

SIEM the Skyscanner Way

Integrating Splunk into our security practice

Marc Santamaria Ortega

Senior Security Engineer | Skyscanner



Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 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. © 2020 Splunk Inc. All rights reserved

© 2020 SPLUNK INC.

Marc Santamaria Ortega

Senior Security Engineer | Skyscanner

splunk> .conf20

[illegible]

Key Takeaways

1. Splunk versatility allows to customize it to your needs
2. Infrastructure as Code can prove very useful on a Splunk environment
3. Automation is very helpful in alerting and monitoring

Best Practice Sharing from Skyscanner

Integrating Splunk in Skyscanner

1) Splunk analytics as code

Infrastructure as Code for Splunk Cloud searches

2) Automating alert processing

Automating processing of Splunk alerts via AWS Lambda

3) How we monitor our alert pipeline

TTD/TTR dashboards, error monitoring, sources and alert health

4) KVStore and log enriching

Correlating company information with Splunk resources

5) Favorite controls

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change
Change management	Have peer reviews on any change and getting automatically notified of changes to review

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change
Change management	Have peer reviews on any change and getting automatically notified of changes to review
Resilience	Being able to easily reproduce/rollback any change

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change
Change management	Have peer reviews on any change and getting automatically notified of changes to review
Resilience	Being able to easily reproduce/rollback any change
Auditability	Have a detailed audit trace of all changes

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change
Change management	Have peer reviews on any change and getting automatically notified of changes to review
Resilience	Being able to easily reproduce/rollback any change
Auditability	Have a detailed audit trace of all changes
Stability	Having a source of truth for our alerts which replaces any manual change

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change
Change management	Have peer reviews on any change and getting automatically notified of changes to review
Resilience	Being able to easily reproduce/rollback any change
Auditability	Have a detailed audit trace of all changes
Stability	Having a source of truth for our alerts which replaces any manual change
Contextuality	Include info that cannot be easily added like tool related, links to internal docs of the log source or its procedure, ...

Splunk Analytics as Code

Why?

In Skyscanner we use Infrastructure as Code (IaC) to manage our Cloud resources

- Doing the same in Splunk allows us to integrate our best practices into it

Benefit	Description
Version control	Keep historic of changes with descriptions or tickets that drove the change
Change management	Have peer reviews on any change and getting automatically notified of changes to review
Resilience	Being able to easily reproduce/rollback any change
Auditability	Have a detailed audit trace of all changes
Stability	Having a source of truth for our alerts which replaces any manual change
Contextuality	Include info that cannot be easily added like tool related, links to internal docs of the log source or its procedure, ...
Usability	Have more control over our 225+ Splunk scheduled searches, allowing for an easier review of them

Splunk Analytics as Code

How?

Splunk API is very powerful and allows to check/modify many configurations

- <https://docs.splunk.com/Documentation/Splunk/latest/RESTREF/RESTsearch#saved.2Fsearches>
- https://docs.splunk.com/Documentation/Splunk/latest/RESTUM/RESTusing#Access_Control_List

We use GitHub as our code repository and store our scheduled searches in separate files with a folder per each Project/Source

We have defined a script as part of our Splunk IaC that for each Splunk scheduled search

- Parses the template defined
- Encodes any needed field
- Create/updates the scheduled search in Splunk Cloud
- Updates permissions of the scheduled search

**Our alert
template allows
to define any
Splunk
parameter we
need and
also to include
custom ones**



```
1 {
2   'name': 'Template - Webhook action with Cron', #Name of the alert in Splunk Cloud
3   'url_tool': 'https://url.tool.display/...', #Link to the tool related with the logs used in the alert
4   'url_source': 'https://url.source.display/...', #Link to the documentation of the log source used
5   'url_alert': 'https://url.alert.display/...', #Link to the documentation of this alert
6   'url_procedure': 'https://url.procedure.display/...', #Link to the documentation of the procedure
7   'description': 'Template of an alert with webhook action and scheduled via cronjob', #Description of this saved search
8   'search': 'index="test"', #Specifies a field used by Splunk Web to denote the app this search should be dispatched in.
9   'request.ui_dispatch_app': 'search', #App where this alert is stored
10  'request.ui_dispatch_view': 'search', #Specifies a field used by Splunk Web to denote the view this search should be displayed in.
11  'cron_schedule': '8 * * * *', #The cron schedule to execute this search https://url.help/en-US/help?location=learnmore
12  'dispatch.earliest_time': '-2h@m', #A time string that specifies the earliest time for this saved search
13  'dispatch.latest_time': '-1h@m', #A time string that specifies the latest time for this saved search
14  'is_scheduled': 1, #Indicates if this search is to be run on a schedule.
15  'is_visible': 1, #Specifies whether this saved search should be listed in the visible saved search list.
16  'disabled': 0, #Specifies whether this saved search is enabled or not.
17  'alert.digest_mode': 1, #Specifies whether alert actions are applied to the entire result set or on each individual result.
18  'alert.severity': 3, Sets the alert severity level. [1 DEBUG, 2 INFO, 3 WARN, 4 ERROR, 5 SEVERE, 6 FATAL]
19  'alert_type': 'number of events', #What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always
20  'alert_comparator': 'greater than', #One of the following strings: [greater than, less than, equal to, rises by, drops by, rises by per
21  'alert_threshold': 0, #Specifies the value to compare before triggering the alert actions
22  'actions': 'slack, webhook', #A comma-separated list of actions to enable.
23  'action.webhook': 1, #Specifies whether the action webhook is enabled or not
24  'action.webhook.param.url': 'https://url.webhook.param.url', #Sets the URL of the destination web
25  'action.slack': 1, #Specifies whether the action slack is enabled or not
26  'action.slack.param.message': 'Alert *$name$', #Sets the content of the Slack message field
27  'action.slack.param.webhook_url_override': 'https://url.slack.param.webhook_url_override', #Sets the URL
28  'perms.read': 'cloudtrail_user,power,api_user,sc_admin', #Properties that indicate resource read permissions.
29  'perms.write': 'api_user,sc_admin', #Properties that indicate write permissions of the resource.
30  'sharing': 'app' #Indicates how the resource is shared. Required for updating any knowledge object ACL properties.
31 }
```

