splunk> .conf2017

The Art of Detection

Using Splunk Enterprise Security

Doug Brown | Senior Information Security Analyst, Red Hat
95B6 922E 47D2 7BC3 D1AF F62C 82BC 992E 7CDD 63B6

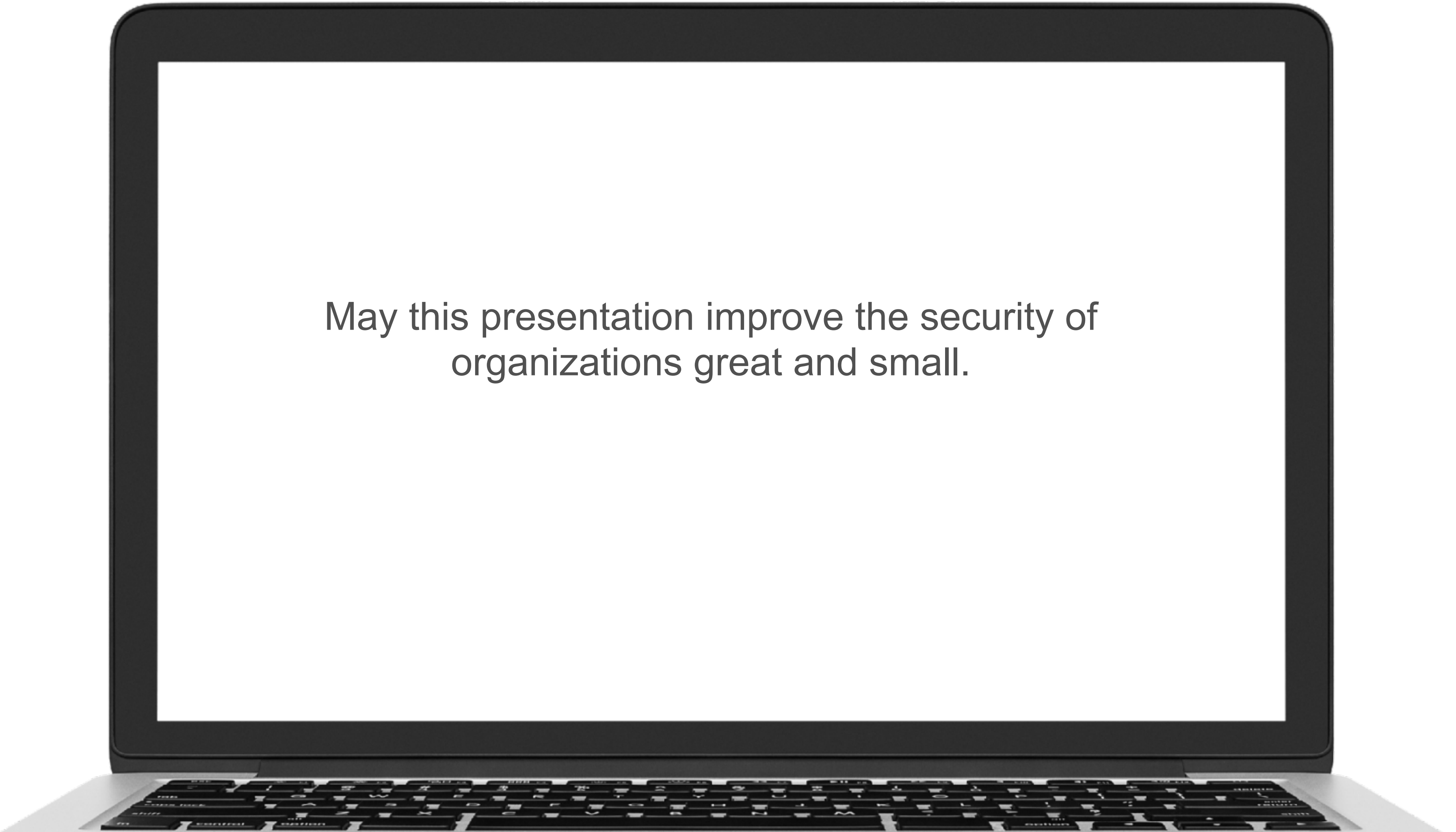
September 27, 2017 | Washington, DC

PRESENTATIONS.

Forward-Looking Statements

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.

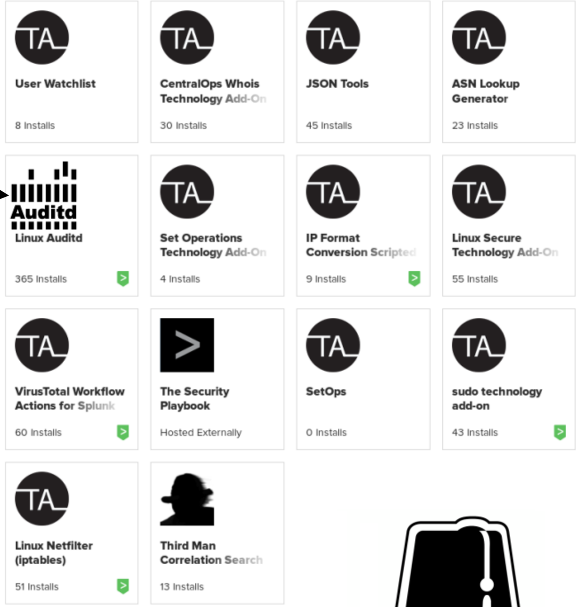
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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.



May this presentation improve the security of organizations great and small.

Speaker Background

- Doug “trustedsubject” Brown
- Fond of SELinux
- SplunkTrust member
- Author of more than a dozen Splunkbase apps, incl Auditd
- 2016 Developer Revolution Award Winner
- Masters degree examining the compositional behavioural properties of computer networks using formal methods: https://eprints.qut.edu.au/93693/1/Douglas_Brown_Thesis.pdf
- Contributor to ES roadmap
- Preparing for a Successful ES Engagement:
  - https://www.splunk.com/blog/2016/10/24/preparing-for-a-successful-enterprise-security-ps-engagement.html



User Watchlist
8 Installs

CentralOps Whois Technology Add-On
30 Installs

JSON Tools
45 Installs

ASN Lookup Generator
23 Installs

Linux Auditd
365 Installs

Set Operations Technology Add-On
4 Installs

IP Format Conversion Scripted
9 Installs

Linux Secure Technology Add-On
55 Installs

VirusTotal Workflow Actions for Splunk
60 Installs

The Security Playbook
Hosted Externally

SetOps
0 Installs

sudo technology add-on
43 Installs

Linux Netfilter (iptables)
51 Installs

Third Man Correlation Search
13 Installs

SPLUNK TRUST

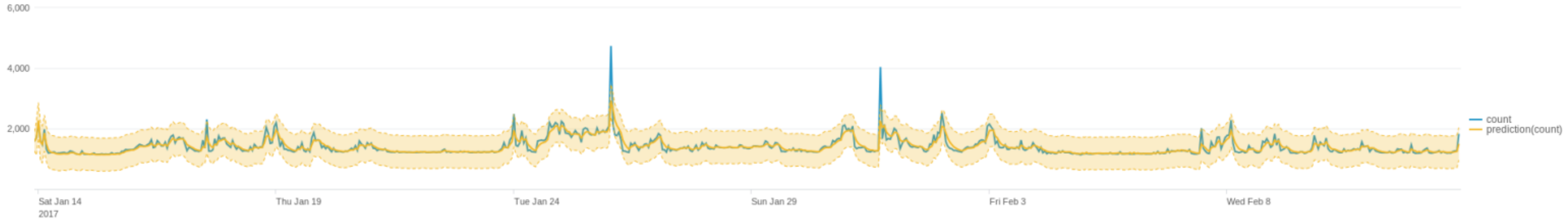
Overview

1. Operational Security at Red Hat
2. A New Triage Paradigm
3. Correlation Search Development Process
4. Extensions and Customizations
5. Case Study

redhat Operational Security

- Leading Open Source vendor
- Global team of 14 people, dealing with various aspects of corporate security
- Splunk customer since v4.1
- TB+ license

- Needed tool to support workflow and whole incident management lifecycle
- Cost & risk of developing/maintaining our own tool was considered greater than ES
- Implemented ES at end of last year



Enterprise Security is just a framework upon which to *build* a world-class security operation

A New Triage Paradigm

Our strategy to address alert fatigue and find what really matters.

What Makes An Alert Actionable?

One or more of these?

- High Confidence?
- A Realised Threat?
- Must Be Rectified By Human?
- Substantial Evidence?

Intrinsically Actionable

Alert Fatigue

Root Cause

- We falsely think we can detect "badness"
- Our detection mechanisms are bias towards early stages of the kill-chain where there's greater entropy and lower fidelity
- The hidden problem is that due to our assumption we're not actually detecting the genuinely bad things that present a real risk to organisation

Solution

- Change-based correlation searches
- Risk-based incident detection
- Auto-close notables (no analyst triage required)
- Triage high-risk *objects*, prioritised by urgency (object priority x aggregated risk)

Alert Fatigue

Result

- Abstract rather than concrete approach to operational security allows unknown threats to be detected
- Analysts can concentrate on hunting and prioritise their triage time
- Analysts triage less than 6 *objects* in a shift (often none)
- Changes the notion of what constitutes a false-positive

Requirements/Assumptions

- Bad actor *changes* something in order to achieve their *actions on objective*
- Sufficient data across attack surface ingested and normalised
- Identity and asset prioritisation
- Team of creative analysts
- Suite of correlation searches

Alert Fatigue

FAQ

- Q: Why bother raising notables if they’re not triaged?
  - A: To summarise and retain evidence
  - A: Provide the means for higher-order correlation searches that perform meta-analysis of trends and anomalies across notables
- Q: If not triaging notables, which dashboards are used first for triage:
  - A: “Security Posture” & “Risk Analysis”
- Q: Why stop triaging notables raised by high-fidelity correlation searches?
  - A: If they are *intrinsically actionable*, then they should be triaged by an analyst

Security Event Tiering

Tier 1

Raw information and events from security tools
Typically low fidelity (“could be bad”) and not intrinsically actionable

Tier 2

Behaviour-based correlation search notables
Typically medium fidelity (“looks bad”) and generally not intrinsically actionable

