

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. ©2021 Splunk Inc. All rights reserved.

How We Maintain Our Correlations in Splunk Enterprise Security at Thales UK

SEC1441A

Gabriel Vasseur

Senior Cyber Security Analyst | Thales UK

splunk> .conf21





Gabriel Vasseur

linkedin.com/in/gabrielvasseur/

- French
- Based in England
- PhD in theoretical physics
- 15 years in the IT Security industry
- Senior Cyber Security Analyst / Data Scientist / **Splunk Guru** @ Thales UK
- Likes to talk Splunk:
 - .conf16 Regex
 - .conf17 Data Model acceleration
 - .conf18 Splunk Change Tracking
 - .conf21 You're looking at it!



Thales UK

Protecting the Company

- Defense & Civil contractor
- UK ~6.5k employees
- UK SOC uses **Splunk** + **Enterprise Security** as SIEM + UBA
- Search head cluster + Indexer cluster, going to Splunk cloud
- ~**150** correlations active in Enterprise Security
- Small team! No fancy dev environment

How can we do more with less?

This Talk

MORNING CHECKS

1

Ensure your correlations **work**

BEST PRACTICES

2

Define **what** your correlations should look like

Ensure they do

TO DO'S

3

Collaborate

Ensure **visibility** of workload

PEER REVIEWS

4

Share knowledge

Promote **quality** and **consistency**

No Time to Look Under the Hood!

gabrielveasseur.com

- Source code!
- Simple XML dashboard tricks!