Versions over time of a search

ory for [SplunkCloudResources](#) / Alerts / SSM / SSM - Patch Compliance


Commits on Jun 23, 2020

20200623 - Update SSM alerts and new Lambda timeout alert (#187) ...

  marcsantamaria authored and OskarBergquist committed on 23 Jun ✓



Commits on Jun 3, 2020

Update SSM - Patch Compliance Association Errors

 marcsantamaria committed on 3 Jun ✓


Commits on May 26, 2020

Update SSM - Patch Compliance Association Errors (#175)

  marcsantamaria authored and OskarBergquist committed on 26 May ✓


Commits on May 20, 2020

Update SSM - Patch Compliance Association Errors

 marcsantamaria committed on 20 May ✓


Commits on May 18, 2020

Update SSM - Patch Compliance Association Errors

 marcsantamaria committed on 18 May ✓


Commits on May 12, 2020

Update SSM - Patch Compliance Association Errors


 marcsantamaria committed on 12 May ✓

Commits on May 11, 2020










Update SSM - Patch Compliance Association Errors

 marcsantamaria committed on 11 May ✓

Update SSM - Patch Compliance Association Errors

 marcsantamaria committed on 11 May ✓

Requests to make changes on searches

<input type="checkbox"/>		1 Open	✓ 218 Closed	Author ▾	Label ▾	Projects ▾	Milestones ▾	Reviews ▾	Assignee ▾	Sort ▾
<input type="checkbox"/>		Create DMARC - partners.skyscanner.net high number of fails in evalut... ✓								 2
#218 by gergokopenczei was merged 8 hours ago • Approved										
<input type="checkbox"/>		Update JAMF - Devices without Cylance ✓								 2
#217 by marcsantamaria was merged yesterday • Approved										
<input type="checkbox"/>		Updating products ✓								 2
#216 by christianmartorella was merged yesterday • Approved										
<input type="checkbox"/>		Create Splunk Info - Log storage Buckets deleted ✓								 1
#215 by marcsantamaria was merged 5 days ago • Approved										

Classification of searches

Branch: master
SplunkCloudResources / Alerts /

Create new file
Upload files
Find file
History

gergokopenczei
Create DMARC - partners.skyscanner.net high number of fails in evalut...

Latest commit c51dfe0 8 hours ago

..


	AWS	Update AWS - Errors detected in Kinesis Firehose	19 days ago
	Aerohive	Create Security Alerts Info (#24)	10 months ago
	Akamai	Add api_user in permissions	11 months ago
	Auth0	Add api_user in permissions	11 months ago
	Azure	Create Azure - Failed signin due to user at risk	2 months ago
	CloudAppSecurity	Update CloudAppSecurity All - Alerts	15 days ago
	CloudTrail	Create CloudTrail Info - SCP policy configuration has changed	12 days ago
	Cylance	Alert changes review (#25)	10 months ago
	DMARC	Create DMARC - partners.skyscanner.net high number of fails in evalut...	8 hours ago
	DomainControllers	Disable alert for password never expires	10 months ago
	GitHub	Update GitHub - Removal of protected branches Quarterly	4 months ago
	GuardDuty	Update GuardDuty - SSH Brute Force attack	5 months ago
	JAMF	Update JAMF - Devices without Cylance (#217)	yesterday


Modification of a scheduled search

Changes from all commits ▾ File filter... ▾ Jump to... ▾ ⚙ 0 / 2 files viewed ⓘ Review changes ▾

▼ ⓘ 2 ■■■■	Alerts/Splunk/Splunk - Host not sending logs in last 2h 📄	<input type="checkbox"/> Viewed ⋮
@@	-23,6 +23,8 @@	
23	23	`comment("Exclude logs that can arrive with 1 day delay")`
24	24	search NOT ((age<90000) AND host IN ("AAPW*"))
25	25	eval lastLog=strftime(lastTime,"%Y-%m-%d %H:%M:%S")
26	+	`comment("Exclude logs that have arrived sparsely")`
27	+	where totalCount>=5
26	28	fields host, lastLog, type
27	29	`comment("Apply temporary exclusions")`
28	30	eval alert="Splunk - Host not sending logs in last 2h"
@@		

Slack notification of repository change

 **Pingu** APP 9:46 AM

 security-squad/SplunkCloudResources - [Update SSM - Critical patches pending in EC2s:](#)

✓ MarcDeMiguel submitted [review](#) [approved]

🎉 MarcDeMiguel merged pull request


Automating Alert Processing

Why?

