



.conf2015

Learn How to Build Powerful Correlation Searches in Splunk Enterprise Security With Extreme Search

Macy Cronkrite

Professional Services, Splunk

Jack Coates

Product Management, 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 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

- Macy Cronkrite, Splunk
- Professional Service Consultant
- Public Sector Team
- Chief Meme Officer
- Jack Coates, Splunk
- Director of PM
- ES PM, 2.0 to 3.0
- Now focused on
“Getting Data In
and Out”
 - Add-ons, Utilities,
& Other



Big Data, Analytics, and Security

“We talk about the need for analytics and business intelligence to help the business make better business decisions. It is time to bring this same technology to the information security department.

What we need is **actionable, prioritized and risk-based insight** from this sea of information. There are some emerging uses cases for information security which can only be handled with big data capabilities.”



Information Security is Becoming a Big Data Problem,
Neil MacDonald, Gartner, April 12, 2011

Agenda

- How correlations work in Enterprise Security:
 - Common Information Model
 - Assets and Identities
 - Risk Scoring Framework
- What is Extreme Search
 - Concepts and Contexts
 - Use human semantic phrases to frame security questions
- EXTREEEMEMEMEEEEEEEEE
 - Discover and Manage security trends
 - Assess changes to enterprise risk exposure by segments of assets and users.

Splunk for Enterprise Security 3.3+

Foundational Knowledge of Enterprise environment

- Common Information Model
- Assets
- Identities
- Risk Framework
- Security Posture Domains – Access, Endpoint, Network, Threat



Extreme Search – A Concept

Qualitative Semantic Term

- A concept is a "Qualitative Semantic Term"... meaning a rich descriptive adjective or adverb that is associated with a field
- A "Semantic Term" comes from data models... the attributes (fields) of a data model are also known as Semantic Terms
- Concepts add qualitative descriptions to these attributes

Extreme Search – A Context

- A collection of concepts that are applied to a field (attribute) is known as a context

Data Models – Semantic Concepts

- The fields of an event (or a data model) are called attributes or Semantic Terms>>>
- If you want some descriptive term for a field, you create a concept.... (a concept is also known as a qualitative semantic term)
- A collection of concepts that describe a field is known as a context

Context Types

Data, User, Anomaly, Crossover

- Contexts can model different types of data.... they can be:
- Data Driven: run calculations against real data to build/update a context
- User Defined: build a context based on what you *think* the data distribution should be
- Anomaly Driven: build a context based on what value are outliers vs what values are typical
- Crossover Driven: build a context based on the "crossover" points.. usually generated by statistics
- These contexts are reduced models of large volumes of data...
- To use all this, you can create conceptual searches....

Not Your Boo

- NOT BOOLEAN
- A boolean query says "show me all of the events that MATCH this query"
- A conceptual query says "show me all of the events that are COMPATIBLE WITH this query"
- This is a key difference... compatibility gives you a range...

STD DEV is ok Not Great

- For example, you might want to get all of the events with a high std dev.
- A boolean query might be "| where stdev is >= 2.0"
- If your std dev is 1.97, it's not 2, so any std dev not at least 2.0 will fail...
- However, with a conceptual query, that wouldn't be the case
- A conceptual query might be "| xsWhere stdev is at least 2.0"
- All of the events that are COMPATIBLE with this query are returned, with a new field added, xsWhereCIX

XS WHERE CIX COMPATIBLE

- xsWhereCIX Is the number that shows how compatible an event is with the query, so you can rank the results if necessary
- A better conceptual query might be "... | xsWhere stddev is at least high"
- Why use this? because what you're really asking for is "show me all the events that have a high standard deviation"

EXTREEEEMEEEEEEE!!!!

- | tstats allow_old_summaries=true count from datamodel=Intrusion_Detection by IDS_Attacks.signature
- | `drop_dm_object_name("IDS_Attacks")`
- | xswhere count from count_by_signature_1h in ids_attacks by signature is above medium
- This says show me all of the signatures over the last hour where the count by signature is above medium
- The query is different from a boolean query

MALWARE

NO BOOLEAN HERE BABY

- You can create different contexts based on different values of fields in an event.... for example, you might create a Context that describes the count of malware violations per day (signature_count_1d)....
- However, there are many different types of signatures and each can have a different range of values...
- So, you can create a different Context based on the value of the field "signature"... that lets you measure qualitatively the level of severity of a malware infestation based on the malware signature....
- A higher number of one type of malware may be more or less severe than another type of malware
- This type of context creation is known as Object Classification
- You classify which context to use based upon the value of an attribute (or field) in an event...
- If malware signature is X, then use the context signature_count_1d/X
- If malware signature is Y, then use the context signature_Count_1d/Y
- The value of malware_signature is different for each event
- Contexts are data reduction tools...
- A context models the data distribution of a field over time by class
- You can take millions of events and create/update contexts to reflect these data values...
- Contexts are small in size
- Contexts can be used on indexers and/or search heads
- Context query commands (xsWhere, xsFindBestConcept) are streaming commands
- This is important because you want to leverage the architecture that splunk provides to get the best performance possible

Questions?



.conf2015

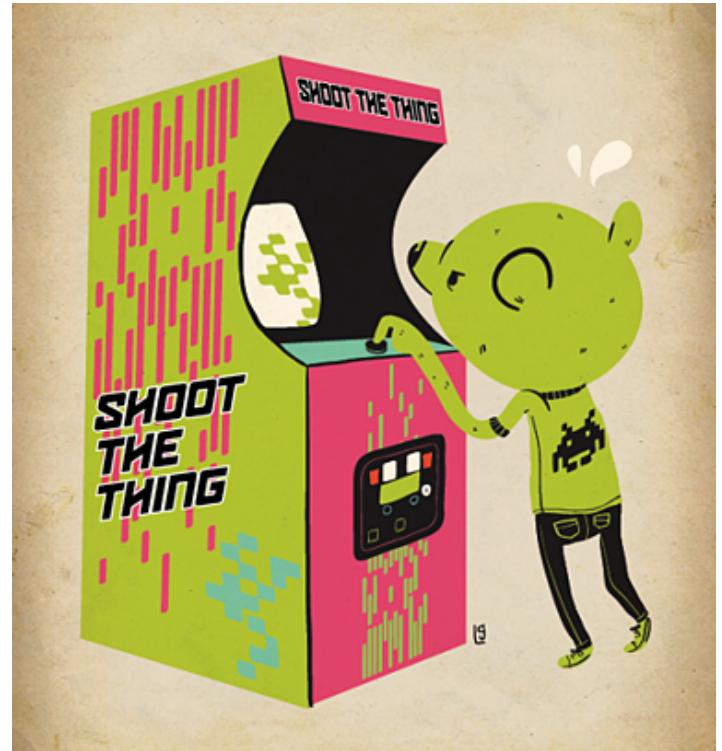
Exercise 1

A Simple Rule

splunk>

Simple Detection

- Name=WZCSV
- Name=WZCSV State=Running
- Name=WZCSV State=Running host_priority=critical
- Name=WZCSV State=Running host_priority=critical host_category=*pci*
- Simple searches can simply be pasted into the Correlation Search Editor form
- Add macros to enrich the event: `get_event_id` | `map_notable_fields`



Correlation Search Editor Fields

- **Correlation Search Name:** A name, such as “My Search”. It will be automatically prepended with the Domain and appended with “– Rule”
- Drill down and throttle by should be discussed





