Risk-Based Alerting

Gabriel Vasseur
gabrielvasseur.com

Goals

- Candid “how we use Splunk as a SIEM” & how RBA fits in
- Not prescriptive! Even though it may sound like it…
- Please debate on the RBA slack channel (or email me):
  - what you liked
  - what you’re worried about
  - how you do things differently/better
- Feel free to ask questions!

gabrielvasseur.com

Plan

- Me & our SOC
- Our approach to the SIEM
- How we manage detections
  - Morning checks
  - Best Practices
  - Peer Reviews
  - TODOs
  - Weekly meeting
  - Monitor hub
- What is RBA?
- RBA implementations elements
  - A&I normalisation
  - Deduplication
  - Investigation dashboard
  - Managing noise
- Recap & Q&A

Presentations

Me: gabrielvasseur.com

- PhD, French, in the UK
- 9 years as main Splunk admin in the SOC
- 4 .conf talks
- 2023 Splunkie "The Inventor" Award nominee

Our SOC:

- 12+ years using Splunk and ES
- small team (no levels, mix of analyst and developer skills)
- no fancy detection as code CI/CD multiple environments etc
- moved to Splunk Cloud in 2021
- SOAR
- Looking at ES8

Our approach to the SIEM – Goes without saying?

- Rely heavily on data models
    - CIM compliance TA work
    - Enhanced DMs
- 100s of correlations (ideally using tstats summariesonly=t)

Notable events (aka findings) in Incident Review must be as helpful as possible:

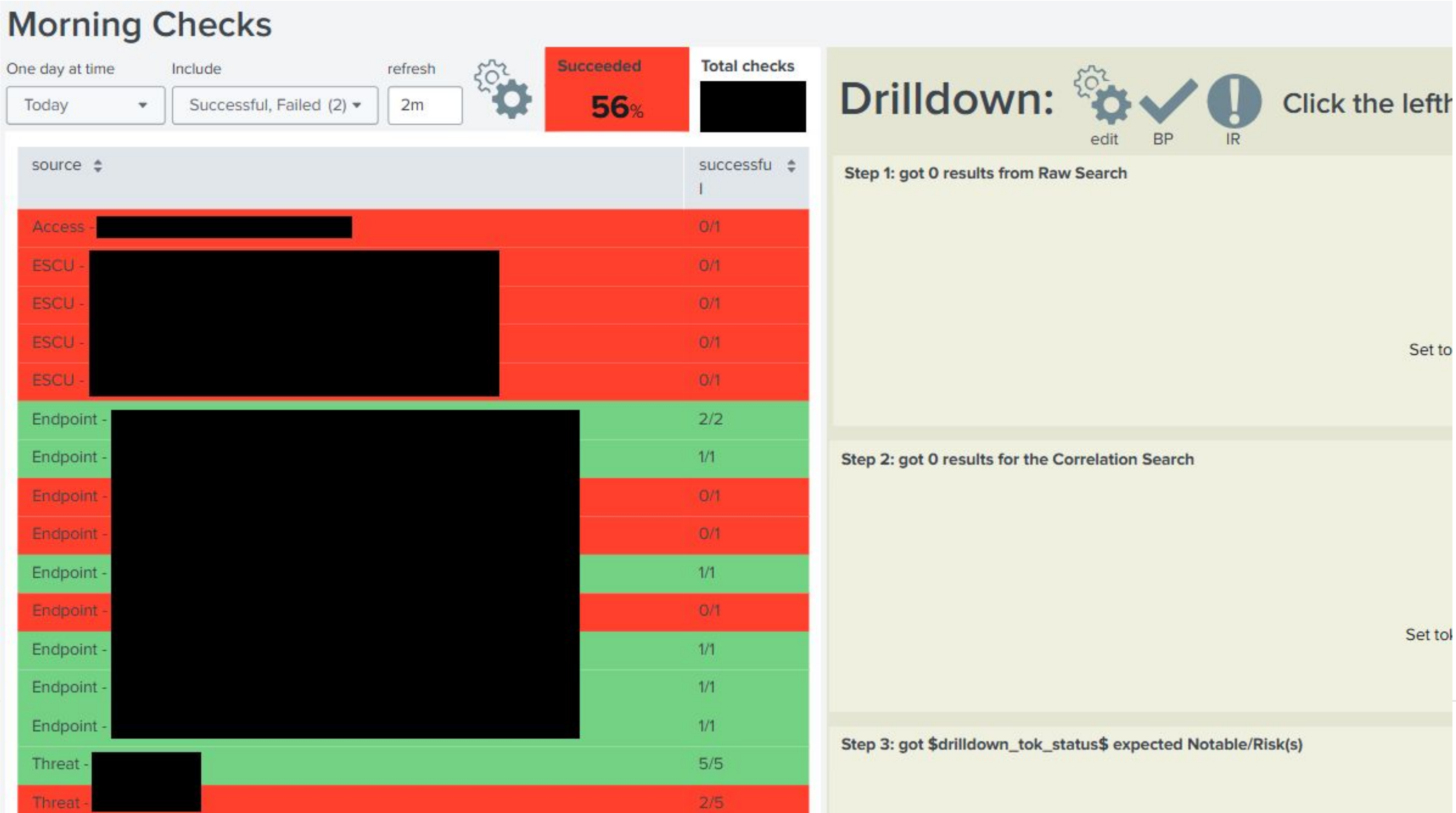
- Detailed title
- Assets & Identities and other enrichment
- Display all the useful (key) fields in IR
- drilldown search runs the correlation search again (concurrent, throttled or risk-only activity)
- workflow action links to analyst guide wiki
- workflow action(s) (drilldown dashboards!?) to investigation dashboards
- workflow action to risk overview dashboard for the entity(ies) involved

RBA makes this more difficult!

Managing the correlations (see .conf21 talk!)

1. Morning checks

- end-to-end tests: e.g. Eicar string → Host with malware alert
- notable suppression for is_morning_check="yes"



Morning Checks

One day at time: Today

Include: Successful, Failed (2)

refresh: 2m

Succeeded: 56%

Total checks: [redacted]

source	successful
Access - [redacted]	0/1
ESCU - [redacted]	0/1
ESCU - [redacted]	0/1
ESCU - [redacted]	0/1
ESCU - [redacted]	0/1
Endpoint - [redacted]	2/2
Endpoint - [redacted]	1/1
Endpoint - [redacted]	0/1
Endpoint - [redacted]	0/1
Endpoint - [redacted]	1/1
Endpoint - [redacted]	0/1
Endpoint - [redacted]	1/1
Endpoint - [redacted]	1/1
Endpoint - [redacted]	1/1
Threat - [redacted]	5/5
Threat - [redacted]	2/5

Drilldown:

Click the lefth

Step 1: got 0 results from Raw Search

Set to

Step 2: got 0 results for the Correlation Search

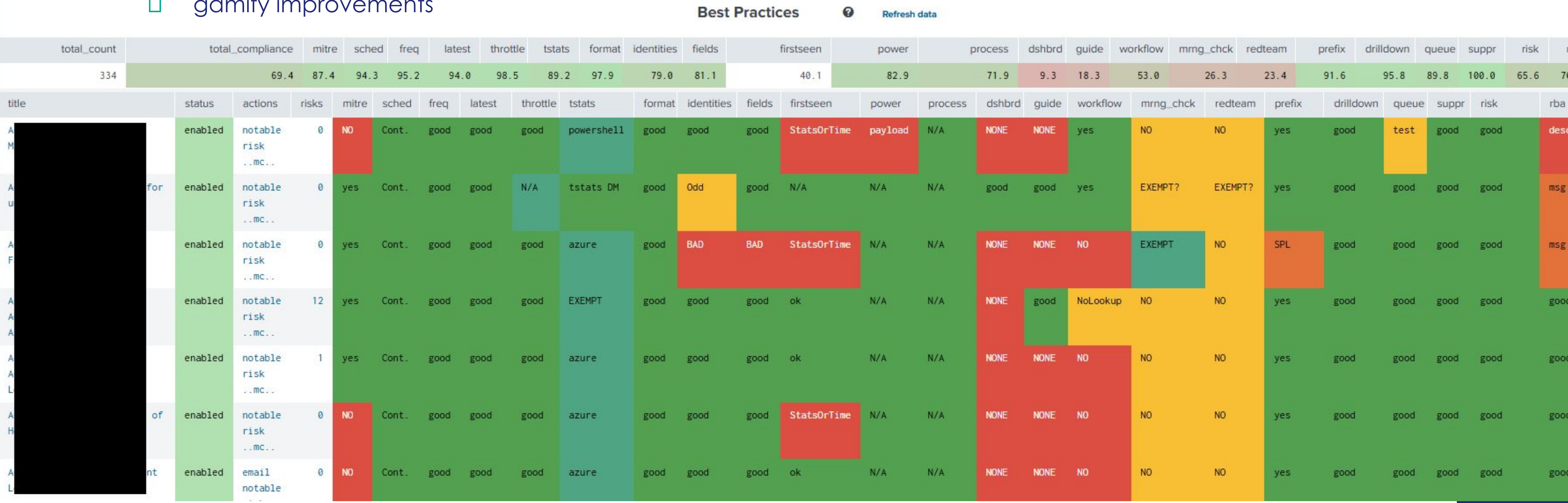
Set tok

Step 3: got $drilldown_tok_status$ expected Notable/Risk(s)

THALES
Building a future we can all trust

Managing the correlations (see .conf21 talk!)

1. **Morning checks**
2. **Correlation Best Practices**
   - agree on list of Best Practices
   - automate assessment (REST + regexes = dashboard)
   - gamify improvements



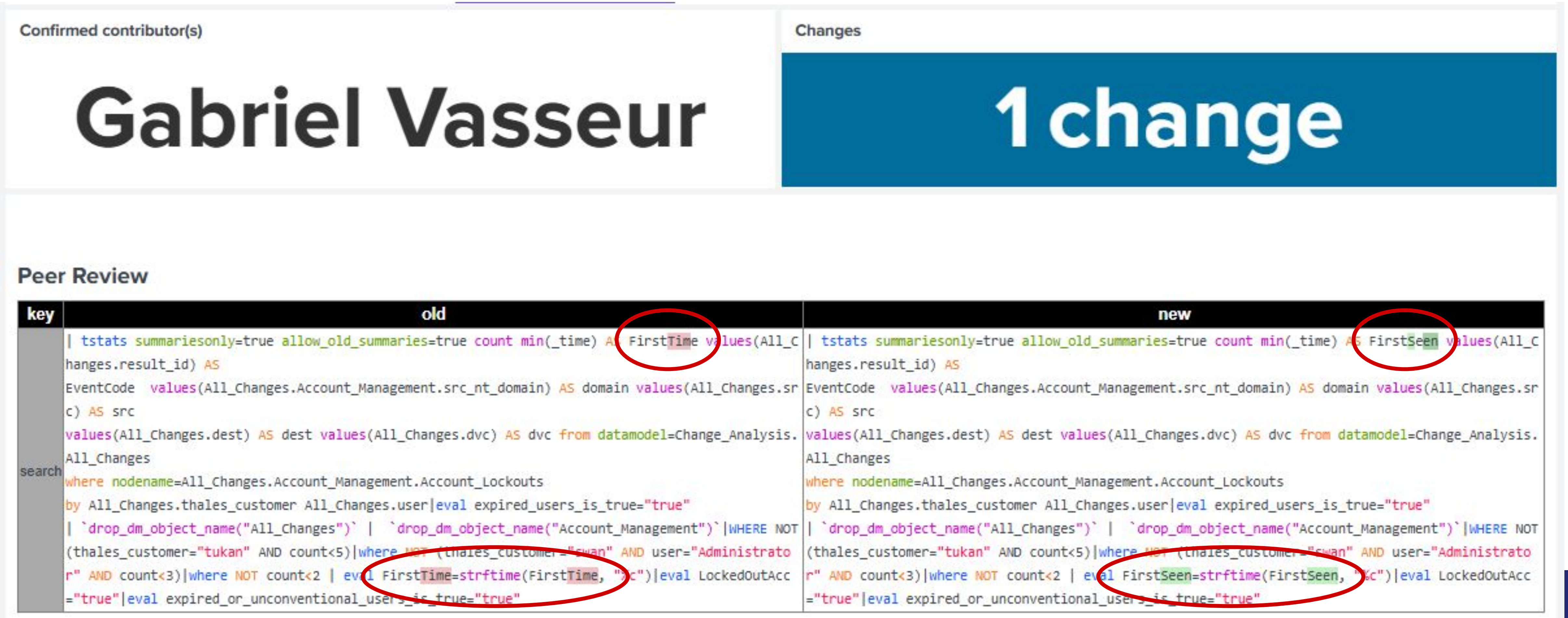
Best Practices ❓ Refresh data

total_count	total_compliance	mitre	sched	freq	latest	throttle	tstats	format	identities	fields	firstseen	power	process	dshbrd	guide	workflow	mrng_chck	redteam	prefix	drilldown	queue	suppr	risk
334	69.4	87.4	94.3	95.2	94.0	98.5	89.2	97.9	79.0	81.1	40.1	82.9	71.9	9.3	18.3	53.0	26.3	23.4	91.6	95.8	89.8	100.0	65.6

title	status	actions	risks	mitre	sched	freq	latest	throttle	tstats	format	identities	fields	firstseen	power	process	dshbrd	guide	workflow	mrng_chck	redteam	prefix	drilldown	queue	suppr	risk	rba
[redacted]	enabled	notable risk ..mc..	0	NO	Cont.	good	good	good	powershell	good	good	good	StatsOrTime	payload	N/A	NONE	NONE	yes	NO	NO	yes	good	test	good	good	des
[redacted]	enabled	notable risk ..mc..	0	yes	Cont.	good	good	N/A	tstats DM	good	Odd	good	N/A	N/A	N/A	good	good	yes	EXEMPT?	EXEMPT?	yes	good	good	good	good	msg
[redacted]	enabled	notable risk ..mc..	0	yes	Cont.	good	good	good	azure	good	BAD	BAD	StatsOrTime	N/A	N/A	NONE	NONE	NO	EXEMPT	NO	SPL	good	good	good	good	msg
[redacted]	enabled	notable risk ..mc..	12	yes	Cont.	good	good	good	EXEMPT	good	good	good	ok	N/A	N/A	NONE	good	NoLookup	NO	NO	yes	good	good	good	good	goo
[redacted]	enabled	notable risk ..mc..	1	yes	Cont.	good	good	good	azure	good	good	good	ok	N/A	N/A	NONE	NONE	NO	NO	NO	yes	good	good	good	good	goo
[redacted]	enabled	notable risk ..mc..	0	NO	Cont.	good	good	good	azure	good	good	good	StatsOrTime	N/A	N/A	NONE	NONE	NO	NO	NO	yes	good	good	good	good	goo
[redacted]	enabled	email notable	0	NO	Cont.	good	good	good	azure	good	good	good	ok	N/A	N/A	NONE	NONE	NO	NO	NO	yes	good	good	good	good	goo

Managing the correlations (see .conf21 talk!)