Slack is our standard way of managing requests


We have some needs that are difficult to cover with Splunk by default Slack integrations


- Show as many results as Slack message limit allows
- Capability to process alerts from Slack and reduce size without losing access to results
- Create a JIRA ticket from a Slack message
- Include documentation to internal procedures, tool that generates the source log and other relevant info
- Do pre-processing in specific alerts to extract information from other systems or automate analysis

 **Sourcetypes not arriving**
Alert Sourcetypes not arriving matched 5 events.
First result:

```
sourcetype
atlassian:confluence
```

You can see the full results here:
[Results in Splunk](#)
[Show more](#)

 Splunk Alert | Today at 3:51 PM

 **Secops_Alerts** APP 10:04 AM
Splunk - Sourcetype logs not arriving in last 2h


Results
[{"sourcetype": "", "lastLog": "2020-07-24 05:01:39", "type": "sourcetypes"}, {"sourcetype": "tenable:io:plugin", "lastLog": "2020-07-25 20:48:13", "type": "sourcetypes"}]

Splunk
[View in Splunk](#)

Alert Procedure
[Splunk Procedures](#)

Alert Documentation
[Splunk Alerts](#)
Tool Portal
[View in Splunk Cloud](#)


[Analysed](#) [False Positive](#) [Create Incident](#)

 **Secops_Alerts** APP 9:00 AM
Splunk - Sourcetype logs not arriving in last 2h

Splunk
[View in Splunk](#)

Alert Procedure
[Splunk Procedures](#)

Alert Documentation
[Splunk Alerts](#)
Tool Portal
[View in Splunk Cloud](#)

 @marc.santamaria Analysed this alert.

Automating Alert Processing

How?

Slack allows to create apps that bring interaction to messages

- <https://api.slack.com/messaging/interactivity>

AWS Lambda allows us to create a serverless function with an API

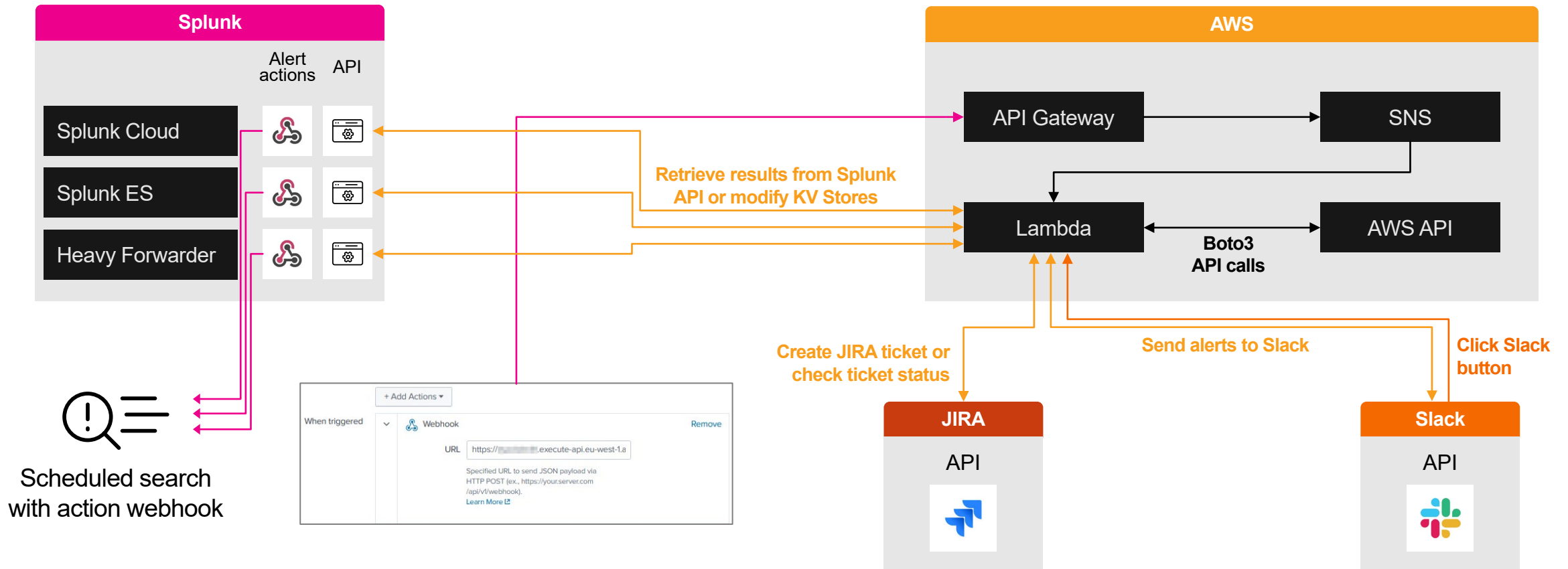
- <https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

We have defined a Python Lambda that does the following:

- Processes requests from both Splunk and Slack
- For each Splunk alert, retrieves all results from Splunk API and depending on each case does automated checks, creates a ticket, updates info on another tool, sends a Slack message, ...
- We classify alerts for the main source that drives them and add context info to Slack messaged

Automating Alert Processing

Diagram



Search Save as

reporter = splunk ORDER BY created DESC

1-50 of 1667

T	Key	Summary	Assignee	Reporter	P	Status	Resolution
		Review S3 bucket		splunk		DONE	Done
		Insecure Security Group in AWS		splunk		NEW	Unresolved
		Splunk - Host not sending logs in last 2h		splunk		DONE	Done
		SOX - New Member in SOX group of Active Directory		splunk		NEW	Unresolved
		SOX - New Member in SOX group of Active Directory		splunk		DONE	Done
		Review S3 bucket		splunk		NEW	Unresolved
		Review S3 bucket		splunk		NEW	Unresolved
		Review S3 bucket		splunk		NEW	Unresolved
		Insecure Security Group in AWS		splunk		NEW	Unresolved
		Insecure Security Group in AWS		splunk		NEW	Unresolved