Tier 3

Object risk/sequence-based correlation searches
High fidelity (“likely bad”) and requires attention

Tier 4

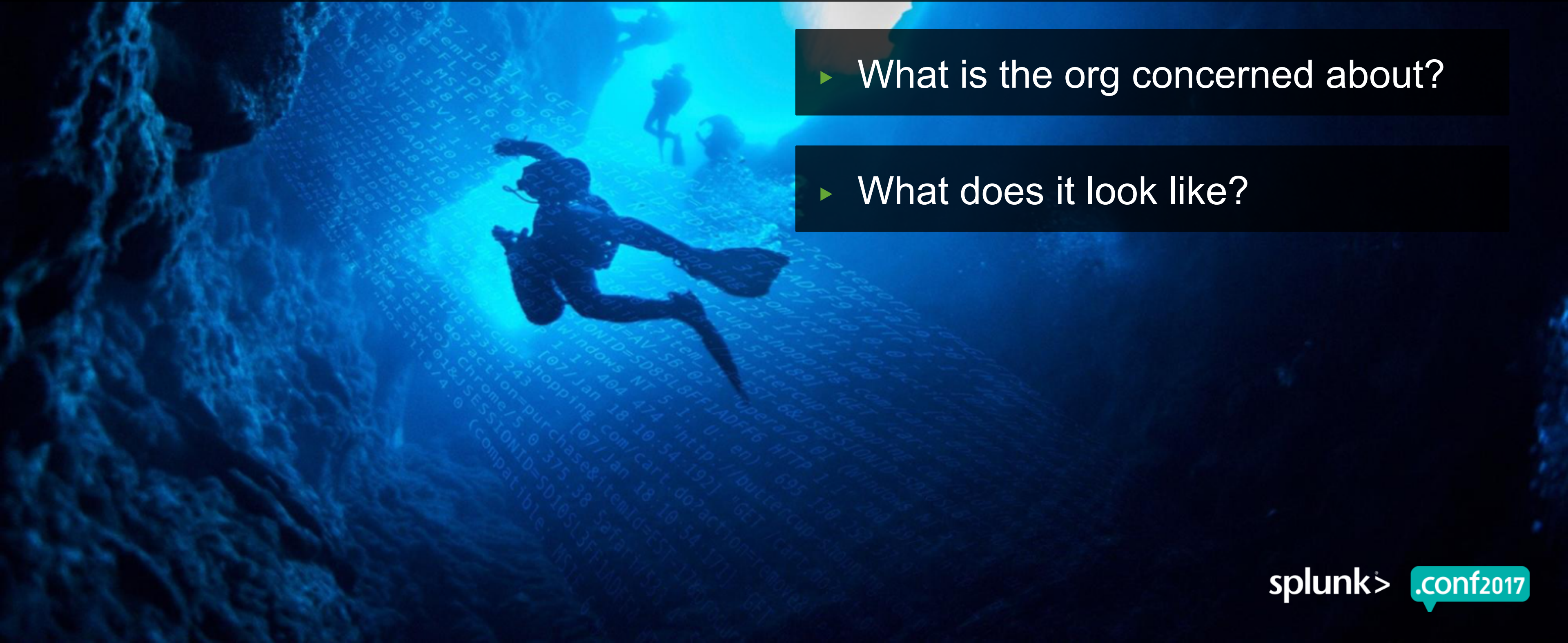
Abstract risk-based correlation searches
High fidelity (“likely bad”) and requires attention

Correlation Search Development Process

splunk> .conf2017

1st: The Idea

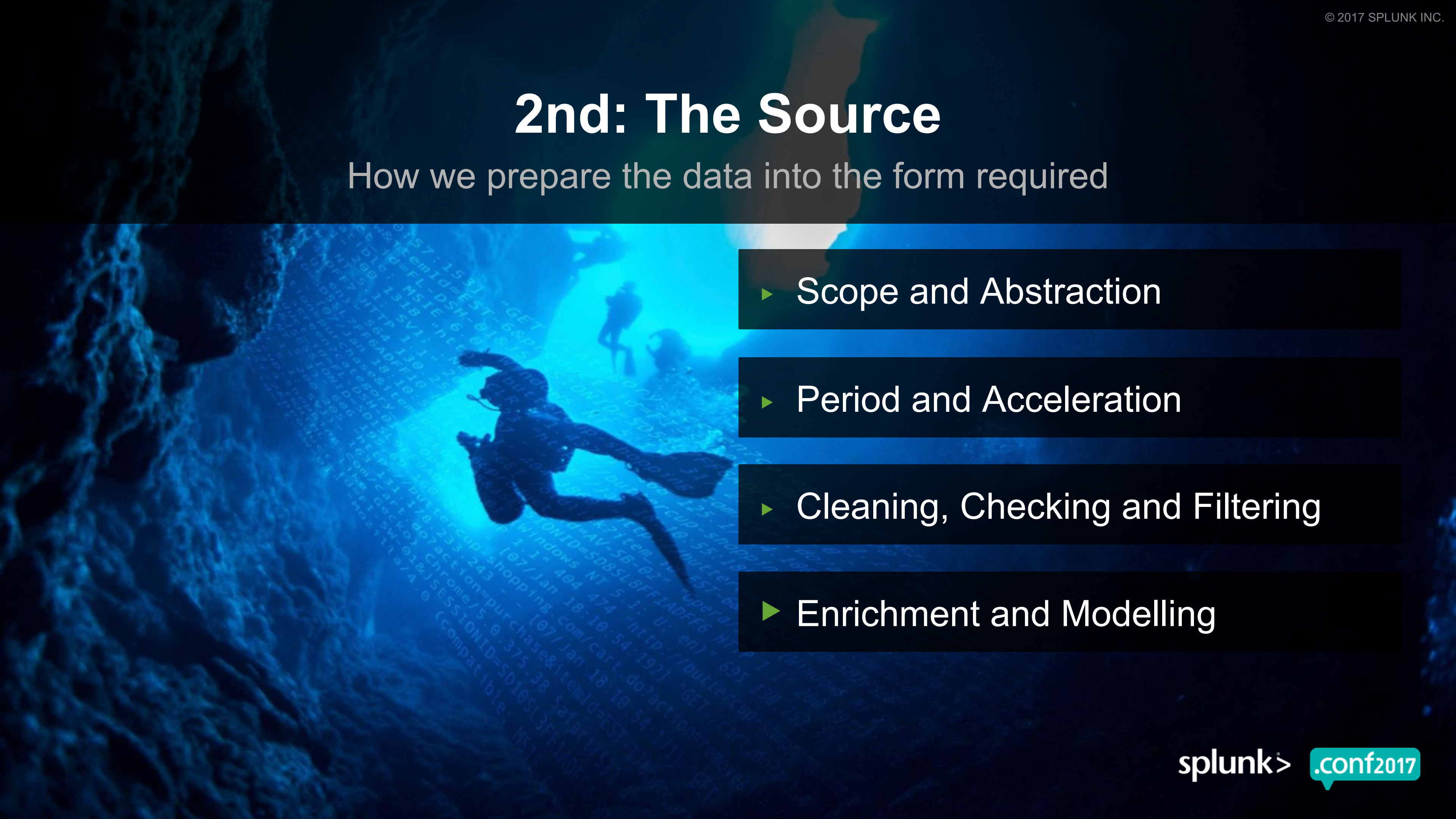
How we produce a behaviour of interest



- What is the org concerned about?
- What does it look like?

2nd: The Source

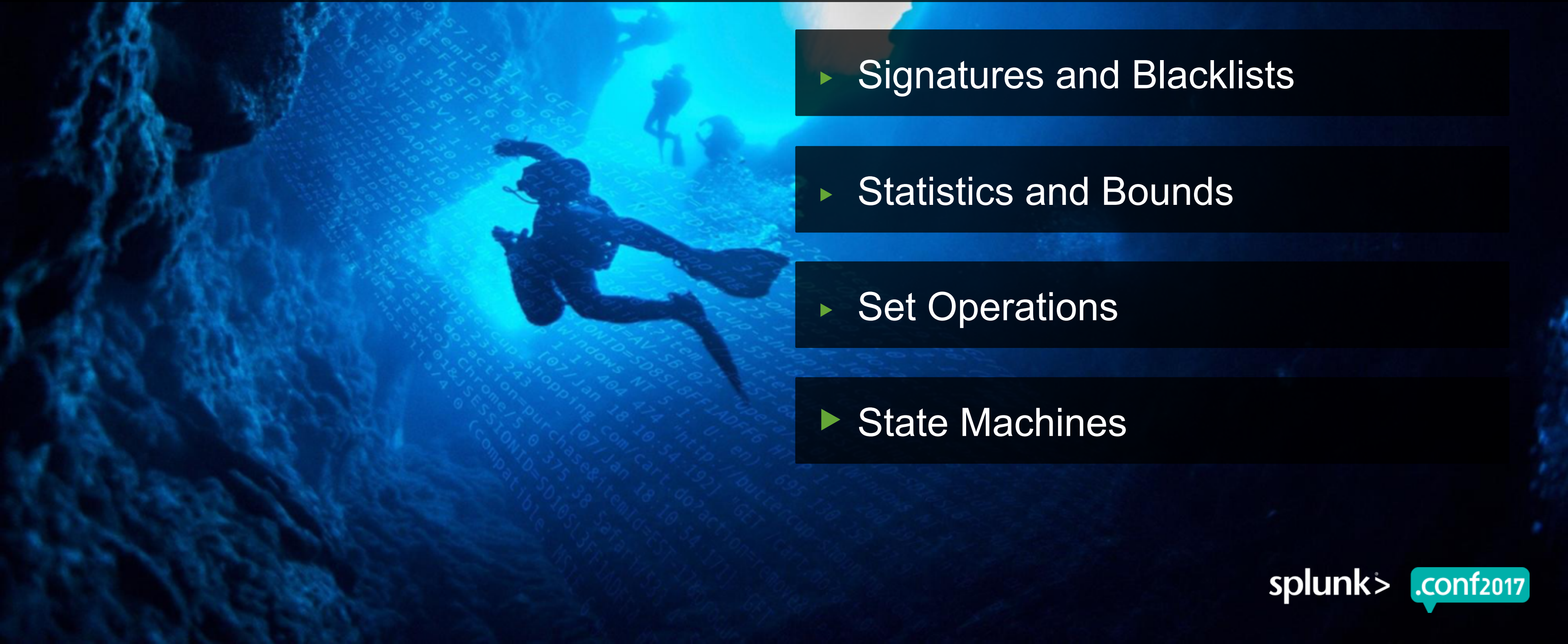
How we prepare the data into the form required



