

ES Multi-Tenancy Fundamentals

Macy Cronkite Professional Services
Architects, Splunk

Mike Barrie
Professional Services Architects, Splunk

.conf2016

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.

Agenda

- Explore Enterprise Security Multi-Tenancy Scenarios
- Asset and Identity Considerations
- Data Models and RBAC Considerations
- Dashboards and Workflow Considerations

What Do We Mean By Multi-tenancy?

- 1. MSSP - Managed Service Provider
 - Handles Alerts on a central ES instance as a 3rd party vendor to separate business organizations.
 - No external access to ES dashboards, black box to the customers.
- 2. ESOC - Enterprise SOC with subsidiary organizations
 - Handles Alerts on a central ES, many universal forwarders
 - Shared access to the dashboards, shared infrastructure, but separate reporting.
 - (Hospital, University)
- 3. TSOC - Tiered SOCS, a global SOC with many sub-local SOCs
 - Different ES clusters, taking notables from separate ES instances.
 - Correlate threat across organizations , look for patterns
 - (Multi-national corporations, with subsidiary companies, Government e.g. State to National)

Architecture Blueprints

MSSP



E-SOC



T-SOC



MSSP = ESOC (Managed by one SOC group.)
TSOC (Many disparate SOC groups.)

Enterprise Security App Considerations

- Assets and Identities
 - Private vs. Public IP addresses
 - Host name collision
- Data Models and RBAC
 - Summary Indexes
 - Data Model Acceleration
- Workflow
 - Incident Review Drilldown
 - Security Posture

Tradeoffs / Drawbacks



Scale / Storage
Management Complexity

Assets And Identities

- Problem:
 - Assets and Identities expansion process is designed to MERGE all assets together.
 - ip,nt_host name collisions (10.0.0.1, webserver1)
- Workaround:
 - Require FDQN, MAC addresses
 - Leverage the OWNER,BUNIT,CATEGORY fields
 - Remember Category is an Mvfield | foo | bar | wow
 - Don't rely on IP, or nt_host to drive matching behavior on internal addresses

Indexes, RBAC, Data Models

- Problem:
 - RBAC, Indexes, summary indexes
 - MSSP – dashboards are developed per customer
 - ESOC – (TRICKY)
 - TSOC – ES is local per organization , master ES has master rights anyways
 - Data Models and Accelerations
 - Data models generate off of the scoped CIM indexes
 - (and Data Model accelerations are tied to the GUID of the SH that created them).
- Workaround
 - ESOC Create different indexes and system user roles for each organization.
 - TSOC
 - Prepare to use A LOT OF disk space for data model accelerations, **one per org.**
 - Update Correlation searches, Key indicators, dashboards to run against specific DMs for each org... OR ... don't use data models at the top tier and rely on drilldown searches.

Dashboards And Incident Review

- Problem
 - Risk Analysis Dashboards: depends on assets and identities data
 - Incident Review Workflow: Priority, Urgency, Severity/Impact
 - Driven by assets and identities
 - Incident Review Drilldowns:
 - TSOC - depends on **correct** orig_raw being captured in correlation search.
 - MSSP/ESOC - Dashboards:
 - Need to be filtered by organization - - give access to some
 - Threat Intel: looks at ip,domain,cert,process,...very agnostic external threat
- Workaround:
 - The INDEXED FIELD es_site can also be applied to data in the Incident Review by adding “es_site=<site_name>” in the Search box.
 - Don't depend on internal ip,nt_host (10.0.0.1/webserver) for correlation

Adding The es_site Indexed Field

props.conf

[host::*]

TRANSFORMS-0_add_es_site = add_es_site

transforms.conf:

[add_es_site]

REGEX = (.*)

FORMAT = es_site::tyrell

WRITE_META = true

fields.conf:

[es_site]