.conf2015

Exercise 2 Correlate Within A Domain

splunk®

Correlate in place

- **Brute Force Access**
- `authentication by action | s

Does this search need updating?

src
s>0

The Correlation Three Step

- Gather a pool of data
- Use a table to form the data for easy numeric tests
- Perform tests to make decisions



Step 1: Gather a Pool of Events

- `authentication`

- Like most Enterprise Security Correlation Searches, this search uses a macro to simplify the final syntax.
- Macros definitions may be found at **Manager > Advanced Search > Search Macros**.
- tag=authentication NOT (action=success user=*\$) | fillnull value=unknown
action,app,src,src_user,dest,user
- `authentication` returns raw events:

```
1 4/30/12      04/30/2012 11:46:04 AM
   11:46:04.000 AM LogName=Security
   EventCode=529
   EventType=16
   Type=Failure Audit
   SourceName=Security
   RecordNumber=999927617
   Category=2
   CategoryString=Logon/Logoff
   ComputerName=HOST-001
   Show all 28 lines
host=HOST-001 | sourcetype=WinEventLog:Security | source=WinEventLog:Security | signature=Unknown user name or bad password | user=Hax0r
```

Step 2: Tabulate the Events for Comparison

- The chart command is then used to tabulate raw events for comparison
- `authentication` | chart count over src by action

	src ↴	failure ↴	success ↴	unknown ↴
1	10.11.36.1	5	2	0
2	10.11.36.2	6	1	0
3	10.11.36.3	2	2	0
4	10.11.36.4	3	4	0
5	10.11.36.5	1	2	0
6	10.11.36.6	8	4	0
7	10.11.36.7	0	1	0
8	10.11.36.8	4	1	0
9	10.11.36.9	5	2	0
10	10.11.36.10	3	1	0

Step 3: Make a Go/No-Go Decision

- The final search command filters to patterns that are worth human attention
- `authentication` | chart count over src by action | search failure>6 success>0
- Over longer time periods, the search may generate many events

18 results in the last 24 hours (from 12:00:00 PM April 29 to 12:16:36 PM April 30, 2012)

	src	failure	success	unknown
1	10.11.36.1	7	3	0
2	10.11.36.2	9	1	0
3	10.11.36.6	12	7	0
4	10.11.36.9	8	2	0
5	10.11.36.13	9	2	0
6	10.11.36.14	7	2	0
7	10.11.36.17	13	1	0
8	10.11.36.20	277	93	0
9	10.11.36.27	9	2	0
10	10.11.36.33	8	1	0

« prev 1 2 next »

Manage Load with Ranges and Throttles

- Use time windows and throttling to prevent duplications or noise

Time range

Start time (optional) Finish time (optional)

Time specifiers: y, mon, d, h, m, s
[Learn more](#)

Throttling

Window Duration

Time specifiers: y, mon, d, h, m, s

Fields to Group By add a field followed by a comma

Select	Options	Time	Security Domain	Title	Urgency	Status	Owner	
<input type="checkbox"/>	<input type="button" value="▼"/>	4/30/12 8:20:55.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.20	! Critical	New	unassigned	Hide details
<p>Description: The system 10.11.36.20 has failed authentication 32 times and successfully authenticated 11 times in the last hour</p> <p>Additional Fields:</p> <p>Source: 10.11.36.20 Source Business Unit: americas Source Category: splunk Source City: Pleasanton Source Country: USA Source IP Address: 10.11.36.20 Source Expected: true Source Latitude: 37.694452 Source Longitude: -121.894461 Source Owner: Bill_williams Source Should Time Synchronize: true Source Should Update: true</p>					<p>Correlation Search: Access - Brute Force Access Behavior Detected - Rule</p> <p>History: View all review activity for this Notable Event</p> <p>Contributing Events: View all login attempts by system 10.11.36.20</p>			
<p><input checked="" type="checkbox"/> Valid: event_id=sc-essdemo.sv.splunk.com@@notable@@479a3a042aa9750657acd157542d278e event_hash=479a3a042aa9750657acd157542d278e eventtype=suppress_src eventtype=notable</p>								



.conf2015

Exercise 3 Correlate Across Multiple Domains

splunk®

Advanced Correlation Searches

- The most challenging and useful correlation searches will leverage multiple sources of information

Should this be merged with the CIM based version?

Access Information – which user accounts are accessing which machines?

Asset and Identity Information – which users and machines are most critical?

Endpoint Information – which machines are currently infected with malware?

Did a high or critical priority user log into an infected machine?



Step One: Authentications

- `authentication` macro gives all access events, but we're only looking for successful authentications... so we copy it and modify it
- **tag=authentication action=success**

511 events in the last 24 hours (from 10:00:00 AM April 29 to 10:54:05 AM April 30, 2012)			
1	 4/30/12 10:45:29.000 AM	04/30/2012 10:45:29 AM LogName=Security SourceName=Security EventCode=552 EventType=8 Type=Success Audit ComputerName=HOST-001 User=SYSTEM Sid=S-1-5-18 SidType=1 Show all 43 lines	« prev 1 2 3 4 5 6 7 8 9 10 next » 10 per page ▾
2	 4/30/12 10:45:18.000 AM	04/30/2012 10:45:18 AM LogName=Security SourceName=Security EventCode=552 EventType=8 Type=Success Audit ComputerName=HOST-001 User=SYSTEM	

Step Two: Priorities

- We have two useful fields to look at in this case, so an OR is used
 - (tag=authentication action=success (user_is_privileged="true" OR user_priority="critical" OR user_priority="high"))

157 events in the last 24 hours (from 10:00:00 AM April 29 to 10:56:02 AM April 30, 2012)

			Export	Options	« prev	1	2	3	4	5	6	7	8	9	10	next »	10 per page ▾
1	4/30/12 10:45:29.000 AM	04/30/2012 10:45:29 AM LogName=Security SourceName=Security EventCode=552 EventType=8 Type=Success Audit ComputerName=HOST-001 User=SYSTEM Sid=S-1-5-18 SidType=1 Show all 43 lines host=HOST-001 sourcetype=WinEventLog:Security source=WinEventLog:Security															
2	4/30/12 10:45:18.000 AM	04/30/2012 10:45:18 AM LogName=Security SourceName=Security EventCode=552 EventType=8 Type=Success Audit ComputerName=HOST-001 User=SYSTEM															

Step Three: Malware

- The `malware` macro provides useful guidance...
- (tag=malware tag=attack action=allowed)

1,437 events in the last 24 hours (from 11:00:00 AM April 29 to 11:02:13 AM April 30, 2012)

			Export	Options	« prev	1	2	3	4	5	6	7	8	9	10	next »	10 per page ▾
1	 4/30/12 10:16:38.000 AM	04/30/2012 10:16:38 AM LogName=Application SourceName=Trend Micro OfficeScan Server EventCode=10 EventType=2 Type=Warning ComputerName=ACMETREND1 User=SYSTEM Sid=S-1-5-18 SidType=1 Show all 18 lines host=sc-essdemo.sv.splunk.com sourcetype=WinEventLog:Application:trendmicro source=WinEventLog:Application															
2	 4/30/12 10:16:11 AM	04/30/2012 10:16:11 AM LogName=Application SourceName=Trend Micro OfficeScan Server EventCode=10 EventType=2 Type=Warning ComputerName=ACMETREND1 User=SYSTEM															

