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> .conf21

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!

splunk> .conf21

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!

gabrielvasseur.com

- Source code!
- Simple XML dashboard tricks!

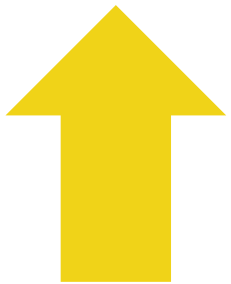
splunk> .conf21

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

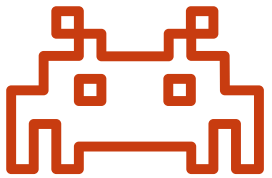
PEER REVIEWS

4

Share knowledge

Promote quality and consistency

The Only Thing you Care About

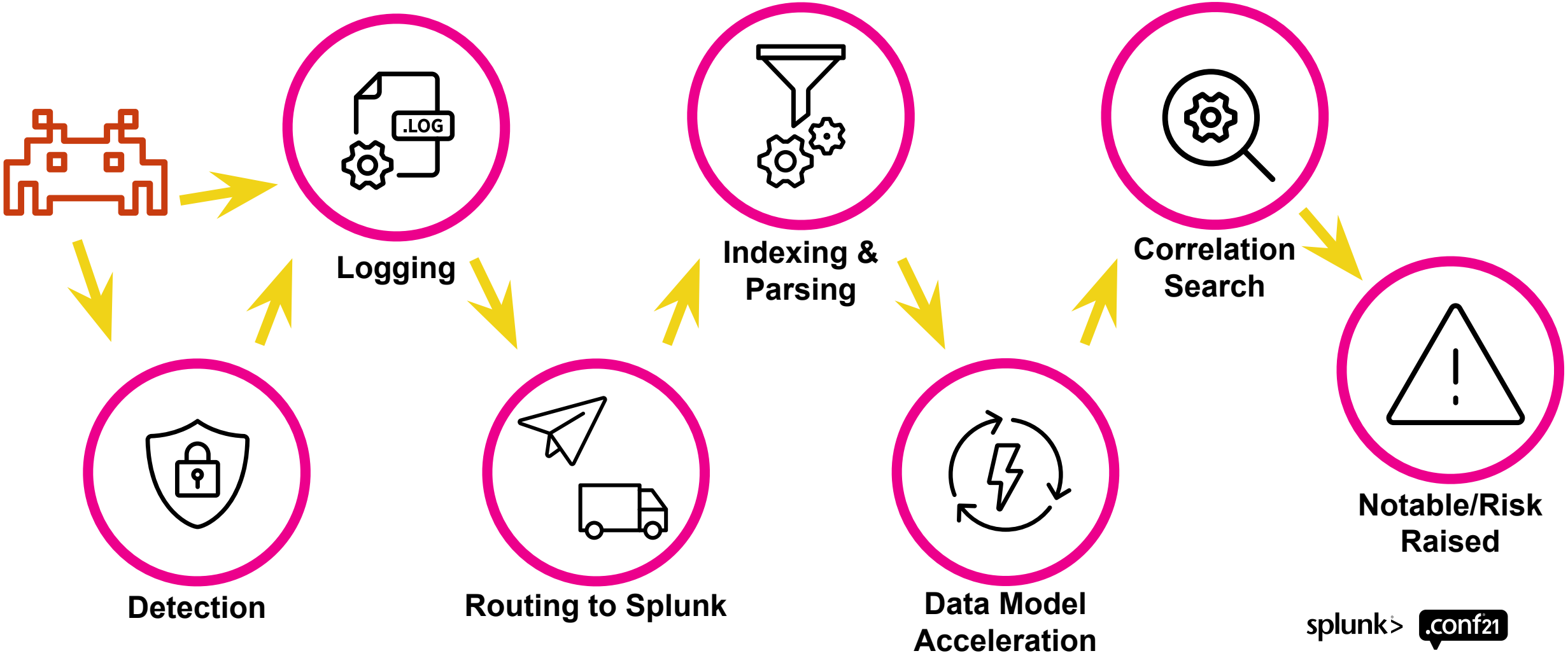


Event / Behaviour

Notable/Risk Raised

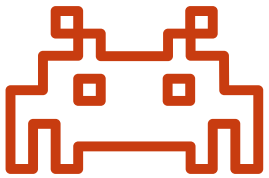
Quiet means quiet… or broken?

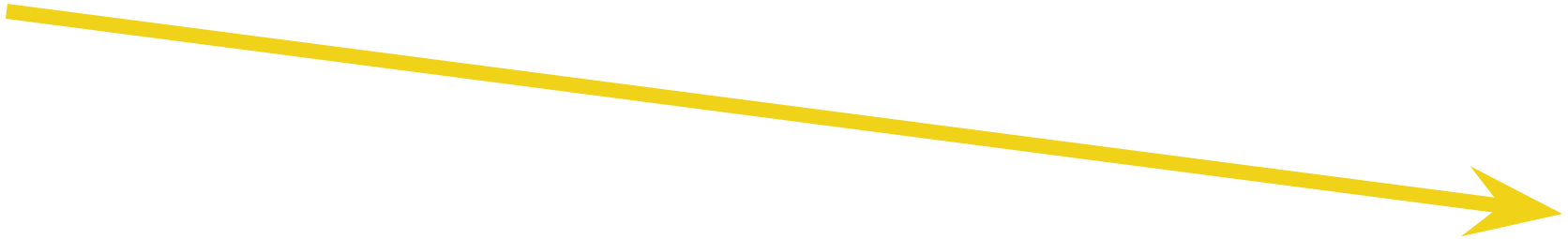
What Could go Wrong?



splunk> .conf21

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

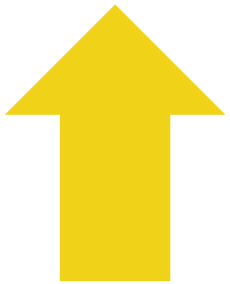
Ensure your correlations work

BEST PRACTICES

2

Define what your correlations should look like

Ensure they do



TO DO'S

3

Collaborate

Ensure visibility of workload

PEER REVIEWS

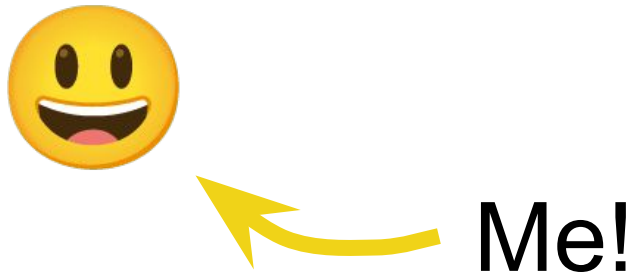
4

Share knowledge

Promote quality and consistency

Has This Ever Happened to You?