- Scope and Abstraction
- Period and Acceleration
- Cleaning, Checking and Filtering
- Enrichment and Modelling

3rd: The Metric

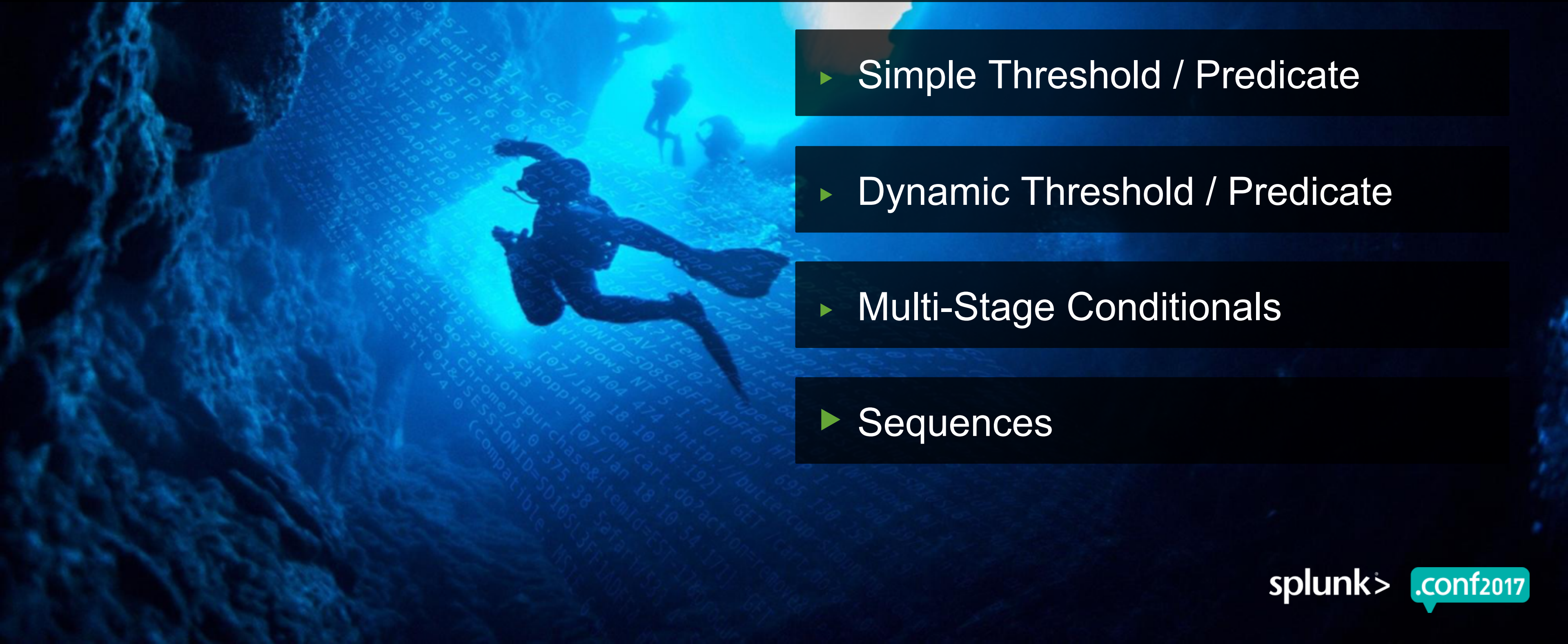
How we measure the behaviour of interest



- Signatures and Blacklists
- Statistics and Bounds
- Set Operations
- State Machines

4th: The Conditions

How do we determine when the behaviour is of interest



- Simple Threshold / Predicate
- Dynamic Threshold / Predicate
- Multi-Stage Conditionals
- Sequences

5th: The Triage

How to interpret and action an event

- Fields and Documentation
- Analysis and Enrichment
- Actions and Remediation
- Fidelity and Refinement

Extensions and Customizations

Developing a SIEM to meet the needs of your team.

splunk> .conf2017

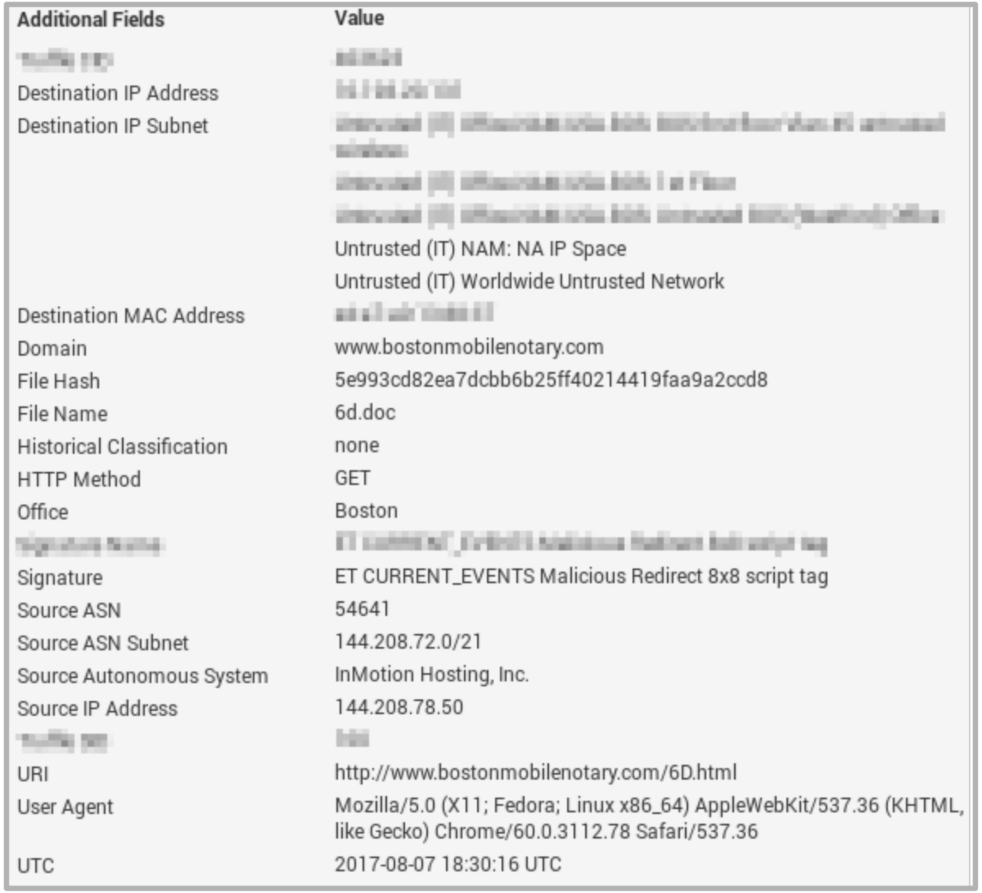
Enrichment

Internal

- Network Sessions (DHCP lease, VPN session)
- User Endpoints (learnt devices)
- pDNS (derived from DNS logs / wire data)
- Notable Comment Key-Value Extraction
- Internal Subnets
- User Watchlist (https://splunkbase.splunk.com/app/3591/)
- Notable Macro

External

- Autonomous System Lookup (https://splunkbase.splunk.com/app/3531/)
- In-line Whois (https://splunkbase.splunk.com/app/3506/)
- pDNS (https://splunkbase.splunk.com/app/3050/)
- Democracy Index



Additional Fields	Value
[redacted]	[redacted]
Destination IP Address	[redacted]
Destination IP Subnet	[redacted] Untrusted (IT) NAM: NA IP Space Untrusted (IT) Worldwide Untrusted Network
Destination MAC Address	[redacted]
Domain	www.bostonmobilenotary.com
File Hash	5e993cd82ea7dcbb6b25ff40214419faa9a2ccd8
File Name	6d.doc
Historical Classification	none
HTTP Method	GET
Office	Boston
[redacted]	[redacted]
Signature	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag
Source ASN	54641
Source ASN Subnet	144.208.72.0/21
Source Autonomous System	InMotion Hosting, Inc.
Source IP Address	144.208.78.50
[redacted]	[redacted]
URI	http://www.bostonmobilenotary.com/6D.html
User Agent	Mozilla/5.0 (X11; Fedora; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.78 Safari/537.36
UTC	2017-08-07 18:30:16 UTC

Enrichment

Network Sessions and BYOD Devices

Attribution of network activity to a specific user/device

Network Sessions lookup:

- Source: VPN session / DHCP lease start events
- KVStore Collection-based temporal lookup
- “Appended” by scheduled search run every few minutes
- Another scheduled search periodically prunes old sessions from the lookup to ensure size doesn’t grow indefinitely
- Fields: start, src_mac, src_ip, user, nt_host, assigned_ip

Check carefully your events aren’t lying to you.

Enrichment

Network Sessions and BYOD Devices

Attribution of device to a specific user

User Endpoints lookup:

- Source: Auth events with src_ip
- KVStore Collection-based lookup
- “Appended” by scheduled search run periodically
- Uses Network Sessions lookup to determine MAC address
- Fields: key(network_session_src_mac), os_type, nt_host, user, updated

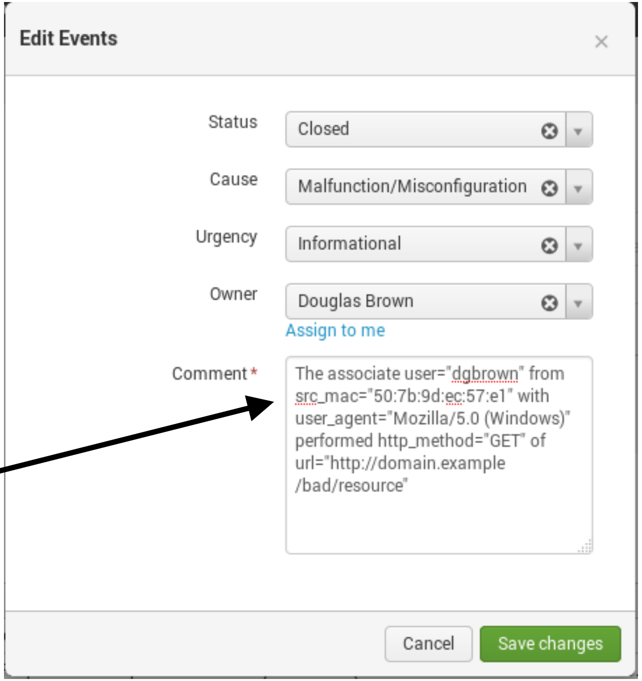
Automatically learns about devices, when last used and who owns them.