Step Four: Access OR Malware OR Privilege

- Construct the total pool of data to make decisions from
 - (tag=authentication action=success (user_is_privileged="true" OR user_priority="critical" OR user_priority="high")) OR (tag=malware tag=attack action=allowed) | tags outputfield=tag | eval group=case(tag=="authentication", "authentication", tag=="malware", "malware")

1,594 events in the last 24 hours (from 11:00:00 AM April 29 to 11:12:39 AM April 30, 2012)

Step Five: Normalize Results

- All the expected fields might not be there in source data, so use evals to fill in with something sensible
- ```
(tag=authentication action=success (user_is_privileged="true" OR user_priority="critical" OR user_priority="high")) OR (tag=malware tag=attack action=allowed) | tags outputfield=tag | eval group=case(tag=="authentication","authentication",tag=="malware","malware") | eval user;if(tag=="malware",null(),user) | eval signature;if(tag=="authentication",null(),signature)
```



# Step Six: Wonder Twins, Form of Table!

- Tabulate the fields that the decision will be made from
- (tag=authentication action=success (user\_is\_privileged="true" OR user\_priority="critical" OR user\_priority="high") ) OR (tag=malware tag=attack action=allowed) | tags outputfield=tag | eval group=case(tag=="authentication","authentication",tag=="malware","malware") | eval user=if(tag=="malware",null(),user) | eval signature=if(tag=="authentication",null(),signature) | stats values(user) as user,values(signature) as signature,dc(group) as group\_count by dest

55 results in the last 24 hours (from 11:00:00 AM April 29 to 11:18:14 AM April 30, 2012)

Export Options

« prev 1 2 3 4 5 6 next » 10 per page

Overlay: None

| dest :          | user : | signature :                         | group_count : |
|-----------------|--------|-------------------------------------|---------------|
| 1 10.11.36.20   |        | Adware.Hotbar                       | 1             |
| 2 ACME-003      |        | Trojan.Vundo                        | 1             |
| 3 ACME-006      |        | SecurityRisk.eGatherer              | 1             |
| 4 ACME-CA0382FD |        | WORM_SOHANAD.WP                     | 1             |
| 5 ACME-FE50DB   |        | TROJ_BREDO.SMGS<br>TROJ_FAKELRT.SMT | 1             |
| 6 ACMETREND     | root   |                                     | 1             |
| 7 ACMETREND1    | root   |                                     | 1             |
| 8 BEE           |        | Mal_Hifrm                           | 1             |
| 9 BENNETTG2     |        | TROJ_FAKEAV.SMBG                    | 1             |
| 10 BLACKTOP     |        | TROJ_FAKEAV.SMZQ                    | 1             |

# Step Seven: Detect the Condition

- group\_count field > 1 is bad
- (tag=authentication action=success (user\_is\_privileged="true" OR user\_priority="critical" OR user\_priority="high") ) OR (tag=malware tag=attack action=allowed) | tags outputfield=tag | eval group=case(tag=="authentication","authentication",tag=="malware","malware") | eval user=if(tag=="malware",null(),user) | eval signature=if(tag=="authentication",null(),signature) | stats values(user) as user,values(signature) as signature,dc(group) as group\_count by dest | search group\_count>1

1 result in the last 24 hours (from 11:00:00 AM April 29 to 11:23:42 AM April 30, 2012)

Export Options

10 per page ▾

Overlay: None

|   | dest     | user | signature | group_count |
|---|----------|------|-----------|-------------|
| 1 | HOST-006 | drew | TSPY_ZBOT | 2           |

# Plug it into the Search Editor

## Time range

Start time (optional)

rt-15m@m

Finish time (optional)

rt

## Attributes

Rule Title

User Accessed Machine Infected with Malware

Rule Description

\$user\$ accessed \$dest\$ which is infected with \$signature\$

Drill-down Name

View event data

Drill-down Search

`authentication(success)` | search (user\_is\_privileged="true" OR user\_i

## Throttling

Window Duration

1d

Time specifiers: y, mon, d, h, m, s

Fields to Group By

dest x user x signature x add a field followed by a comma

- Drill down can use a different search – efficiency is not as important, and the results desired don't require a count
- `authentication(success)` | search (user\_is\_privileged="true" OR user\_priority="critical" OR user\_priority="high") | stats values(user) as user by dest | join dest [search `malware` | search action=allowed | stats values(signature) as signature by dest]

1 result in the last 24 hours (from 11:00:00 AM April 29 to 11:30:18 AM April 30, 2012)

Export Options

Overlay: None

dest :

HOST-006

user :

drew

signature :

TSPY\_ZBOT

# The Resulting Notable Event

| Select                   | Options                          | Time                      | Security Domain | Title                                         | Urgency                                       | Status | Owner        |                              |
|--------------------------|----------------------------------|---------------------------|-----------------|-----------------------------------------------|-----------------------------------------------|--------|--------------|------------------------------|
| <input type="checkbox"/> | <input type="button" value="▼"/> | 4/30/12<br>8:20:22.000 AM | Audit ▾         | User Accessed Machine Infected with Malware ▾ | <span style="color: red;">!</span> Critical ▾ | New ▾  | unassigned ▾ | <a href="#">Hide details</a> |

**Description:**  
drew accessed HOST-006 which is infected with TSPY\_ZBOT

**Additional Fields:**

Destination: HOST-006 ▾  
Destination Business Unit: emea ▾  
Destination Category: pcl ▾  
Destination City: Havant ▾  
Destination Country: UK ▾  
Destination Latitude: 50.84436 ▾  
Destination Longitude: -0.98451 ▾  
Destination NT Hostname: HOST-006 ▾  
Destination PCI Domain: wireless ▾  
Destination Should Time Synchronize: true should\_timesync ▾  
Destination Should Update: true should\_update ▾  
Signature: TSPY\_ZBOT ▾  
User: drew ▾

**Correlation Search:**  
[Audit - High or Critical Priority Individual Logging into Infected Machine - Rule](#)

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

**Contributing Events:**  
[View event data](#)

Valid. event\_id=sc-essdemo.sv.splunk.com@@notable@@98544b0808141a9665222e08db0b72ff ▾ | event\_hash=98544b0808141a9665222e08db0b72ff ▾ | eventtype=notable ▾



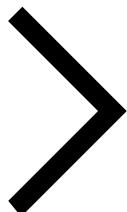
.conf2015

## Exercise 4 – Use the CIM, Luke!

splunk®

# Normalization: Not Just a Dirty Word

```
(tag=malware tag=attack
action=allowed)
```



```
(sourcetype=SYMC “Delete
failed”) OR (product=“VirusScan
Enterprise” action=would*) OR
(SourceName=“Trend Micro
OfficeScan Server” “Action: *
cannot *”)
```

- Normalizing at index time is pretty lame
- Normalizing the data before it's stored is VERY lame
- Normalizing with tags and fields at search time is very AWESOME

# Data Models Create Common Understanding

- Normalization without data reduction
- Customized for different data types
- RBAC maintained
- Data model reporting speeds optimized

Data Models

Data models enable users to easily create reports in the Pivot tool. [Learn More](#)