Correlation	Job
C	✓



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?

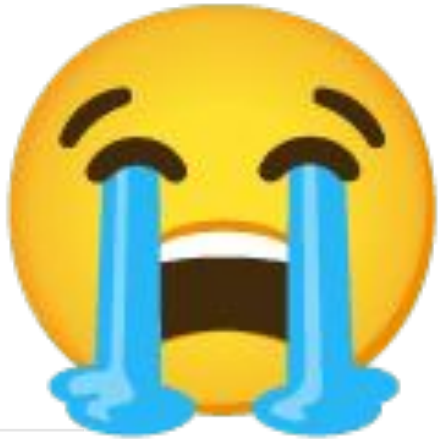
Correlation	Job	Issue 1	Issue 2
A		✓	✓
B		✓	✓
C	✓	✓	✓
D		✓	✓
E		✓	✓
F		✓	✓
...		?	?

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

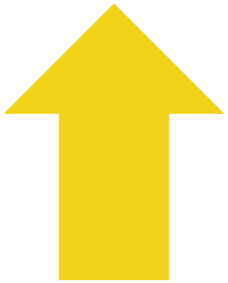
Ensure they do

TO DO'S

3

Collaborate

Ensure visibility of workload



PEER REVIEWS

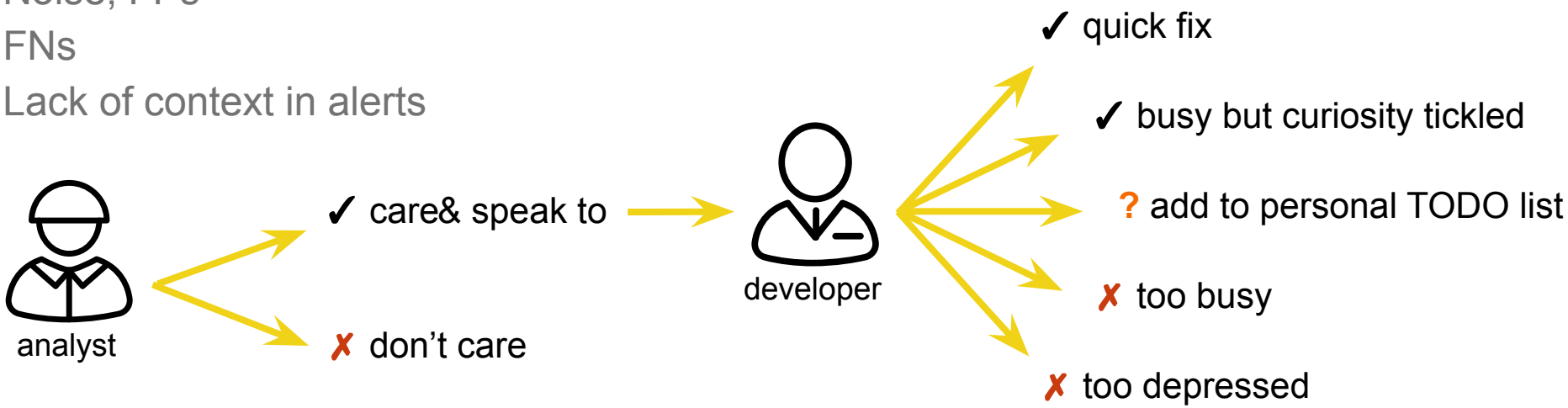
4

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

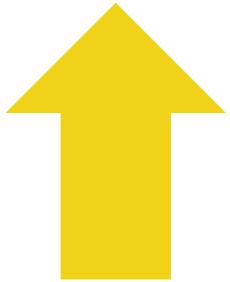
Ensure visibility of workload

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

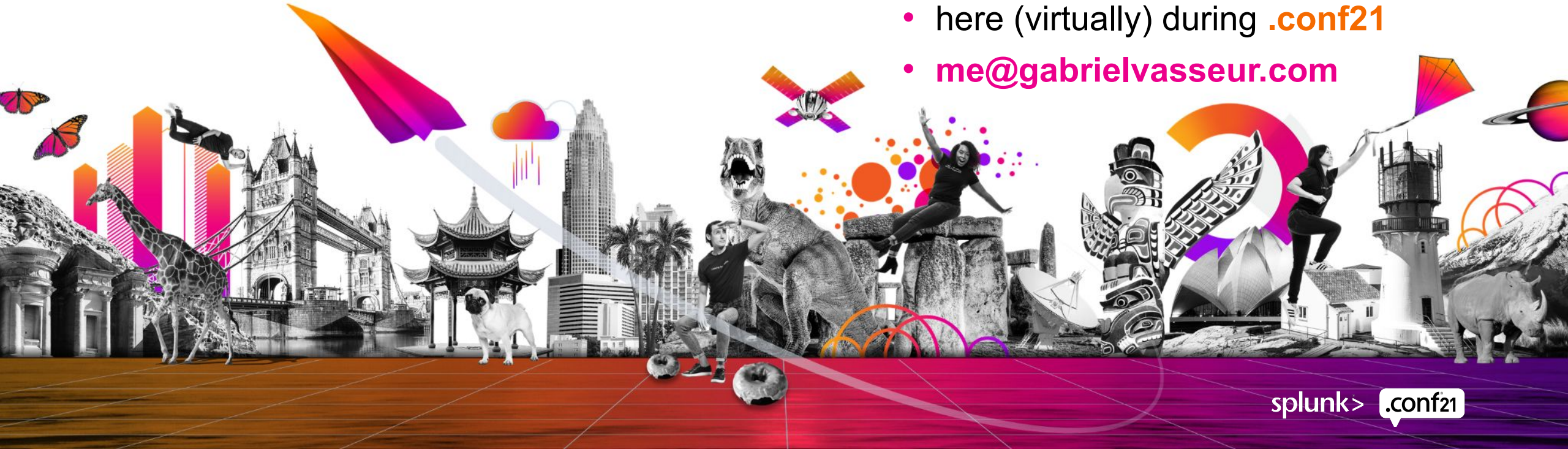
source code & more at
gabrielvasseur.com