ES asset source with asset priority mirroring the user that owns the device.

Enrichment

Notable Comment-derived Dynamic Enrichment

- The fields in notables are fixed* but analysts find information during triage
- We want to be able to add field values dynamically so they can be pivoted upon and to ensure the investment of analyst time in triaging notables is most effectively reused
- If we associate a notable with a user, it can then appear in their swimlane
- Free-form prose with Key-Value pairs according to CIM-based taxonomy.



Edit Events

Status: Closed

Cause: Malfunction/Misconfiguration

Urgency: Informational

Owner: Douglas Brown

Comment *: The associate user="dgbrown" from src_mac="50:7b:9d:ec:57:e1" with user_agent="Mozilla/5.0 (Windows)" performed http_method="GET" of url="http://domain.example /bad/resource"

Enrichment

Scheduled Search To Build Extraction Lookup

```
|`incident_review`

| rename comment as _raw | extract mv_add=true | rename _raw as comment

| search user=* OR src_ip=* OR …

| stats values(user) as user values(src) as src ... by rule_id

| mvexpand <multi_value_fields>

| outputlookup incident_review_comment_extractions
```

Enrichment

Dynamic Notable Enrichment

SA-ThreatIntelligence/local/macros.conf:

```
[notable_by_id(1)]
definition = `get_notable_index` \

| `get_event_id` \

| search event_id="$event_id$" \

| ... \

| lookup user_watchlist _key AS user OUTPUT start AS watchlist_start, end AS watchlist_end, reason AS watchlist_reason,
comment AS watchlist_comment, creator AS watchlist_creator \

| eval watchlist=if(isnotnull(watchlist_start),if(watchlist_start<_time AND watchlist_end>_time,watchlist_reason + ": " +
if(isnull(watchlist_comment),"no comment",watchlist_comment) + " (" + watchlist_creator + ")","On watchlist either before or
after this notable"),null())
```

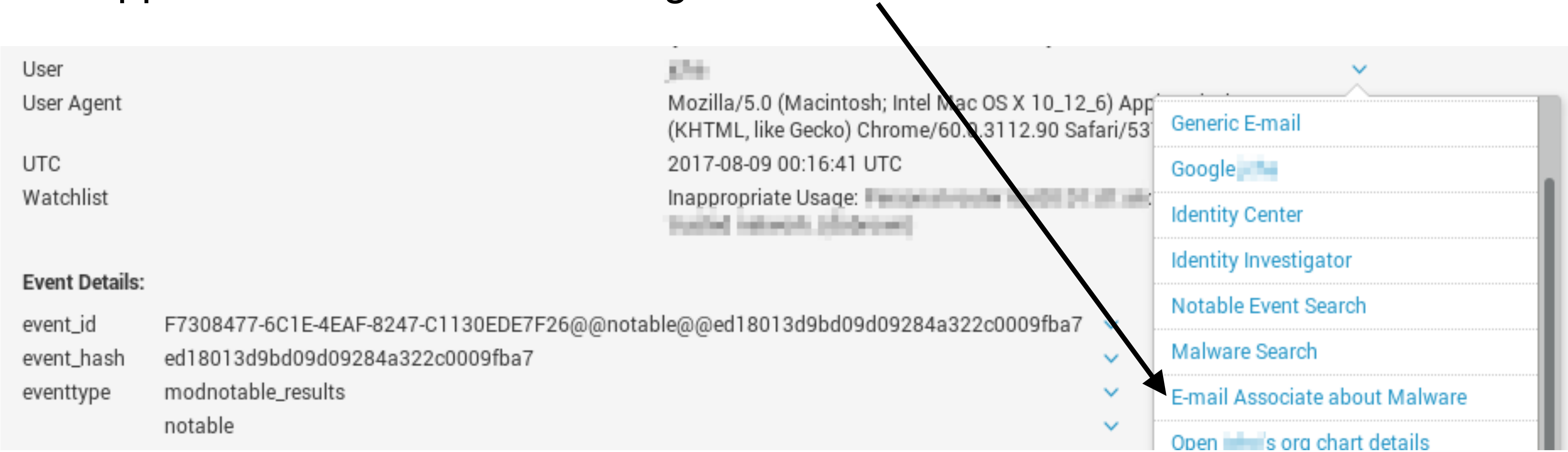
This macro is used by **all** ES' notable dashboards, etc.

Example of custom commands appended to macro to add arbitrary and *dynamic* notable enrichment

Customizations

E-mail Workflow Action

- Workflow actions are just links
- We can use url encoded mailto: links with tokens
- Each workflow action is then an e-mail template that auto populates
- Approach allows us to PGP sign e-mails



User	[redacted]
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) App (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/53
UTC	2017-08-09 00:16:41 UTC
Watchlist	Inappropriate Usage: [redacted]

Event Details:

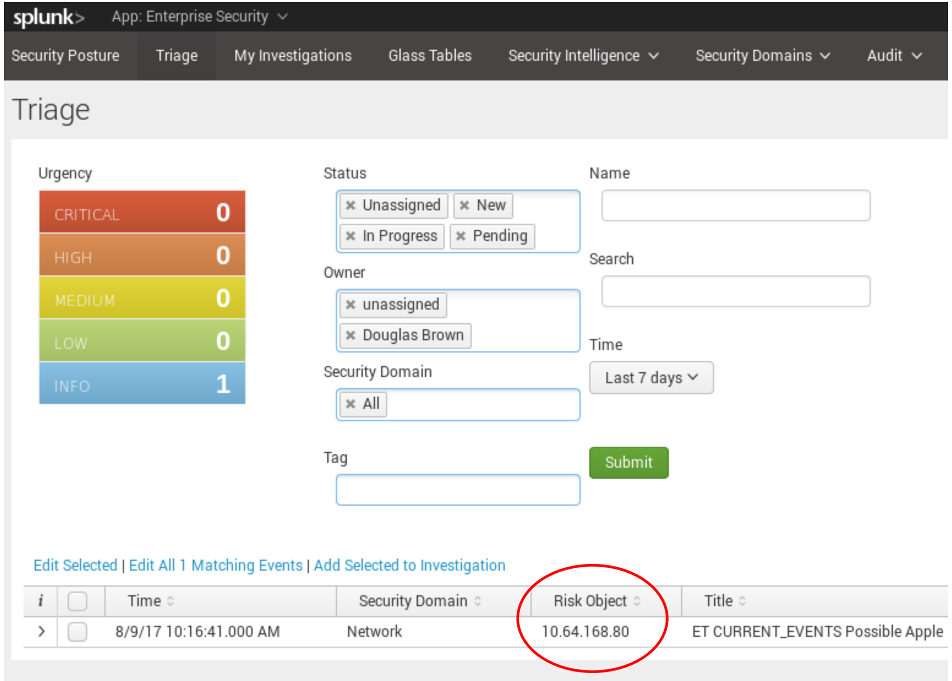
event_id	F7308477-6C1E-4EAF-8247-C1130EDE7F26@@notable@@ed18013d9bd09d09284a322c0009fba7
event_hash	ed18013d9bd09d09284a322c0009fba7
eventtype	modnotable_results notable

Customizations

Risk Object Value

- Provides means to sort notable table and search across notables

- Use eval in correlation searches to add "risk_object_value" field to notables
- Add "Table Attribute" via "Incident Review Settings" dashboard



Triage

Urgency

CRITICAL	0
HIGH	0
MEDIUM	0
LOW	0
INFO	1

Status: × Unassigned × New × In Progress × Pending

Owner: × unassigned × Douglas Brown

Security Domain: × All

Tag:

Name:

Search:

Time: Last 7 days

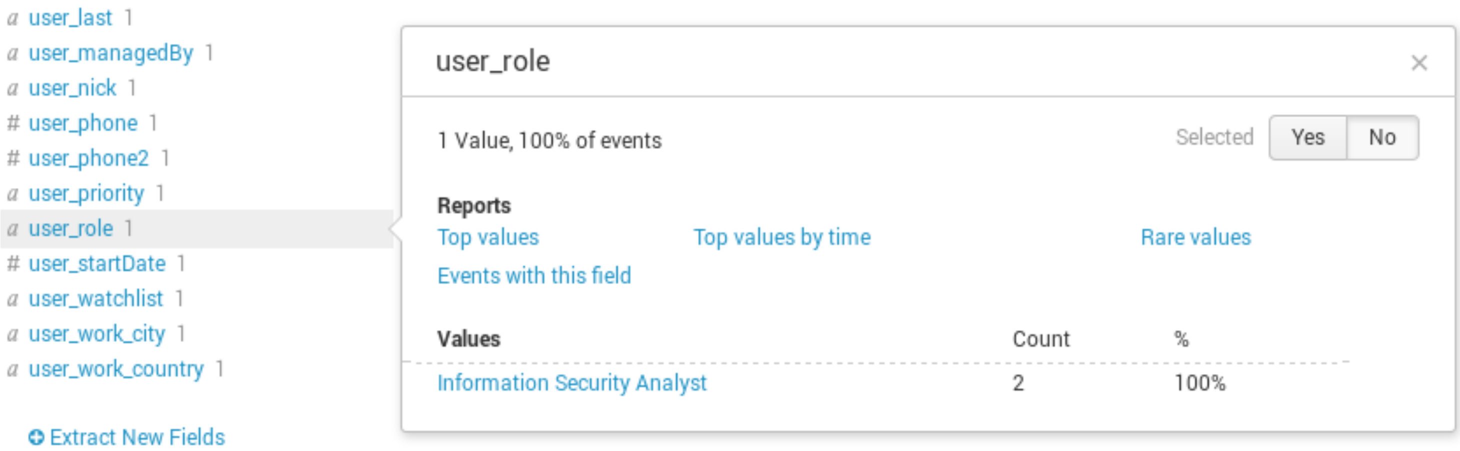
i	□	Time	Security Domain	Risk Object	Title
>	□	8/9/17 10:16:41.000 AM	Network	10.64.168.80	ET CURRENT_EVENTS Possible Apple

e.g. … | eval risk_object_value=if(like(src_ip,"10.%"),src_ip,dest_ip)