1. Morning checks
2. Correlation Best Practices
3. Peer Review system



Confirmed contributor(s)

Gabriel Vasseur

Changes

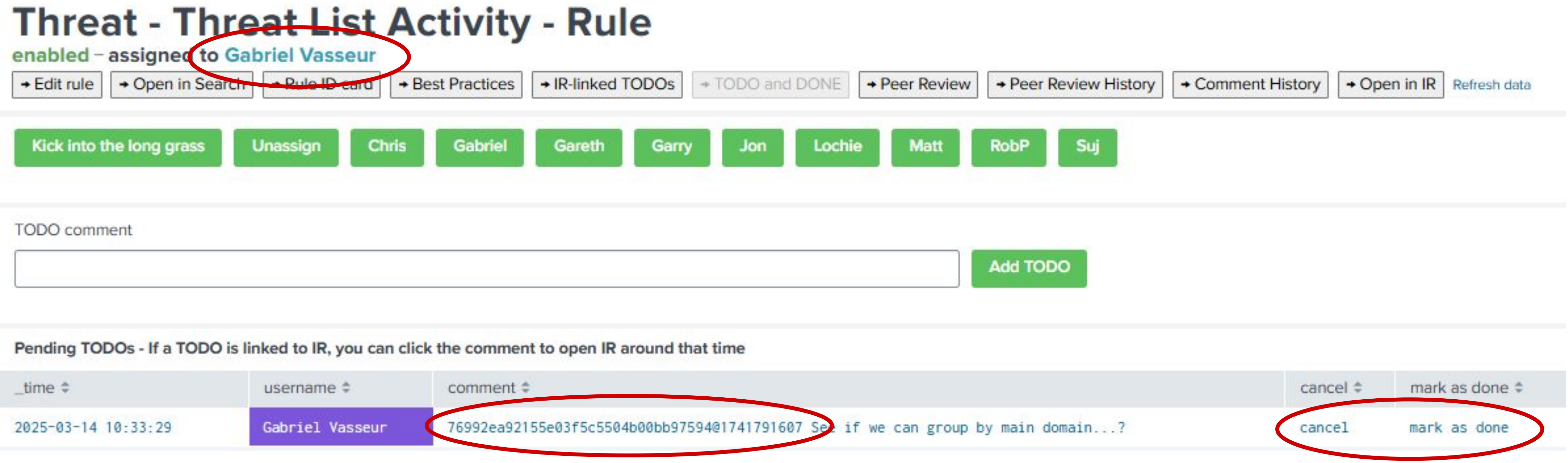
1 change

Peer Review

<table>
<tr><th>key</th><th>old</th><th>new</th></tr>
<tr><td>search</td><td>| tstats summariesonly=true allow_old_summaries=true count min(_time) AS FirstTime values(All_Changes.result_id) AS
EventCode values(All_Changes.Account_Management.src_nt_domain) AS domain values(All_Changes.src) AS src
values(All_Changes.dest) AS dest values(All_Changes.dvc) AS dvc from datamodel=Change_Analysis.All_Changes
where nodename=All_Changes.Account_Management.Account_Lockouts
by All_Changes.thales_customer All_Changes.user|eval expired_users_is_true="true"
| `drop_dm_object_name("All_Changes")` | `drop_dm_object_name("Account_Management")`|WHERE NOT (thales_customer="tukan" AND count<5)|where NOT (thales_customer="swan" AND user="Administrator" AND count<3)|where NOT count<2 | eval FirstTime=strftime(FirstTime, "%c")|eval LockedOutAcc="true"|eval expired_or_unconventional_users_is_true="true"</td><td>| tstats summariesonly=true allow_old_summaries=true count min(_time) AS FirstSeen values(All_Changes.result_id) AS
EventCode values(All_Changes.Account_Management.src_nt_domain) AS domain values(All_Changes.src) AS src
values(All_Changes.dest) AS dest values(All_Changes.dvc) AS dvc from datamodel=Change_Analysis.All_Changes
where nodename=All_Changes.Account_Management.Account_Lockouts
by All_Changes.thales_customer All_Changes.user|eval expired_users_is_true="true"
| `drop_dm_object_name("All_Changes")` | `drop_dm_object_name("Account_Management")`|WHERE NOT (thales_customer="tukan" AND count<5)|where NOT (thales_customer="swan" AND user="Administrator" AND count<3)|where NOT count<2 | eval FirstSeen=strftime(FirstSeen, "%c")|eval LockedOutAcc="true"|eval expired_or_unconventional_users_is_true="true"</td></tr>
</table>

Managing the correlations (see .conf21 talk!)

1. Morning checks
2. Correlation Best Practices
3. Peer Review system
4. TODO system



Threat - Threat List Activity - Rule

enabled – assigned to Gabriel Vasseur

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 ⬍
2025-03-14 10:33:29	Gabriel Vasseur	76992ea92155e03f5c5504b00bb97594@1741791607 See if we can group by main domain...?	cancel	mark as done

Managing the correlations

1. **Morning checks**
2. **Correlation Best Practices**
3. **Peer Review system**
4. **TODO system**
5. **Weekly meeting**
   - new and pending TODOs
   - trends (noise VS quiet)
   - show-and-tell
6. **Monitor dashboard hub**
   - data feeds
   - enrichment feeds (A&I, CTI, etc)
   - morning checks status
   - rota & task list
   - pending TODOs and reviews
   - expiring local accounts ant other alerts
   - license usage

}

ES Choreographer https://splunkbase.splunk.com/app/6309

https://conf.splunk.com/files/2021/recordings/SEC1441A.mp4

+

Conf Manager https://splunkbase.splunk.com/app/6895

- Powerful and fast searching of K.O.
- Change tracking
- Cool tools: search results diff, macro explorer, etc

= **Poor man's "detection as code"!**

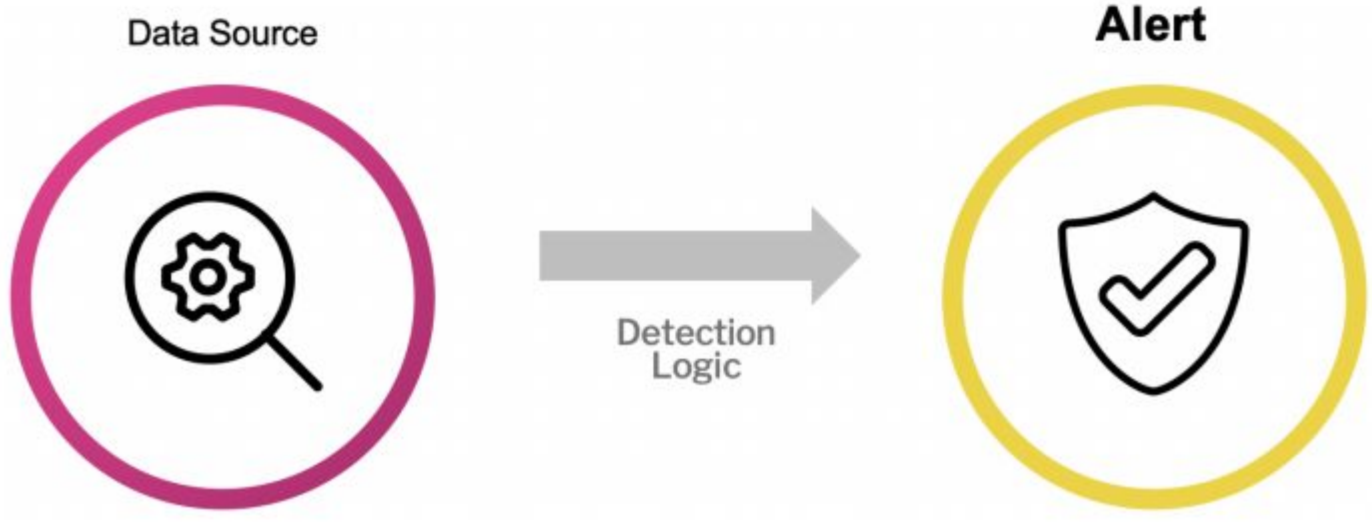
What is Risk Based Alerting?

- **A technique that aggregates and accumulates disparate security events, so that an alert is only raised when necessary**

- **Benefits:**

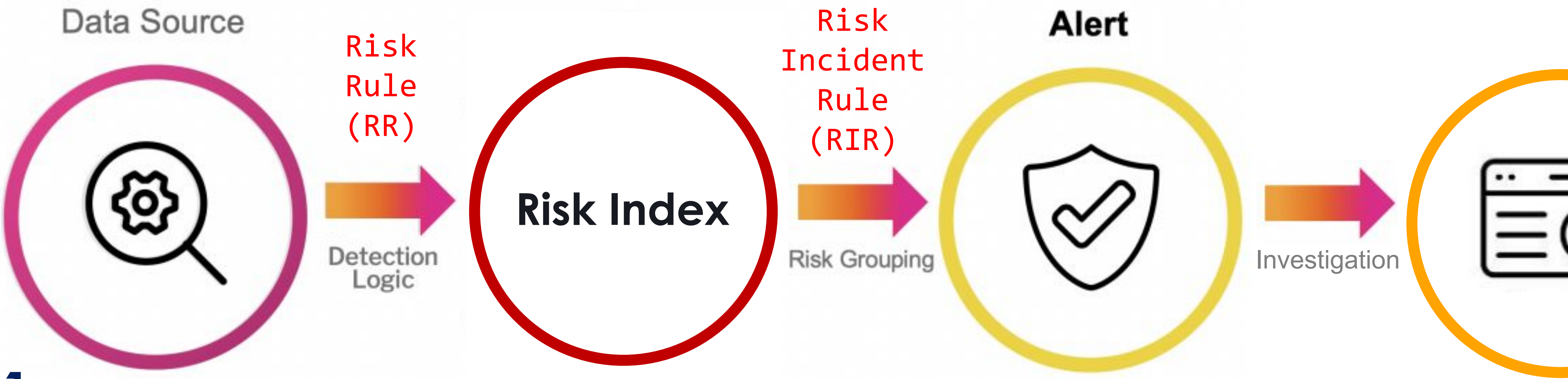
- alert volume typically reduced by 50% to 90%
- increased alert fidelity
- more context for analysis
- more chance of detecting low-and-slow attacks

Traditional Alerting



- “High” confidence alerts only
- High volume of FPs abandoned/suppressed alerts AND/OR burnout/situational numbness
- One incident = several alerts more difficult to investigate, easier to ignore