Please provide feedback via the

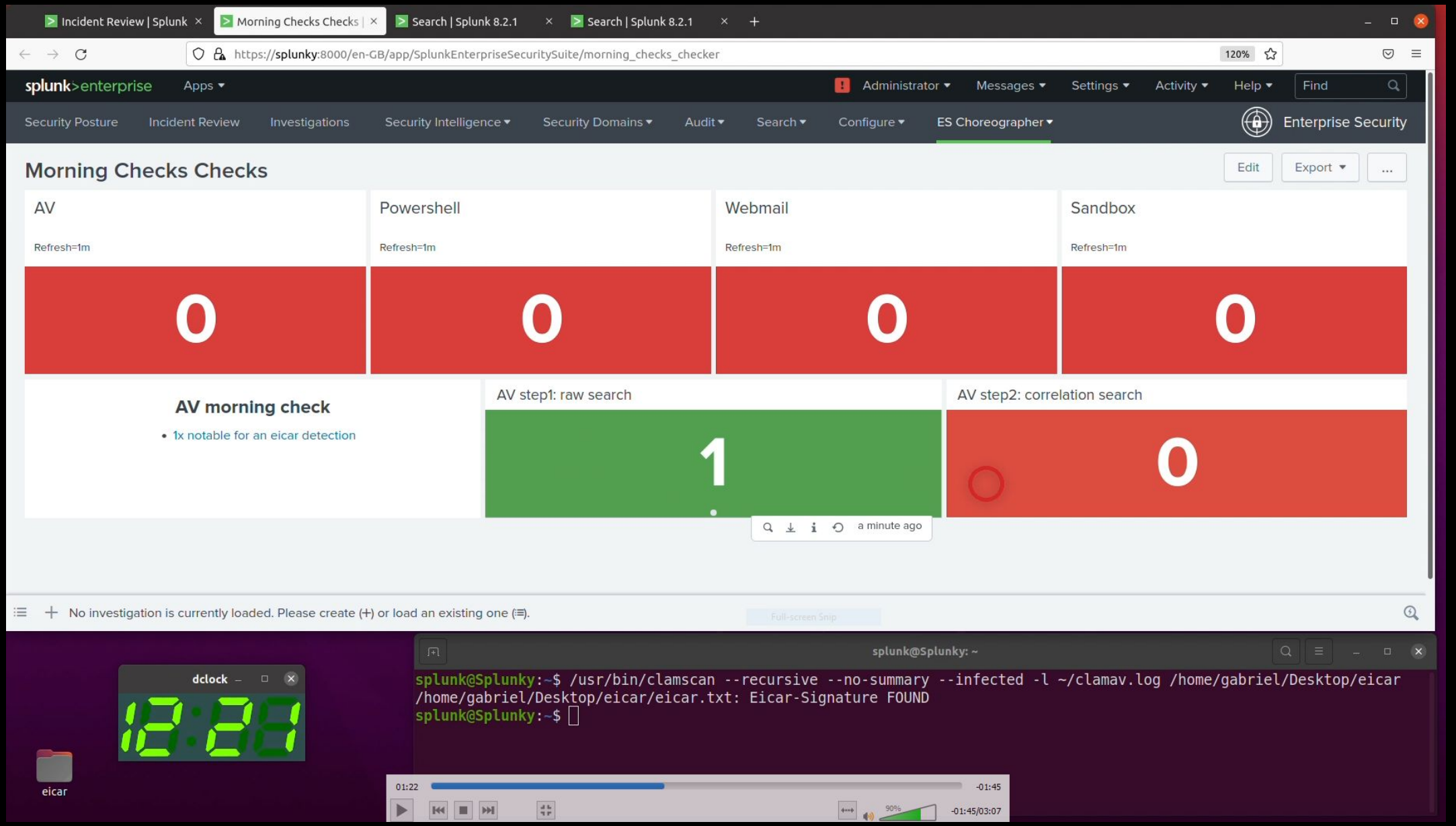
SESSION SURVEY

Please get in touch!

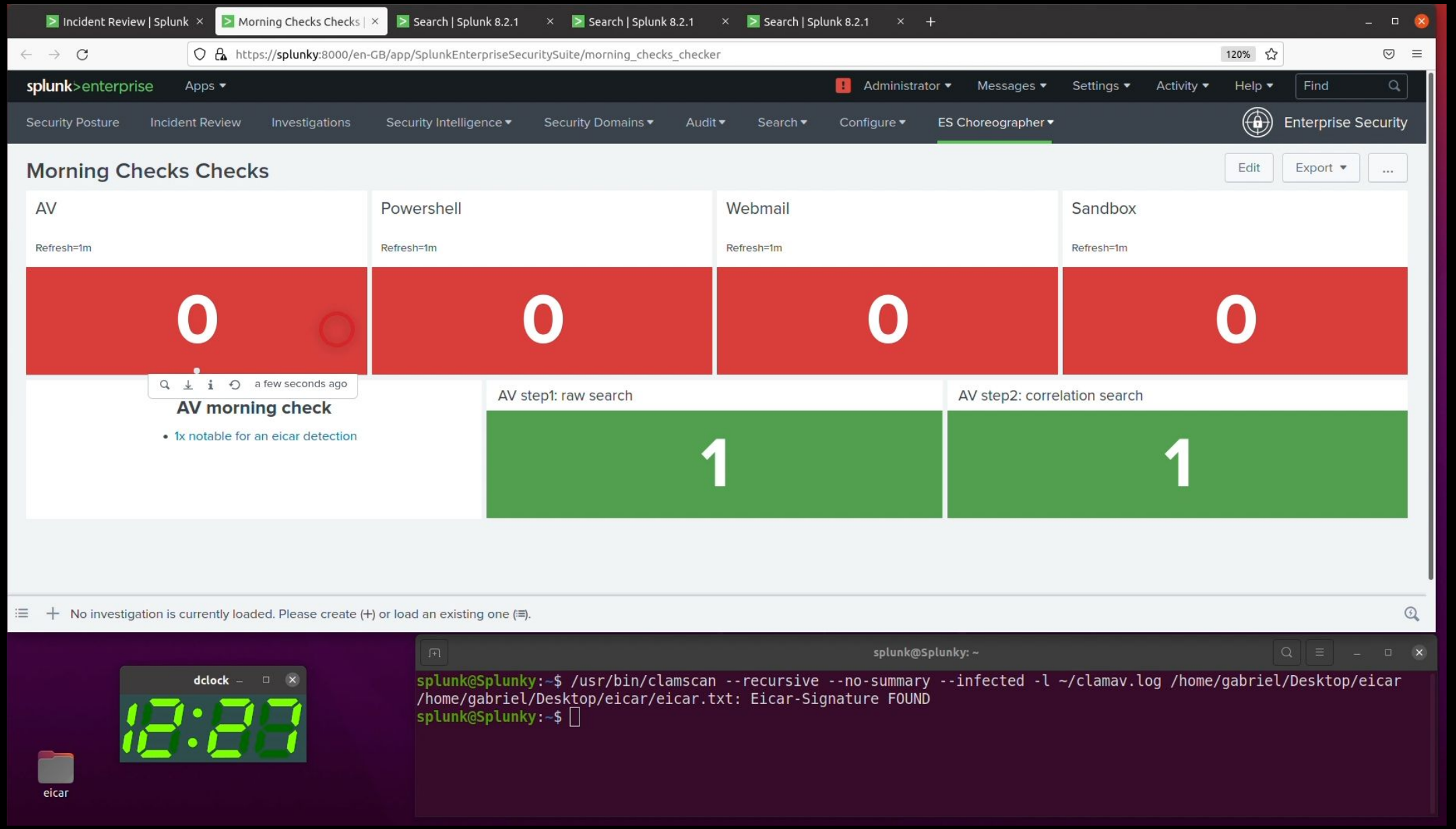
- here (virtually) during .conf21
- me@gabrielvasseur.com