Where We're At

MORNING CHECKS

1

Ensure your
correlations work



BEST PRACTICES

2

Define what your
correlations should
look like

Ensure they do

TO DO'S

3

Collaborate

Ensure visibility of
workload

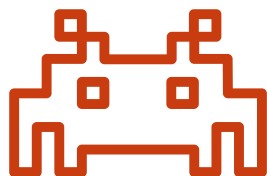
PEER REVIEWS

4

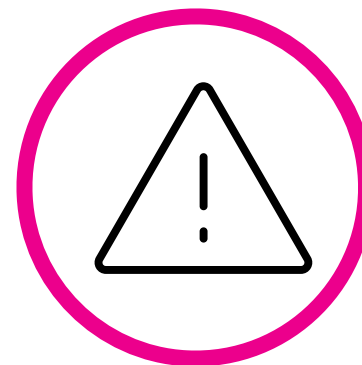
Share knowledge

Promote quality
and consistency

The Only Thing you Care About



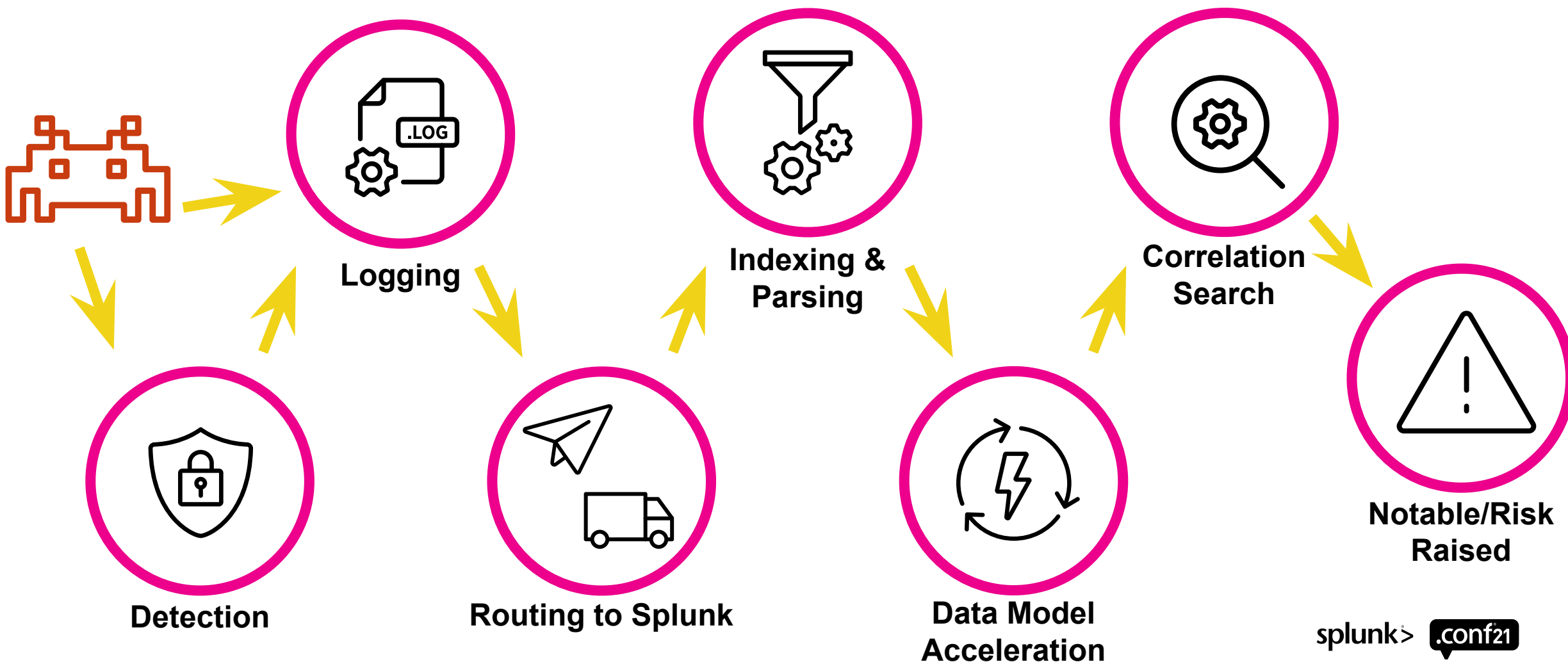
Event / Behaviour



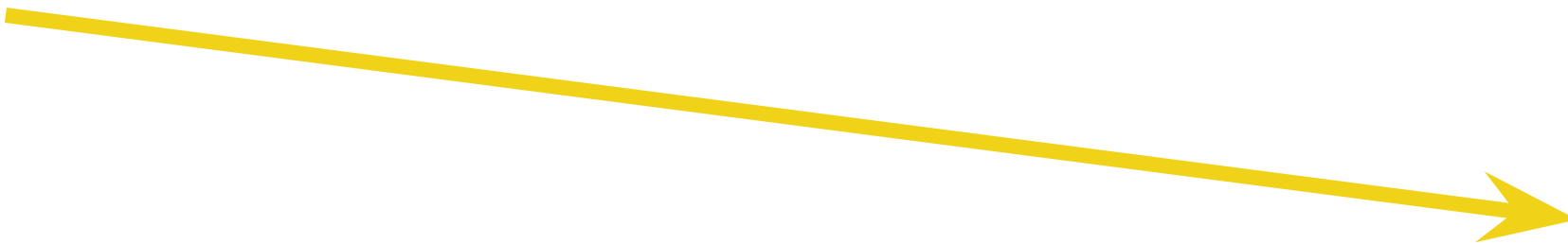
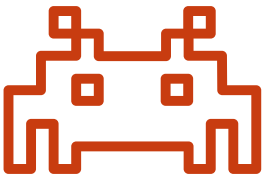
Notable/Risk
Raised

Quiet means quiet... or broken?

What Could go Wrong?



Need End-to-End Tests!



**Notable/Risk
Raised**

Morning Checks in 3 Easy Steps

1

Automate harmless triggers for your correlations

- Eicar string
- Browse to website to trigger IDS tests, blacklist, etc
- Send email that triggers auto-reply from the outside with links/attachments to trigger IDS tests
- (Manually) plug in a USB stick to trigger DLP use cases
-

2

Have your rules handle morning checks

- Mark as informational
- Reduce risk score to 0

3

Have a **morning checks checks** dashboard

↑
Not a typo!

Where We're At

MORNING CHECKS

1

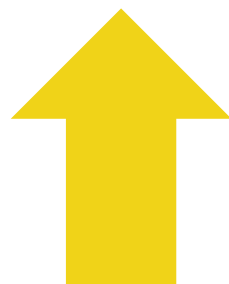
Ensure your
correlations work

BEST PRACTICES

2

Define what your
correlations should
look like

Ensure they do



TO DO'S

3

Collaborate

Ensure visibility of
workload

PEER REVIEWS

4

Share knowledge

Promote quality
and consistency

Has This Ever Happened to You?

Correlation

Job

C



Me!

Has This Ever Happened to You?

Correlation

Job

Issue 1

C



Has This Ever Happened to You?

Correlation

Job

Issue 1

C



Has This Ever Happened to You?

Correlation	Job	Issue 1
A		?
B		?
C	✓	✓
D		?
E		?
F		?
...		?



Has This Ever Happened to You?

Correlation	Job	Issue 1
A		✓
B		✓
C	✓	✓
D		✓
E		?
F		?
...		?



Has This Ever Happened to You?

Correlation	Job	Issue 1	Issue 2
A		✓	
B		✓	
C	✓	✓	
D		✓	!
E		?	
F		?	
...		?	