Risk Based Alerting: 2 Stages



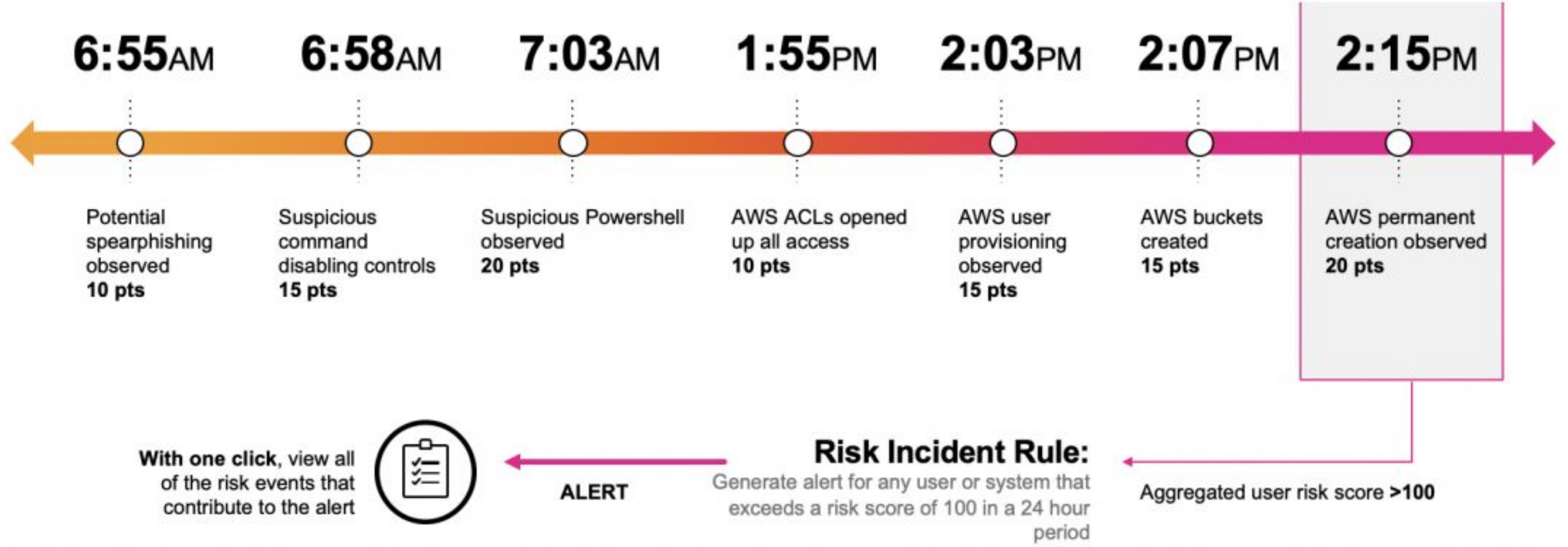
Stage 1

- **Detections don't have to be high-confidence, because they don't have to be all investigated**
- **Each risk event:**
  - is associated with an entity
  - has a risk score
  - has a description or risk_message

Stage 2

- **Aggregates risk events by entity over time (24h, 7d...)**
- **Alerts only if some logic is satisfied, e.g.:**
  - total score > threshold
  - OR more than X detections fired, regardless of score
  - etc...

A clear picture painted with events too noisy to alert on individually



6:55AM

Potential spearphishing observed
10 pts

6:58AM

Suspicious command disabling controls
15 pts

7:03AM

Suspicious Powershell observed
20 pts

1:55PM

AWS ACLs opened up all access
10 pts

2:03PM

AWS user provisioning observed
15 pts

2:07PM

AWS buckets created
15 pts

2:15PM

AWS permanent creation observed
20 pts

Aggregated user risk score **>100**

Risk Incident Rule:
Generate alert for any user or system that exceeds a risk score of 100 in a 24 hour period

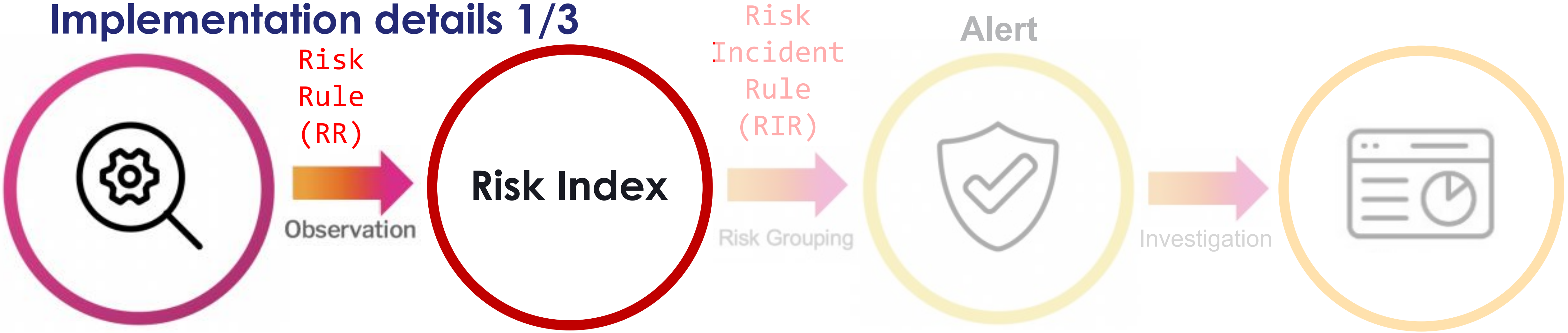
ALERT

With one click, view all of the risk events that contribute to the alert

WHAT IS THIS ENTITY’S RISK SCORE RIGHT NOW?

It depends!

Implementation details 1/3

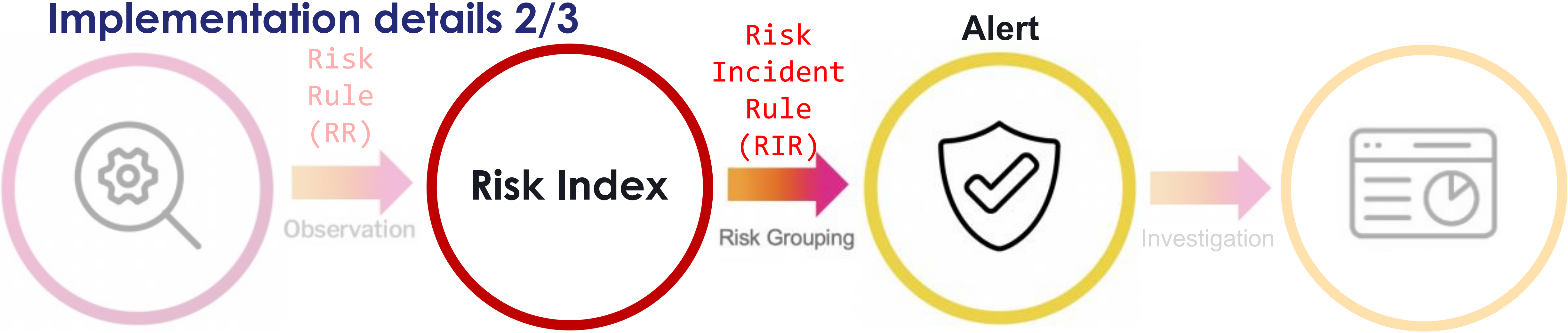


- **The more, the better (RBA too cold!)**
  - Signature-based feeds are ideal (EDR)
  - Sweep noisy detections under the RBA rug
  - Add risk to existing notable alert (not pure RBA)
- **Assets & Identities normalization** ★
- **Risk score setting**
- **Description/risk_message** ★

- **SPL logic "powershell use" example:**
  - If morning check: set is_morning_check to "yes" and risk_score to 1
  - if department=IT set is_suppressed="yes" and risk_score to 10
  - else risk_score=50
- **Risk factors**
- **Threat objects**

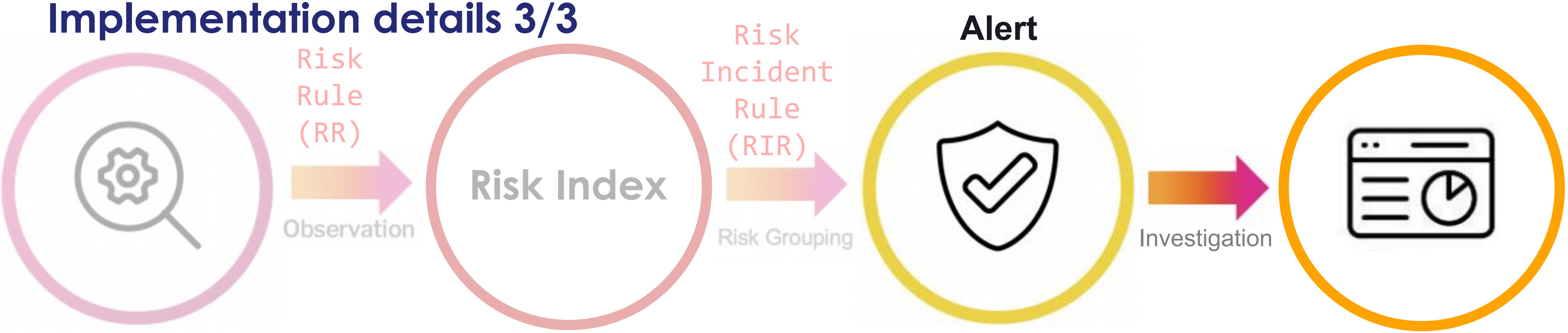
- **QA mode?**
- **Health dashboard**
  - invalid type
  - object doesn't match type
  - "unknown"
  - no or same description
- **Trend dashboard**

Implementation details 2/3



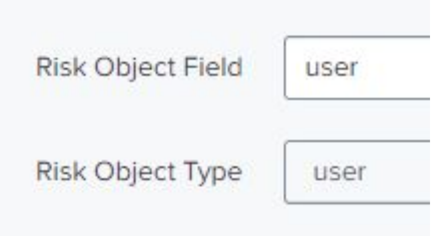
- Risk alerts (start with built-in)
- Deduplication (RBA too hot!) ★
- Further Assets & Identities grouping ★
- Fancy throttling
- Identify noisy contributors / correlated contributors ★

Implementation details 3/3



- **IR built-in risk pop-up**
- **Dedicated investigation dashboard emulating IR:**
  - key fields
  - drilldown search
  - link to analyst guide
  - workflow actions dashboard
  - …
- **SOAR?**

Identity Normalization – Correlation search



Risk Object Field	user
Risk Object Type	user

- **User name**

user
Domain\GVasseur

→

user	user_original	username	user_category	user_...
gvasseur	Domain\GVasseur	Gabs	Security Analyst	...

- **Admin account**

user
GVasseurADM

→

user	user_original	username	user_category	user_...
gvasseur	GVasseurADM	Gabs	Security Analyst	...

- **Email address**

user
gvasseur@company.com

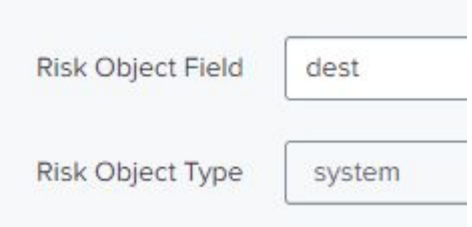
→

user	user_original	user_id	username	user_category	user_...
gvasseur@company.com	gvasseur@company.com	gvasseur	Gabs	Security Analyst	...

```
| eval risk_object=if( isnotnull(user_id), user_id, user )
```

- **`thales_get_identity4events(user)` in every detection**

Asset Normalization – Correlation search



Risk Object Field: dest

Risk Object Type: system

- **Hostname**

_time	dest
this morning 7:27	GabsLaptop.domain.name

_time	dest	dest_original	dest_owner	dest_...
this morning 7:27	gabslaptop	GabsLaptop.domain.name	gvasseur	...

- **Unknown IP but there’s a hostname**

_time	dest	dest_nt_host
this morning 7:27	10.1.2.3	GabsLaptop

_time	dest	dest_original	dest_ip	dest_owner	dest_...
this morning 7:27	gabslaptop	10.1.2.3	10.1.2.3	gvasseur	...

- **DHCP IP**

_time	dest
this morning 7:27	10.10.1.2

_time	dest	dest_original	dest_ip	dest_owner	dest_...
this morning 7:27	gabslaptop	10.10.1.2	10.10.1.2	gvasseur	...

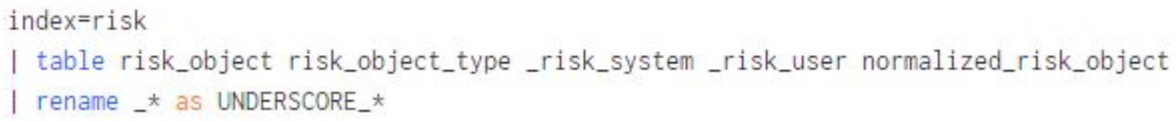
- **VPN IP**

_time	dest
this morning 7:27	10.20.1.2

_time	dest	dest_original	dest_vpn_user	dest_vpn_username	dest_...
this morning 7:27	10.20.1.2	10.20.1.2	gvasseur	Gabs	...