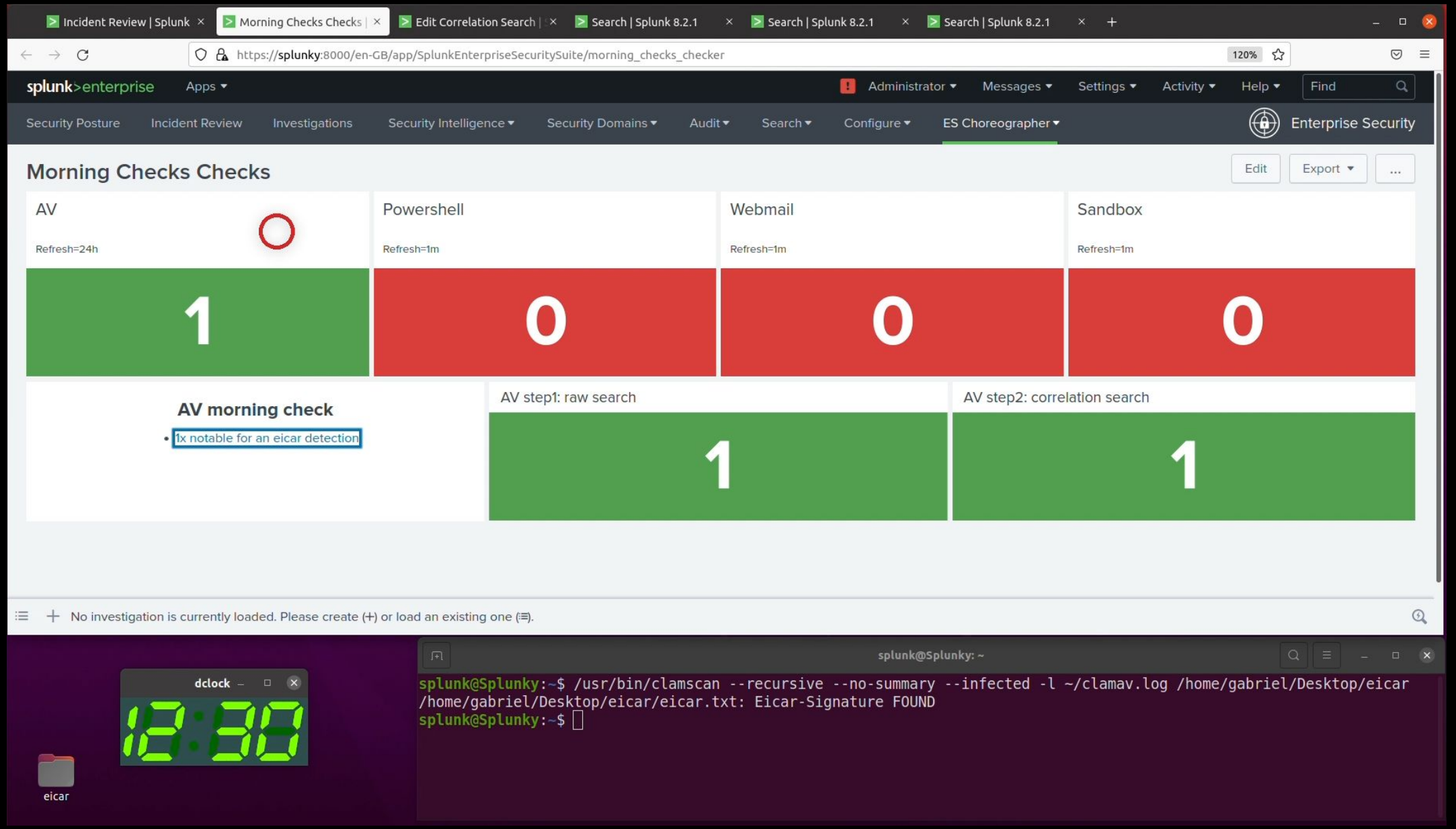
splunk> .conf21



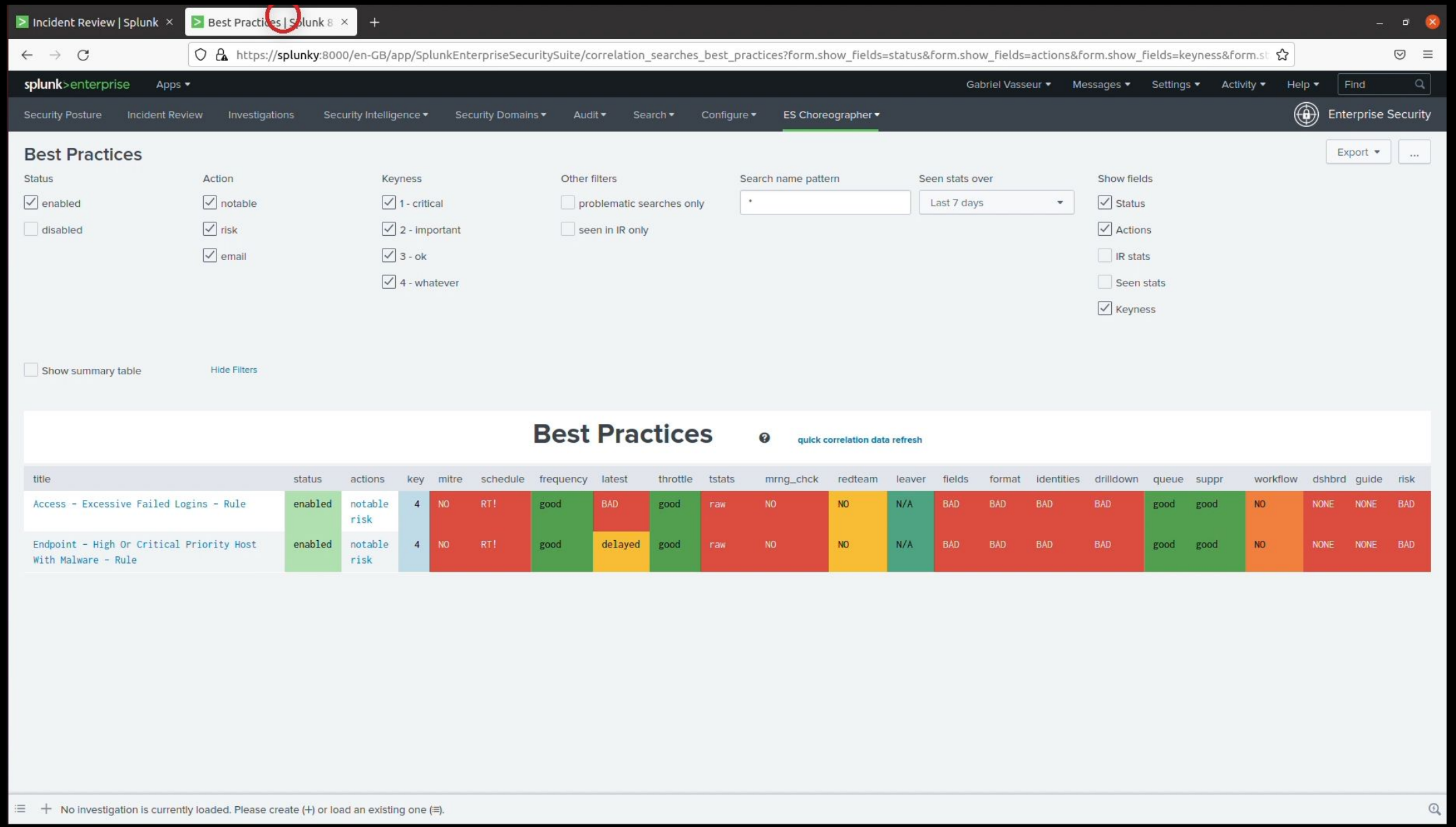