JIRA tickets created by the Lambda

Example of different functions/integrations of the Lambda

```

alert_functions.py: def sox_new_member_ad(resultsJSON, authorization, context):
alert_functions.py: def sox_admin_change_union(resultsJSON, authorization, context):
alert_functions.py: def sox_admin_change_strudel(resultsJSON, authorization, context):
alert_functions.py: def sox_strudel_logs_not_arriving(resultsJSON, authorization, context):
alert_functions.py: def aws_ssm_databricks_multiple_ami(resultsJSON, bodyJSON, authorization, context):
alert_functions.py: def aws_ssm_critical_patches(resultsJSON, bodyJSON, searchname, authorization, splunk_api, context):
alert_functions.py: def aws_ssm_session_no_project(resultsJSON, authorization, context):
alert_functions.py: def aws_breakglassadmin_access_splunk(resultsJSON, authorization, context):
alert_functions.py: def aws_identity_account_access_splunk(resultsJSON, authorization, context):
alert_functions.py: def aws_insecure_security_groups_splunk(resultsJSON, authorization, context):
alert_functions.py: def aws_open_s3_buckets_policy_splunk(bodyJSON, resultsJSON, authorization, context):
alert_functions.py: def aws_open_s3_buckets_acl_splunk(bodyJSON, resultsJSON, authorization, context):
alert_functions.py: def slack_button(bodyJSON, authorization, context):
boto3.py: def get_instance_project_tag(auxinstance, auxaccount, auxregion, context):
boto3.py: def get_security_group_tag(auxsg, auxaccount, auxregion, context):
boto3.py: def get_bucket_tagging(auxbucket, auxaccount, auxregion, context):
jira.py: def jira_api_create_splunk_comment(jira_ticket, table, authorization, alertid, context):
jira.py: def jira_api_get_issue_status(authorization, issueid, context):
jira.py: def jira_api_create_splunk_issue(auxuser, table, authorization, alertid, context):
jira.py: def jira_api_create_incident(requestJSON, authorization, context):
slack.py: def generate_slack_message(bodyJSON, results, authorization, context):
splunk.py: def add_kvstore_entry_ssm_tickets(kvstore, kvstoreentry, splunk_api, jira_ticket, status, context):
splunk.py: def update_kvstore_entry_ssm_tickets(kvstore, splunk_api, jira_ticket, status, context):
splunk.py: def get_search_results(bodyJSON, bodyRequest, results_link, sid, splunk_api, authorization, context):

```

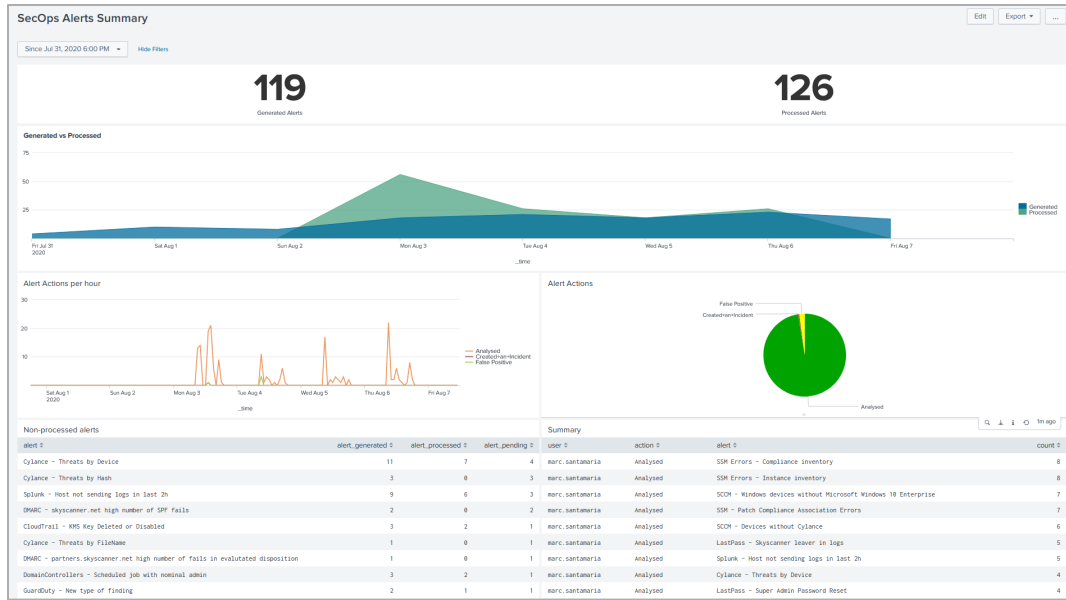
How we Monitor our Alert Pipeline

Systems always can fail and with alerts depending on different systems we need to ensure that issues in all steps are detected (log source system, Splunk, Lambda, ...)

- Detect if logs are arriving as expected into Splunk (both by host or sourcetype)
- Detect issues with Splunk (processing or integration errors, unexpected changes, ...)
- Detect issues with the Lambda (timeouts, errors/exceptions caught, alerts not processed, ...)

