



Tales From a Threat Team

Lessons and Strategies for Succeeding with a Risk-Based Approach

Stuart McIntosh
Outpost Security

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>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2019 Splunk Inc. All rights reserved.

Agenda

1. The Situation Report
2. The Notables
3. The Platform
4. The New Rules



The Situation Report

Where is our RBA?

The Situation Report

Why Risk-Based Approach (RBA)

RBA Worked!

- Flat SOC Staffing with 4x the amount of detections
- Absorbed and works with a multiple platforms and environments with negligible changes
 - On-Premise, AWS, O365

Other RBA Presentations For Background

[SEC1479](#) - Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach (.conf 2018)

[SEC1803](#) - Modernize and Mature Your SOC with Risk-Based Alerting

[SEC1538](#) - Getting Started with Risk-Based Alerting and MITRE

The Situation Report

Overview of Our RBA Deployment

Ran in Parallel for 3 months

- Was running RBA and Single Detection Alerts to measure accuracy and impact

Production for 14 months

- Sole source of alerting for this period of time

112 Production Risk Rules

- Unique detections of anomalies in the environment

The Situation Report

By The Numbers

Event log data
analyzed per
week



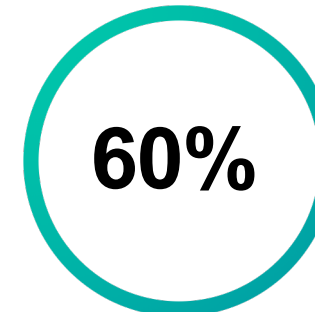
Risk attributions
per week



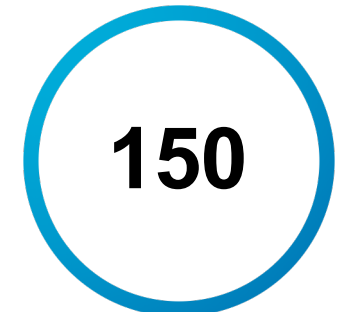
Notables per week
*Have processed over
15k RBA notables



True positive
rate of notables
for malicious
activity



Incidents sent to
HR for
investigation for
the year





The Notables

What about RBA Notables?

The Notables

Analyst Work

- Prescribed Playbooks Too Fragile
- Decision Tree/Web Approach
- Escalating Response



The Notables

Tagging

Have I Seen This? What's Different?

Quick view of previous notable history and close status

Indicates when risk is increasing for an object

Risk_Object	server-185-153-198-196.cloudedic.net	▼
Risk_Object_Type	external_system	▼
Risk_Rule	High Connections Ingress Web - Network Traffic	▼
	Matched Content - Network - Threat Intelligence	▼
Risk Time	1565921580.000000	▼
Rule_Phases	command_and_control	▼
	discovery	▼
System	server-185-153-198-196.cloudedic.net	▼
Tags	modaction_result	▼
	Previous Notable-Last 7 days	▼
	Previous Notable-Additional Risk	▼
	Previous Notable-Different Risk Score	▼
	Previous Notable-Malicious	▼
	Previous Notable-Composite-Score-Exceeded	▼

The Notables

Volume Issues

Multiple notables for same attribution

Specific matrix of action

Leverage the tagging as knowledge

Chose to distill on if it matches score and rules then suppress

alert	previous notable	previous status	matched rules	matched score
yes	FALSE	FALSE	FALSE	FALSE
yes	TRUE	non-malicious	FALSE	FALSE
yes	TRUE	non-malicious	FALSE	TRUE
yes	TRUE	non-malicious	TRUE	FALSE
no	TRUE	non-malicious	TRUE	TRUE
yes	TRUE	malicious	FALSE	FALSE
yes	TRUE	malicious	FALSE	TRUE
yes	TRUE	malicious	TRUE	FALSE
no	TRUE	malicious	TRUE	TRUE



The Platform

How Do You Know RBA Is Running Well?