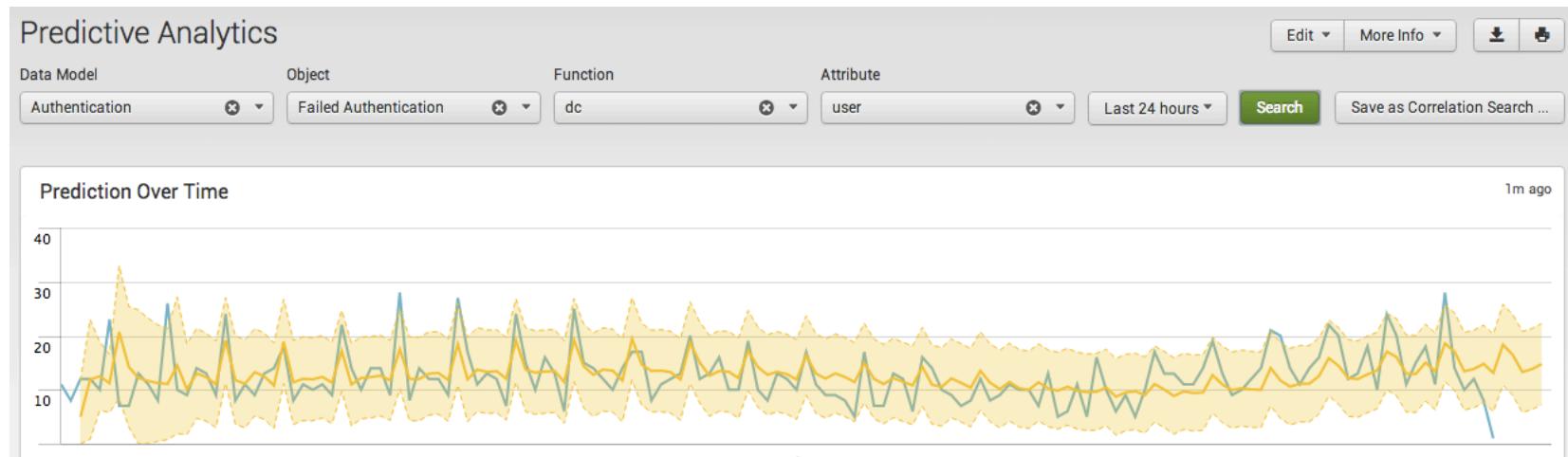
New Data Model

| i | Title                 | Actions        | App                       | Owner  | Sharing |
|---|-----------------------|----------------|---------------------------|--------|---------|
| ▶ | Alerts                | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Application State     | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Assets And Identities | ⚡ Edit ⚡ Pivot | SA-IdentityManagement     | nobody | Global  |
| ▶ | Authentication        | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Change Analysis       | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Compute_Inventory     | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Incident Management   | ⚡ Edit ⚡ Pivot | SA-ThreatIntelligence     | nobody | Global  |
| ▶ | Intrusion Detection   | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Malware               | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Network Traffic       | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Performance           | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Splunk Audit Logs     | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Threat Lists          | ⚡ Edit ⚡ Pivot | SA-ThreatIntelligence     | nobody | Global  |
| ▶ | Updates               | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Vulnerabilities       | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |
| ▶ | Web                   | ⚡ Edit ⚡ Pivot | SA-CommonInformationModel | body   | Global  |

# Make Correlation Searches from Datamodels

Predictive Analytics -> Pointy-Clicky detection of deviations from norm

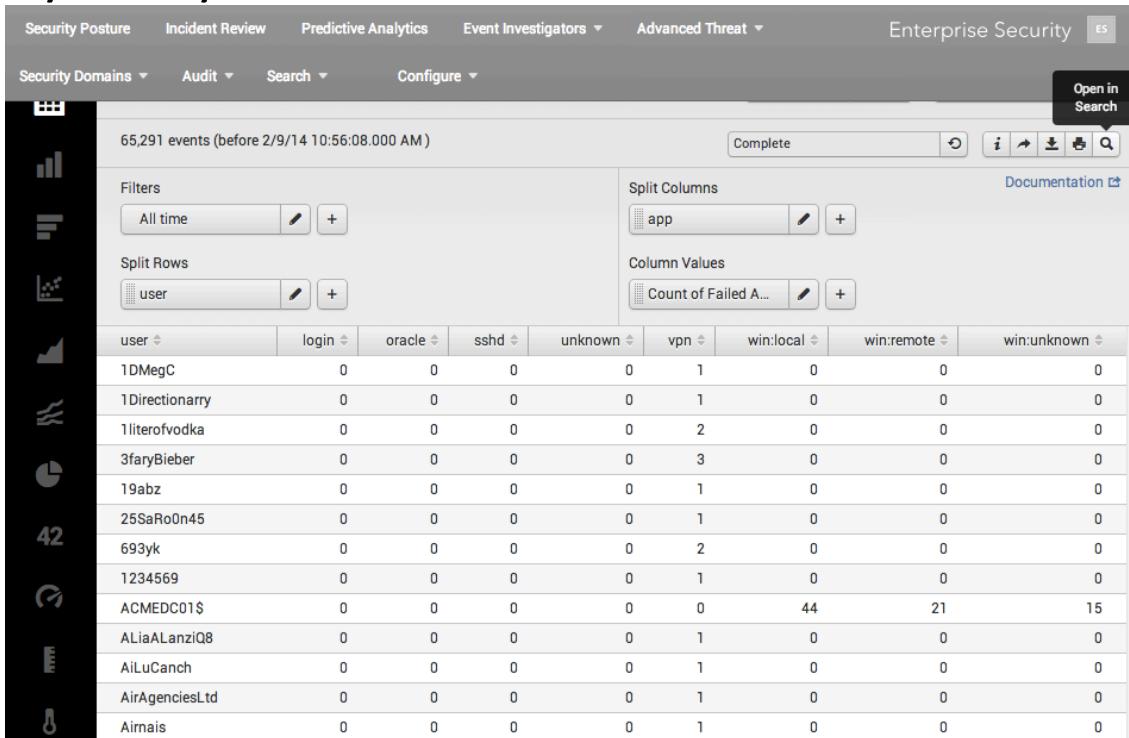
- Events and domains, not individual entities
  - YES: The number of failing accounts is different than normal
  - NO: SPLUNK/JCOATES is failing logins more than normal



# Make Correlation Searches from Datamodels

Search:Pivot -> Pointy-Clicky construction of data sets

- Gather a collection of normalized data
- Join with another
- Filter for interest
- Paste into New Correlation Search form



The screenshot shows the Splunk Enterprise Security interface. The top navigation bar includes links for Security Posture, Incident Review, Predictive Analytics, Event Investigators, Advanced Threat, and Enterprise Security. A sidebar on the left contains various icons for different security functions like Security Domains, Audit, Search, and Configure. The main area displays a table of 65,291 events from before February 9, 2014, at 10:56:08 AM. The table has columns for user, login, oracle, sshd, unknown, vpn, win:local, win:remote, and win:unknown. The first few rows of data are:

| user           | login | oracle | sshd | unknown | vpn | win:local | win:remote | win:unknown |
|----------------|-------|--------|------|---------|-----|-----------|------------|-------------|
| 1DMegC         | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| 1Directionary  | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| 1literofvodka  | 0     | 0      | 0    | 0       | 2   | 0         | 0          | 0           |
| 3faryBieber    | 0     | 0      | 0    | 0       | 3   | 0         | 0          | 0           |
| 19abz          | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| 25SaRoOn45     | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| 693yk          | 0     | 0      | 0    | 0       | 2   | 0         | 0          | 0           |
| 1234569        | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| ACMEDC01\$     | 0     | 0      | 0    | 0       | 0   | 44        | 21         | 15          |
| ALiaALanziQB   | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| AiLuCanch      | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| AirAgenciesLtd | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |
| Airmais        | 0     | 0      | 0    | 0       | 1   | 0         | 0          | 0           |