We have also built a Splunk dashboard that correlates Splunk audit information and Lambda logs

- Offers visibility on TTD and TTR of alerts (Time to detect and time to response)
- Allows us to do quarterly alert reviews knowing which alerts raise more often, which ones are ignored or false positives, which ones take longer to process, ...

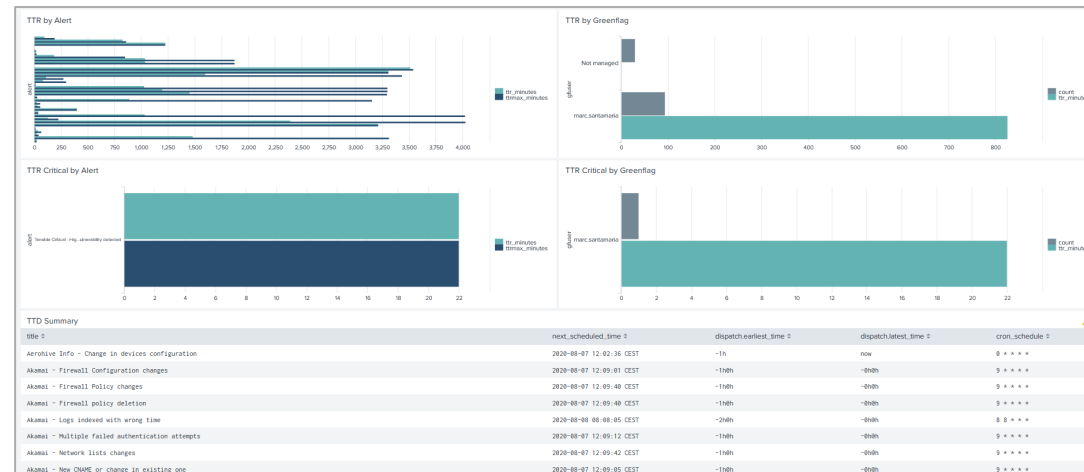


Alert review dashboard

Monitoring searches in Splunk

i	Title
>	Splunk - Alert not processed by Lambda
>	Splunk - Alert not processed by Splunk
>	Splunk - Apps pending to be updated
>	Splunk - DBConnect error
>	Splunk - DBConnect query failed
>	Splunk - Delete permission changes
>	Splunk - Error in Python scripts
>	Splunk - Error in Slack Lambda
>	Splunk - Error in alert execution
>	Splunk - Host not sending logs in last 2h
>	Splunk - License of 100GB surpassed
>	Splunk - Multiple failed login attempt
>	Splunk - Multiple failed login attempt followed by successful one
>	Splunk - New host sending logs
>	Splunk - New sourcetype sending logs
>	Splunk - Possible logs deleted in Splunk Cloud
>	Splunk - SecOps Lambda has timedout
>	Splunk - SkyScanner leaver in logs
>	Splunk - Sourcetype logs not arriving in last 2h
>	Splunk - Summary of alerts not managed by GF yesterday
>	Splunk Info - Alert changes
>	Splunk Info - App changes
>	Splunk Info - Log storage Buckets deleted
>	Splunk Info - Object changes
>	Splunk Info - Server restarted

TTD/TTR dashboard



Alert review template

Attendees

- Type attendees here using "@"

Discussion items

Review:

- Alerts with summary dashboard
 - [https://splunk.com/en-US/app/search/secops_alerts_summary](#)
- Suggestions on Confluence page
 - [Alert Review Suggestions](#)
- Review pending tasks from previous Alert Reviews
- Review top hosts/sourcetypes not sending logs
 - [https://splunk.com/en-US/app/search/analysis_of_resources_not_sending_logs](#)
- Review current temporary exceptions
 - [https://splunk.com/en-US/app/search/alerts_exceptions](#)

Gather feedback on:

- Which alerts create more noise
- Reason to not action some alerts
- Alerts which management/procedures is not clear
- Comments on Splunk alerts

Decide

- Alerts that should be disabled/changed
- Alerts that we should work on
- Alerts that will be migrated first into Hefesto for automation
- ...

Action items

General tasks

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

Alerts to be created

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

Alerts to be modified

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

Alerts to be deleted

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

New VictorOps alerts

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

Alerts to be automated

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

Exceptions

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

Procedures to be modified

- ☐ Type your task here, using "@" to assign to a user and "/" to select a due date

KVStore and Log Enriching

We ingest into Splunk data from multiple sources but some of it is specially useful to include in KV Stores to enrich Splunk alerts and dashboards on search time

