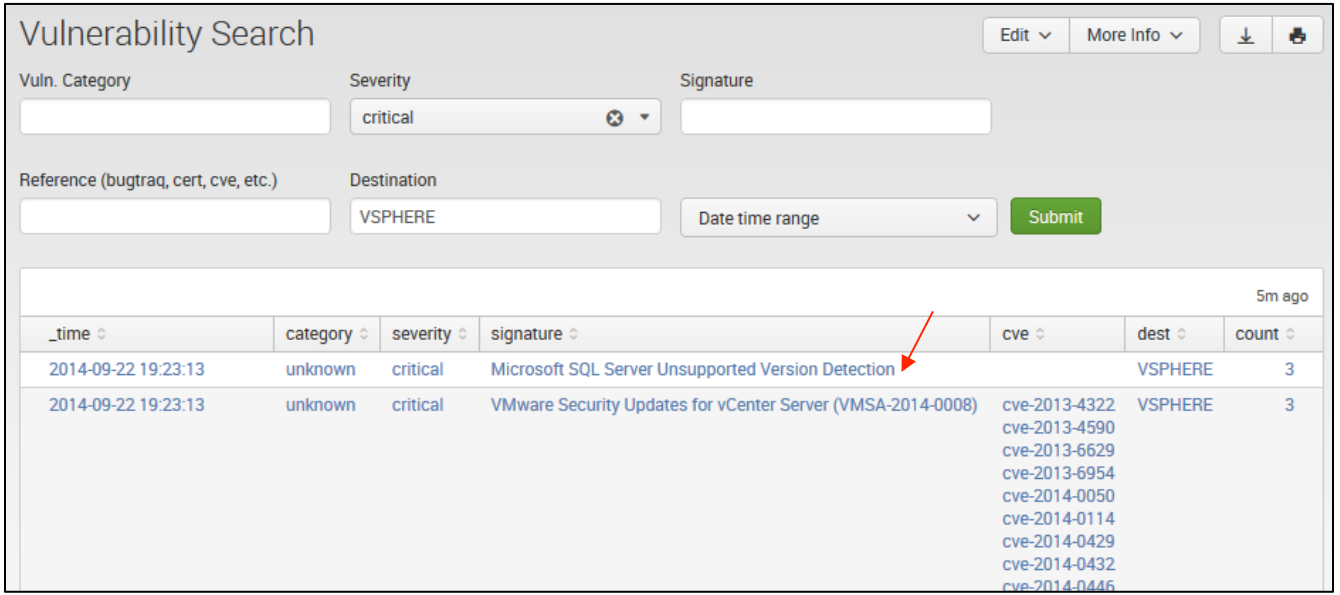


Managing Scanned Discoveries

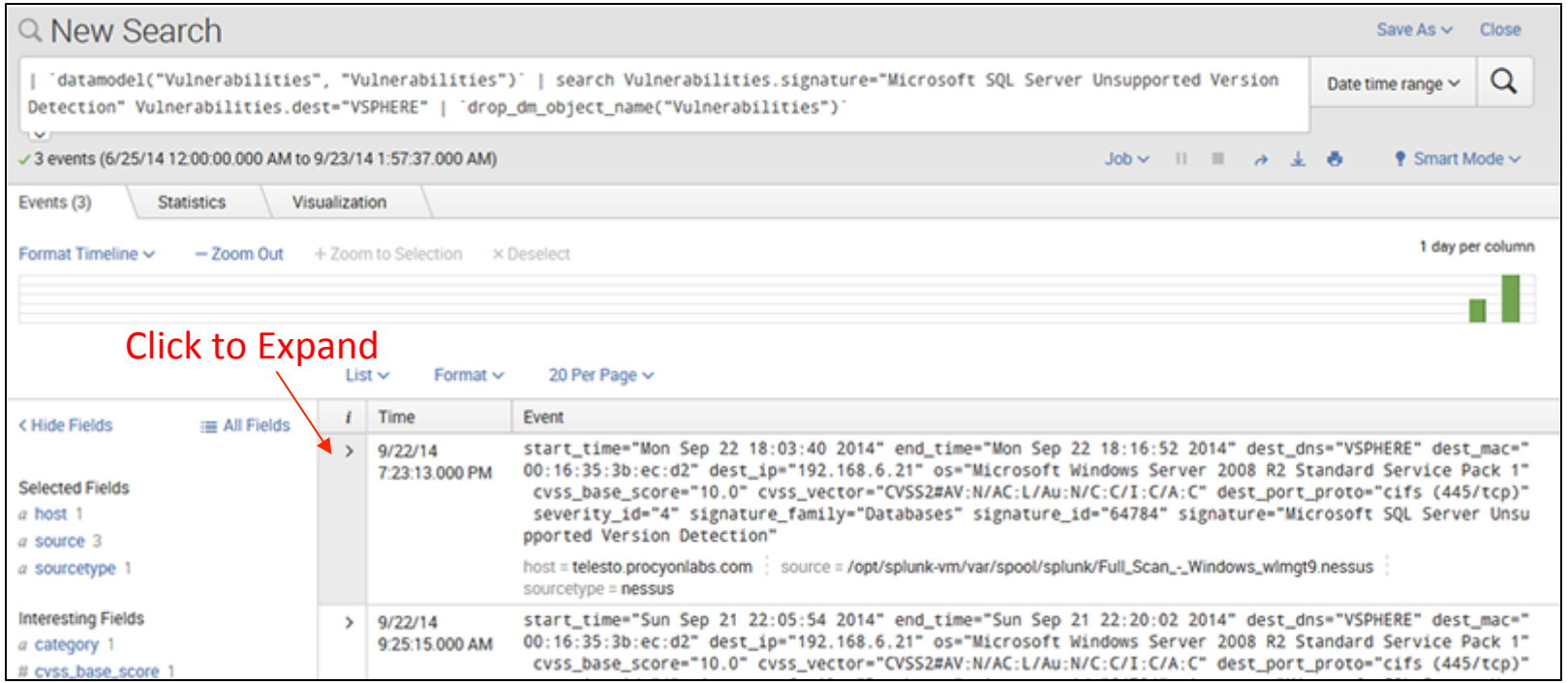
Creating Alerts from Vulnerabilities

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.