Customizations

Custom Identity and Asset Information

- Inability to add arbitrary identity/asset information is a common complaint
- Create a csv lookup and apply to [default] stanza in props.conf
    - LOOKUP-zd_identities_supplementary = identities_supplementary user



a user_last 1
a user_managedBy 1
a user_nick 1
# user_phone 1
# user_phone2 1
a user_priority 1
a user_role 1
# user_startDate 1
a user_watchlist 1
a user_work_city 1
a user_work_country 1

Extract New Fields

user_role

1 Value, 100% of events

Selected Yes No

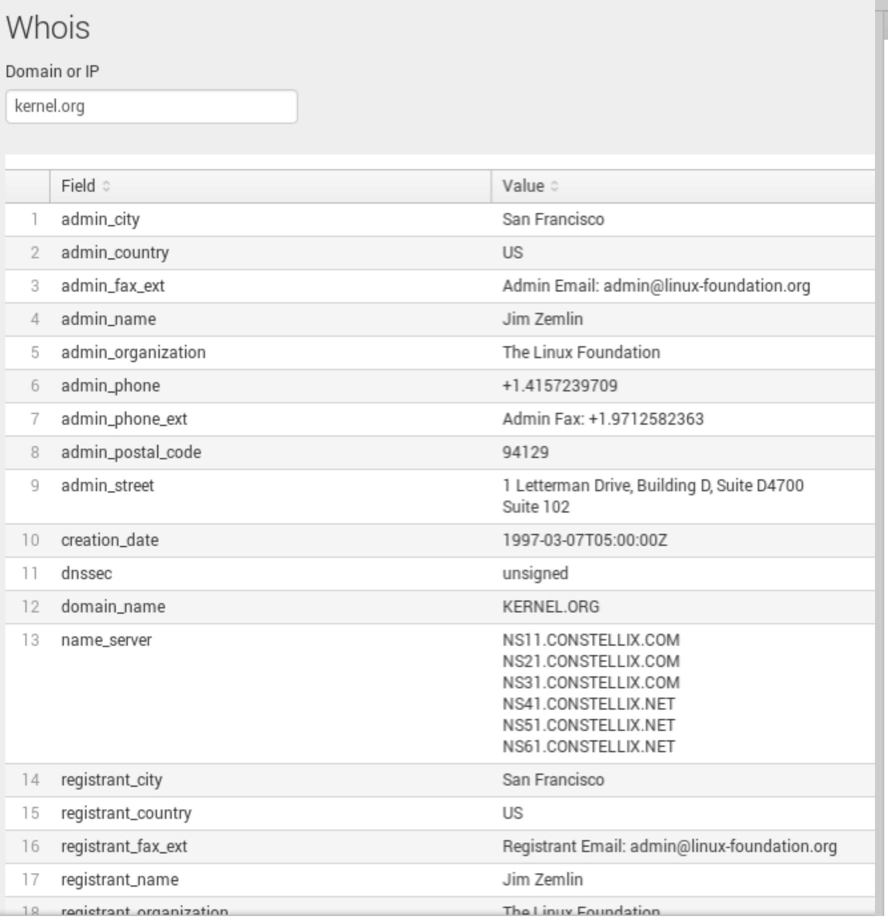
Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
Information Security Analyst	2	100%

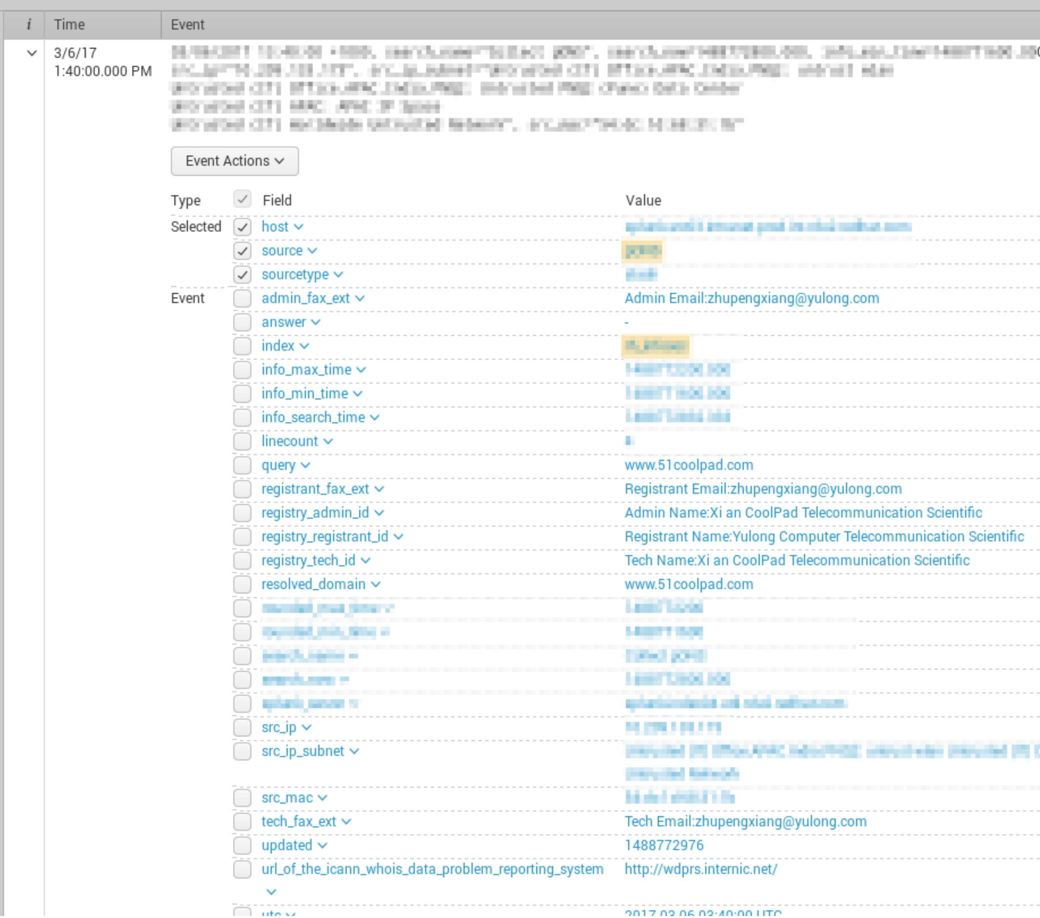
splunk> .conf2017



Whois

Domain or IP: kernel.org

	Field	Value
1	admin_city	San Francisco
2	admin_country	US
3	admin_fax_ext	Admin Email: admin@linux-foundation.org
4	admin_name	Jim Zemlin
5	admin_organization	The Linux Foundation
6	admin_phone	+1.4157239709
7	admin_phone_ext	Admin Fax: +1.9712582363
8	admin_postal_code	94129
9	admin_street	1 Letterman Drive, Building D, Suite D4700 Suite 102
10	creation_date	1997-03-07T05:00:00Z
11	dnssec	unsigned
12	domain_name	KERNEL.ORG
13	name_server	NS11.CONSTELLIX.COM NS21.CONSTELLIX.COM NS31.CONSTELLIX.COM NS41.CONSTELLIX.NET NS51.CONSTELLIX.NET NS61.CONSTELLIX.NET
14	registrant_city	San Francisco
15	registrant_country	US
16	registrant_fax_ext	Registrant Email: admin@linux-foundation.org
17	registrant_name	Jim Zemlin
18	registrant_organization	The Linux Foundation



i	Time	Event
	3/6/17 1:40:00.000 PM	[redacted]

Type	✓	Field	Value
Selected	☑	host	[redacted]
	☑	source	[redacted]
	☑	sourcetype	[redacted]
Event	□	admin_fax_ext	Admin Email:zhupengxiang@yulong.com
	□	answer	-
	□	index	[redacted]
	□	info_max_time	[redacted]
	□	info_min_time	[redacted]
	□	info_search_time	[redacted]
	□	linecount	[redacted]
	□	query	www.51coolpad.com
	□	registrant_fax_ext	Registrant Email:zhupengxiang@yulong.com
	□	registry_admin_id	Admin Name:Xi an CoolPad Telecommunication Scientific
	□	registry_registrant_id	Registrant Name:Yulong Computer Telecommunication Scientific
	□	registry_tech_id	Tech Name:Xi an CoolPad Telecommunication Scientific
	□	resolved_domain	www.51coolpad.com
	□	[redacted]	[redacted]
	□	[redacted]	[redacted]
	□	[redacted]	[redacted]
	□	[redacted]	[redacted]
	□	[redacted]	[redacted]
	□	src_ip	[redacted]
	□	src_ip_subnet	[redacted]
	□	src_mac	[redacted]
	□	tech_fax_ext	Tech Email:zhupengxiang@yulong.com
	□	updated	1488772976
	□	url_of_the_icann_whois_data_problem_reporting_system	http://wdprs.internic.net/
	□	utc	2017-03-06 03:40:00 UTC