# Step One: Authentications

- Authentications, successful, privileged

- | `datamodel("Authentication", "Authentication")` | search Authentication.action="success" | `drop\_dm\_object\_name("Authentication")` | search is\_Privileged\_Authentication=1

100 events (2/8/14 11:00:00.000 AM to 2/9/14 11:06:29.000 AM)

Events (100) Statistics Visualization Job ▾ Complete

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾ 1 2

| Hide Fields     | All Fields                                | i | Time                   | Event                                                                                                                         |
|-----------------|-------------------------------------------|---|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Selected Fields | a host 26<br>a source 7<br>a sourcetype 6 | ▶ | 2/9/14 11:06:05.000 AM | Feb 09 11:06:05 cm1.acmetech.net auth security:info su: [ID 366847 auth.info] 'su dmsys' succeeded for root on /dev/???       |
|                 |                                           | ▶ | 2/9/14 11:05:36.000 AM | host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure                  |
|                 |                                           | ▶ | 2/9/14 11:05:36.000 AM | Feb 09 11:05:36 HOST0170 sshd[25089]: [ID 800047 auth.info] Accepted publickey for naughtyuser from 10.11.36.19 port 50241 ss |
|                 |                                           | ▶ | 2/9/14 11:05:36.000 AM | host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure                  |
|                 |                                           | ▶ | 2/9/14 11:05:13.000 AM | Feb 09 11:05:13 10.84.34.15 auth security:notice su: [ID 366847 auth.notice] 'su root' succeeded for mgarrahy on /dev/pts/107 |
|                 |                                           | ▶ | 2/9/14 11:05:13.000 AM | host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure                  |
|                 |                                           | ▶ | 2/9/14 11:05:02.000 AM | Feb 09 11:05:02 10.84.34.15 auth security:notice su: [ID 366847 auth.notice] 'su root' succeeded for mgarrahy on /dev/pts/107 |
|                 |                                           | ▶ | 2/9/14 11:05:02.000 AM | host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure                  |
|                 |                                           | ▶ | 2/9/14 11:04:41.000 AM | Feb 09 11:04:41 HOST0170 sshd[25089]: [ID 800047 auth.info] Accepted publickey for naughtyuser from 10.11.36.26 port 50241 ss |
|                 |                                           | ▶ | 2/9/14 11:04:41.000 AM | host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure                  |

.conf2015

splunk>

# Step Two: Malware

- Malware Attacks, Allowed

- | `datamodel("Malware", "Malware\_Attacks")` | search Malware\_Attacks.action="allowed" | `drop\_dm\_object\_name("Malware\_Attacks")`

100 events (2/8/14 11:00:00.000 AM to 2/9/14 11:23:09.000 AM) Job ▾ Complete 

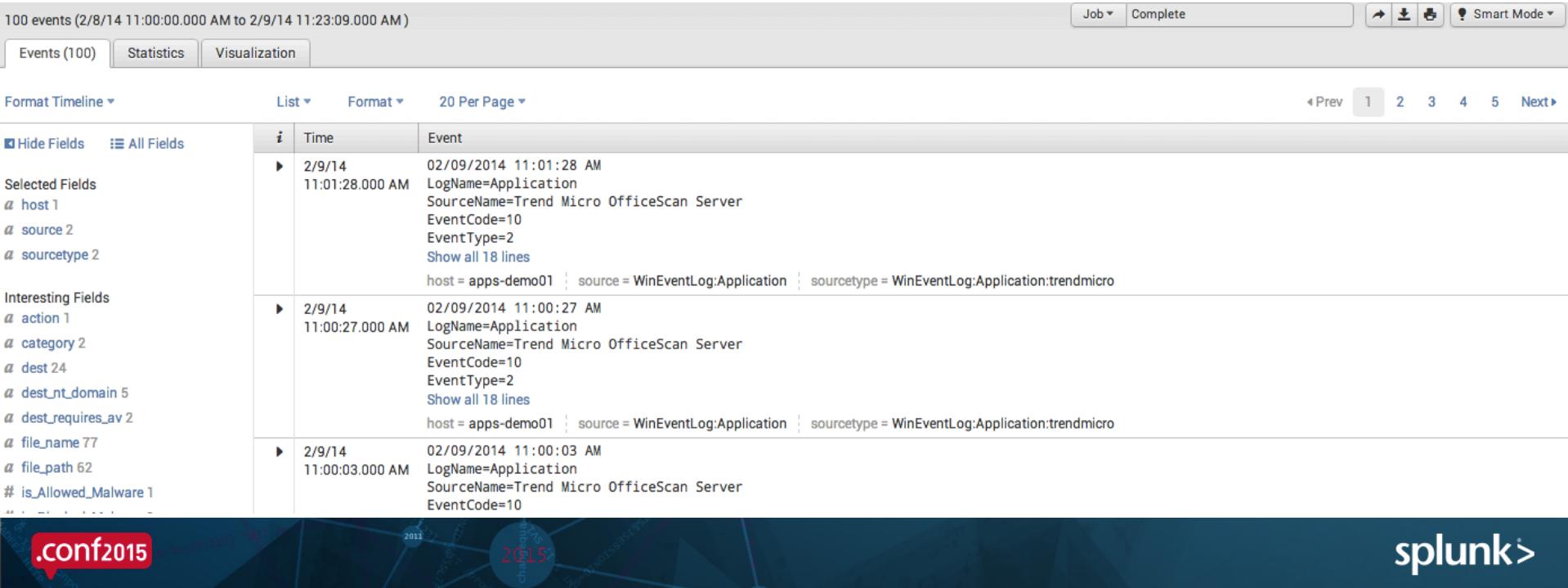
Events (100) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾ 

| Time                   | Event                                                                                                                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2/9/14 11:01:28.000 AM | 02/09/2014 11:01:28 AM<br>LogName=Application<br>SourceName=Trend Micro OfficeScan Server<br>EventCode=10<br>EventType=2<br>Show all 18 lines<br>host = apps-demo01   source = WinEventLog:Application   sourcetype = WinEventLog:Application:trendmicro |
| 2/9/14 11:00:27.000 AM | 02/09/2014 11:00:27 AM<br>LogName=Application<br>SourceName=Trend Micro OfficeScan Server<br>EventCode=10<br>EventType=2<br>Show all 18 lines<br>host = apps-demo01   source = WinEventLog:Application   sourcetype = WinEventLog:Application:trendmicro |
| 2/9/14 11:00:03.000 AM | 02/09/2014 11:00:03 AM<br>LogName=Application<br>SourceName=Trend Micro OfficeScan Server<br>EventCode=10                                                                                                                                                |

Selected Fields  
[host 1](#)  
[source 2](#)  
[sourcetype 2](#)

Interesting Fields  
[action 1](#)  
[category 2](#)  
[dest 24](#)  
[dest\\_nt\\_domain 5](#)  
[dest\\_requires\\_av 2](#)  
[file\\_name 77](#)  
[file\\_path 62](#)  
[# is\\_Allowed\\_Malware 1](#)