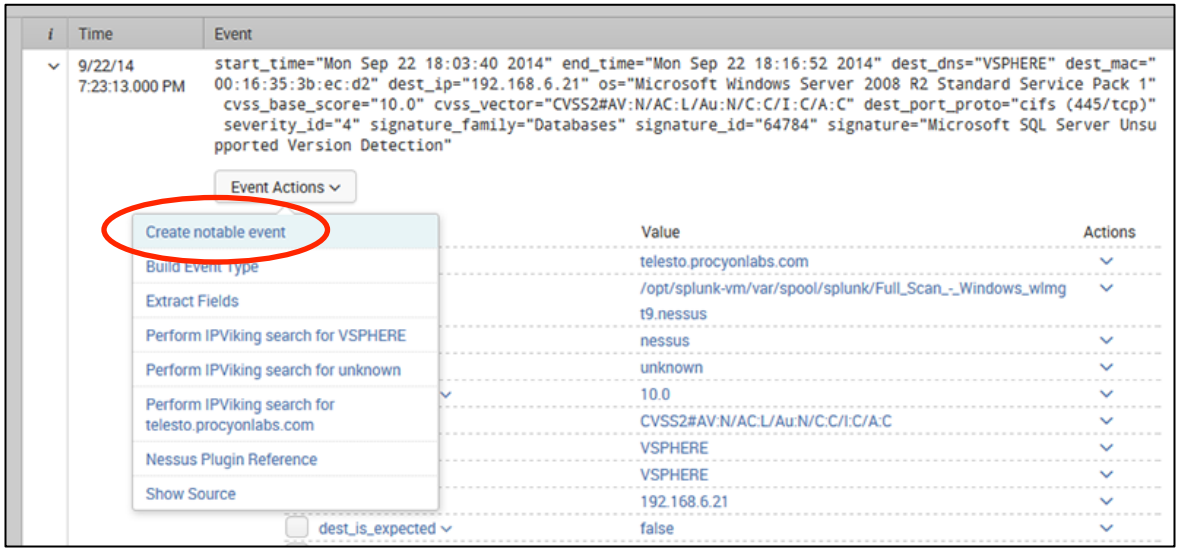


Managing Scanned Discoveries



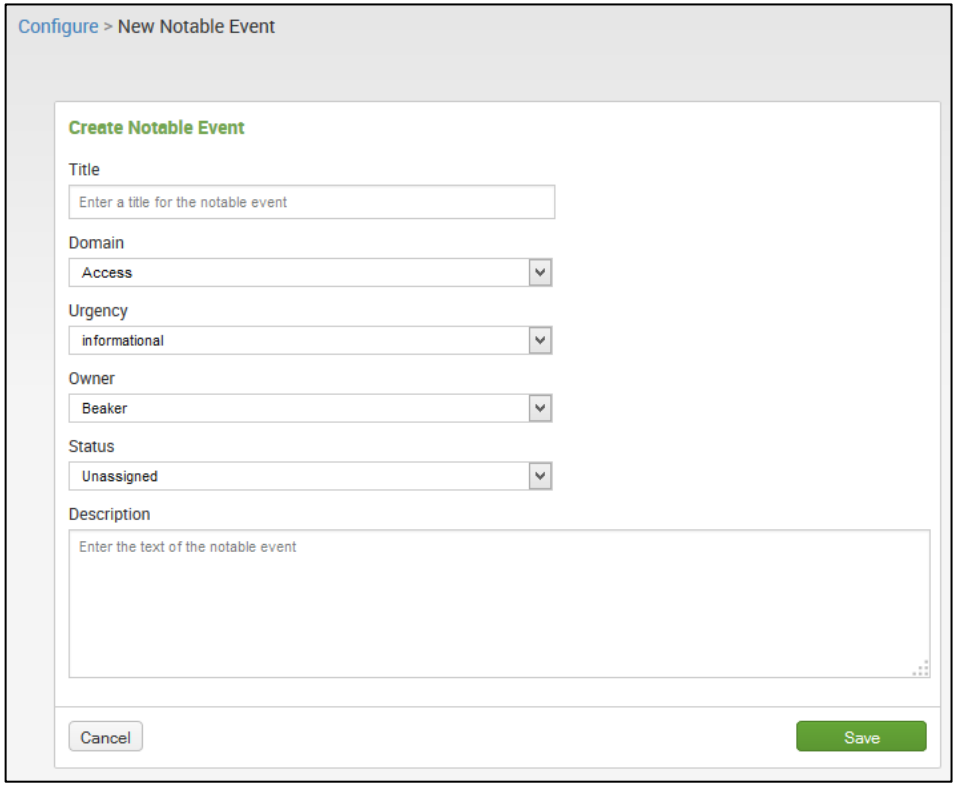
Managing Scanned Discoveries

- 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