splunk> .conf21



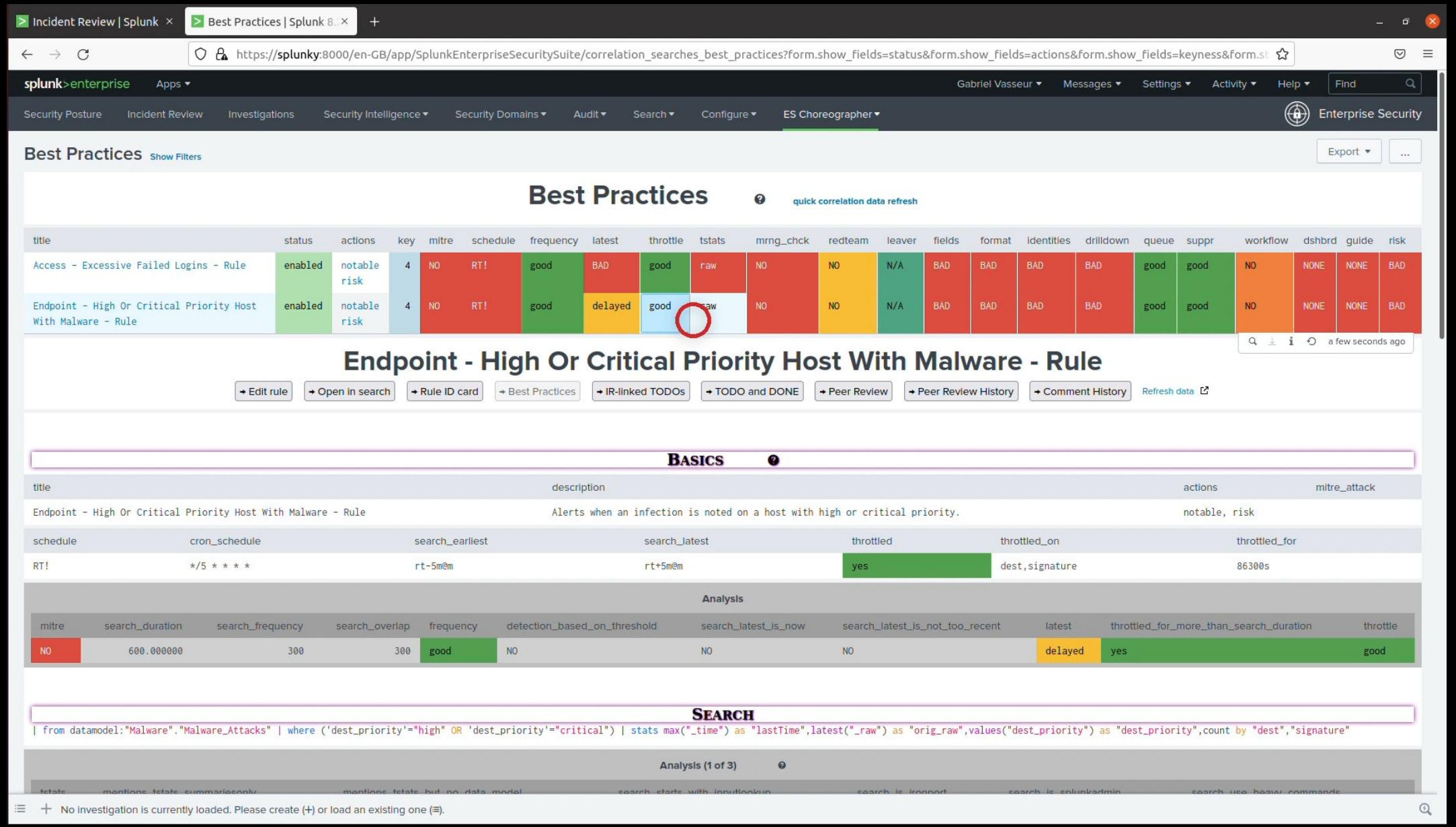
splunk> .conf21



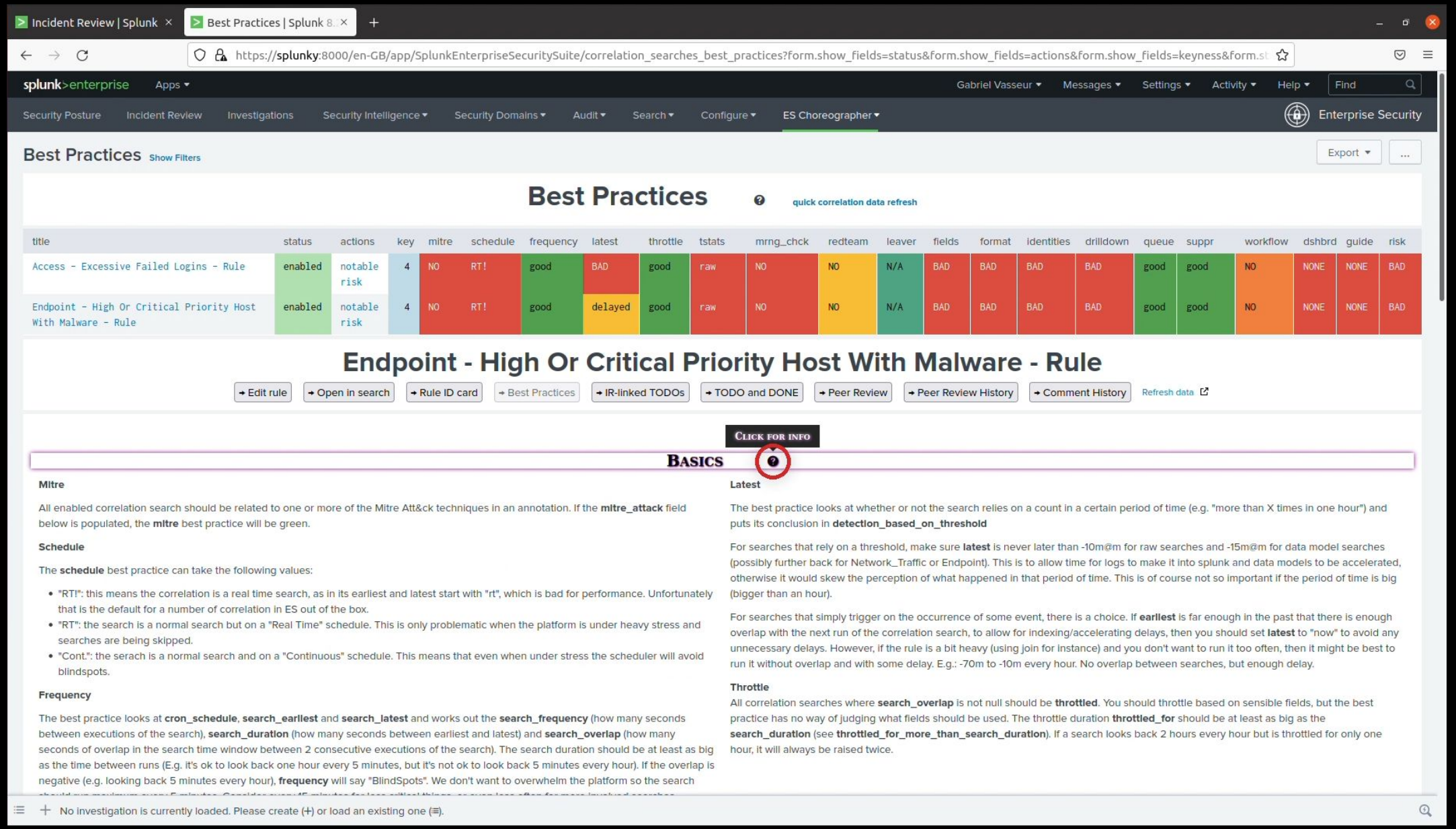