.conf2015  splunk > 

# Step Three: Access OR Malware

- Construct the total pool of data to make decisions from
  - | `datamodel("Authentication", "Authentication")`
  - | search Authentication.action="success"
  - | `drop\_dm\_object\_name("Authentication")`
  - | search is\_Privileged\_Authentication=1
  - | append [
  - | `datamodel("Malware", "Malware\_Attacks")`
  - | search Malware\_Attacks.action="allowed"
  - | `drop\_dm\_object\_name("Malware\_Attacks")`
  - ]

26,268 events (2/8/14 2:00:00.000 PM to 2/9/14 2:36:14.000 PM)

Events (26,268) Statistics Visualization

Format Timeline ▾ Show Fields List ▾ Format ▾ 20 Per Page ▾

| i | Time                  | Event                                                                                                                                                                                                                                      |
|---|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ▶ | 2/9/14 2:36:10.000 PM | Feb 09 14:36:10 cm1.acmetech.net auth security:info su: [ID 366847 auth.info] 'su dmsys' succeeded for root on /dev/??? host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure       |
| ▶ | 2/9/14 2:36:01.000 PM | Feb 09 14:36:01 cm1.acmetech.net auth security:info su: [ID 366847 auth.info] 'su dmsys' succeeded for root on /dev/??? host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure       |
| ▶ | 2/9/14 2:33:55.000 PM | Feb 09 14:33:55 acmepayroll ftpd[463]: [ID 124999 daemon.info] FTP LOGIN FROM 10.16.1.6 [10.16.1.6], root host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/syslog.nix   sourcetype = linux_secure                   |
| ▶ | 2/9/14 2:33:21.000 PM | Feb 09 14:33:21 10.84.34.15 auth security:notice su: [ID 366847 auth.notice] 'su root' succeeded for mgarrahy on /dev/pts/107 host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure |
| ▶ | 2/9/14 2:33:19.000 PM | Feb 09 14:33:19 cm1.acmetech.net auth security:info su: [ID 366847 auth.info] 'su dmsys' succeeded for root on /dev/??? host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure       |
| ▶ | 2/9/14 2:33:06.000 PM | Feb 09 14:33:06 cm1.acmetech.net auth security:info su: [ID 366847 auth.info] 'su mercury' succeeded for root on /dev/??? host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure     |
| ▶ | 2/9/14 2:31:34.000 PM | Feb 09 14:31:34 acmepayroll ftpd[463]: [ID 124999 daemon.info] FTP LOGIN FROM 10.16.1.6 [10.16.1.6], root host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/syslog.nix   sourcetype = linux_secure                   |
| ▶ | 2/9/14 2:31:28.000 PM | 02/09/2014 02:31:28 PM<br>LogName=Security<br>SourceName=Security<br>EventCode=552<br>EventType=8<br>Show all 28 lines<br>host = HOST-001   source = WinEventLog:Security   sourcetype = WinEventLog:Security                              |
| ▶ | 2/9/14 2:31:05.000 PM | Feb 09 14:31:05 10.84.34.15 auth security:crit su: [ID 810491 auth.crit] 'su root' failed for mgarrahy on /dev/pts/107 host = apps-demo01   source = /usr/local/bamboo/splunk/var/spool/splunk/auth.nix   sourcetype = linux_secure        |

# Step Four: Count the Matches

- Tabulate the fields that the decision will be made from
- | `datamodel("Authentication", "Authentication")` | search Authentication.action="success" | `drop\_dm\_object\_name("Authentication")` | search is\_Privileged\_Authentication=1 | append [| `datamodel("Malware", "Malware\_Attacks")` | search Malware\_Attacks.action="allowed" | `drop\_dm\_object\_name("Malware\_Attacks")` ]]
- | eval group = case(is\_Successful\_Authentication==1, "authentication", is\_Allowed\_Malware==1, "malware")
- | stats values(user) as user, values(signature) as signature, distinct\_count(group) as group\_count by dest

0 events (2/8/14 3:00:00.000 PM to 2/9/14 3:15:16.000 PM)

Events Statistics (34) Visualization

20 Per Page ▾ Format ▾ Preview ▾

| dest     | user                      | signature        |
|----------|---------------------------|------------------|
| ACME-002 | fohn<br>raiche<br>unknown | EICAR-AV-Test    |
| ACME-003 | korn<br>unknown<br>urban  | EICAR-AV-Test    |
| ACME-004 | handzlik<br>heinis        | Hacktool.Rootkit |

# Step Five: Detect the Condition

- group\_count field > 1 is bad, and there's our correlation search
- | `datamodel("Authentication", "Authentication")` | search Authentication.action="success" | `drop\_dm\_object\_name("Authentication")` | search is\_Privileged\_Authentication=1| append [| `datamodel("Malware", "Malware\_Attacks")` | search Malware\_Attacks.action="allowed" | `drop\_dm\_object\_name("Malware\_Attacks")`] | eval group = case(is\_Successful\_Authentication==1,"authentication",is\_Allowed\_Malware==1,"malware") | stats values(user) as user, values(signature) as signature, distinct\_count(group) as group\_count by dest
- | search group\_count>1
- | `get\_event\_id`
- | fields - group\_count

| dest        | user    | signature     |
|-------------|---------|---------------|
| ops-sys-006 | unknown | EICAR-AV-Test |



.conf2015

# Exercise 5

## Create and Use Lookups

splunk®

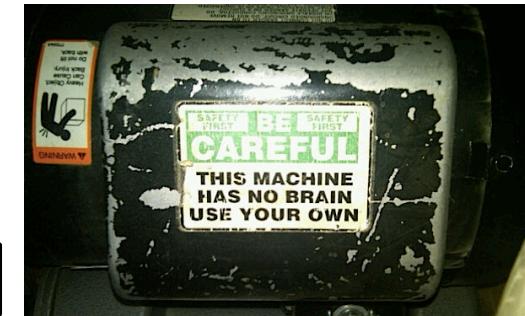
# Working with Lookups

- Some things are impractical to continually discover or recalculate in real time

Network Traffic Flows are expensive to monitor, so save the important information in a lookup

IP ranges of prohibited sites may be stored in another lookup (several are provided by default)

Did an internal system communicate with an embargoed network?



# Generating a Lookup

- Search for the material in question (tstats, raw, whatevs)
- Join with previously discovered lookup contents
- Write the new lookup
- Example: Port and Protocol Tracker, shows what transport/port combinations are in use on the network over time

```
| tstats `summariesonly` min(_time) as firstTime,max(_time)
as lastTime from datamodel=Network_Traffic where
All_Traffic.action=allowed by
All_Traffic.transport,All_Traffic.dest_port |
`drop_dm_object_name("All_Traffic")` | inputlookup append=T
port_protocol_tracker | stats min(firstTime) as
firstTime,max(lastTime) as lastTime by transport,dest_port
| outputlookup port_protocol_tracker | stats count
```

# Search for the Material in Question

- In this case an accelerated data model holds the goods

```
| tstats `summariesonly` min(_time) as firstTime,max(_time) as lastTime from datamodel=Network_Traffic where All_Traffic.action=allowed by All_Traffic.transport,All_Traffic.dest_port | `drop_dm_object_name("All_Traffic")`
```