Has This Ever Happened to You?

Correlation	Job	Issue 1	Issue 2
A		✓	?
B		✓	?
C	✓	✓	?
D		✓	✓
E		?	?
F		?	?
...		?	?



Has This Ever Happened to You?

Correlation	Job	Issue 1	Issue 2
A		✓	✓
B		✓	✓
C	✓	✓	✓
D		✓	✓
E		✓	✓
F		✓	✓
...		?	?



Has This Ever Happened to You?

Correlation	Job	Issue 1	Issue 2	Issue 3
A		✓	✓	
B		✓	✓	
C	✓	✓	✓	
D		✓	✓	
E		✓	✓	
F		✓	✓	!
...		?	?	



Has This Ever Happened to You?

Correlation	Job	Issue 1	Issue 2	Issue 3
A		✓	✓	?
B		✓	✓	?
C	✓	✓	✓	?
D		✓	✓	?
E		✓	✓	?
F		✓	✓	!
...		?	?	?



Consistency is Key to Quality and Maintainability

Yet it is Difficult to Achieve...

- Correlation's past history
 - Built-in
 - Custom
- Quality is in the eye of the beholder
 - Personal style
 - Skill level
 - Today's motivation level



Best Practices in 3 Easy Steps

1

Agree on your own Correlation Best Practices

- Mitre Att&ck technique in annotation (RBA!)
- Use `tstats summariesonly=t`
- Has morning check, handles it, has morning check check
- ...!

2

Automate assessment

- REST command
- Regular Expressions
- Logic

3

Dashboard to gamify improvements

- See demo!

Where We're At

MORNING CHECKS

1

Ensure your
correlations work

BEST PRACTICES

2

Define what your
correlations should
look like

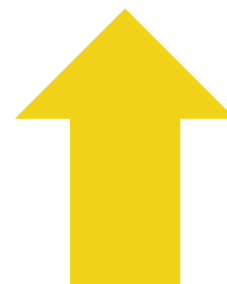
Ensure they do

TO DO'S

3

Collaborate

**Ensure visibility of
workload**



PEER REVIEWS

4

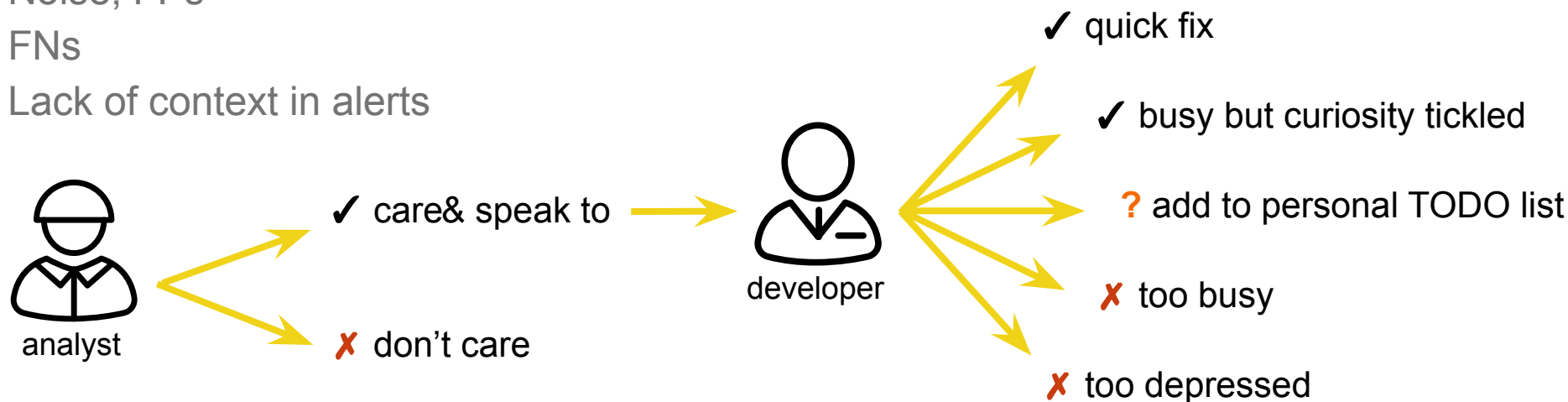
Share knowledge

Promote quality
and consistency

Maintenance Needs a Process

- Analysts are at the forefront of the issues

- Noise, FPs
- FNs
- Lack of context in alerts



- Workload managed by individuals
- No visibility

A simple TO DO framework can fix this!