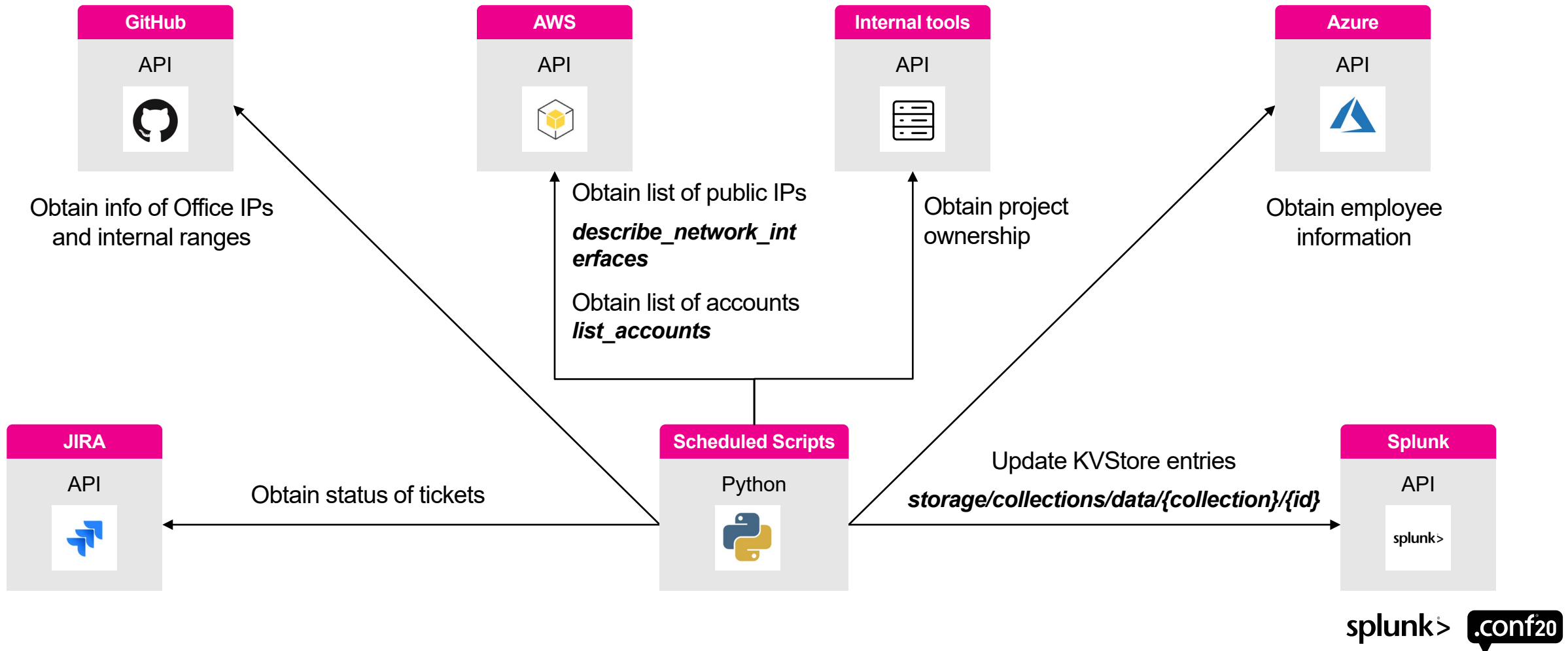
- Skyscanner office IP ranges
- Skyscanner Cloud accounts info and IP ranges
- Ownership of Projects by Skyscanner teams
- Status of tickets opened
- Old employees
- Temporary exceptions in alerts

We automatically manage our KVStores via Splunk API and keep them up to date

- <https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/usetherestapitomanagekv/>

KVStore and Log Enriching

Diagram



SSM Info - AWS Project without known owner

```

index="aws" sourcetype="aws:ssm:instances" NOT State IN ("stopped", "terminated")
| lookup kvs_ssm_ownership aws_project as Project OUTPUT squad_name, slack_channel, slack_gf, jira_project
| where isNull(squad_name) AND Project!="null"
| fillnull value="N/A" AccountName, Project, Stack
| stats count by AccountName, Project, Stack

```

✓ 13 events (6/1/20 12:00:00.000 AM to 8/7/20 12:32:26.000 PM) No Event Sampling ▼

Events Patterns **Statistics (2)** Visualization

100 Per Page ▼ Format Preview ▼

AccountName ↕	Project ↕	Stack ↕
sandbox		
sandbox	private-test-project	

Lookups

New Lookup

Health ▾

Search ▾

Lookups

All

Global

Mine

Type: All ▾

App: Search & Reporting ▾

kvs

Name ↕	Type ▲
kvs_skyranges_internal	KV Store Lookup
kvstore_alert_exceptions	KV Store Lookup
kvstore_leavers	KV Store Lookup
kvstore_mimecast_pgs	KV Store Lookup
kvstore_skyaws	KV Store Lookup
kvstore_skyip	KV Store Lookup
kvstore_skyranges	KV Store Lookup
kvstore_ssm_ownership	KV Store Lookup
kvstore_ssm_tickets	KV Store Lookup
kvstore_tenablescans	KV Store Lookup

Temporary exceptions on kvs_alert_exceptions

alertname ↕	exceptionfield ↕	expirationtime ↕
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/08/10 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Host not sending logs in last 2h		2020/09/01 09:00:00
Splunk - Sourcetype logs not arriving in last 2h		2020/09/01 09:00:00

Usage of KVStore kvs_alert_exceptions

type ↕	app ↕	title ↕	owner ↕
search	search	JAMF - Devices without Cylance	security@skyscanner.net
search	search	SCCM - Devices without Cylance	security@skyscanner.net
search	search	Splunk - Host not sending logs in last 2h	security@skyscanner.net
search	search	Splunk - Sourcetype logs not arriving in last 2h	security@skyscanner.net
dashboard	search	alerts_exceptions	marcsantamaria@skyscanner.net