- **`thales_get_asset(dest)` in every detection**
- **Scheduled “Lookup Gen” searches to update timed lookups for DHCP and VPN + ES’s assets**

Asset & Identity Normalization – Risk index



```
index=risk
| table risk_object risk_object_type _risk_system _risk_user normalized_risk_object
| rename _* as UNDERSCORE_*
```

- user risk object

risk_object	risk_object_type	_risk_user	normalized_risk_object	…
gvasseur	user	gvasseur	gvasseur	…

- hostname risk object

risk_object	risk_object_type	_risk_system	normalized_risk_object	risk_object_owner	…
gabslaptop	system	gabslaptop	gabslaptop	gvasseur	…

- VPN IP risk object

risk_object	risk_object_type	_risk_system	normalized_risk_object	risk_object_vpn_user	…
10.20.1.2	system	10.20.1.2	10.20.1.2	gvasseur	…

Automated lookup of _risk_system in asset_lookup_by_str

- + 2 new calculated fields in the Risk Data Model:

Risk Data Model

target_risk_object

target_risk_object_type

Asset & Identity Normalization – Conclusion

- **Now aggregating activity whether happening to/by:**
  - my main identifier
  - my other accounts (e.g. admin)
  - my laptop hostname
  - a DHCP IP my laptop is given
  - a VPN IP I’m logged on to

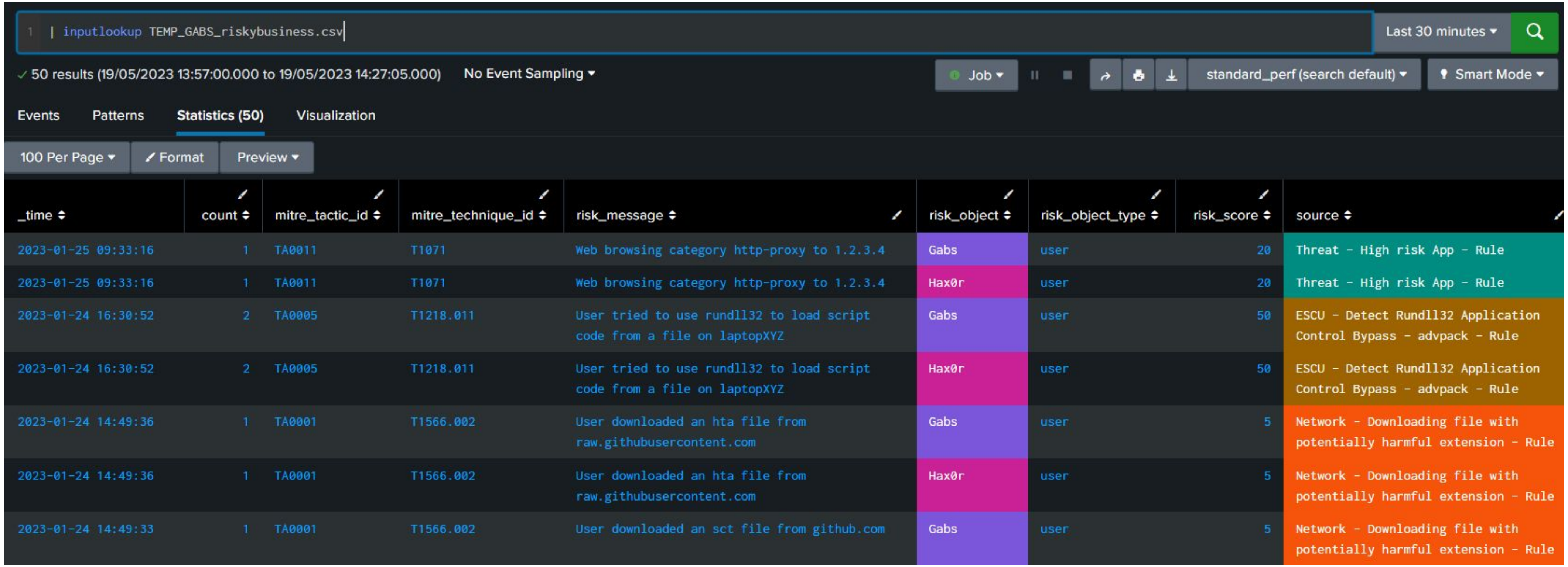
- **Possible race condition for VPN if enough time elapses between detection and data model acceleration**
  - `| eval risk_object_vpn_user = dest_vpn_user   ???`

- **Timed lookup are expensive! Don’t call the get_asset macro on thousands of results…**
  - we have `thales_get_asset_far(dest)` for when we need to look back about a month

risk_message VS description

- **risk_message**
  - can be configured in the ES correlation search configuration (or in the SPL)
  - no default!
- **description**
  - can be specified in the SPL
  - if not, defaults to the description of the correlation search (better than nothing!)
- **We used description before risk_message was a thing, now we use both:**
  - description is used for deduplication (can be tweaked to affect deduplication)
  - risk_message is geared towards analyst (more detail is better)

Deduplication – Example of risk events

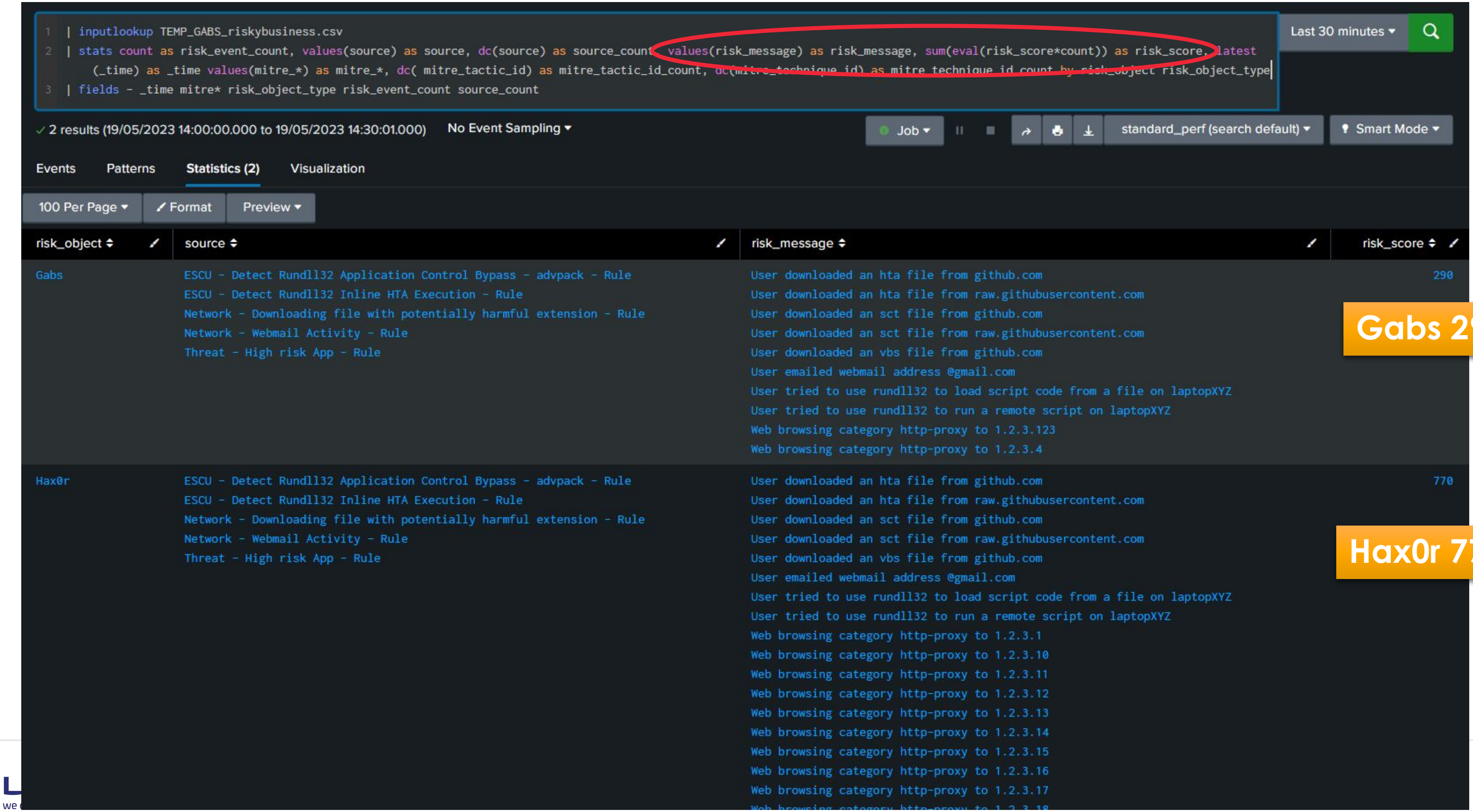


```
| inputlookup TEMP_GABS_riskybusiness.csv
```

✓ 50 results (19/05/2023 13:57:00.000 to 19/05/2023 14:27:05.000)

_time	count	mitre_tactic_id	mitre_technique_id	risk_message	risk_object	risk_object_type	risk_score	source
2023-01-25 09:33:16	1	TA0011	T1071	Web browsing category http-proxy to 1.2.3.4	Gabs	user	20	Threat - High risk App - Rule
2023-01-25 09:33:16	1	TA0011	T1071	Web browsing category http-proxy to 1.2.3.4	Hax0r	user	20	Threat - High risk App - Rule
2023-01-24 16:30:52	2	TA0005	T1218.011	User tried to use rundll32 to load script code from a file on laptopXYZ	Gabs	user	50	ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule
2023-01-24 16:30:52	2	TA0005	T1218.011	User tried to use rundll32 to load script code from a file on laptopXYZ	Hax0r	user	50	ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule
2023-01-24 14:49:36	1	TA0001	T1566.002	User downloaded an hta file from raw.githubusercontent.com	Gabs	user	5	Network - Downloading file with potentially harmful extension - Rule
2023-01-24 14:49:36	1	TA0001	T1566.002	User downloaded an hta file from raw.githubusercontent.com	Hax0r	user	5	Network - Downloading file with potentially harmful extension - Rule
2023-01-24 14:49:33	1	TA0001	T1566.002	User downloaded an sct file from github.com	Gabs	user	5	Network - Downloading file with potentially harmful extension - Rule

Without Deduplication



```
| inputlookup TEMP_GABS_riskybusiness.csv
| stats count as risk_event_count, values(source) as source, dc(source) as source_count, values(risk_message) as risk_message, sum(eval(risk_score*count)) as risk_score, latest
  (_time) as _time values(mitre_*) as mitre_*, dc( mitre_tactic_id) as mitre_tactic_id_count, dc(mitre_technique_id) as mitre_technique_id_count by risk_object risk_object_type
| fields - _time mitre* risk_object_type risk_event_count source_count
```

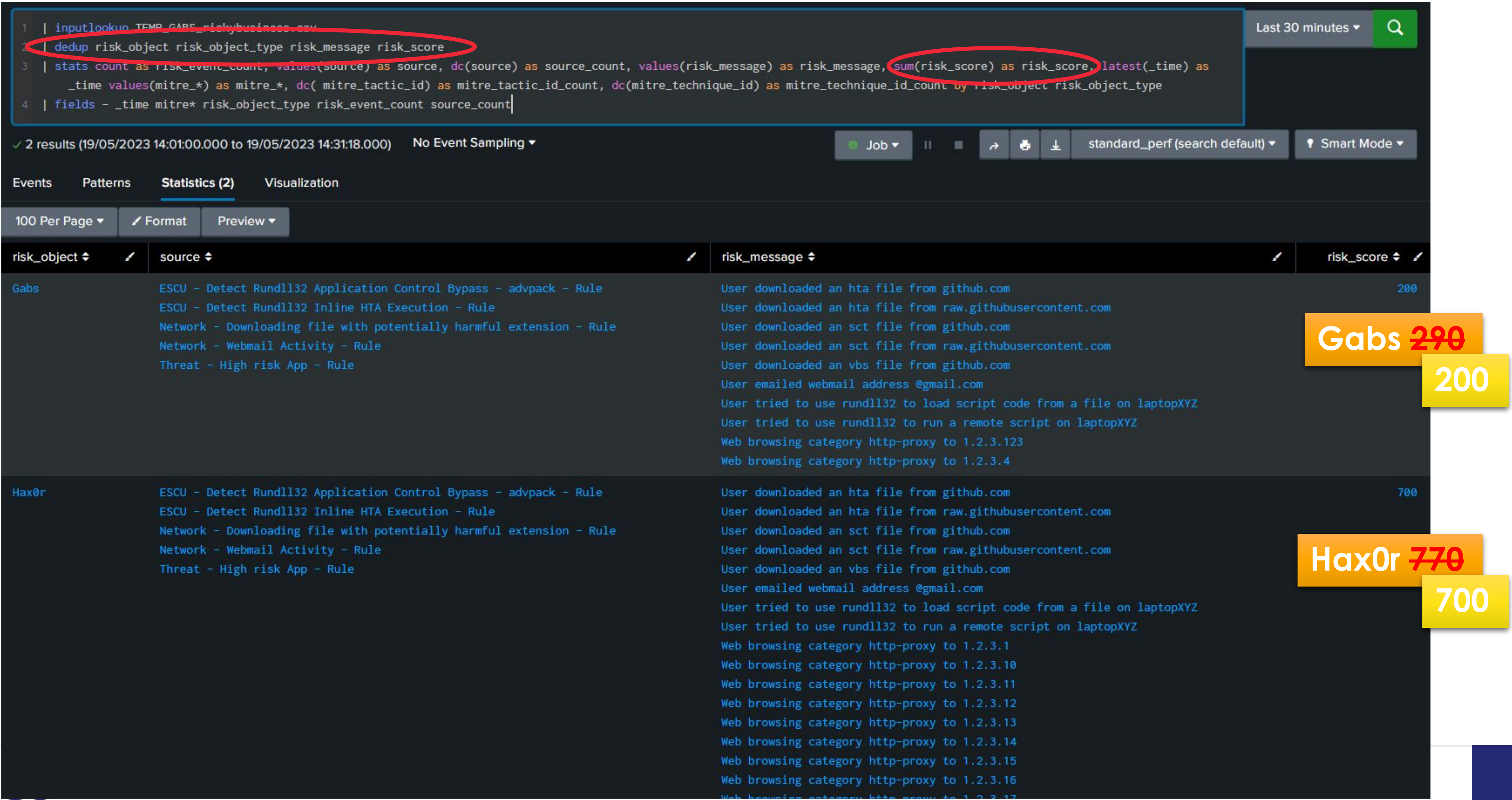
✓ 2 results (19/05/2023 14:00:00.000 to 19/05/2023 14:30:01.000)