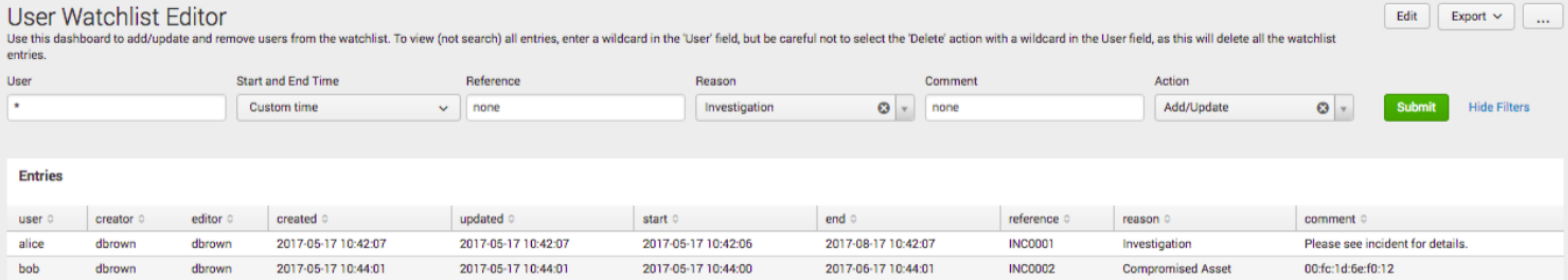
https://splunkbase.splunk.com/app/3506/

User Watchlist Editor

https://splunkbase.splunk.com/app/3591/

- Provides interface to add/edit/remove watchlist users and meta-data
- Able to be integrated with ES Identity sources:

```
...
| lookup user_watchlist _key AS identity OUTPUT end AS watchlist_end
| eval watchlist=if(isnotnull(watchlist_end),if(watchlist_end>now(),"true",null()),null())
| fields - watchlist_end
```



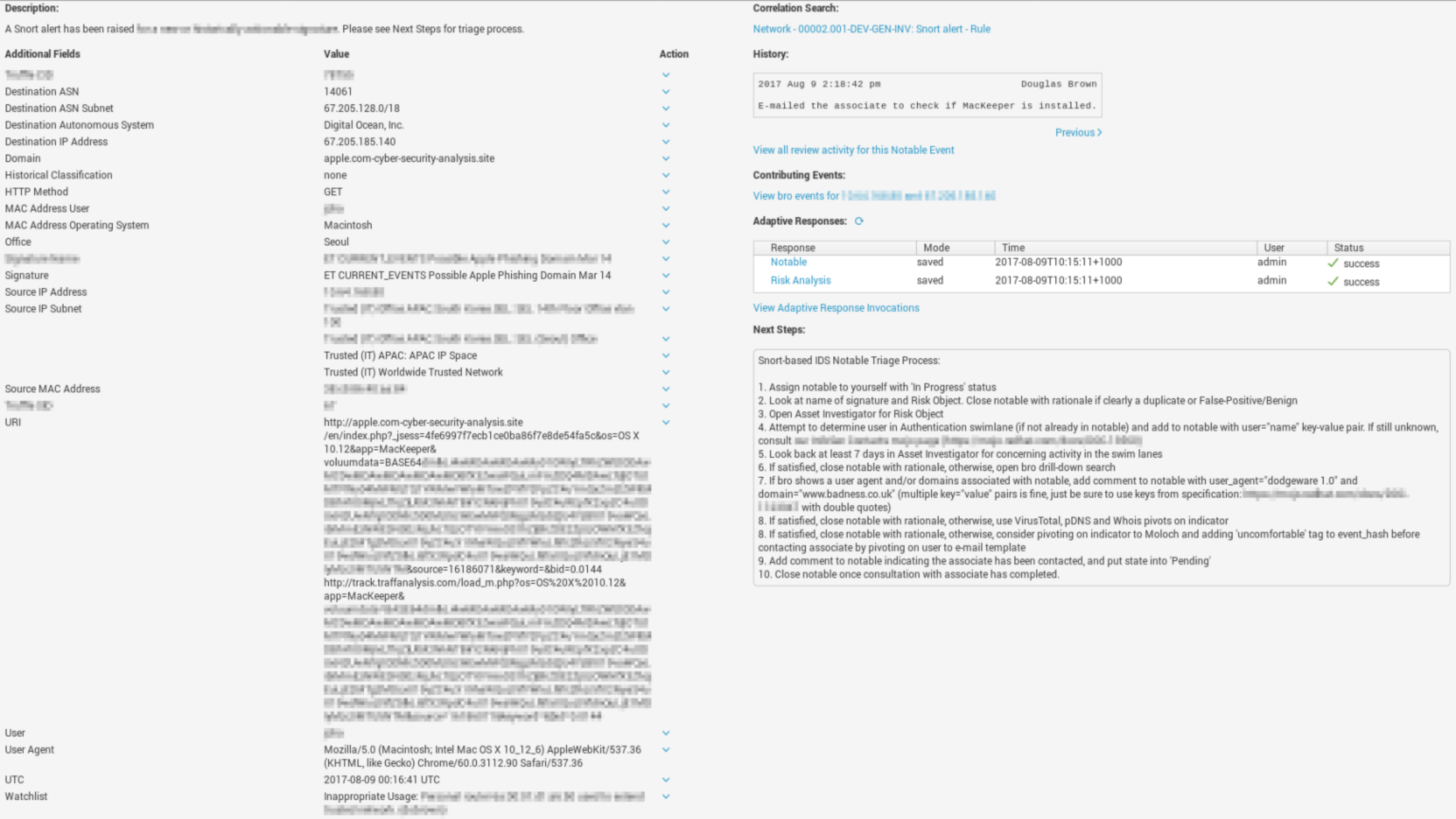
User Watchlist Editor

Use this dashboard to add/update and remove users from the watchlist. To view (not search) all entries, enter a wildcard in the 'User' field, but be careful not to select the 'Delete' action with a wildcard in the User field, as this will delete all the watchlist entries.

User	Start and End Time	Reference	Reason	Comment	Action
*	Custom time	none	Investigation	none	Add/Update

Entries

user	creator	editor	created	updated	start	end	reference	reason	comment
alice	dbrown	dbrown	2017-05-17 10:42:07	2017-05-17 10:42:07	2017-05-17 10:42:06	2017-08-17 10:42:07	INC0001	Investigation	Please see incident for details.
bob	dbrown	dbrown	2017-05-17 10:44:01	2017-05-17 10:44:01	2017-05-17 10:44:00	2017-06-17 10:44:01	INC0002	Compromised Asset	00:fc:1d:6e:f0:12



Description:

A Snort alert has been raised [redacted]. Please see Next Steps for triage process.

Additional Fields	Value	Action
[redacted]	[redacted]	⌄
Destination ASN	14061	⌄
Destination ASN Subnet	67.205.128.0/18	⌄
Destination Autonomous System	Digital Ocean, Inc.	⌄
Destination IP Address	67.205.185.140	⌄
Domain	apple.com-cyber-security-analysis.site	⌄
Historical Classification	none	⌄
HTTP Method	GET	⌄
MAC Address User	[redacted]	⌄
MAC Address Operating System	Macintosh	⌄
Office	Seoul	⌄
[redacted]	[redacted]	⌄
Signature	ET CURRENT_EVENTS Possible Apple Phishing Domain Mar 14	⌄
Source IP Address	[redacted]	⌄
Source IP Subnet	[redacted]	⌄
	[redacted]	⌄
	Trusted (IT) APAC: APAC IP Space	⌄
	Trusted (IT) Worldwide Trusted Network	⌄
Source MAC Address	[redacted]	⌄
[redacted]	[redacted]	⌄
URI	http://apple.com-cyber-security-analysis.site /en/index.php?_jsess=4fe6997f7ecb1ce0ba86f7e8de54fa5c&os=OS X 10.12&app=MacKeeper& voluumdata=BASE64[redacted]&source=16186071&keyword=&bid=0.0144 http://track.traffanalysis.com/load_m.php?os=OS%20X%2010.12& app=MacKeeper&[redacted]	⌄
User	[redacted]	⌄
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36	⌄
UTC	2017-08-09 00:16:41 UTC	⌄
Watchlist	Inappropriate Usage: [redacted]	⌄

Correlation Search:

Network - 00002.001-DEV-GEN-INV: Snort alert - Rule

History:

```
2017 Aug 9 2:18:42 pm                                    Douglas Brown

E-mailed the associate to check if MacKeeper is installed.
```

Previous ›

View all review activity for this Notable Event

Contributing Events:

View bro events for [redacted]

Adaptive Responses: ⟳

Response	Mode	Time	User	Status
Notable	saved	2017-08-09T10:15:11+1000	admin	✓ success
Risk Analysis	saved	2017-08-09T10:15:11+1000	admin	✓ success