INDEXED = true

(Drilldown)Anatomy Of An Notable Event

- 06/15/2016 18:06:00 -0700,
search_name="Access - Insecure Or
Cleartext Authentication - Rule",
search_now=0.000,
info_min_time=1466039160.000,
info_max_time=1466039760.000,
info_search_time=1466028640.407,
app="win:remote", count=1,
dest="ACME-002", lastTime=1466039382,
orig_raw="06/15/2016 06:09:42 PM
LogName=Security EventCode=529
EventType=16 Type=Failure Audit
SourceName=Security
RecordNumber=327572524 Category=2
CategoryString=Logon/Logoff
ComputerName<snip>", orig_rid=0,
orig_sid="rt_scheduler__admin_U0EtQWNj
ZXNzUHJvdGVjdGlvbG__RMD58c5c64bca
ddbda9_at_1466028608_2.9895",
orig_tag="alert|authentication|cleartext|
error|failure|os|remote|security|
should_timesync|should_update|windows"

What we know:

- search_name: what generated the notable
- orig_raw: The event, in some cases.
- org_sid: important! The SID of the search that was running
- From the event itself we know the host that generated it

What we can derive:

- A Drill-Down search (if one was defined)
- The indexers on which to run that drilldown search against
- Information about the assets and identities (by combining the src/dest/user with the host that generated the event)
- The history of the notables workflow

What is Harder to Know:

- Investigations are stored in the KVStore on each ES instance and difficult to understand.

TSOC - Solution

- Create an indexed field (es_site) on all forwarders, syslogers, inputs...
- Maintain assets and identities with fdqn and dns, and a category that includes the site name
- Update Urgencies and priorities by organization
- Ignore local ip,nt_host (10.0.0.1/webserver) in correlation searches, asset/identity investigator
- Disable the data models and update the correlation searches on the top tier ES Search Head
- Disable risk analysis and threat intelligence, the Top tier ES Search Head is for cross-site investigations and correlating patterns of notable events

TSOC - Correlation Search

- ES correlation searches are **disabled** on the top tier instance, they are just there to define incident review drilldown
 - (TSOC top level can't really work events – view the notables out of sub-Soc, but workflow is not synched.)
- Drilldown searches include the INDEXED FIELD `es_site=es_site` in the drilldown search:
 - `| datamodel Authentication Authentication search | search Authentication.src="src" es_site="es_site"`
 - `es_site` can be used in the description and title fields

Tyrell Corp

Incident Review

Urgency

CRITICAL	0
HIGH	23
MEDIUM	2
LOW	1
INFO	0

Status

Name

Owner

Search

Security Domain

Time

Tag

Submit

✓ 26 events (9/12/16 4:00:00.000 AM to 9/13/16 4:59:36.000 AM)

Job v || ■ Smart Mode v

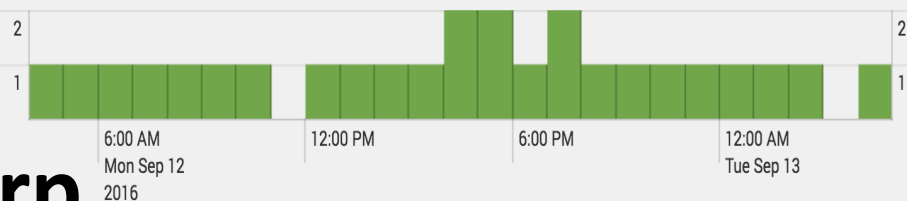
Format Timeline v

Zoom Out

+ Zoom to Selection

x Deselect

1 hour per column



Tyrell Corp

[Edit Selected](#) | [Edit All 26 Matching Events](#) | [Add Selected to Investigation](#)

« prev 1 2 next »

i	<input type="checkbox"/>	Time ↕	Security Domain ↕	Title ↕	Urgency ↕	Status ↕	Owner ↕	Actions
>	<input type="checkbox"/>	9/13/16 4:00:17.000 AM	Network	Tyrell Specific Thing Happened	High	New	unassigned	▼
>	<input type="checkbox"/>	9/13/16 2:55:11.000 AM	Network	Tyrell Specific Thing Happened	High	New	unassigned	▼
>	<input type="checkbox"/>	9/13/16 1:55:05.000 AM	Network	Tyrell Specific Thing Happened	High	New	unassigned	▼
>	<input type="checkbox"/>	9/13/16 12:50:10.000 AM	Network	Tyrell Specific Thing Happened	High	New	unassigned	▼