splunk> .conf21



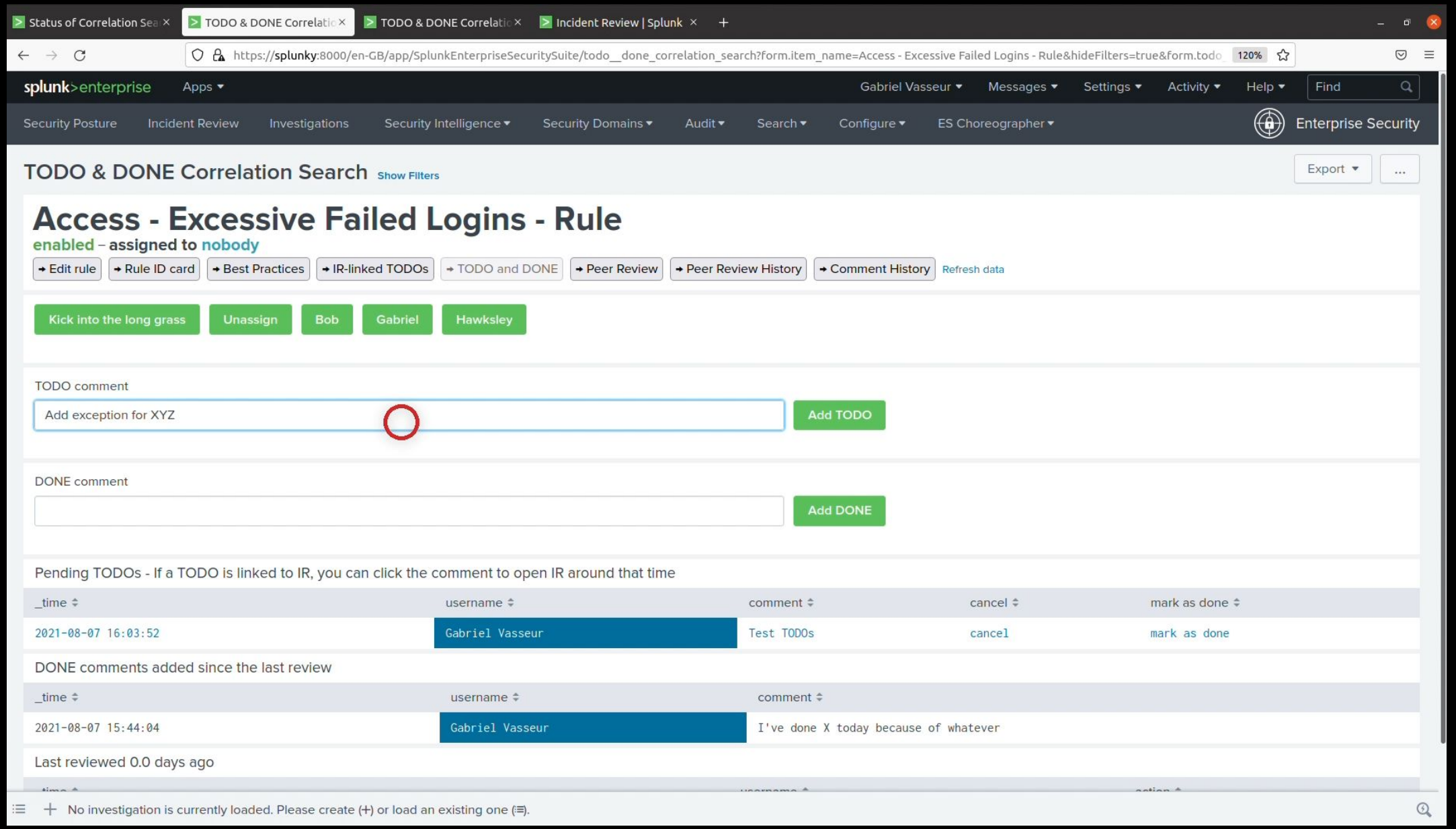
splunk> .conf21