The Platform

Person of Interest - Watchlist

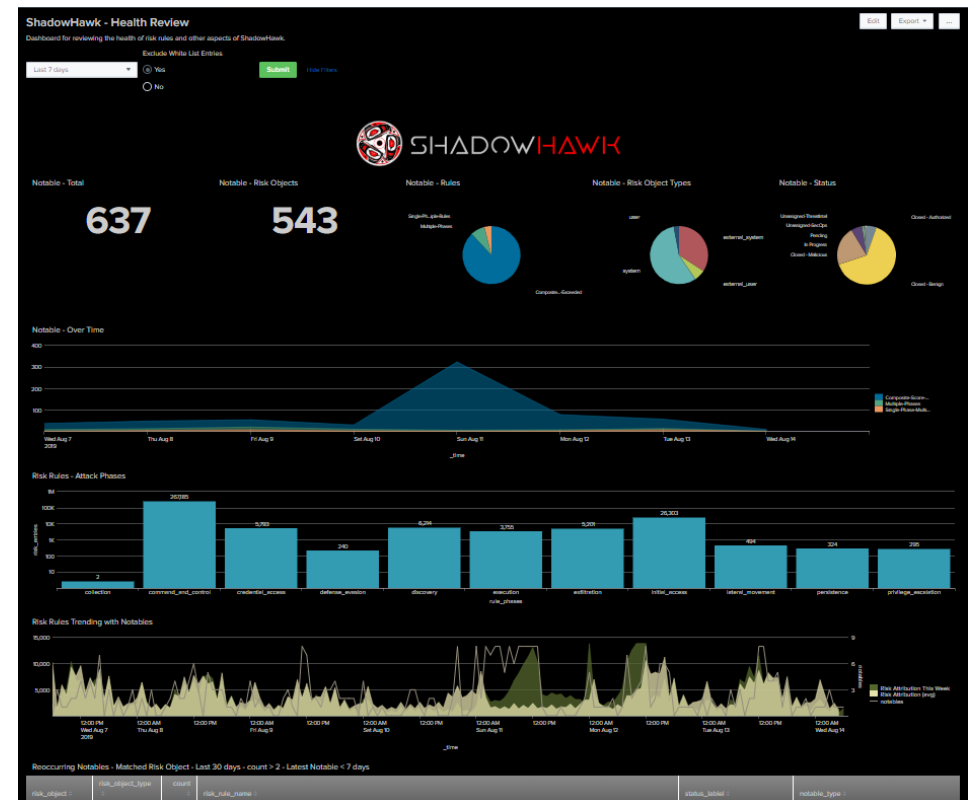
Additions and Removals

Expiration Based

Allows Specification of Requestor

Leverages What's in Enterprise Security

- watchlist=true



The Platform

Health Analysis – Reoccurring Notables

risk_object	risk_object_type	count	risk_rule_name	status_label	notable_type
system		14	1564432561-Unsanctioned SSH - Network Traffic	1564432561-Closed - Benign	1564432561-AFI-RN-Composite-Score-Exceeded
			1564521666-Unsanctioned SSH - Network Traffic WildFire Malware Event - Network Traffic	1564521666-In Progress	1564521666-AFI-RN-Composite-Score-Exceeded
			1564528476-Matched Content - Network - Threat Intelligence	1564528476-Closed - Malicious	1564528476-AFI-RN-Multiple-Phases
			Unsanctioned SSH - Network Traffic	1564608181-In Progress	1564608181-AFI-RN-Composite-Score-Exceeded
			1564608181-Unsanctioned SSH - Network Traffic	1564694770-In Progress	1564694770-AFI-RN-Composite-Score-Exceeded
			1564694770-Unsanctioned SSH - Network Traffic	1564781448-In Progress	1564781448-AFI-RN-Composite-Score-Exceeded
			1564781448-Unsanctioned SSH - Network Traffic	1564794836-Closed - Malicious	1564794836-AFI-RN-Multiple-Phases
			1564794836-Matched Content - Network - Threat Intelligence	1565048135-In Progress	1565048135-AFI-RN-Composite-Score-Exceeded
			Unsanctioned SSH - Network Traffic	1565199334-In Progress	1565199334-AFI-RN-Composite-Score-Exceeded
			1565048135-Unsanctioned SSH - Network Traffic	1565237610-In Progress	1565237610-AFI-RN-Multiple-Phases
			1565199334-Unsanctioned SSH - Network Traffic WildFire Malware Event - Network Traffic	1565285861-In Progress	1565285861-AFI-RN-Composite-Score-Exceeded
			1565237610-Unsanctioned SSH - Network Traffic		
			WildFire Malware Event - Network Traffic		
			1565285861-Unsanctioned SSH - Network Traffic		
1565642336-Matched Content - Network - Threat Intelligence Unsanctioned SSH - Network Traffic					
1565739372-Unsanctioned SSH - Network Traffic					
1565826057-Unsanctioned SSH - Network Traffic					
system		8	1565630461-Suspicious URL Category - Web Traffic Young Domain - Domain Analysis		
			1565716428-Suspicious URL Category - Web Traffic		
			Young Domain - Domain Analysis		
			1565720754-Suspicious URL Category - Web Traffic Young Domain - Domain Analysis		
			1565806405-Suspicious URL Category - Web Traffic		
			Young Domain - Domain Analysis		
			1565807259-Suspicious URL Category - Web Traffic Young Domain - Domain Analysis		
			1565892835-Suspicious URL Category - Web Traffic		
			Young Domain - Domain Analysis		
			1565893855-Suspicious URL Category - Web Traffic Young Domain - Domain Analysis		
1565979242-Suspicious URL Category - Web Traffic					
Young Domain - Domain Analysis					
system		6	1565033149-Suspicious URL Category - Web Traffic		