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Contains the search command: `| tstats `summariesonly` min(_time) as firstTime,max(_time) as lastTime from datamodel=Network_Traffic where All_Traffic.action=allowed by All_Traffic.transport,All_Traffic.dest_port | `drop_dm_object_name("All_Traffic")``.
- Time Range:** Set to "Last 24 hours".
- Results:** 720 events from March 4, 2014, to March 5, 2014.
- Job Status:** Job is complete.
- Format:** Set to "Events".
- Table Data:** A table showing network traffic details. The columns are: transport, dest\_port, firstTime, and lastTime. The data rows are:

| transport | dest_port | firstTime  | lastTime   |
|-----------|-----------|------------|------------|
| tcp       | 139       | 1393961661 | 1394044817 |
| tcp       | 389       | 1393961437 | 1394045094 |
| tcp       | 443       | 1393961263 | 1394045198 |
| tcp       | 80        | 1393961153 | 1394045279 |
| udp       | 123       | 1393961186 | 1394045004 |
| udp       | 137       | 1393961511 | 1394044820 |
| udp       | 53        | 1393961142 | 1394045100 |
| unknown   | 0         | 1393961412 | 1394045252 |

# Join With the Older Lookup

- This is critical because if the new search provides no results, the old lookup will be wiped out

```
| tstats `summariesonly` min(_time) as firstTime,max(_time) as lastTime from datamodel=Network_Traffic where All_Traffic.action=allowed by All_Traffic.transport,All_Traffic.dest_port | `drop_dm_object_name("All_Traffic")`
| inputlookup append=T port_protocol_tracker
```



# Deal With Time

- Order, format, label

```
| tstats `summariesonly` min(_time) as firstTime,max(_time) as lastTime from datamodel=Network_Traffic where All_Traffic.action=allowed by All_Traffic.transport,All_Traffic.dest_port | `drop_dm_object_name("All_Traffic")`
| inputlookup append=T port_protocol_tracker
| stats min(firstTime) as firstTime,max(lastTime) as lastTime by transport,dest_port
```

---

- You might also want to dedup events

```
| dedup firstTime,lastTime,transport,dest_port
```

---

- To keep the lookup from growing forever, you can filter by time and calculate a difference

```
| convert timeformat="%m-%d-%Y" mktime(date) as _time | eval timeDiff=now()-_time | search timeDiff<86400
```

# Write the Resulting Lookup File

- Replace the lookup with the new results

```
| tstats `summariesonly` min(_time) as firstTime,max(_time) as lastTime from datamodel=Network_Traffic where All_Traffic.action=allowed by All_Traffic.transport,All_Traffic.dest_port | `drop_dm_object_name("All_Traffic")`
| inputlookup append=T port_protocol_tracker
| stats min(firstTime) as firstTime,max(lastTime) as lastTime by transport,dest_port
| outputlookup port_protocol_tracker
```

20 Per Page ▾ Format ▾ Preview ▾

| dest_port | firstTime  | lastTime   | transport |
|-----------|------------|------------|-----------|
| 139       | 1386119390 | 1394044817 | tcp       |
| 22        | 1388784710 | 1392695785 | tcp       |
| 389       | 1386119665 | 1394045094 | tcp       |
| 443       | 1386119183 | 1394045198 | tcp       |
| 80        | 1386119185 | 1394045279 | tcp       |
| 123       | 1386119355 | 1394045004 | udp       |
| 137       | 1386119590 | 1394044820 | udp       |
| 53        | 1386119104 | 1394045100 | udp       |
| 0         | 1386119107 | 1394045252 | unknown   |

# Using Lookups in Correlation Searches

## The Correlation Three Step

- Gather a pool of data
- Use a table to form the data for easy numeric tests
- Perform tests to make decisions

POOL: | inputlookup append=T src\_dest\_tracker | lookup local=true ip\_tor\_lookup src OUTPUTNEW src\_ip as src\_tor\_ip,src\_is\_tor | lookup local=true ip\_tor\_lookup dest OUTPUTNEW dest\_ip as dest\_tor\_ip,dest\_is\_tor | search dest\_is\_tor=true OR src\_is\_tor=true

297 results in the last 24 hours (from 1:00:00 PM April 29 to 1:47:25 PM April 30, 2012)

|   | date       | dest        | dest_is_tor | dest_tor_ip | sourcetype         | src               | src_is_tor | src_tor_ip |
|---|------------|-------------|-------------|-------------|--------------------|-------------------|------------|------------|
| 1 | 04-30-2012 | 10.11.36.35 |             |             | netscreen:firewall | 10.11.36.19       |            |            |
| 2 | 04-30-2012 | 10.11.36.50 |             |             | netscreen:firewall | 10.11.36.29       |            |            |
| 3 | 04-30-2012 | 10.11.36.45 |             |             | netscreen:firewall | 10.11.36.7        |            |            |
| 4 | 04-30-2012 | unknown     |             |             | airdefense         | 0b:4a:fe:06:36:92 |            |            |

The data is already tabular!

TEST: | eval tor\_ip=if(dest\_is\_tor=="true",dest\_tor\_ip,tor\_ip) | eval tor\_ip=if(src\_is\_tor=="true",src\_tor\_ip,tor\_ip) | fields + sourcetype,src,dest,tor\_ip

FINAL: | inputlookup append=T src\_dest\_tracker | lookup local=true ip\_tor\_lookup src OUTPUTNEW src\_ip as src\_tor\_ip,src\_is\_tor | lookup local=true ip\_tor\_lookup dest OUTPUTNEW dest\_ip as dest\_tor\_ip,dest\_is\_tor | search dest\_is\_tor=true OR src\_is\_tor=true | eval tor\_ip=if(dest\_is\_tor=="true",dest\_tor\_ip,tor\_ip) | eval tor\_ip=if(src\_is\_tor=="true",src\_tor\_ip,tor\_ip) | fields + sourcetype,src,dest,tor\_ip

# Using a Static Lookup

- You can define a non-dynamic lookup even more easily

Embargo definition, used by a custom block-listed traffic correlation search

Embargo.CSV content sample

```
SA-ThreatIntelligence/local/transforms.conf
[ip_embargo]
file=embargo.csv
max_matches = 1
match_type = CIDR(src)

"src","blocked"
"2.144.0.0/14",1
"2.176.0.0/12",1
"31.7.64.0/18",1
"31.7.128.0/20",1
"0.0.0.0/0",0

| inputlookup append=T src_dest_tracker | lookup local=true ip_embargo src
OUTPUTNEW src_ip as src_embargo_ip,src_is_embargoed | lookup local=true
ip_embargo dest OUTPUTNEW dest_ip as dest_embargo_ip,dest_is_embargo | search
dest_is_embargo=true OR src_is_embargo=true | eval
embargo_ip=if(dest_is_embargo=="true",dest_embargo_ip,embargo_ip) | eval
embargo_ip=if(src_is_embargo=="true",src_embargo_ip,embargo_ip) | fields +
sourcetype,src,dest,embargo_ip
```

.conf2015

# THANK YOU

**splunk®**



.conf2015

# Reference Material

## Types of Correlation Searches

splunk®

# ES Correlation Search Types

- Within a single domain, a **threshold** has occurred.
  - Within a single domain, a **threshold** has been breached once.
  - Within a single domain, a **threshold** has been breached **by many**.
  - Within a single domain, a **blacklisted item** has been matched.
  - Within a single domain, a **desired item** has not been matched.
  - Within a single domain, a known bad **event correlation** has been matched.
  - Within a single domain, a **desired event correlation** has not been matched.
  - Within a single domain, a measured value is anomalous from **recorded history**.
  - Within a single domain, a measured value is anomalous from **computed baseline**.
  - Across **multiple domains**, a single recognized event has occurred.
  - Across multiple domains, a **correlation** of recognized events has been matched.
- Does this list need updating?