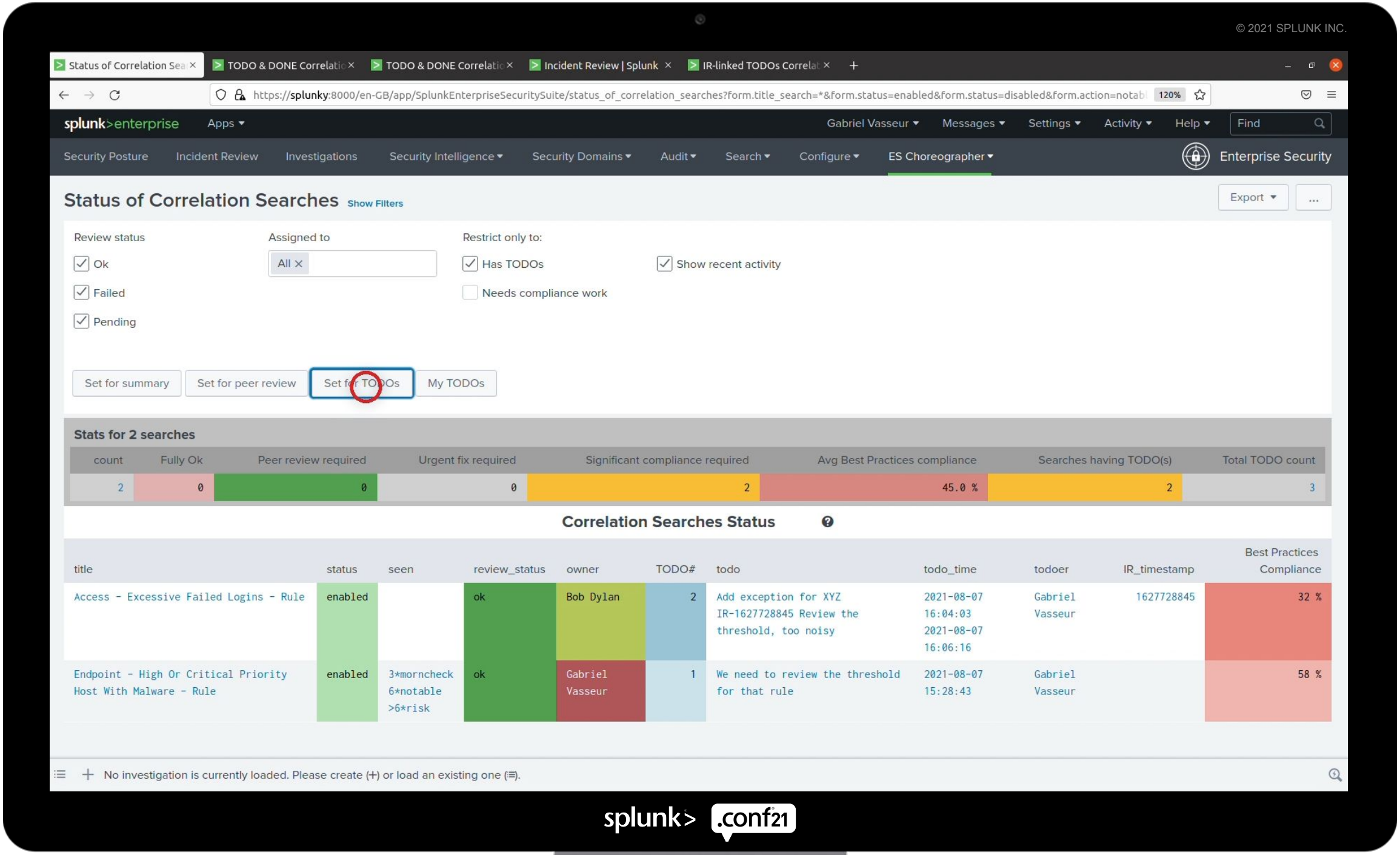
splunk> .conf21



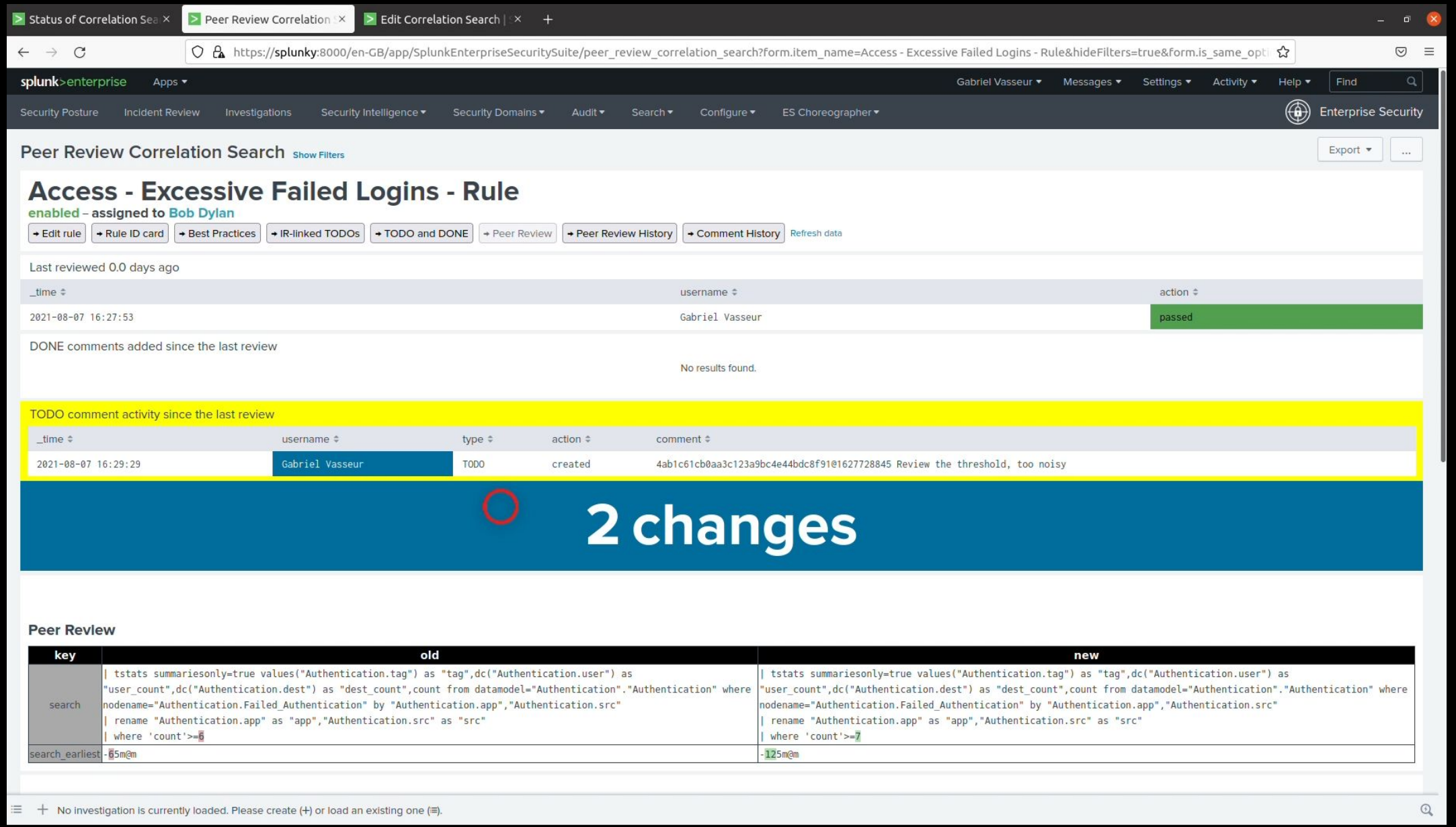
splunk> .conf21