Managing Scanned Discoveries

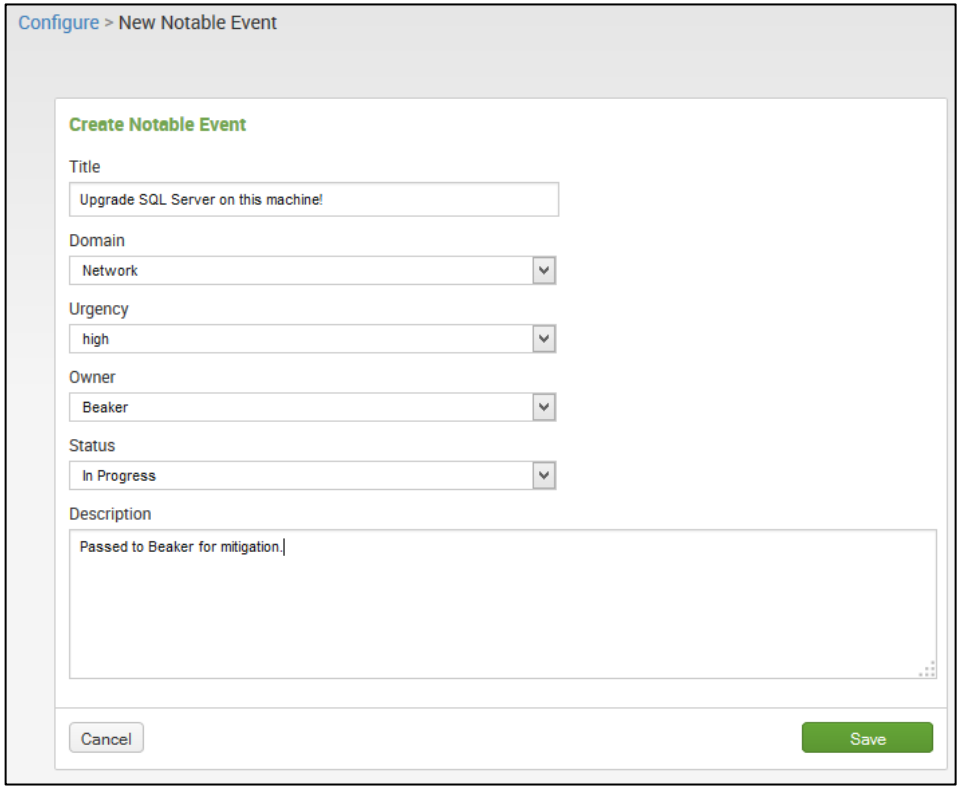
This is where we begin to define properties to help us track the progress of this event.