Where We're At

MORNING CHECKS

1

Ensure your
correlations work

BEST PRACTICES

2

Define what your
correlations should
look like

Ensure they do

TO DO'S

3

Collaborate

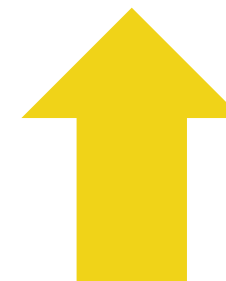
Ensure visibility of
workload

PEER REVIEWS

4

Share knowledge

Promote quality
and consistency



Why Peer Reviews

- Mistakes happen
 - Subtle edge cases
 - Embarrassing copy-paste disaster
- Morning checks + monitoring **scheduler errors** only catches the worst
- People are different
 - Skill level
 - Awareness level of limitations and subtleties
 - More than one way to do things, but not all equal!

Challenging but Rewarding

- Technical challenge
 - No built-in change control or versioning in Splunk
 - Can do DIY change tracking, but not easy [see my .conf18 talk](#)
 - Need in-splunk friendly system - see demo!
- Cultural challenge
 - Shift from defensive to grateful
- Worth it!
 - Catch more issues earlier
 - Spread knowledge
 - Increase consistency

Enough talk, demo please!

Conclusions

MORNING CHECKS

1

Morning **checks** and morning **check checks** are **paramount** to ensure your SIEM works

BEST PRACTICES

2

Well defined **Best Practices** promote quality and **consistency**

Automated audit promotes compliance through gamified workflow

TO DO'S

3

A simple **TO DO** system brings **visibility** to your on-going workload and achievements

PEER REVIEWS

4

A friendly **peer review** system reduces bugs and promotes **knowledge sharing**

Thank You

source code & more at
gabrielvasseur.com

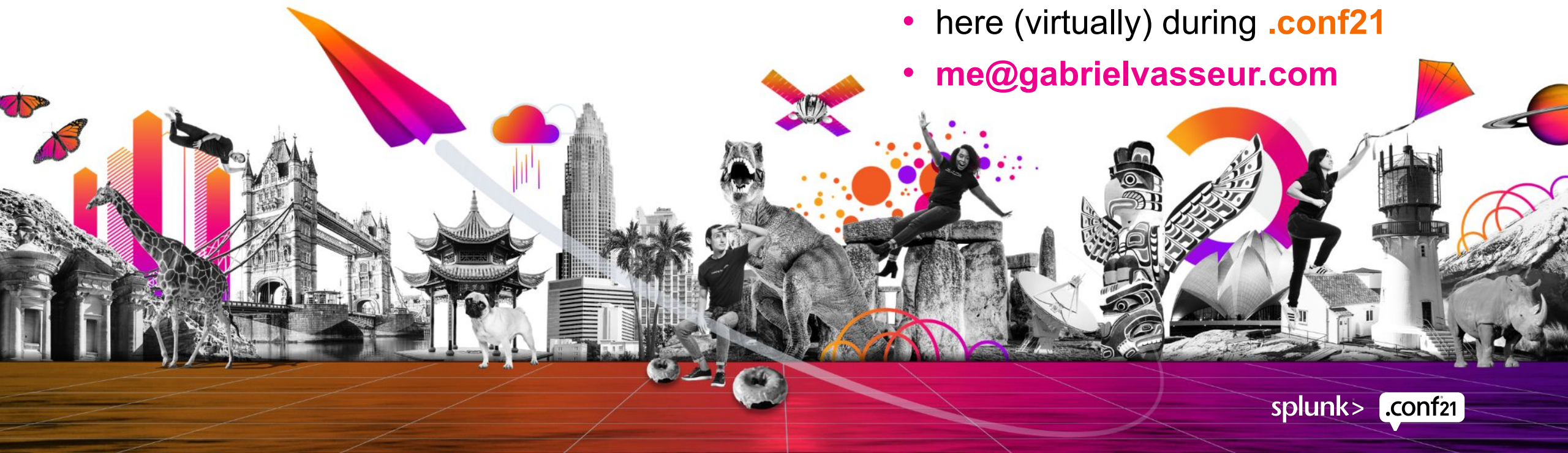
Please provide feedback via the

SESSION SURVEY



Please get in touch!

- here (virtually) during **.conf21**
- **me@gabrielvasseur.com**



Incident Review | Splunk × Morning Checks Checks | × Search | Splunk 8.2.1 × Search | Splunk 8.2.1 × +

https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/morning_checks_checker 120% ☆

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ ES Choreographer ▾ Enterprise Security

Morning Checks Checks

Edit Export ▾ ...