			1565468743-Suspicious URL Category - Web Traffic		
			1565714082-Matched Content - Network - Threat Intelligence		
			Suspicious URL Category - Web Traffic		
			1565817951-Matched Content - Network - Threat Intelligence Suspicious URL Category - Web Traffic		
1565822078-Matched Content - Network - Threat Intelligence					

```

index=notable
| eval `get_event_id`meval`,rule_id=event_id
| fields - host_*
| tags outputfield=tag
| `mvappend_field(tag,orig_tag)`
| dedup rule_id
| `notable_xref_lookup`
| `get_correlations`
| `get_current_status`
| `get_owner`
| `get_urgency`

| fillnull value="" system user orig_tag
| nomv risk_rule_name
| eval risk_rule_name=_time."-".risk_rule_name
| eval rule_name=_time."-".rule_name
| eval status_label=_time."-".status_label
| stats count, values(risk_rule_name) as risk_rule_name, values(status_label) as status_label, values
  (rule_name) as notable_type, max(_time) as newest_notable by risk_object,risk_object_type
| eval time_range=relative_time(now(),"-7d")
| where count>2 and newest_notable>time_range
| fields - time_range, newest_notable
| sort - count

```

The Platform

Health Analysis – Risk Rule Searches

csearch_name	cron_schedule	schedule_window	dispatch.earliest_time	dispatch.latest_time	alert.suppress	alert.suppress.fields	alert.suppress.period	sparkvisual	avg_entry_count	total_entries	notable_count
Threat - AFI-RR-NonStandardPorts-WebTraffic - Rule	07 * * * *	auto	-1h@h	@h	0				28844	230748	604
Threat - AFI-RR-IntrusionDetection-AllEvents-NetworkTraffic - Rule	10 * * * *	auto	-1h@h	@h	0				1369	10950	99
Threat - AFI-RR-SuspiciousWebCategory-WebTraffic - Rule	23 * * * *	auto	-1h@h	@h	0				751	6011	67
Threat - AFI-RR-MatchedContent-Network-ThreatIntel - Rule	11 * * * *	auto	-1h@h	@h	0				3460	27683	48
Threat - AFI-RR-YoungDomain-DomainAnalysis - Rule	18 */6 * * *	auto	-6h@h	@h	0				396	3165	36
Threat - AFI-RR-HighRiskDomain-Email-DomainAnalysis - Rule	22 */2 * * *	0	-2h@h	@h	0				1206	9648	29
Threat - AFI-RR-Potential-RawIPDNS-Phish-Email - Rule	31 * * * *	auto	-1h@h	@h	0				1337	9360	26
Threat - AFI-RR-LongConnections-NetworkTraffic - Rule	21 */2 * * *	auto	-2h@h	@h	0				1793	14343	21
Threat - AFI-RR-HighConnectionsIngressWeb-NetworkTraffic - Rule	42 */4 * * *	auto	-4h@h	@h	0				280	2243	15
Threat - AFI-RR-Data-Exfil-Removable-Media - Rule	28 */4 * * *	auto	-4h@h	@h	0				82	652	10
Threat - AFI-RR-Malware-TempDirectoryBlock-Endpoint - Rule	36 * * * *	auto	-1h@h	@h	0				21	104	8
Threat - AFI-RR-HighKerberosUsage-DirectoryServices - Rule	27 */1 * * *	0	-4h@h	@h	0				70	563	7
Threat - AFI-RR-MFA-Anomalies-0365 - Rule	9 */2 * * *	auto	-2h@h	@h	0				47	376	7
Threat - AFI-RR-HighConnectionsIngressWeb-AWS - Rule	7 */4 * * *	auto	-4h@h	@h	0				459	3672	6
Threat - AFI-RR-Potential-BlankSubject-Phish-Email - Rule	42 */4 * * *	auto	-4h@h	@h	0				157	786	4