Managing Scanned Discoveries

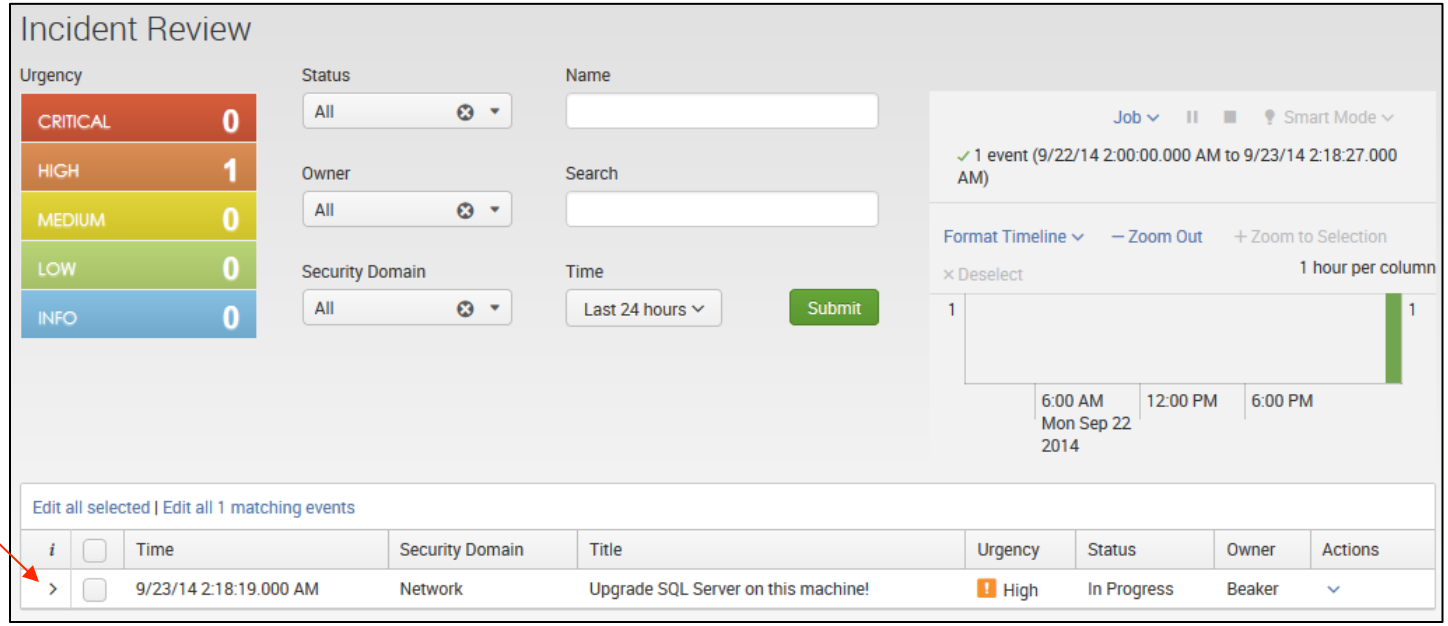
Here we have done the following to create this event:

- 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



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.