AV	Powershell	Webmail	Sandbox
Refresh=1m	Refresh=1m	Refresh=1m	Refresh=1m
0	0	0	0

AV morning check

- 1x notable for an eicar detection

AV step1: raw search

1

AV step2: correlation search

0

a minute ago

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

Full-screen Snip

dclock 18:38

eicar

```
splunk@Splunky: ~  
splunk@Splunky:~$ /usr/bin/clamscan --recursive --no-summary --infected -l ~/clamav.log /home/gabriel/Desktop/eicar  
/home/gabriel/Desktop/eicar/eicar.txt: Eicar-Signature FOUND  
splunk@Splunky:~$
```

01:22 -01:45

90% -01:45/03:07

Incident Review | Splunk × Morning Checks Checks × Search | Splunk 8.2.1 × Search | Splunk 8.2.1 × Search | Splunk 8.2.1 × +

https://splunk:8000/en-GB/app/SplunkEnterpriseSecuritySuite/morning_checks_checker 120% ☆

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ ES Choreographer ▾ Enterprise Security

Morning Checks Checks

Edit Export ▾ ...

AV	Powershell	Webmail	Sandbox
Refresh=1m	Refresh=1m	Refresh=1m	Refresh=1m
0	0	0	0
<div><div>🔍 ⬇️ ⓘ ↻ a few seconds ago</div><div>AV morning check</div><div>• 1x notable for an eicar detection</div></div>	AV step1: raw search	AV step2: correlation search	
	1	1	

⋮ + No investigation is currently loaded. Please create (+) or load an existing one (⋮). 🔍

dclock 18:33

eicar

splunk@Splunk: ~
splunk@Splunk:~\$ /usr/bin/clamscan --recursive --no-summary --infected -l ~/clamav.log /home/gabriel/Desktop/eicar
/home/gabriel/Desktop/eicar/eicar.txt: Eicar-Signature FOUND
splunk@Splunk:~\$

Incident Review | Splunk × Morning Checks Checks × Edit Correlation Search × Search | Splunk 8.2.1 × Search | Splunk 8.2.1 × Search | Splunk 8.2.1 ×

https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/morning_checks_checker 120%

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Security Posture Incident Review Investigations Security Intelligence Security Domains Audit Search Configure ES Choreographer Enterprise Security

Morning Checks Checks

Edit Export ...

AV Refresh=24h	Powershell Refresh=1m	Webmail Refresh=1m	Sandbox Refresh=1m
1	0	0	0

AV morning check

- 1x notable for an eicar detection

AV step1: raw search 1

AV step2: correlation search 1

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

dclock 18:30

eicar

```
splunk@Splunky: ~  
splunk@Splunky:~$ /usr/bin/clamscan --recursive --no-summary --infected -l ~/clamav.log /home/gabriel/Desktop/eicar  
/home/gabriel/Desktop/eicar/eicar.txt: Eicar-Signature FOUND  
splunk@Splunky:~$
```

Incident Review | Splunk x Best Practices | Splunk x +

← → ↻ https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/correlation_searches_best_practices?form.show_fields=status&form.show_fields=actions&form.show_fields=keyness&form.st ☆

splunk>enterprise Apps ▾ Gabriel Vasseur ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ ES Choreographer ▾ Enterprise Security

Best Practices

Export ▾ ...

Status
☒ enabled
☐ disabled

Action
☒ notable
☒ risk
☒ email

Keyness
☒ 1 - critical
☒ 2 - Important
☒ 3 - ok
☒ 4 - whatever

Other filters
☐ problematic searches only
☐ seen in IR only

Search name pattern
*

Seen stats over
Last 7 days ▾

Show fields
☒ Status
☒ Actions
☐ IR stats
☐ Seen stats
☒ Keyness

☐ Show summary table [Hide Filters](#)

Best Practices

quick correlation data refresh

title	status	actions	key	mitre	schedule	frequency	latest	throttle	tstats	mrng_chk	redteam	leaver	fields	format	identities	drilldown	queue	suppr	workflow	dshbrd	guide	risk
Access - Excessive Failed Logins - Rule	enabled	notable risk	4	NO	RT!	good	BAD	good	raw	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD
Endpoint - High Or Critical Priority Host With Malware - Rule	enabled	notable risk	4	NO	RT!	good	delayed	good	raw	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

Incident Review | Splunk x Best Practices | Splunk 8.0 x +

https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/correlation_searches_best_practices?form.show_fields=status&form.show_fields=actions&form.show_fields=keyness&form.st

splunk>enterprise Apps ▾ Gabriel Vasseur ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ ES Choreographer ▾ Enterprise Security

Best Practices Show Filters

Export ▾ ...