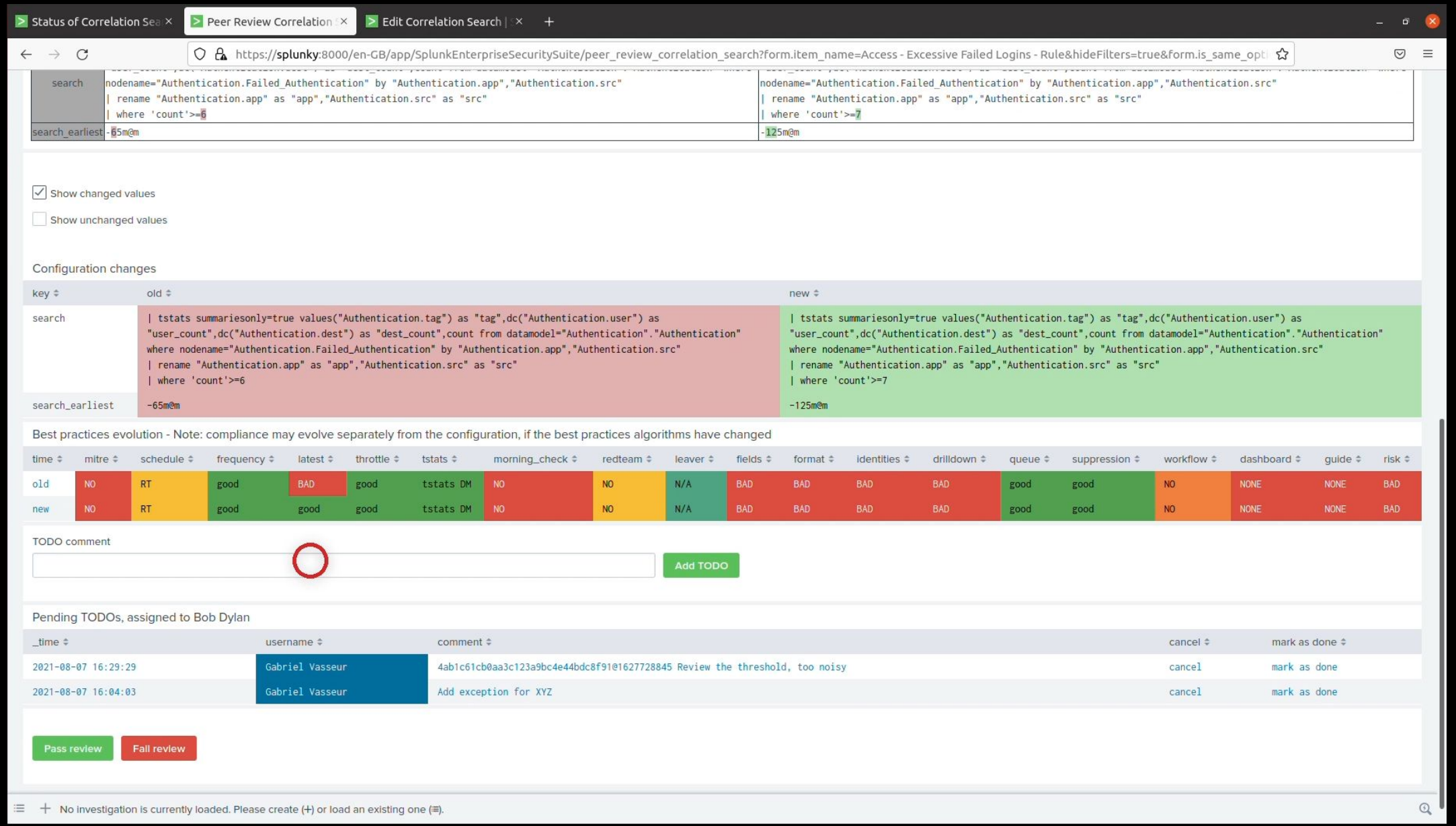
splunk> .conf21



splunk> .conf21



splunk> .conf21



splunk> .conf21