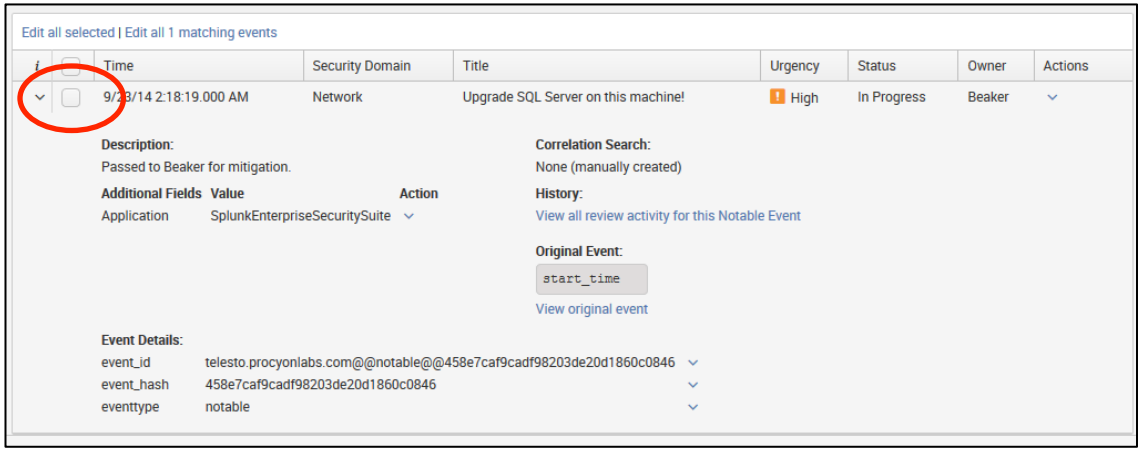


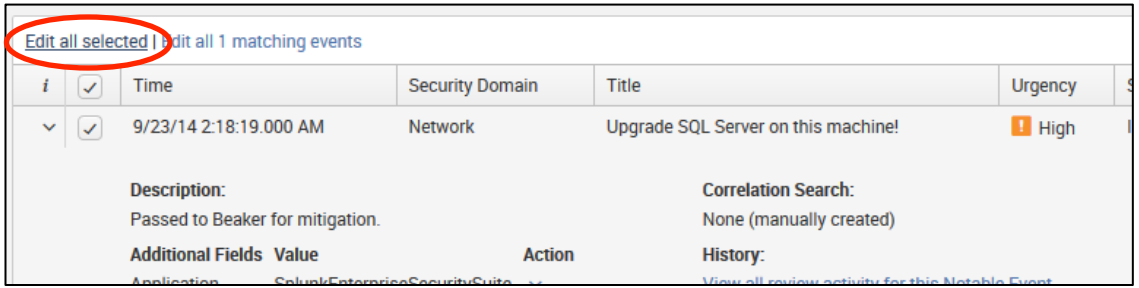
Managing Scanned Discoveries

Here, we have even more options.

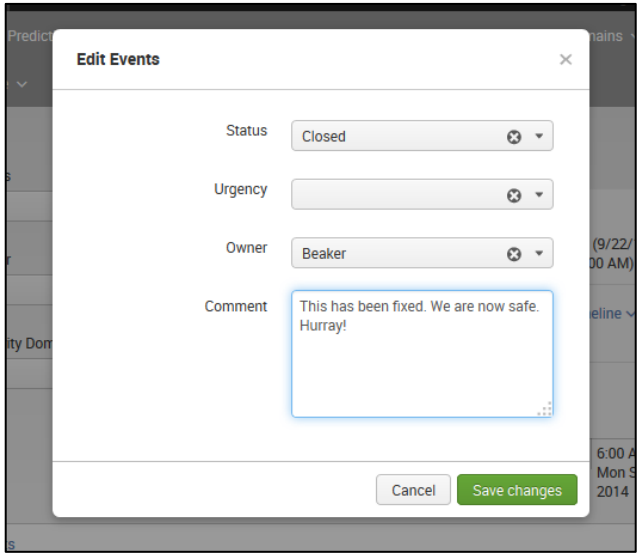
Checking the edit box, and then clicking “Edit all selected” for this event allows us to perform more actions.

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





Managing Scanned Discoveries



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	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	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!