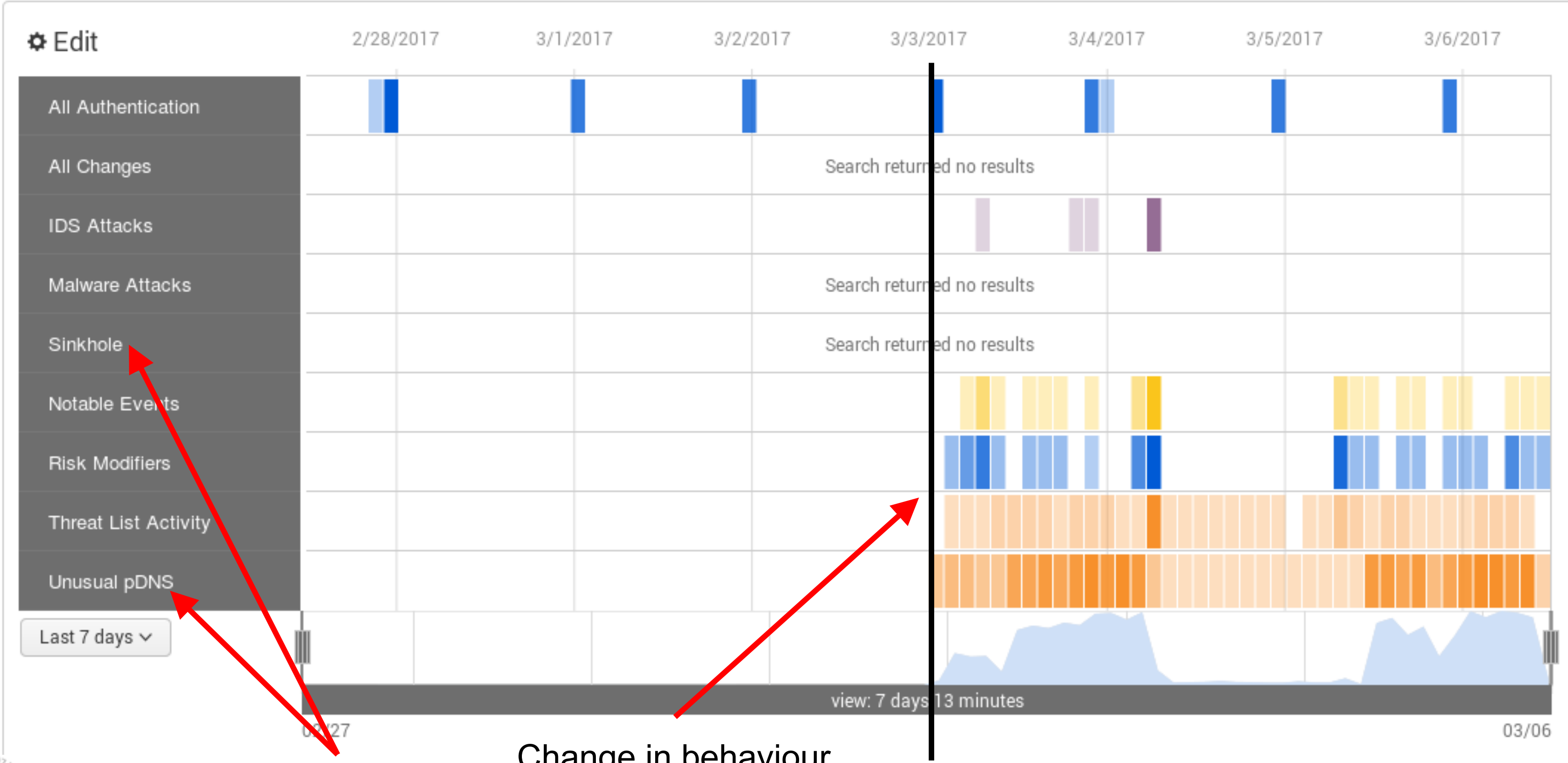
View Adaptive Response Invocations

Next Steps:

Snort-based IDS Notable Triage Process:

1. Assign notable to yourself with 'In Progress' status
2. Look at name of signature and Risk Object. Close notable with rationale if clearly a duplicate or False-Positive/Benign
3. Open Asset Investigator for Risk Object
4. Attempt to determine user in Authentication swimlane (if not already in notable) and add to notable with user="name" key-value pair. If still unknown, consult [redacted]
5. Look back at least 7 days in Asset Investigator for concerning activity in the swim lanes
6. If satisfied, close notable with rationale, otherwise, open bro drill-down search
7. If bro shows a user agent and/or domains associated with notable, add comment to notable with user_agent="dodgeware 1.0" and domain="www.badness.co.uk" (multiple key="value" pairs is fine, just be sure to use keys from specification: [redacted] with double quotes)
8. If satisfied, close notable with rationale, otherwise, use VirusTotal, pDNS and Whois pivots on indicator
8. If satisfied, close notable with rationale, otherwise, consider pivoting on indicator to Moloch and adding 'uncomfortable' tag to event_hash before contacting associate by pivoting on user to e-mail template
9. Add comment to notable indicating the associate has been contacted, and put state into 'Pending'
10. Close notable once consultation with associate has completed.

User and Asset Investigator Dashboards



Search returned no results

Search returned no results

Search returned no results

Change in behaviour

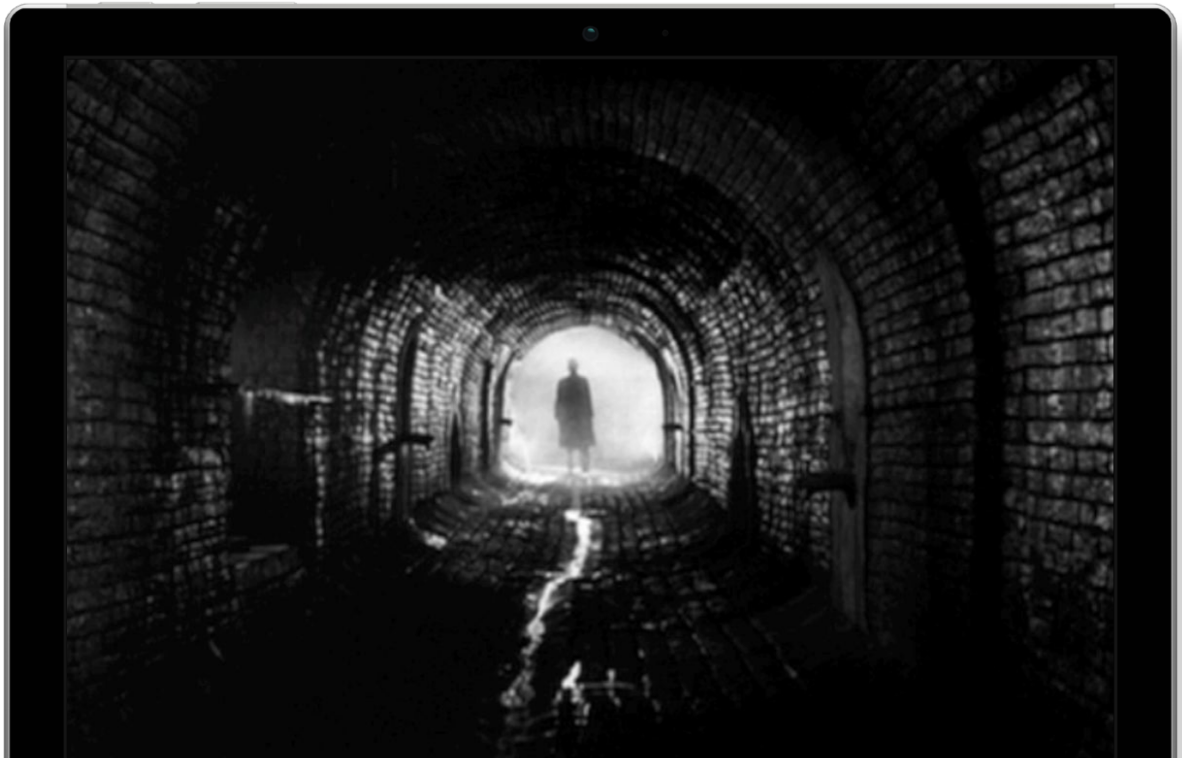
Custom swimlanes

Case Study

Third Man Correlation Search

Third Man Correlation Search

https://splunkbase.splunk.com/app/2830/



1st: The Idea

- No 2FA?
- Can we detect the use of phished credentials?
- Humans are predictable ∴ changes in pattern can be detected?

splunk> .conf2017

Third Man Correlation Search

2nd: The Source

Scope and Abstraction

- Authentication data model
- “Period” is abstraction of time

```
eval period=case(date_hour<5, 0,
date_hour<8, 1, date_hour<12, 2,
date_hour<17, 3, date_hour<20, 4,
date_hour<24, 5)
```

Period and Acceleration

- 30 days+
- Accelerated datamodel used to periodically update model
- Requires scheduled search to periodically remove old model entries

Cleaning, Checking and Filtering

- Check CIM normalisation
- Filter out new users

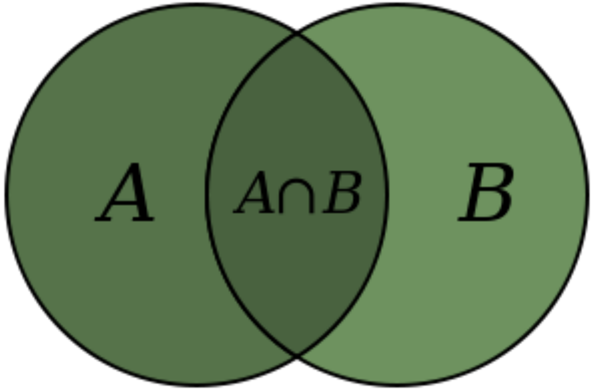
Enrichment and Modelling

- Autonomous System lookup: https://splunkbase.splunk.com/app/3531/
- KVStore lookup model: user, src_as, dest, app, wday, period (5 vectors)

Third Man Correlation Search

3rd: The Metric

- Set Operations Technology Add-On: https://splunkbase.splunk.com/app/3516/
- “unique_vectors” metric produced by *distinctfields* custom search command

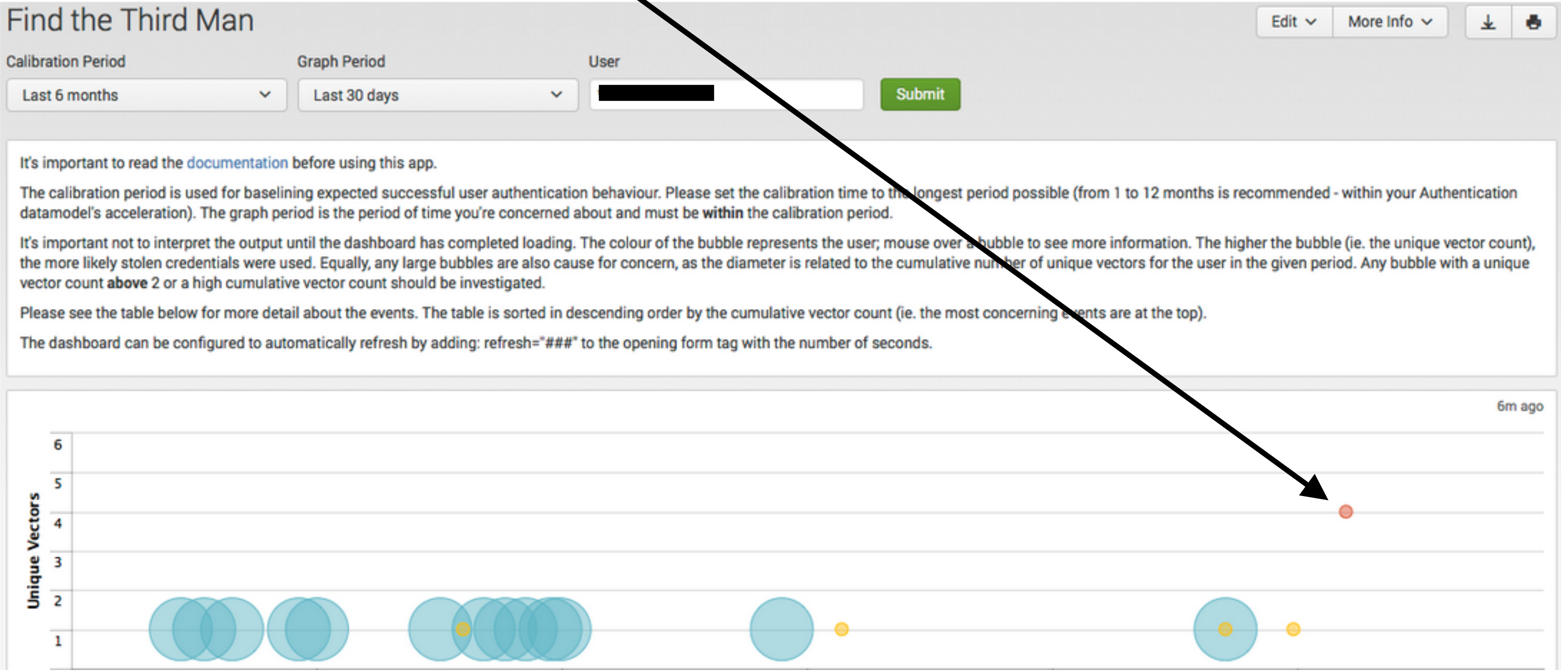


* Diagram used for illustrative purposes only - does not represent a distinct set.