risk_object	source	risk_message	risk_score
Gabs	ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule ESCU - Detect Rundll32 Inline HTA Execution - Rule Network - Downloading file with potentially harmful extension - Rule Network - Webmail Activity - Rule Threat - High risk App - Rule	User downloaded an hta file from github.com User downloaded an hta file from raw.githubusercontent.com User downloaded an sct file from github.com User downloaded an sct file from raw.githubusercontent.com User downloaded an vbs file from github.com User emailed webmail address @gmail.com User tried to use rundll32 to load script code from a file on laptopXYZ User tried to use rundll32 to run a remote script on laptopXYZ Web browsing category http-proxy to 1.2.3.123 Web browsing category http-proxy to 1.2.3.4	290
Hax0r	ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule ESCU - Detect Rundll32 Inline HTA Execution - Rule Network - Downloading file with potentially harmful extension - Rule Network - Webmail Activity - Rule Threat - High risk App - Rule	User downloaded an hta file from github.com User downloaded an hta file from raw.githubusercontent.com User downloaded an sct file from github.com User downloaded an sct file from raw.githubusercontent.com User downloaded an vbs file from github.com User emailed webmail address @gmail.com User tried to use rundll32 to load script code from a file on laptopXYZ User tried to use rundll32 to run a remote script on laptopXYZ Web browsing category http-proxy to 1.2.3.1 Web browsing category http-proxy to 1.2.3.10 Web browsing category http-proxy to 1.2.3.11 Web browsing category http-proxy to 1.2.3.12 Web browsing category http-proxy to 1.2.3.13 Web browsing category http-proxy to 1.2.3.14 Web browsing category http-proxy to 1.2.3.15 Web browsing category http-proxy to 1.2.3.16 Web browsing category http-proxy to 1.2.3.17 Web browsing category http-proxy to 1.2.3.18	770

Gabs 290

Hax0r 770

Basic Deduplication



```
| inputlookup TEMP_GABS_riskybusiness.csv
| dedup risk_object risk_object_type risk_message risk_score
| stats count as risk_event_count, values(source) as source, dc(source) as source_count, values(risk_message) as risk_message, sum(risk_score) as risk_score, latest(_time) as
   _time values(mitre_*) as mitre_*, dc( mitre_tactic_id) as mitre_tactic_id_count, dc(mitre_technique_id) as mitre_technique_id_count by risk_object risk_object_type
| fields - _time mitre* risk_object_type risk_event_count source_count
```

✓ 2 results (19/05/2023 14:01:00.000 to 19/05/2023 14:31:18.000)   No Event Sampling ▾

risk_object	source	risk_message	risk_score
Gabs	ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule ESCU - Detect Rundll32 Inline HTA Execution - Rule Network - Downloading file with potentially harmful extension - Rule Network - Webmail Activity - Rule Threat - High risk App - Rule	User downloaded an hta file from github.com User downloaded an hta file from raw.githubusercontent.com User downloaded an sct file from github.com User downloaded an sct file from raw.githubusercontent.com User downloaded an vbs file from github.com User emailed webmail address @gmail.com User tried to use rundll32 to load script code from a file on laptopXYZ User tried to use rundll32 to run a remote script on laptopXYZ Web browsing category http-proxy to 1.2.3.123 Web browsing category http-proxy to 1.2.3.4	200
Hax0r	ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule ESCU - Detect Rundll32 Inline HTA Execution - Rule Network - Downloading file with potentially harmful extension - Rule Network - Webmail Activity - Rule Threat - High risk App - Rule	User downloaded an hta file from github.com User downloaded an hta file from raw.githubusercontent.com User downloaded an sct file from github.com User downloaded an sct file from raw.githubusercontent.com User downloaded an vbs file from github.com User emailed webmail address @gmail.com User tried to use rundll32 to load script code from a file on laptopXYZ User tried to use rundll32 to run a remote script on laptopXYZ Web browsing category http-proxy to 1.2.3.1 Web browsing category http-proxy to 1.2.3.10 Web browsing category http-proxy to 1.2.3.11 Web browsing category http-proxy to 1.2.3.12 Web browsing category http-proxy to 1.2.3.13 Web browsing category http-proxy to 1.2.3.14 Web browsing category http-proxy to 1.2.3.15 Web browsing category http-proxy to 1.2.3.16 Web browsing category http-proxy to 1.2.3.17	700

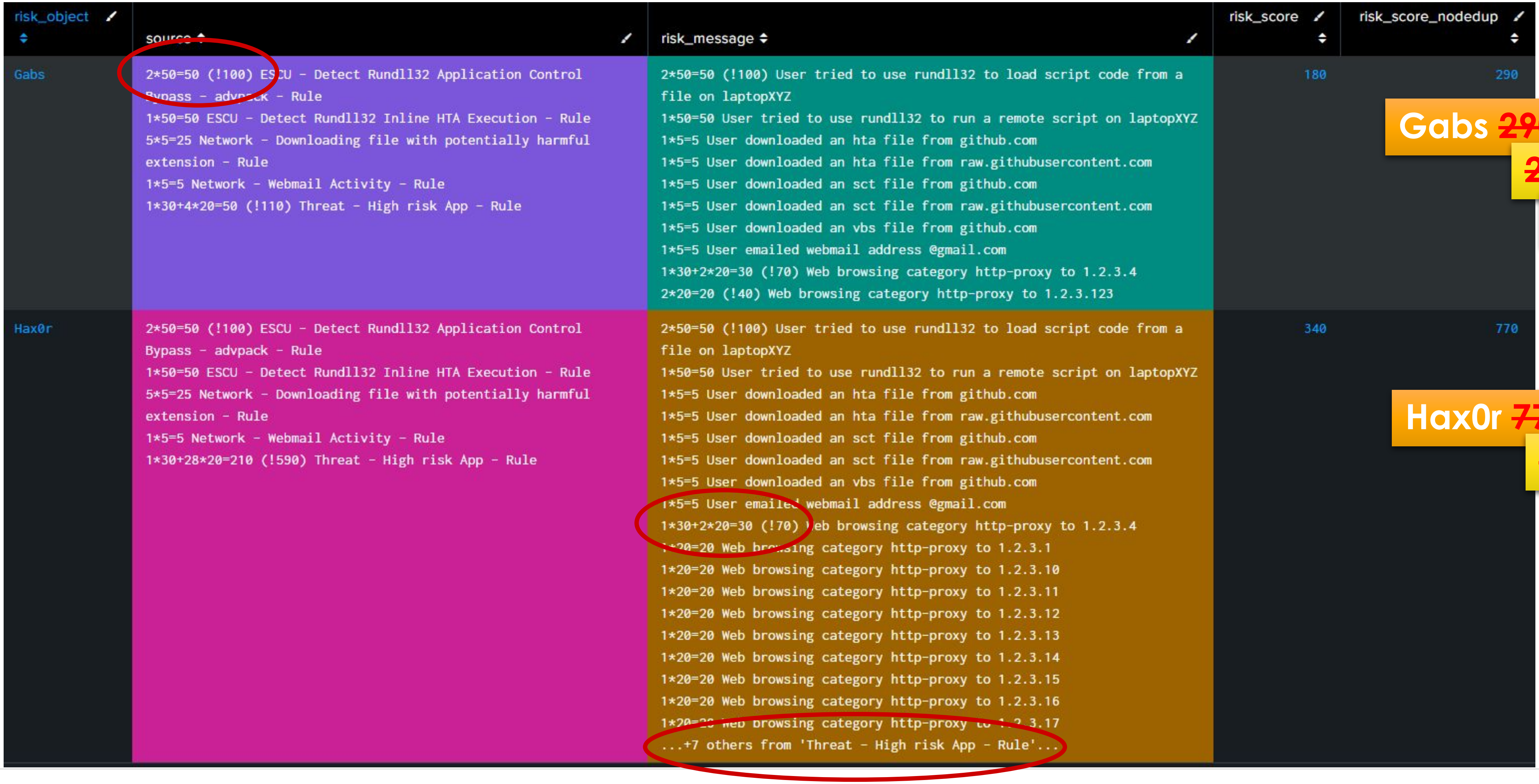
Gabs ~~290~~

200

Hax0r ~~770~~

700

Fancy Deduplication – See blog post



risk_object	source	risk_message	risk_score	risk_score_nodedup
Gabs	2*50=50 (!100) ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule 1*50=50 ESCU - Detect Rundll32 Inline HTA Execution - Rule 5*5=25 Network - Downloading file with potentially harmful extension - Rule 1*5=5 Network - Webmail Activity - Rule 1*30+4*20=50 (!110) Threat - High risk App - Rule	2*50=50 (!100) User tried to use rundll32 to load script code from a file on laptopXYZ 1*50=50 User tried to use rundll32 to run a remote script on laptopXYZ 1*5=5 User downloaded an hta file from github.com 1*5=5 User downloaded an hta file from raw.githubusercontent.com 1*5=5 User downloaded an sct file from github.com 1*5=5 User downloaded an sct file from raw.githubusercontent.com 1*5=5 User downloaded an vbs file from github.com 1*5=5 User emailed webmail address @gmail.com 1*30+2*20=30 (!70) Web browsing category http-proxy to 1.2.3.4 2*20=20 (!40) Web browsing category http-proxy to 1.2.3.123	180	290
Hax0r	2*50=50 (!100) ESCU - Detect Rundll32 Application Control Bypass - advpack - Rule 1*50=50 ESCU - Detect Rundll32 Inline HTA Execution - Rule 5*5=25 Network - Downloading file with potentially harmful extension - Rule 1*5=5 Network - Webmail Activity - Rule 1*30+28*20=210 (!590) Threat - High risk App - Rule	2*50=50 (!100) User tried to use rundll32 to load script code from a file on laptopXYZ 1*50=50 User tried to use rundll32 to run a remote script on laptopXYZ 1*5=5 User downloaded an hta file from github.com 1*5=5 User downloaded an hta file from raw.githubusercontent.com 1*5=5 User downloaded an sct file from github.com 1*5=5 User downloaded an sct file from raw.githubusercontent.com 1*5=5 User downloaded an vbs file from github.com 1*5=5 User emailed webmail address @gmail.com 1*30+2*20=30 (!70) Web browsing category http-proxy to 1.2.3.4 1*20=20 Web browsing category http-proxy to 1.2.3.1 1*20=20 Web browsing category http-proxy to 1.2.3.10 1*20=20 Web browsing category http-proxy to 1.2.3.11 1*20=20 Web browsing category http-proxy to 1.2.3.12 1*20=20 Web browsing category http-proxy to 1.2.3.13 1*20=20 Web browsing category http-proxy to 1.2.3.14 1*20=20 Web browsing category http-proxy to 1.2.3.15 1*20=20 Web browsing category http-proxy to 1.2.3.16 1*20=20 Web browsing category http-proxy to 1.2.3.17 ...+7 others from 'Threat - High risk App - Rule'...	340	770