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

Creating a Correlation Search

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

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 occurence

- 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

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 Vulnerabilies)
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

The Vulnerability Data Model

splunk>

Data Model Overview

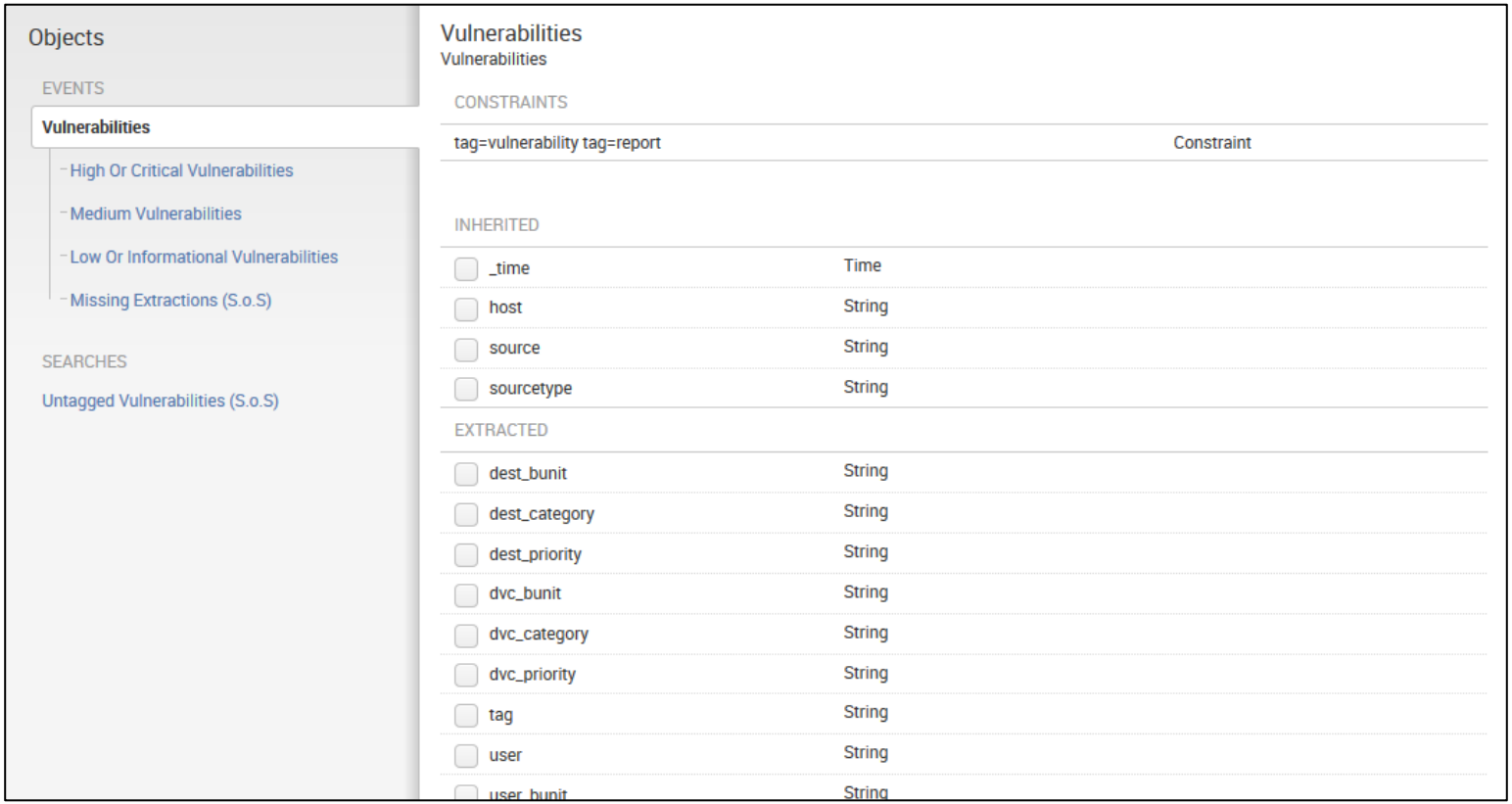
A data model in Splunk is a hierarchically structured, search-time mapping of semantic knowledge about one or more datasets that encode the domain knowledge necessary to generate specialized searches of those datasets. Splunk Enterprise uses these specialized searches to generate reports for Pivot users.

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



The Vulnerability Data Model

user_bunit	String	
user_category	String	
user_priority	String	
CALCULATED		
bugtraq	String	Eval Expression
category	String	Eval Expression
cert	String	Eval Expression
cve	String	Eval Expression
dest	String	Eval Expression
dvc	String	Eval Expression
msft	String	Eval Expression
mskb	String	Eval Expression
severity	String	Eval Expression
signature	String	Eval Expression
vendor_product	String	Eval Expression
xref	String	Eval Expression

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


Questions?

THANK YOU

beaker@splunk.com

splunk>