Best Practices

quick correlation data refresh

title	status	actions	key	mitre	schedule	frequency	latest	throttle	tstats	mrng_chk	redteam	leaver	fields	format	Identities	drilldown	queue	suppr	workflow	dshbrd	guide	risk
Access - Excessive Failed Logins - Rule	enabled	notable risk	4	NO	RT!	good	BAD	good	raw	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD
Endpoint - High Or Critical Priority Host With Malware - Rule	enabled	notable risk	4	NO	RT!	good	delayed	good	raw	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD

Search a few seconds ago

Endpoint - High Or Critical Priority Host With Malware - Rule

[Edit rule](#)
[Open in search](#)
[Rule ID card](#)
[Best Practices](#)
[IR-linked TODOs](#)
[TODO and DONE](#)
[Peer Review](#)
[Peer Review History](#)
[Comment History](#)
[Refresh data](#)

BASICS

title	description		actions	mitre_attack
Endpoint - High Or Critical Priority Host With Malware - Rule	Alerts when an infection is noted on a host with high or critical priority.		notable, risk	

schedule	cron_schedule	search_earliest	search_latest	throttled	throttled_on	throttled_for
RT!	* / 5 * * * *	rt-5m@m	rt+5m@m	yes	dest,signature	86300s

Analysis

mitre	search_duration	search_frequency	search_overlap	frequency	detection_based_on_threshold	search_latest_is_now	search_latest_is_not_too_recent	latest	throttled_for_more_than_search_duration	throttle
NO	600.000000	300	300	good	NO	NO	NO	delayed	yes	good

SEARCH

```
| from datamodel:"Malware"."Malware_Attacks" | where ('dest_priority'="high" OR 'dest_priority'="critical") | stats max("_time") as "lastTime",latest("_raw") as "orig_raw",values("dest_priority") as "dest_priority",count by "dest","signature"
```

Analysis (1 of 3)

tstats	mentions_tstats_summariesonly	mentions_tstats_but_no_data_model	search_starts_with_lookup	search_is_truncated	search_is_splunkadmin	search_uses_heavy_commands

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

Incident Review | Splunk x Best Practices | Splunk 8.0 x +

https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/correlation_searches_best_practices?form.show_fields=status&form.show_fields=actions&form.show_fields=keyness&form.st

splunk>enterprise Apps ▾

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ ES Choreographer ▾

Enterprise Security

Best Practices [Show Filters](#)

Export ▾ ...

Best Practices

[quick correlation data refresh](#)

title	status	actions	key	mitre	schedule	frequency	latest	throttle	tstats	mrng_chk	redteam	leaver	fields	format	identities	drilldown	queue	suppr	workflow	dshbrd	guide	risk
Access - Excessive Failed Logins - Rule	enabled	notable risk	4	NO	RT!	good	BAD	good	raw	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD
Endpoint - High Or Critical Priority Host With Malware - Rule	enabled	notable risk	4	NO	RT!	good	delayed	good	raw	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD

Endpoint - High Or Critical Priority Host With Malware - Rule

[Edit rule](#)
[Open in search](#)
[Rule ID card](#)
[Best Practices](#)
[IR-linked TODOs](#)
[TODO and DONE](#)
[Peer Review](#)
[Peer Review History](#)
[Comment History](#)
[Refresh data](#)

CLICK FOR INFO

BASICS

Mitre

All enabled correlation search should be related to one or more of the Mitre Att&ck techniques in an annotation. If the **mitre_attack** field below is populated, the **mitre** best practice will be green.

Schedule

The **schedule** best practice can take the following values:

- "RT!": this means the correlation is a real time search, as in its earliest and latest start with "rt", which is bad for performance. Unfortunately that is the default for a number of correlation in ES out of the box.
- "RT": the search is a normal search but on a "Real Time" schedule. This is only problematic when the platform is under heavy stress and searches are being skipped.
- "Cont.": the search is a normal search and on a "Continuous" schedule. This means that even when under stress the scheduler will avoid blindspots.

Frequency

The best practice looks at **cron_schedule**, **search_earliest** and **search_latest** and works out the **search_frequency** (how many seconds between executions of the search), **search_duration** (how many seconds between earliest and latest) and **search_overlap** (how many seconds of overlap in the search time window between 2 consecutive executions of the search). The search duration should be at least as big as the time between runs (E.g. it's ok to look back one hour every 5 minutes, but it's not ok to look back 5 minutes every hour). If the overlap is negative (e.g. looking back 5 minutes every hour), **frequency** will say "BlindSpots". We don't want to overwhelm the platform so the search should be scheduled to run every 5 minutes. Searches that are scheduled to run every 5 minutes but are throttled to run every 10 minutes will be flagged as "BlindSpots".