Gabs ~~290~~

~~200~~

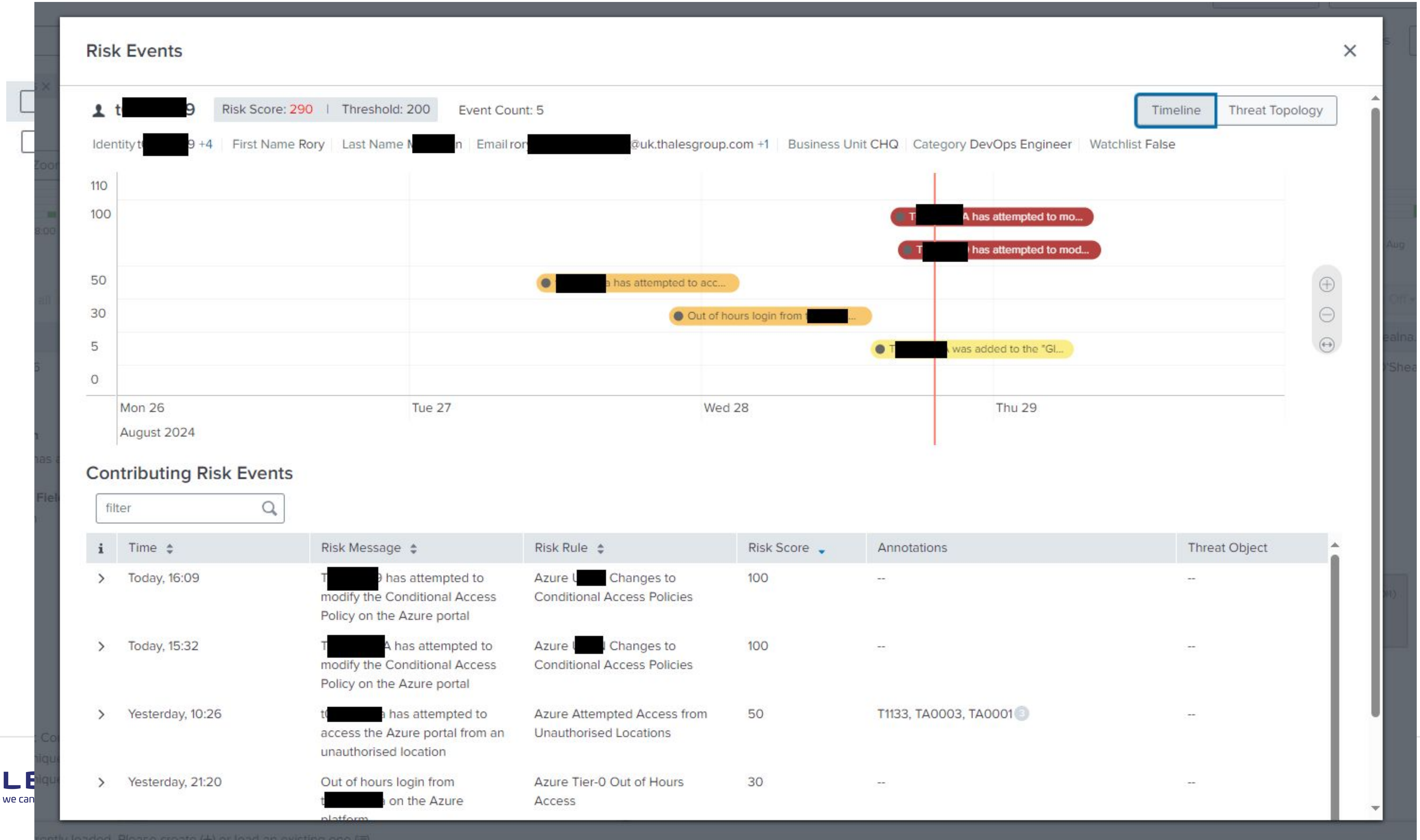
180

Hax0r ~~770~~

~~700~~

340

IR Risk Event Timeline



Risk Events

t[redacted]9 | Risk Score: 290 | Threshold: 200 | Event Count: 5

Identity t[redacted]9 +4 | First Name Rory | Last Name [redacted]n | Email ror[redacted]@uk.thalesgroup.com +1 | Business Unit CHQ | Category DevOps Engineer | Watchlist False

Timeline
Threat Topology
110
100
50
30
5
0
T[redacted] has attempted to mo...
T[redacted] has attempted to mod...
[redacted] has attempted to acc...
Out of hours login from [redacted]...
T[redacted] was added to the "Gl...
Mon 26
August 2024
Tue 27
Wed 28
Thu 29

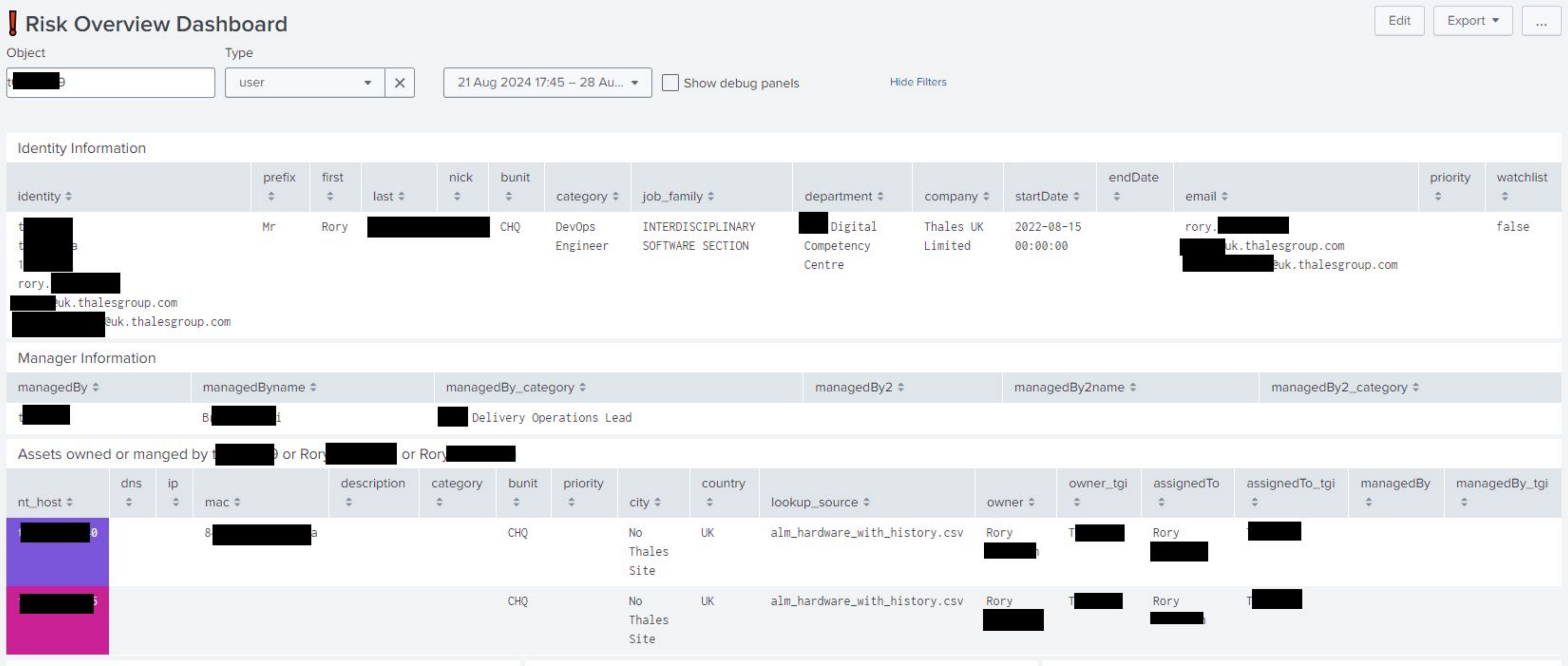
Contributing Risk Events

filter

i	Time	Risk Message	Risk Rule	Risk Score	Annotations	Threat Object
›	Today, 16:09	T[redacted] has attempted to modify the Conditional Access Policy on the Azure portal	Azure [redacted] Changes to Conditional Access Policies	100	--	--
›	Today, 15:32	T[redacted] has attempted to modify the Conditional Access Policy on the Azure portal	Azure [redacted] Changes to Conditional Access Policies	100	--	--
›	Yesterday, 10:26	t[redacted] has attempted to access the Azure portal from an unauthorised location	Azure Attempted Access from Unauthorised Locations	50	T1133, TA0003, TA0001 3	--
›	Yesterday, 21:20	Out of hours login from t[redacted] on the Azure platform	Azure Tier-0 Out of Hours Access	30	--	--

THALES
Building a future we can

Risk Overview Dashboard



Risk Overview Dashboard

Object: [redacted]

Type: user ▾ ✕

21 Aug 2024 17:45 – 28 Au... ▾

□ Show debug panels

Identity Information

identity	prefix	first	last	nick	bunit	category	job_family	department	company	startDate	endDate	email	priority	watchlist
[redacted] rory.[redacted] [redacted]uk.thalesgroup.com [redacted]@uk.thalesgroup.com	Mr	Rory	[redacted]		CHQ	DevOps Engineer	INTERDISCIPLINARY SOFTWARE SECTION	[redacted] Digital Competency Centre	Thales UK Limited	2022-08-15 00:00:00		rory.[redacted] [redacted]uk.thalesgroup.com [redacted]@uk.thalesgroup.com		false

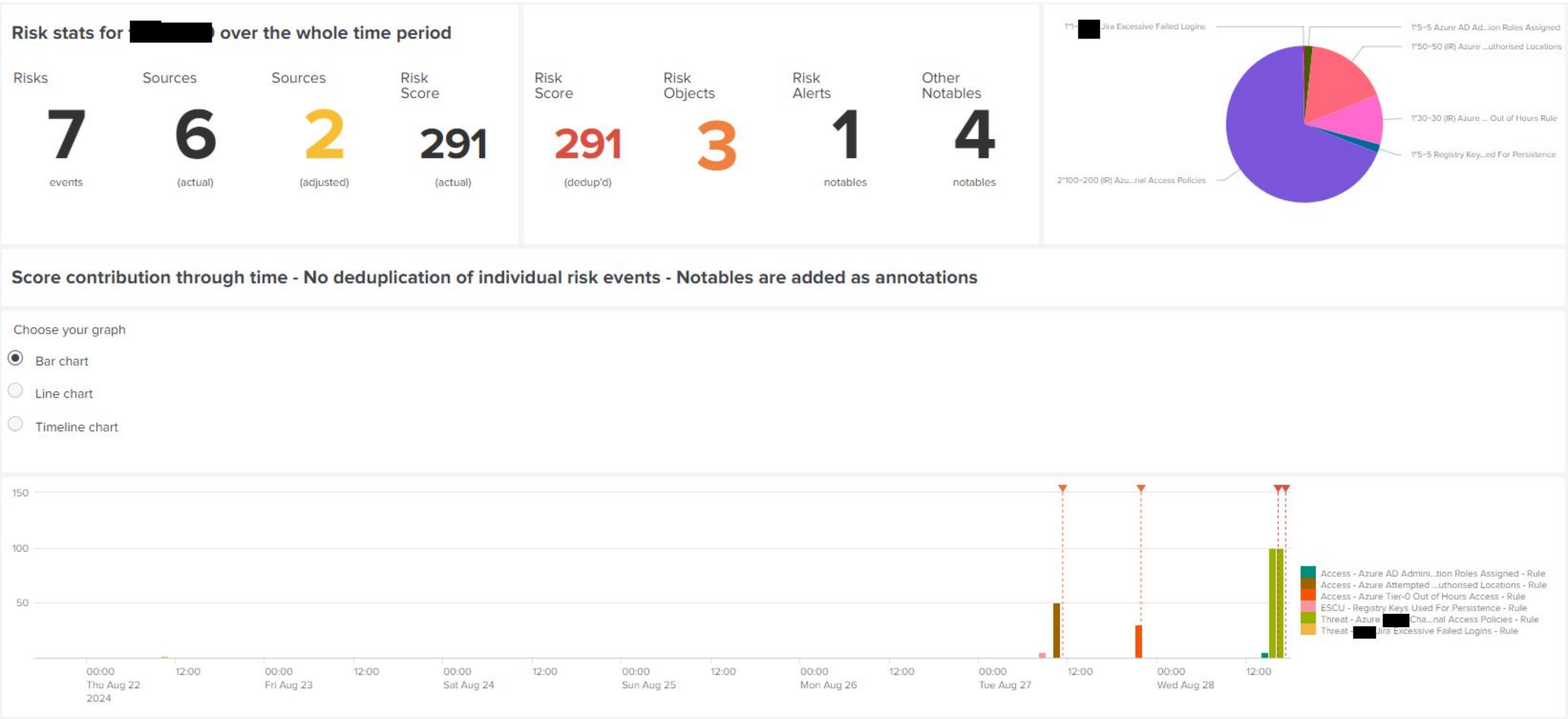
Manager Information

managedBy	managedByname	managedBy_category	managedBy2	managedBy2name	managedBy2_category
[redacted]	[redacted]	[redacted] Delivery Operations Lead			

Assets owned or manged by [redacted] or Ror[redacted] or Rory[redacted]

nt_host	dns	ip	mac	description	category	bunit	priority	city	country	lookup_source	owner	owner_tgi	assignedTo	assignedTo_tgi	managedBy	managedBy_tgi
[redacted]			[redacted]			CHQ		No Thales Site	UK	alm_hardware_with_history.csv	Rory [redacted]	[redacted]	Rory [redacted]	[redacted]		
[redacted]						CHQ		No Thales Site	UK	alm_hardware_with_history.csv	Rory [redacted]	[redacted]	Rory [redacted]	[redacted]		

Risk Overview Dashboard



Risk stats for [redacted] over the whole time period

Risks	Sources	Sources	Risk Score	Risk Score	Risk Objects	Risk Alerts	Other Notables
7	6	2	291	291	3	1	4
events	(actual)	(adjusted)	(actual)	(dedup'd)		notables	notables

1*1-[redacted]Jira Excessive Failed Logins
1*5-5 Azure AD Ad...ion Roles Assigned
1*50-50 (IR) Azure ...uthorised Locations
1*30-30 (IR) Azure ... Out of Hours Rule
1*5-5 Registry Key...ed For Persistence
2*100-200 (IR) Azu...nal Access Policies

Score contribution through time - No deduplication of individual risk events - Notables are added as annotations