Favorite Controls

VictorOps

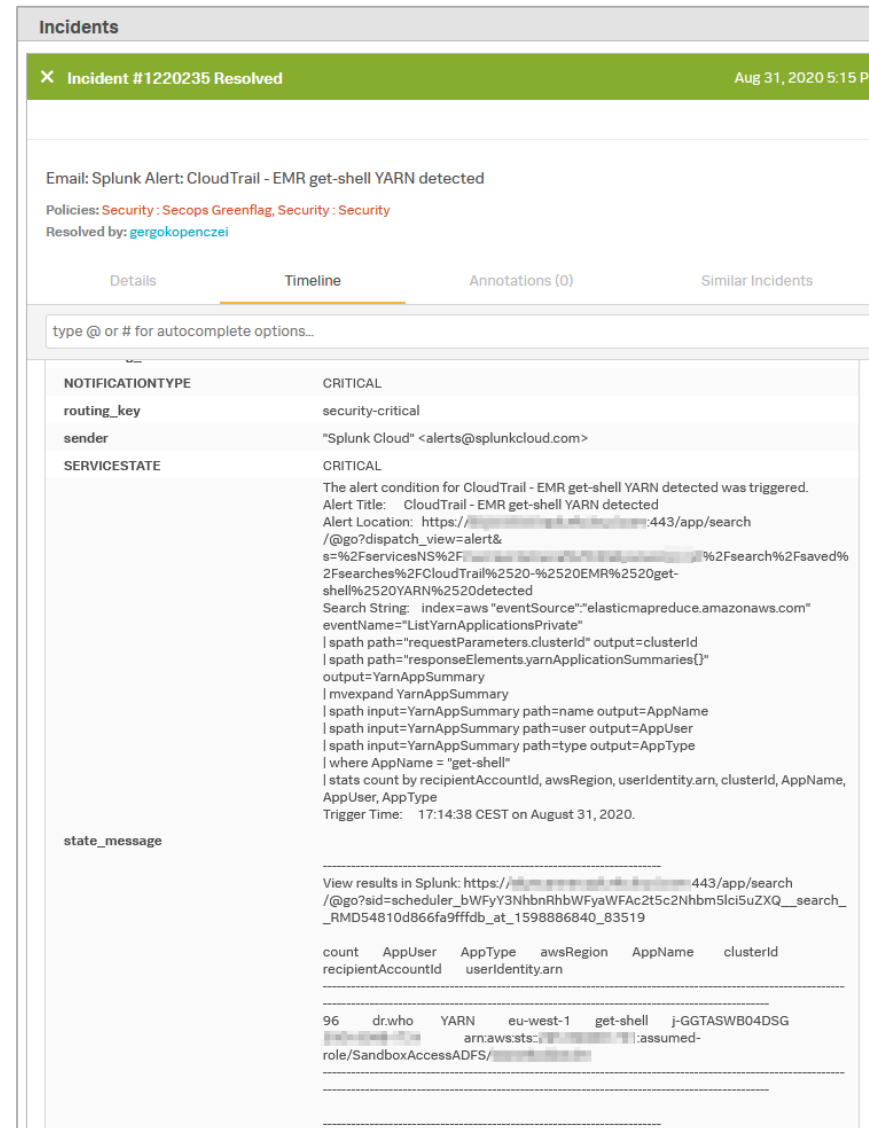
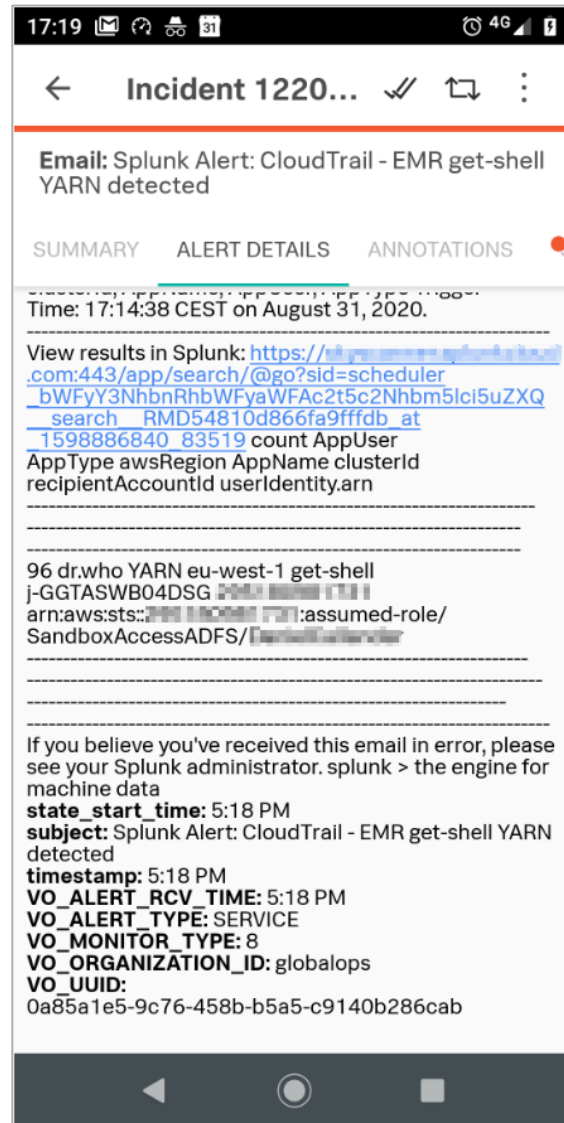
For Out of Hours (OOH) notifications in Skyscanner we use VictorOps

Splunk and VictorOps can be integrated in several ways

- Via Splunk app for VictorOps
- Via VictorOps API
- **Via mails to VictorOps**
 - {Tenant}+{Routing Key}@alert.victorops.com

Allows to notify OOH support in an easy way with all the data needed to handle the alert

The screenshot shows the 'Send email' configuration panel in Splunk. It includes fields for 'To' (with a placeholder email address and a link to 'Show CC and BCC'), 'Priority' (set to 'Normal'), 'Subject' (with a placeholder 'Splunk Alert: \$name\$'), and 'Message' (with a placeholder 'The alert condition for \$name\$ was triggered.'). Below these are 'Include' checkboxes for 'Link to Alert', 'Link to Results', 'Search String', 'Inline', 'Trigger', 'Attach CSV', 'Trigger Time', and 'Attach PDF'. The 'Type' is set to 'HTML & Plain Text'. A 'Remove' link is in the top right corner.