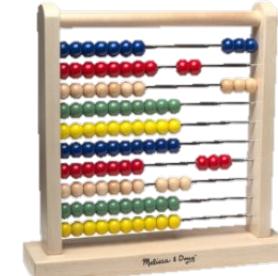
# Within a Single Domain, a **Recognized Event** has Occurred

- Threat - Watchlisted Events – Rule
- tag=watchlist NOT sourcetype=stash | `get\_event\_id` | `map\_notable\_fields`
- Events that look bad, add fields and tags.



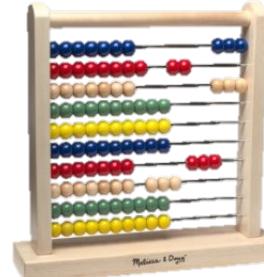
# Within a Single Domain, a Configured Threshold has Been Breached Once

- Access - Excessive Failed Logins - Rule
- `authentication(failure)` | tags outputfield=tag | stats values(tag) as tag,dc(user) as user\_count,dc(dest) as dest\_count,count by app,src | `settags("access")` | search count>=6
- Events that look bad, add fields and tags, count them, add fields and tags, test if greater than threshold.



# Within a Single Domain, a Configured Threshold has Been Breached by Many

- Network - Vulnerability Scanner Detection (by targets) - Rule
- ```
tag=attack | tags outputfield=tag | stats values(tag) as tag,dc(dest) as count by src | search count>25 | `settags("network")`
```
- Events that look bad, add fields and tags, count them, add fields and tags, test if greater than threshold



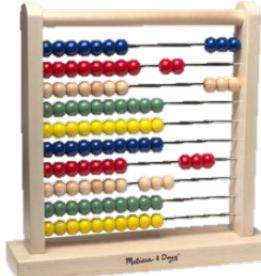
Within a Single Domain, a Blacklisted Item has Been Matched

- Endpoint - Prohibited Process Detection - Rule
- NOT sourcetype=stash `localprocesses` | `get_interesting_processes` | search is_prohibited=true | `get_event_id` | `map_notable_fields` | fields + orig_event_id,orig_raw,dest,process,note
- All the useful records, match the blacklist, add fields and tags



Within a Single Domain, a Desired Item has Not Been Matched

- Audit - Potential Gap in Data - Rule
- ```
index=_internal * sourcetype="scheduler" status=success (app=SA-* OR app=DA-* OR app=SplunkEnterpriseSecuritySuite OR app=SplunkPCIComplianceSuite) | head 1 | stats count(sourcetype) as count | where count=0 | eval problem="true"
```
- Relevant events that are good, count them, test if count = 0



# Within a Single Domain, a Known Bad Event Correlation has Been Matched

- Access - Brute Force Access Behavior Detected - Rule
- `authentication` | tags outputfield=tag | stats values(tag) as tag, count(eval(action=="failure")) as failure, count(eval(action=="success")) as success by src | search failure>6 success>0 | `settags("access")`
- Relevant events, count by types, test if two thresholds are breached, add fields and tags.



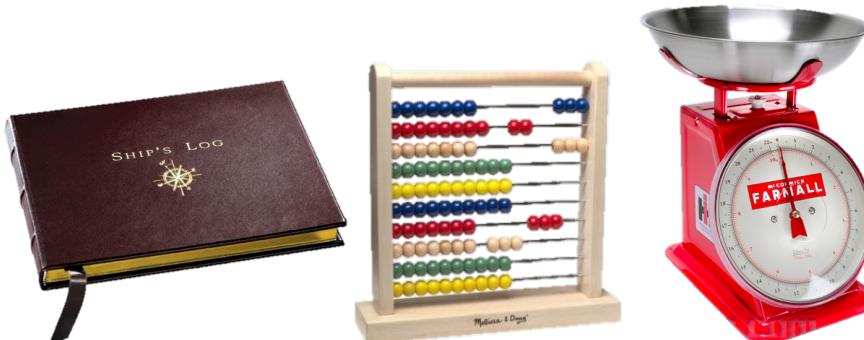
# Within A Single Domain, A Desired Event Correlation Has Not Been Matched

- No shipping rule matches this pattern
- N/A
- Customers often will do something like this:
  - Access to important system
  - Change Event on that system
  - Service Desk ticket referencing the system **is absent**



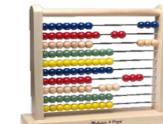
# Within a Single Domain, a Measured Value is Anomalous from Recorded History

- Endpoint - Anomalous New Processes - Rule
- | inputlookup append=T localprocesses\_tracker | eval \_time=firstTime | `hoursago(24)` | stats dc(dest) as dest\_count by process | search dest\_count>9
- Load recorded history, bucket by time, count and compare to threshold



# Within a Single Domain, a Measured Value is Anomalous From Computed Baseline

- Access - Brute Force Access Behavior Detected – Rule
  - | tstats `summariesonly` count from datamodel=Intrusion\_Detection by \_time,IDS\_Attacks.signature span=30m | `drop\_dm\_object\_name("IDS\_Attacks")` | `timeDiff` | appendpipe [search timeDiff<=86400 | stats max(\_time) as \_time,sum(count) as count by signature | eval group="Last 24 hours"] | eval group=if(\_time<relative\_time(time(),"@d") AND timeDiff<=5184000,"Last 60 days",group) | bin \_time span=1d | stats sum(count) as count by \_time,group,signature | eval temp=if(group="Last 60 days",signature,null()) | eventstats stdev(count) as stdev,avg(count) as avg by temp | eventstats max(stdev) as stdev,max(avg) as avg by signature | dedup signature sortby -\_time | eval limit=(3\*stdev)+avg | eval diff=count-limit | search diff>0
- Relevant events, sort types into a table, test if two thresholds are breached, add fields and tags.



# Across Multiple Domains, a Recognized Event has Occurred

- Threat - Threat List Activity - Rule
  - | `src\_dest\_tracker("allowed")` | `threatlist\_lookup(src)` | `threatlist\_lookup(dest)` | eval threat\_ip=if(isnotnull(src\_threatlist\_name), src, if(isnotnull(dest\_threatlist\_name), dest, threat\_ip)) | search threat\_ip=\* | fields + sourcetype,threat\_ip,src,src\_threatlist\_category,src\_threatlist\_description,src\_threatlist\_name,dest,dest\_threatlist\_category,dest\_threatlist\_description,dest\_threatlist\_name
- Events of the right type, recognized bad things, add fields and tags, filter by match, add more fields and tags.



# Across Multiple Domains, a Correlation of Recognized Events has Been Matched

- Access - High or Critical Priority Individual Logging into Infected Machine - Rule
- (tag=authentication action=success (user\_is\_privileged="true" OR user\_priority="critical" OR user\_priority="high") ) OR (tag=malware tag=attack action=allowed) | tags outputfield=tag | eval group=case(tag=="authentication","authentication",tag=="malware","malware") | eval user;if(tag=="malware",null(),user) | eval signature;if(tag=="authentication",null(),signature) | stats values(user) as user,values(signature) as signature,dc(group) as group\_count by dest | search group\_count>1
- All of the potentially interesting events, add fields and tags, count and test.