Choose your graph

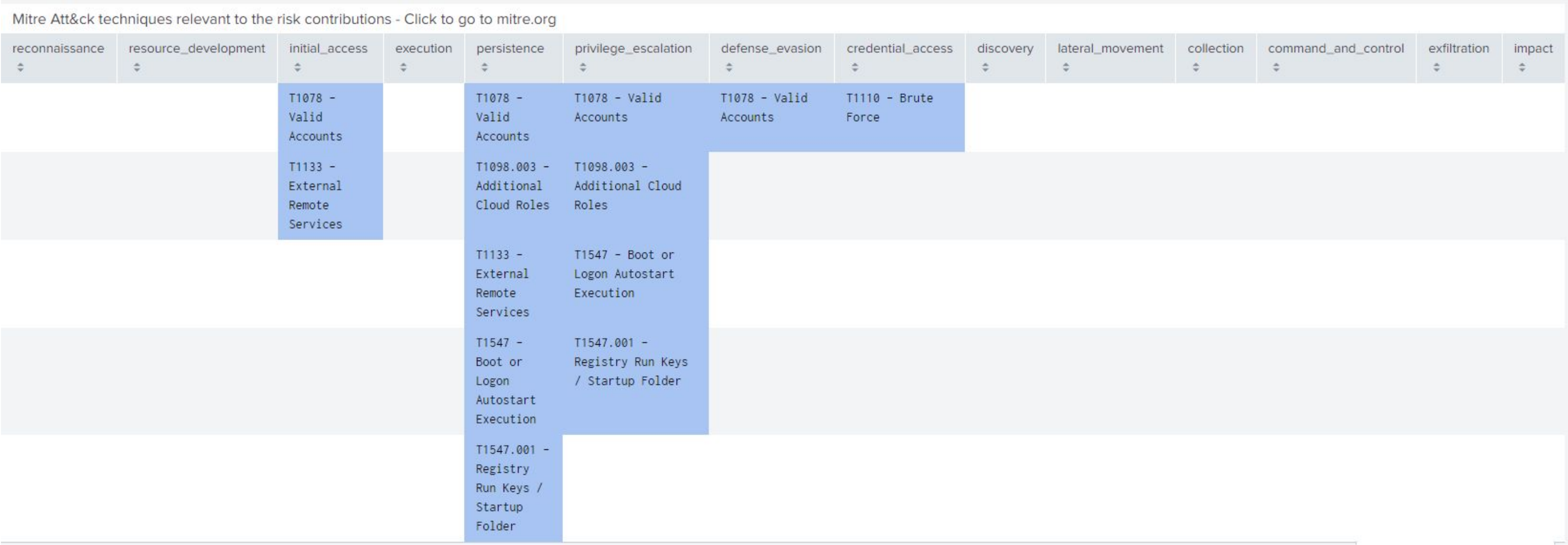
● Bar chart

○ Line chart

○ Timeline chart

150
100
50
00:00
Thu Aug 22
2024
12:00
00:00
Fri Aug 23
12:00
00:00
Sat Aug 24
12:00
00:00
Sun Aug 25
12:00
00:00
Mon Aug 26
12:00
00:00
Tue Aug 27
12:00
00:00
Wed Aug 28
12:00
Access - Azure AD Admini...tion Roles Assigned - Rule
Access - Azure Attempted ...uthorised Locations - Rule
Access - Azure Tier-0 Out of Hours Access - Rule
ESCU - Registry Keys Used For Persistence - Rule
Threat - Azure [redacted]Cha...nal Access Policies - Rule
Threat - [redacted]Jira Excessive Failed Logins - Rule

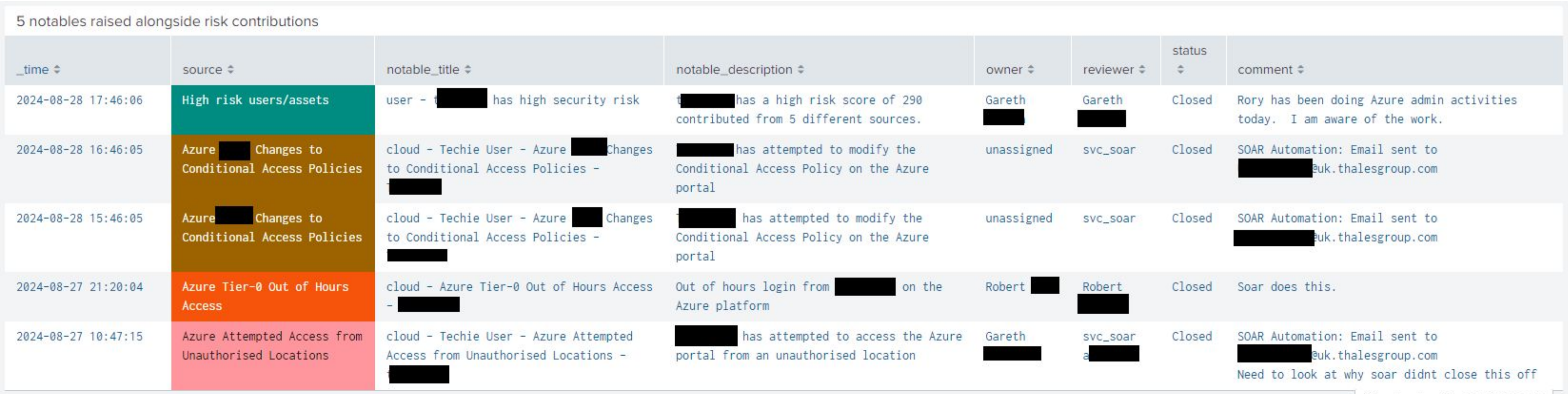
Risk Overview Dashboard



Mitre Att&ck techniques relevant to the risk contributions - Click to go to mitre.org

reconnaissance	resource_development	initial_access	execution	persistence	privilege_escalation	defense_evasion	credential_access	discovery	lateral_movement	collection	command_and_control	exfiltration	impact
		T1078 - Valid Accounts		T1078 - Valid Accounts	T1078 - Valid Accounts	T1078 - Valid Accounts	T1110 - Brute Force						
		T1133 - External Remote Services		T1098.003 - Additional Cloud Roles	T1098.003 - Additional Cloud Roles								
				T1133 - External Remote Services	T1547 - Boot or Logon Autostart Execution								
				T1547 - Boot or Logon Autostart Execution	T1547.001 - Registry Run Keys / Startup Folder								
				T1547.001 - Registry Run Keys / Startup Folder									

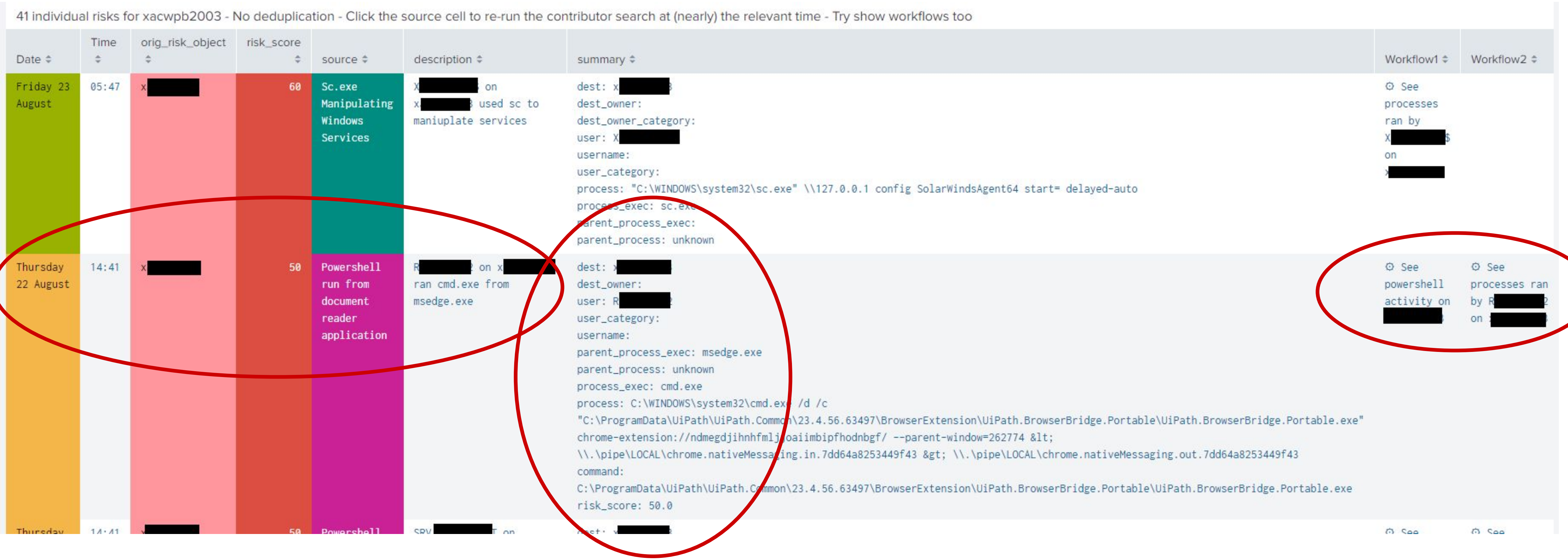
THALES
Building a future we can all trust



5 notables raised alongside risk contributions

_time	source	notable_title	notable_description	owner	reviewer	status	comment
2024-08-28 17:46:06	High risk users/assets	user - [redacted] has high security risk	[redacted] has a high risk score of 290 contributed from 5 different sources.	Gareth [redacted]	Gareth [redacted]	Closed	Rory has been doing Azure admin activities today. I am aware of the work.
2024-08-28 16:46:05	Azure [redacted] Changes to Conditional Access Policies	cloud - Techie User - Azure [redacted] Changes to Conditional Access Policies - [redacted]	[redacted] has attempted to modify the Conditional Access Policy on the Azure portal	unassigned	svc_soar	Closed	SOAR Automation: Email sent to [redacted]@uk.thalesgroup.com
2024-08-28 15:46:05	Azure [redacted] Changes to Conditional Access Policies	cloud - Techie User - Azure [redacted] Changes to Conditional Access Policies - [redacted]	[redacted] has attempted to modify the Conditional Access Policy on the Azure portal	unassigned	svc_soar	Closed	SOAR Automation: Email sent to [redacted]@uk.thalesgroup.com
2024-08-27 21:20:04	Azure Tier-0 Out of Hours Access	cloud - Azure Tier-0 Out of Hours Access - [redacted]	Out of hours login from [redacted] on the Azure platform	Robert [redacted]	Robert [redacted]	Closed	Soar does this.
2024-08-27 10:47:15	Azure Attempted Access from Unauthorised Locations	cloud - Techie User - Azure Attempted Access from Unauthorised Locations - [redacted]	[redacted] has attempted to access the Azure portal from an unauthorised location	Gareth [redacted]	svc_soar [redacted]	Closed	SOAR Automation: Email sent to [redacted]@uk.thalesgroup.com Need to look at why soar didnt close this off

Risk Overview Dashboard



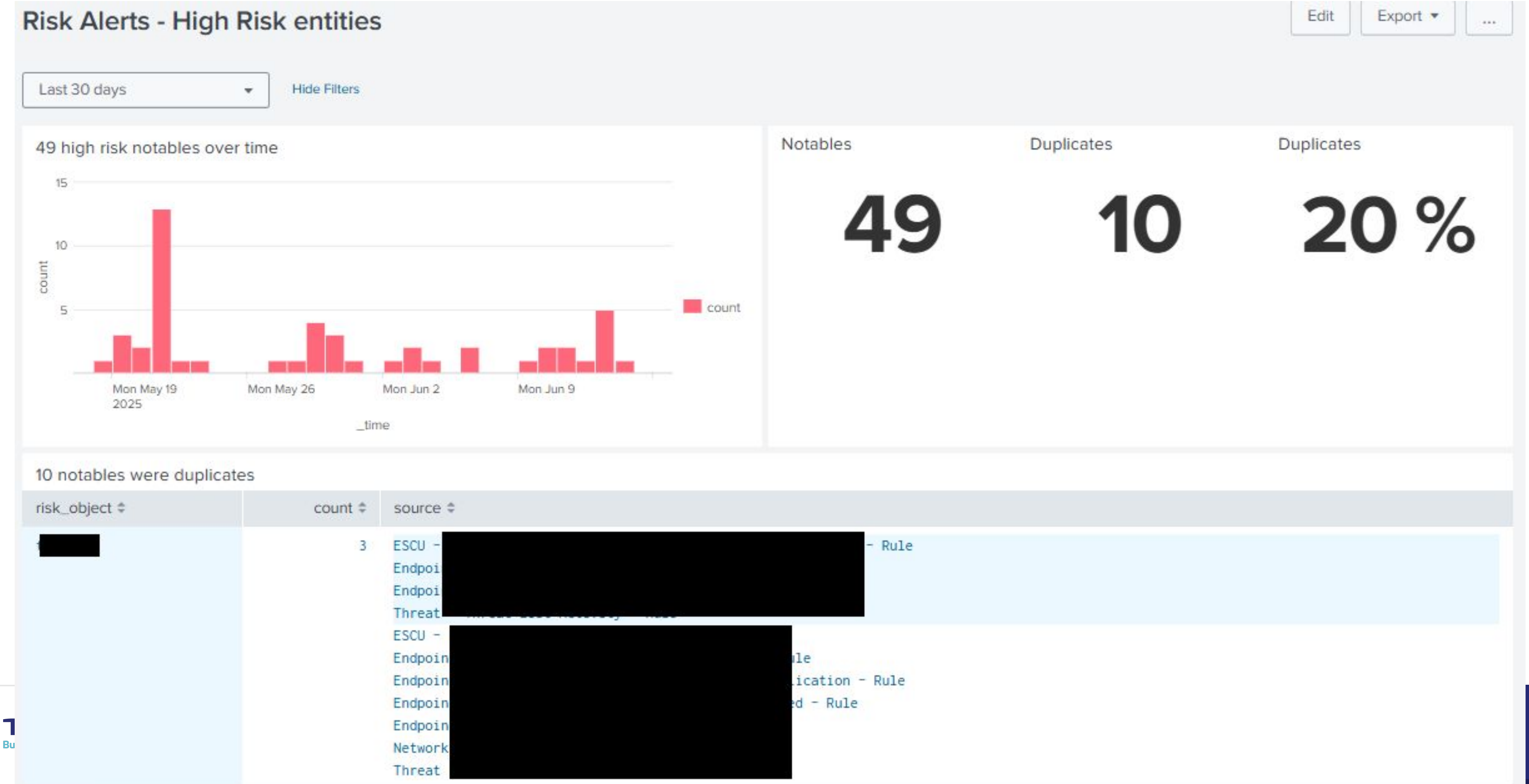
41 individual risks for xacwpb2003 - No deduplication - Click the source cell to re-run the contributor search at (nearly) the relevant time - Try show workflows too