Latest

The best practice looks at whether or not the search relies on a count in a certain period of time (e.g. "more than X times in one hour") and puts its conclusion in **detection_based_on_threshold**

For searches that rely on a threshold, make sure **latest** is never later than -10m@m for raw searches and -15m@m for data model searches (possibly further back for Network_Traffic or Endpoint). This is to allow time for logs to make it into splunk and data models to be accelerated, otherwise it would skew the perception of what happened in that period of time. This is of course not so important if the period of time is big (bigger than an hour).

For searches that simply trigger on the occurrence of some event, there is a choice. If **earliest** is far enough in the past that there is enough overlap with the next run of the correlation search, to allow for indexing/accelerating delays, then you should set **latest** to "now" to avoid any unnecessary delays. However, if the rule is a bit heavy (using join for instance) and you don't want to run it too often, then it might be best to run it without overlap and with some delay. E.g.: -70m to -10m every hour. No overlap between searches, but enough delay.

Throttle

All correlation searches where **search_overlap** is not null should be **throttled**. You should throttle based on sensible fields, but the best practice has no way of judging what fields should be used. The throttle duration **throttled_for** should be at least as big as the **search_duration** (see **throttled_for_more_than_search_duration**). If a search looks back 2 hours every hour but is throttled for only one hour, it will always be raised twice.

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

Status of Correlation Sea ×

TODO & DONE Correlatio ×

TODO & DONE Correlatio ×

Incident Review | Splunk ×

+

← → ↺ https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/todo__done_correlation_search?form.item_name=Access - Excessive Failed Logins - Rule&hideFilters=true&form.todo 120% ☆

splunk>enterprise Apps ▾ Gabriel Vasseur ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ ES Choreographer ▾ Enterprise Security

TODO & DONE Correlation Search [Show Filters](#) Export ▾ ...

Access - Excessive Failed Logins - Rule

enabled – assigned to nobody

[→ Edit rule](#) [→ Rule ID card](#) [→ Best Practices](#) [→ IR-linked TODOs](#) [→ TODO and DONE](#) [→ Peer Review](#) [→ Peer Review History](#) [→ Comment History](#) [Refresh data](#)

[Kick into the long grass](#) [Unassign](#) [Bob](#) [Gabriel](#) [Hawksley](#)

TODO comment

[Add TODO](#)

DONE comment

[Add DONE](#)

Pending TODOs - If a TODO is linked to IR, you can click the comment to open IR around that time

_time ↕	username ↕	comment ↕	cancel ↕	mark as done ↕
2021-08-07 16:03:52	Gabriel Vasseur	Test TODOs	cancel	mark as done

DONE comments added since the last review

_time ↕	username ↕	comment ↕
2021-08-07 15:44:04	Gabriel Vasseur	I've done X today because of whatever

Last reviewed 0.0 days ago

⌵ + No investigation is currently loaded. Please create (+) or load an existing one (≡).

🔍

Status of Correlation Searches [Show Filters](#) Export ...

Review status: ☒ Ok ☒ Failed ☒ Pending

Assigned to: All x

Restrict only to: ☒ Has TODOs ☐ Needs compliance work ☒ Show recent activity

Set for summary Set for peer review Set for TODOs My TODOs

Stats for 2 searches

count	Fully Ok	Peer review required	Urgent fix required	Significant compliance required	Avg Best Practices compliance	Searches having TODO(s)	Total TODO count
2	0	0	0	2	45.0 %	2	3

Correlation Searches Status ?

title	status	seen	review_status	owner	TODO#	todo	todo_time	todoer	IR_timestamp	Best Practices Compliance
Access - Excessive Failed Logins - Rule	enabled		ok	Bob Dylan	2	Add exception for XYZ IR-1627728845 Review the threshold, too noisy	2021-08-07 16:04:03 2021-08-07 16:06:16	Gabriel Vasseur	1627728845	32 %
Endpoint - High Or Critical Priority Host With Malware - Rule	enabled	3*morncheck 6*notable >6*risk	ok	Gabriel Vasseur	1	We need to review the threshold for that rule	2021-08-07 15:28:43	Gabriel Vasseur		58 %

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

Status of Correlation SearchPeer Review Correlation SearchEdit Correlation Search

https://splunk:8000/en-GB/app/SplunkEnterpriseSecuritySuite/peer_review_correlation_search?form.item_name=Access - Excessive Failed Logins - Rule&hideFilters=true&form.is_same_opti

splunk>enterpriseAppsGabriel VasseurMessagesSettingsActivityHelpFind

Security PostureIncident ReviewInvestigationsSecurity IntelligenceSecurity DomainsAuditSearchConfigureES ChoreographerEnterprise Security

Peer Review Correlation Search [Show Filters](#)

Export...