Favorite Controls

DMARC

DMARC allows to protect your email domains and prevent unauthorized usage for phishing, spoofing and other scams

Managing and monitoring multiple email domains usually is a hassle or too expensive

Splunk allows you to easily ingest the data and prepare your own dashboards and controls

- TA-dmarc add-on for Splunk - <https://splunkbase.splunk.com/app/3752/>
- SEC1106 of .conf19 - <https://conf.splunk.com/files/2019/slides/SEC1106.pdf>

DMARC - All domains

Edit Export ...

Last 30 days

Hide Filters

Disposition not none

127

Total count

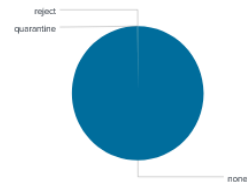
29,292,175

DMARC policy disposition

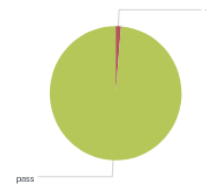
Not none disposition should be investigated

feedback[record.row.policy_evaluated.disposition]	count
none	166483
quarantine	97
reject	30

DMARC policy applied



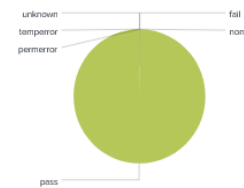
SPF policy evaluated



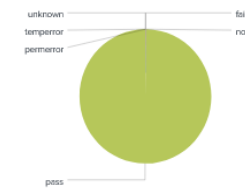
DKIM evaluated



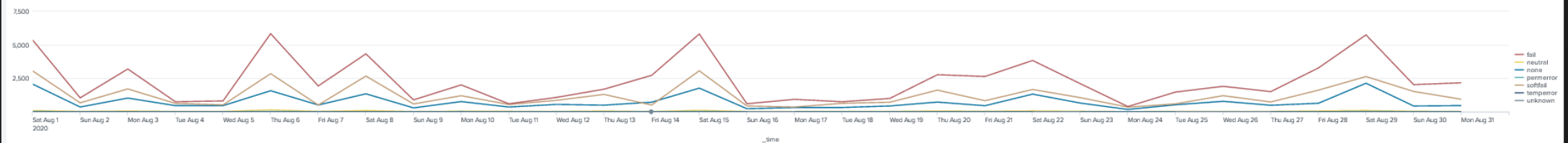
SPF results



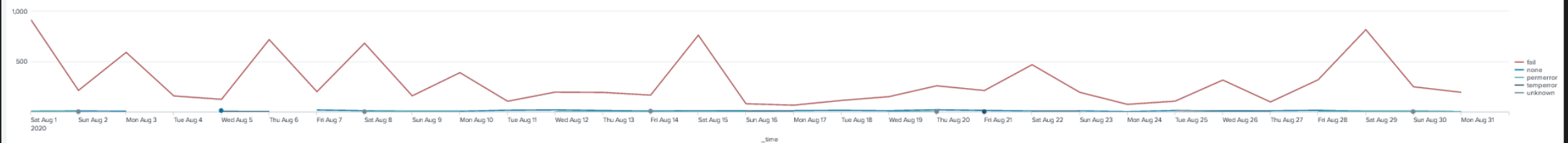
DKIM results



SPF restuls (pass excluded)



DKIM results (pass excluded)



What's Next with Splunk in Skyscanner?

Improve our Operational Threat Intelligence with Splunk Enterprise Security

Migrate more Splunk configurations to Infrastructure as Code

Replace the Lambda that processes Splunk Alerts with a microservice shared between all the Security members to unify automations and reuse integrations

Correlate information from our Vulnerability DBs and scanners with our inventories of both servers and workstations to revamp our Vulnerability Management

Links Related with the Presentation

Application	Links
Splunk	https://docs.splunk.com/Documentation/Splunk/latest/RESTREF/RESTsearch#saved.2Fsearches https://docs.splunk.com/Documentation/Splunk/latest/RESTUM/RESTusing#Access_Control_List https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/usetherestapitomanagekv/ https://conf.splunk.com/files/2019/slides/SEC1106.pdf https://splunkbase.splunk.com/app/3752/
AWS	https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html https://docs.aws.amazon.com/sns/latest/dg/welcome.html https://docs.aws.amazon.com/lambda/latest/dg/welcome.html
Boto3	https://boto3.amazonaws.com/v1/documentation/api/latest/index.html https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/organizations.html#Organizations.Client.list_accounts https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/ec2.html#EC2.Client.describe_network_interfaces
Slack	https://api.slack.com/start https://api.slack.com/messaging/interactivity
JIRA	https://developer.atlassian.com/server/jira/platform/rest-apis/
GitHub	https://developer.github.com/v3/
Active Directory	https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-aduser https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-adobject



Thank You

Please provide feedback via the
SESSION SURVEY