Date ⇕	Time ⇕	orig_risk_object ⇕	risk_score ⇕	source ⇕	description ⇕	summary ⇕	Workflow1 ⇕	Workflow2 ⇕
Friday 23 August	05:47	x[redacted]	60	Sc.exe Manipulating Windows Services	X[redacted] on x[redacted] used sc to maniuplate services	dest: x[redacted] dest_owner: dest_owner_category: user: X[redacted] username: user_category: process: "C:\WINDOWS\system32\sc.exe" \\127.0.0.1 config SolarWindsAgent64 start= delayed-auto process_exec: sc.exe parent_process_exec: parent_process: unknown	⚙ See processes ran by X[redacted] on x[redacted]	
Thursday 22 August	14:41	x[redacted]	50	Powershell run from document reader application	R[redacted] on x[redacted] ran cmd.exe from msedge.exe	dest: x[redacted] dest_owner: user: R[redacted] user_category: username: parent_process_exec: msedge.exe parent_process: unknown process_exec: cmd.exe process: C:\WINDOWS\system32\cmd.exe /d /c "C:\ProgramData\UiPath\UiPath.Common\23.4.56.63497\BrowserExtension\UiPath.BrowserBridge.Portable\UiPath.BrowserBridge.Portable.exe" chrome-extension://ndmegdjihnhfmljjoaiimbipfhodnbgf/ --parent-window=262774 &lt; \\.\pipe\LOCAL\chrome.nativeMessaging.in.7dd64a8253449f43 &gt; \\.\pipe\LOCAL\chrome.nativeMessaging.out.7dd64a8253449f43 command: C:\ProgramData\UiPath\UiPath.Common\23.4.56.63497\BrowserExtension\UiPath.BrowserBridge.Portable\UiPath.BrowserBridge.Portable.exe risk_score: 50.0	⚙ See powershell activity on [redacted]	⚙ See processes ran by R[redacted] on [redacted]
Thursday	14:41	x[redacted]	50	Powershell	SRV[redacted]T on	dest: x[redacted]	⚙ See	⚙ See

- + extra table for analyst guides and TODOs
- + last 90 days trends

THALES
Building a future we can all trust

Managing noise: High Risk Notable



Risk Alerts - High Risk entities

Last 30 days ▾ Hide Filters

49 high risk notables over time

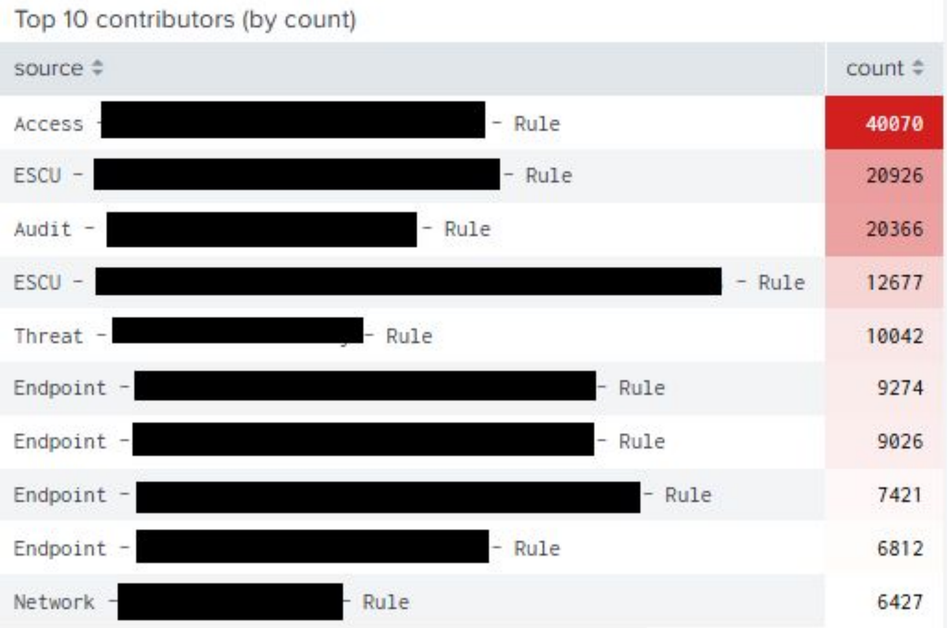
Notables	Duplicates	Duplicates
49	10	20 %

10 notables were duplicates

risk_object ⇕	count ⇕	source ⇕
[redacted]	3	ESCU - [redacted] - Rule Endpoi Endpoi Threat ESCU - [redacted] Endpoin ule Endpoin ication - Rule Endpoin ed - Rule Endpoin Network Threat

Managing noise: High Risk Notable

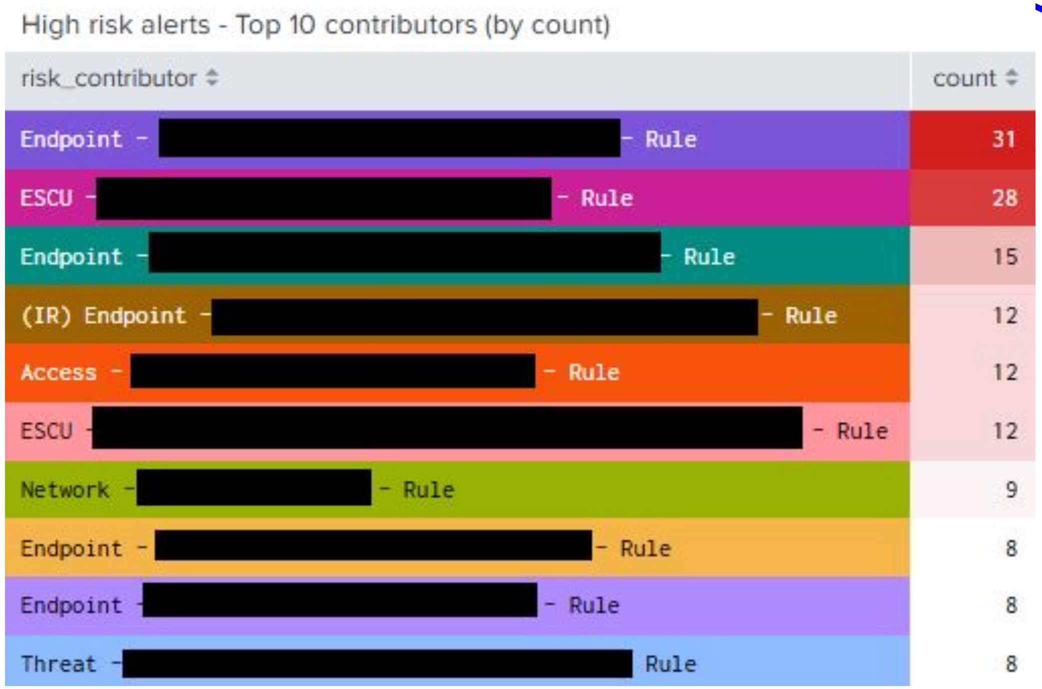
Looking at all risk contributors:



Top 10 contributors (by count)

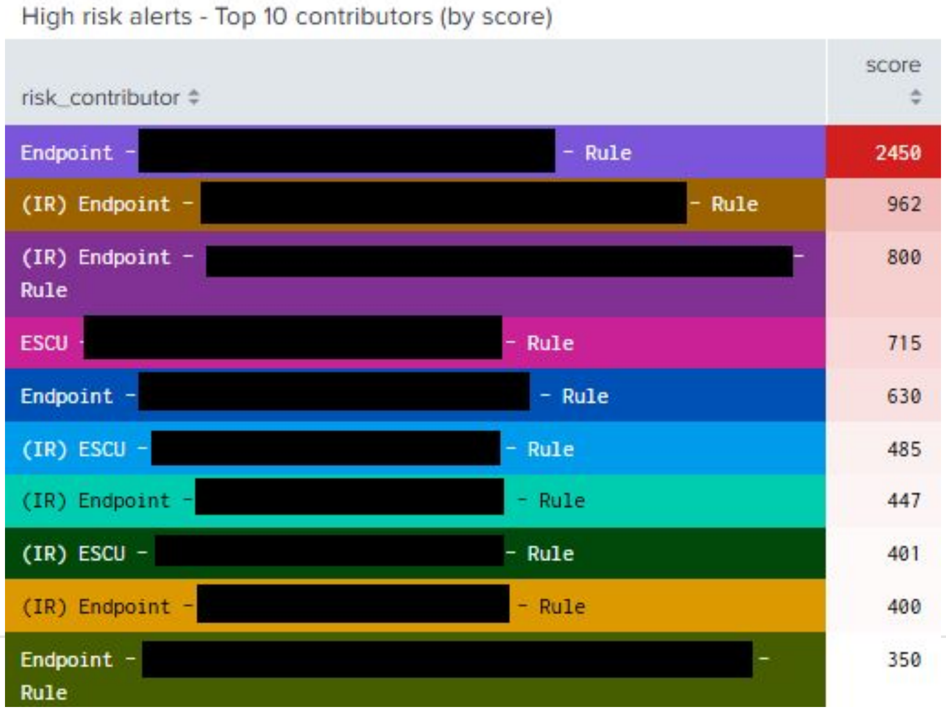
source	count
Access [redacted] - Rule	40070
ESCU - [redacted] - Rule	20926
Audit - [redacted] - Rule	20366
ESCU - [redacted] - Rule	12677
Threat - [redacted] - Rule	10042
Endpoint - [redacted] - Rule	9274
Endpoint - [redacted] - Rule	9026
Endpoint - [redacted] - Rule	7421
Endpoint - [redacted] - Rule	6812
Network - [redacted] Rule	6427

Looking only at risk contributors who are part of a high-risk alert:



High risk alerts - Top 10 contributors (by count)

risk_contributor	count
Endpoint - [redacted] - Rule	31
ESCU - [redacted] - Rule	28
Endpoint - [redacted] - Rule	15
(IR) Endpoint - [redacted] - Rule	12
Access - [redacted] - Rule	12
ESCU [redacted] - Rule	12
Network - [redacted] - Rule	9
Endpoint - [redacted] - Rule	8
Endpoint [redacted] - Rule	8
Threat - [redacted] Rule	8



High risk alerts - Top 10 contributors (by score)

risk_contributor	score
Endpoint - [redacted] - Rule	2450
(IR) Endpoint - [redacted] - Rule	962
(IR) Endpoint - [redacted] - Rule	800
ESCU [redacted] - Rule	715
Endpoint - [redacted] - Rule	630
(IR) ESCU - [redacted] - Rule	485
(IR) Endpoint - [redacted] - Rule	447
(IR) ESCU - [redacted] - Rule	401
(IR) Endpoint - [redacted] - Rule	400
Endpoint - [redacted] - Rule	350

+ Search for notables contributed to by a specific contributor

Recap, references & Thank You!

- Our SOC’s setup & approach to the SIEM
- ES Choreographer: https://splunkbase.splunk.com/app/6309
  - □ Morning checks
  - □ Correlation Best Practices
  - □ Peer Reviews
  - □ TODOs

.conf21 SEC1441A "How We Maintain Our Correlations in Splunk Enterprise Security at Thales UK" https://conf.splunk.com/files/2021/recordings/SEC1441A.mp4

- Conf Manager: https://splunkbase.splunk.com/app/6895
- What is RBA:
  - □ ebook The Splunk Guide to Risk-Based Alerting by Haylee Mills
  - □ RBA community https://rba.community/
- My technical posts on gabrielvasseur.com:
  - □ RBA: a better way to dedup risk events
  - □ RBA: Aggregate user & system risks!
  - □ Risk overview dashboard (coming up, maybe)
  - □ Risk noise management dashboard (maybe in next version of ES Choreographer)
  - □ COMING SOON: divide your Windows Event Logs license usage by 2 to 4 with ingest actions
- Thank YOU! Q&A now. Or go to slack to praise / debate / ask questions!

Random plug: Security Now podcast!