TSOC – Incident Review Drilldown

Drilldowns from the top tier are connected by category to the site name:

Edit Selected | Edit All 54 Matching Events | Add Selected to Investigation

< prev 1 2 3 next >

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
<input type="checkbox"/>	9/13/16 4:10:10.000 AM	Threat	Threat Activity Detected (25.156.230.137)	Low	New	unassigned	▼

Description:
Threat activity (25.156.230.137) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection

Additional Fields	Value	Action
Destination	25.156.230.137	▼
Destination Expected	false	▼
Destination PCI Domain	untrust	▼
Destination Requires Antivirus	false	▼
Destination Should Time Synchronize	false	▼
Destination Should Update	false	▼
Source	10.1.1.181	▼
Source Business Unit	Finance	▼
Source Category	EvilCorp	▼
Source DNS	device	▼
Source IP Address	SRV-435@evil.com	▼
Source Expected	10.1.1.181	▼
Source NT Hostname	SRV-435	▼
Source Owner	Ykautz	▼
Source PCI Domain	untrust	▼
Source Requires Antivirus	false	▼
Source Should Time Synchronize	false	▼
Source Should Update	false	▼
Threat Category	threatlist	▼

Correlation Search:
[Threat - Threat List Activity - Rule](#)

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

Contributing Events:
[View all threat activity involving dest="25.156.230.137"](#)

Original Event:
09/13/2016 03:15:00 +0000, search_name="Threat - Source And Destination Matches - Threat Gen", search_now=1473736500.000, info_min_time=1473728400.000, info_max_time=1473736500.000, info_search_time=1473736514.486, dest="25.156.230.137", orig_sourcetype="cisco:wsa:squid", src="10.1.1.181", threat_collection=ip_intel_1, threat_collection_key="iblocklist_logmein|25.0.0.0-25.255.255.255", threat_key=iblocklist_logmein, threat_match_field=dest, threat_match_value="25.156.230.137"
[View original event](#)

New Search Save As Close

```
* index=threat_activity | 'get_event_id' | search indexer_guid=FC81F110-8384-4673-884B-9DCB6097A720 | search event_hash=0c3878d4c5748de1b8108fce72a3fd77 | head 1
```


1 event (before 9/13/16 5:17:05.000 AM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 millisecond per column