Third Man Correlation Search

4th: The Conditions

- … | where unique_vectors>2



Find the Third Man

Calibration Period: Last 6 months

Graph Period: Last 30 days

User: [redacted]

It's important to read the documentation before using this app.

The calibration period is used for baselining expected successful user authentication behaviour. Please set the calibration time to the longest period possible (from 1 to 12 months is recommended - within your Authentication datamodel's acceleration). The graph period is the period of time you're concerned about and must be **within** the calibration period.

It's important not to interpret the output until the dashboard has completed loading. The colour of the bubble represents the user; mouse over a bubble to see more information. The higher the bubble (ie. the unique vector count), the more likely stolen credentials were used. Equally, any large bubbles are also cause for concern, as the diameter is related to the cumulative number of unique vectors for the user in the given period. Any bubble with a unique vector count **above** 2 or a high cumulative vector count should be investigated.

Please see the table below for more detail about the events. The table is sorted in descending order by the cumulative vector count (ie. the most concerning events are at the top).

The dashboard can be configured to automatically refresh by adding: refresh="###" to the opening form tag with the number of seconds.

Third Man Correlation Search

5th: The Triage

Fields and Documentation

- user, src_ip, src_as, dest, app, unique_vectors, unique_vector_count

Analysis and Enrichment

- Drilldown search to table of user’s authentication activity

Actions and Remediation

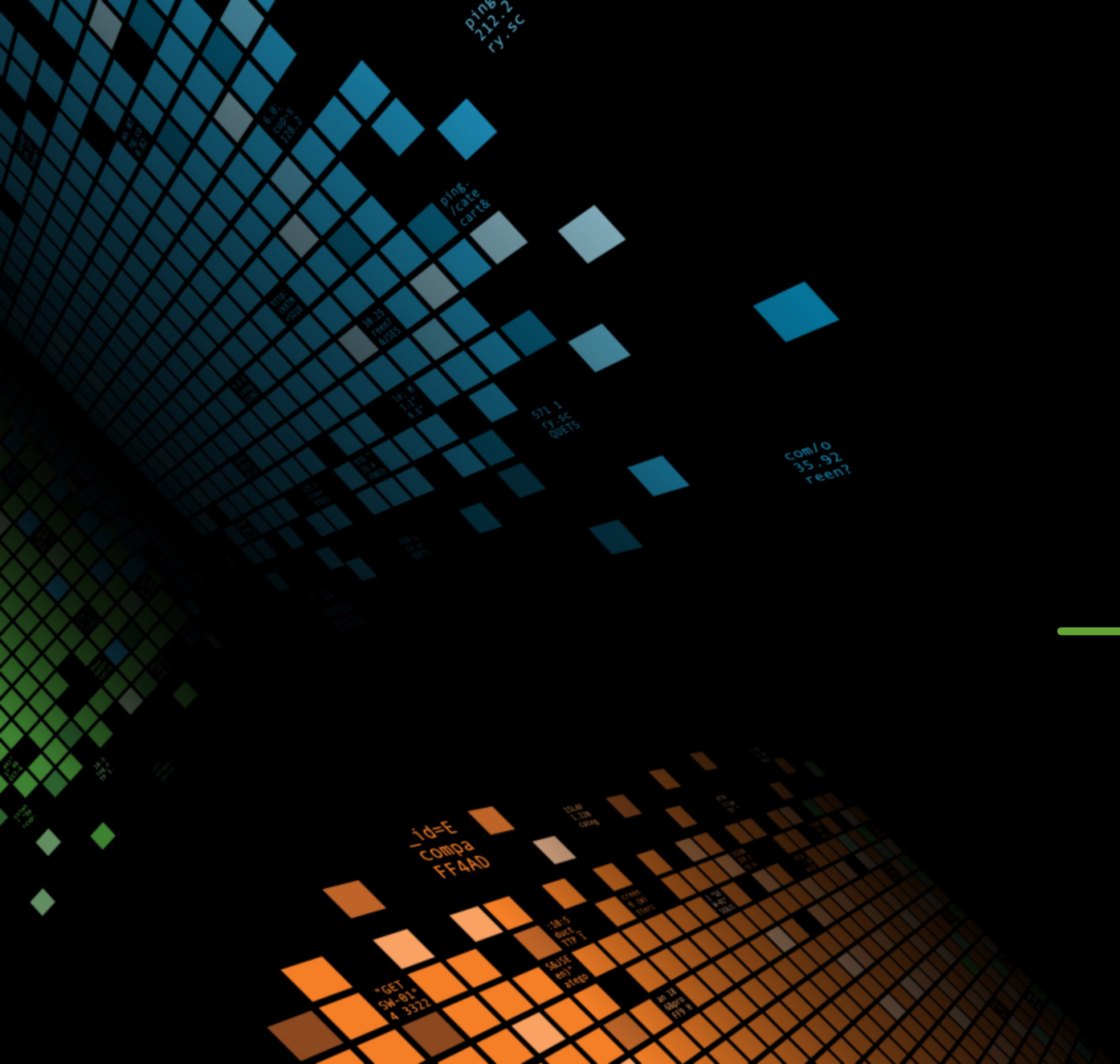
- Raise notable
- Aggregate risk - scaled dynamically in-line by number of *unique vectors*
- Place user on watchlist? (https://splunkbase.splunk.com/app/3591/)

Fidelity and Refinement

- Check for apps or other vector values to filter out
- Check CIM normalisation for inconsistencies
- Consider extending earliest time to improve fidelity

Key Takeaways

1. How to build your SIEM with ES
2. “intrinsically actionable”
3. Changes in behaviour are key
4. Risk-centric view to incident detection
5. How to develop detection techniques


ping
212.2
ry.sc
ping.
/cate
cart&
571 1
ry.sc
QUETS
com/o
35.92
reen?
_id=E
compa
FF4AD
"GET
SW-01"
4 3322

Q&A

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017

Bonus Material

UTC field in all events/notables

- You may have noticed the ‘utc’ field in the screenshots
- Geographically distributed security teams have to speak a common time
- This is especially important when extracting evidence
  - … | table _time utc index source sourcetype host _raw

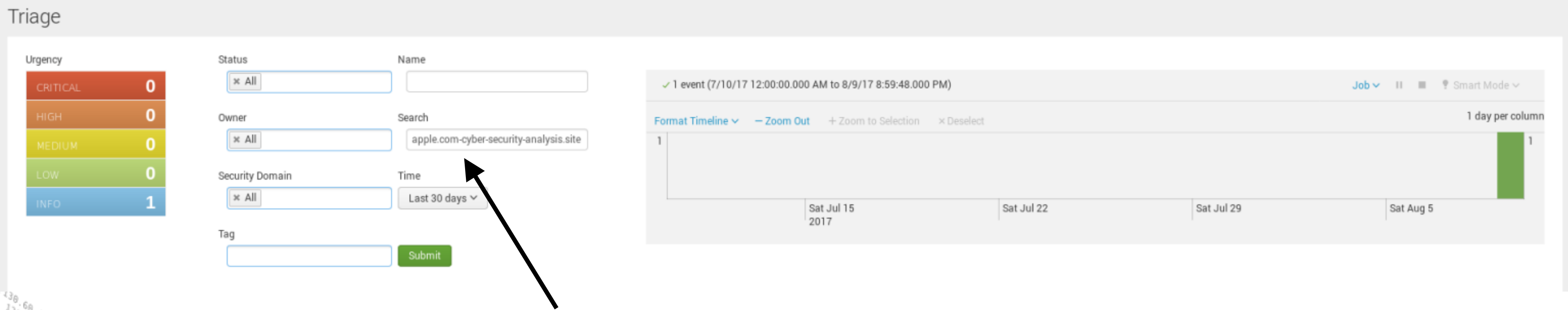
props.conf:

```
[default]
EVAL-utc = strftime(_time - (60 * 60 * tonumber(substr(strftime(_time,"%z"),2,2))) + (60 * tonumber(substr(strftime(_time,"%z"),4,2))), "%Y-%m-%d %H:%M:%S UTC")
```

Bonus Material

_raw search in Incident Review dashboard

- Much of the information in notables is not searchable without knowing fieldnames
- One solution is to “recreate” _raw to include *all* the enrichment fields
- JSON Tools app (https://splunkbase.splunk.com/app/3540/)
- In the *notable_by_id(1)* macro, add:
  - … | mkjson
  - Must be before the $event_id$ search command but after enrichment



Triage

Urgency

CRITICAL	0
HIGH	0
MEDIUM	0
LOW	0
INFO	1

Status: × All

Name:

Owner: × All

Search: apple.com-cyber-security-analysis.site

Security Domain: × All

Time: Last 30 days

Tag:

✓ 1 event (7/10/17 12:00:00.000 AM to 8/9/17 8:59:48.000 PM)

Notable search now works like core Splunk search.