Access - Excessive Failed Logins - Rule

enabled – assigned to Bob Dylan

[Edit rule](#)[Rule ID card](#)[Best Practices](#)[IR-linked TODOs](#)[TODO and DONE](#)[Peer Review](#)[Peer Review History](#)[Comment History](#)[Refresh data](#)

Last reviewed 0.0 days ago

_time	username	action
2021-08-07 16:27:53	Gabriel Vasseur	passed

DONE comments added since the last review

No results found.

TODO comment activity since the last review

_time	username	type	action	comment
2021-08-07 16:29:29	Gabriel Vasseur	TODO	created	4ab1c61cb0aa3c123a9bc4e44bdc8f9101627728845 Review the threshold, too noisy

2 changes

Peer Review

key	old	new
search	tstats summariesonly=true values("Authentication.tag") as "tag",dc("Authentication.user") as "user_count",dc("Authentication.dest") as "dest_count",count from datamodel="Authentication"."Authentication" where nodename="Authentication.Failed_Authentication" by "Authentication.app","Authentication.src" rename "Authentication.app" as "app","Authentication.src" as "src" where 'count'>=5	tstats summariesonly=true values("Authentication.tag") as "tag",dc("Authentication.user") as "user_count",dc("Authentication.dest") as "dest_count",count from datamodel="Authentication"."Authentication" where nodename="Authentication.Failed_Authentication" by "Authentication.app","Authentication.src" rename "Authentication.app" as "app","Authentication.src" as "src" where 'count'>=7
search_earliest	-65m@m	-125m@m

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Status of Correlation SearchPeer Review Correlation SearchEdit Correlation Search

https://splunky:8000/en-GB/app/SplunkEnterpriseSecuritySuite/peer_review_correlation_search?form.item_name=Access - Excessive Failed Logins - Rule&hideFilters=true&form.is_same_opti

search

nodename="Authentication.Failed_Authentication" by "Authentication.app","Authentication.src"
| rename "Authentication.app" as "app","Authentication.src" as "src"
| where 'count'>=6

search_earliest-65m@m

search

nodename="Authentication.Failed_Authentication" by "Authentication.app","Authentication.src"
| rename "Authentication.app" as "app","Authentication.src" as "src"
| where 'count'>=7

search_earliest-125m@m

☒ Show changed values
☐ Show unchanged values

Configuration changes

key	old	new
search	tstats summariesonly=true values("Authentication.tag") as "tag",dc("Authentication.user") as "user_count",dc("Authentication.dest") as "dest_count",count from datamodel="Authentication"."Authentication" where nodename="Authentication.Failed_Authentication" by "Authentication.app","Authentication.src" rename "Authentication.app" as "app","Authentication.src" as "src" where 'count'>=6	tstats summariesonly=true values("Authentication.tag") as "tag",dc("Authentication.user") as "user_count",dc("Authentication.dest") as "dest_count",count from datamodel="Authentication"."Authentication" where nodename="Authentication.Failed_Authentication" by "Authentication.app","Authentication.src" rename "Authentication.app" as "app","Authentication.src" as "src" where 'count'>=7
search_earliest	-65m@m	-125m@m

Best practices evolution - Note: compliance may evolve separately from the configuration, if the best practices algorithms have changed

time	mitre	schedule	frequency	latest	throttle	tstats	morning_check	redteam	leaver	fields	format	identities	drilldown	queue	suppression	workflow	dashboard	guide	risk
old	NO	RT	good	BAD	good	tstats DM	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD
new	NO	RT	good	good	good	tstats DM	NO	NO	N/A	BAD	BAD	BAD	BAD	good	good	NO	NONE	NONE	BAD

TODO comment

Add TODO

Pending TODOs, assigned to Bob Dylan

_time	username	comment	cancel	mark as done
2021-08-07 16:29:29	Gabriel Vasseur	4ab1c61cb0aa3c123a9bc4e44bdc8f91@1627728845 Review the threshold, too noisy	cancel	mark as done
2021-08-07 16:04:03	Gabriel Vasseur	Add exception for XYZ	cancel	mark as done

Pass review

Fall review

No investigation is currently loaded. Please create (+) or load an existing one (≡).