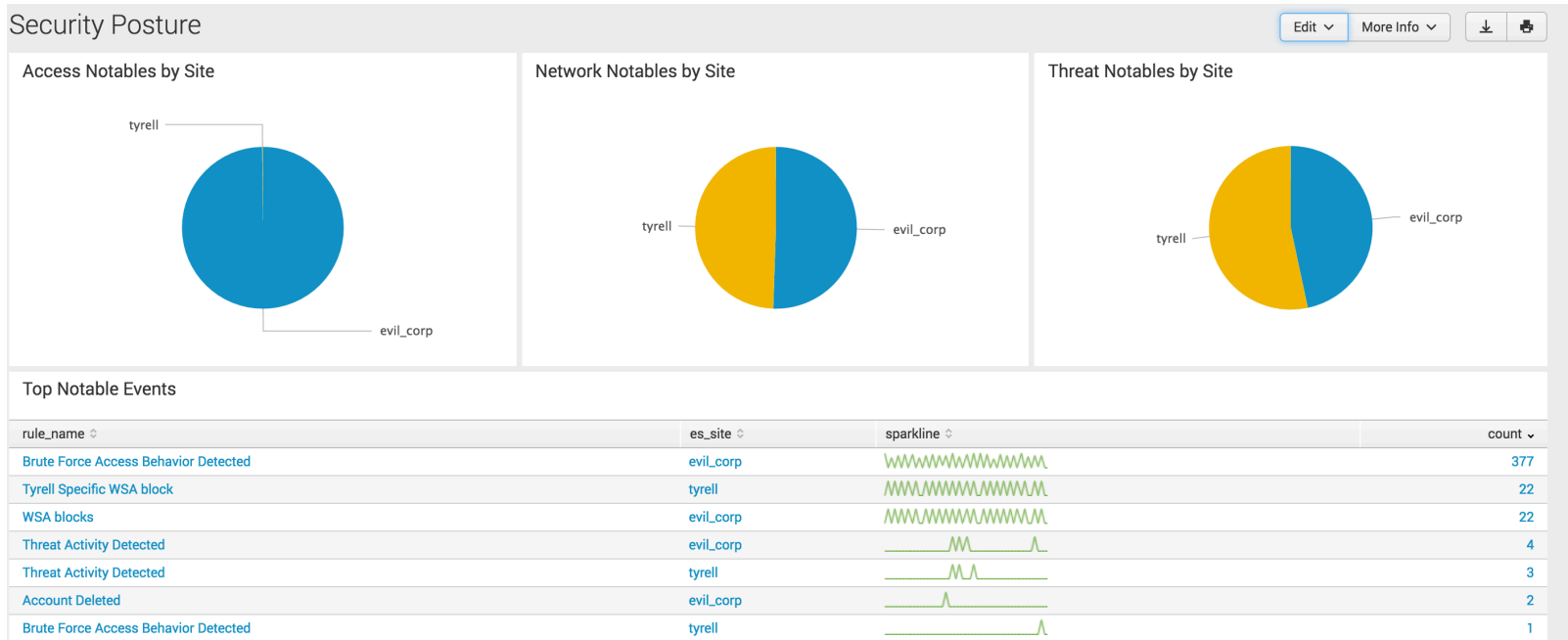
f	Time	Event
>	9/13/16 3:15:00.000 AM	09/13/2016 03:15:00 +0000, search_name="Threat - Source And Destination Matches - Threat Gen", search_now=1473736500.000, info_min_time=1473728400.000, info_max_time=1473736500.000, info_search_time=1473736514.486, dest="25.156.230.137", orig_sourcetype="cisco:wsa:squid", src="10.1.1.181", threat_collection=ip_intel, threat_collection_key="iblocklist_logmein 25.0.0.0-25.255.255.255", threat_key=iblocklist_logmein, threat_match_field=dest, threat_match_value="25.156.230.137"

Selected Fields
host 1
source 1
sourcetype 1
host = es1 | source = Threat - Source And Destination Matches - Threat Gen | sourcetype = stash



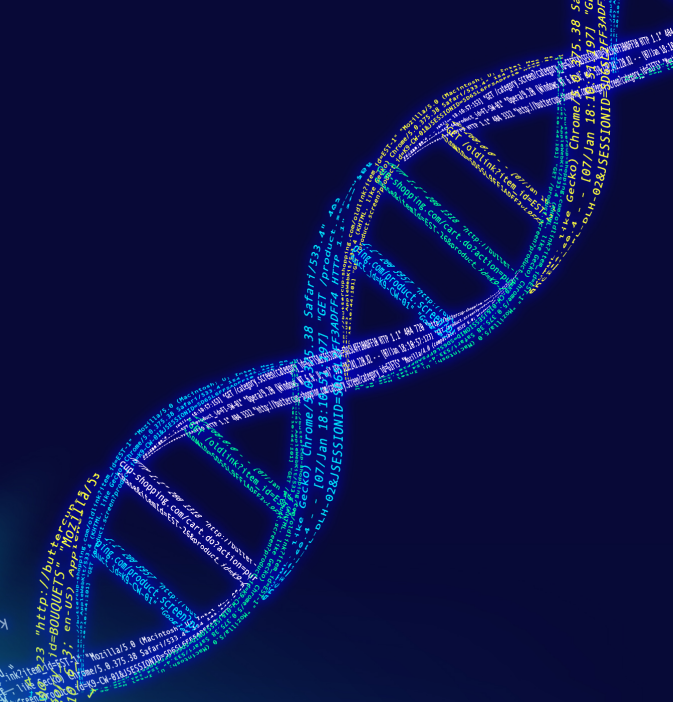
TSOC - Dashboards

Dashboards can now be modified to reflect site trends using es_site...



THANK YOU

.conf2016



DEMO TIME!!!!!!

- <https://54.218.17.71:8000/en-US/manager/search/accesscontrols>