The Platform

Person Of Interest - Watchlist

Additions and Removals

Expiration Based

Allows Specification of Requestor

Leverages What's in Enterprise Security

- watchlist=true

ShadowHawk - Adjust Watchlist Users

Dashboard for updating the users marked on the watch list

UserID:

Requestor: (Dropdown menu: Human Resources, Physical Security, Cyber Security, Corporate Fraud)

Timeframe: (Dropdown)

Mode: Add Remove

Hide Filters

SHADOWHAWK

Today's Entries

Current Entries

added_date	contact	user	requesting_group	expire_date
2019-07-29			Cyber Security	2019-08-12
2019-07-25			Cyber Security	2020-07-25
2019-07-17			Cyber Security	2019-08-17
2019-07-10			Cyber Security	2019-10-10

The Platform

Person Of Interest - Dashboard

Combines Different Views

- Security Alerts
- Risk Rules
- Email
- Web Browsing
- Removable Media

Business Line Self-Service

SHADOW HAWK

----- User Details -----

Risk Details

360 Total Risk **1** Attack Phase Count **1** Risk Modifier Count **3** Risk Rule Count **user** Risk Object Type

Object Details

column #	row #
risk_object	
category	employee
priority	medium
bunit	Information Technology Area
email	
manager	
nick	
object_type	user

Logon Counts: No results found.

Failed Logons: No results found.

Count by VPN Method and Location: No results found.

----- Risk Details -----

Risk Rules Impacted

rule_name #	count #	Attack Phases	count #
High Risk Domain - Email - Domain Analysis	7	initial_access	10
Potential Raw IP DNS Phish - Email	2		

Suspicious URL Category - Email

Security Alerts

Risk Events

#	_time	rule_name #
> 1	8/17/19 4:42:19.000 AM	Suspicious URL Category - Email
> 2	8/17/19 4:42:19.000 AM	Suspicious URL Category - Email
> 3	8/16/19 2:24:40.000 PM	High Risk Domain - Email - Domain Analysis
> 4	8/16/19 1:31:41.000 PM	Potential Raw IP DNS Phish - Email
> 5	8/16/19 1:31:41.000 PM	Potential Raw IP DNS Phish - Email
> 6	8/16/19 1:31:40.000 PM	Potential Raw IP DNS Phish - Email

----- Data Exfil Details -----

Files Written to Removable Media - Over Time

Files Written to Removable Media - By Extension

Files Written to Removable Media - Details

_time #	UserName #	host #	Device_Action #	Filename #	file_extension #	file_size #	DeviceName #	De #
2019-08-09 07:52:44			WRITE-GRANTED	E:\Work\ [redacted] Employment\Agency Manual 2.0\Agency Information\ Table of Contents.docx	docx	13618	USB FLASH DRIVE USB Device, Disk drive, (Standard disk drive)	Ren

The Platform

Culture Necessities

- Environment of Experimentation
- Analysts Need to Analyze
- Impact & Effectiveness > Metrics
- Criticalness of Leadership Support



The New Rules

What Are New Approaches To Risk Rules?

The New Rules

Dynamic Rules and Settings

Malware - All Infections - Endpoint

```

...
| eval rule_impact_default="High"

| eval rule_confidence_default="High"

| eval rule_impact_course=case(action == "allowed", "High", action
== "blocked", "Medium", action == "deferred", "High")

| eval rule_confidence_course=case(action == "allowed", "Medium",
action == "blocked", "High", action == "deferred", "Medium")

| lookup MalwareImpactLookup action signature

| eval rule_impact=coalesce(rule_impact_fine, rule_impact_course,
rule_impact_default)

| eval rule_confidence=coalesce(rule_confidence_fine,
rule_confidence_course, rule_confidence_default)

```

Leveraging **case**, **coalesce** and **lookups** you can make rules more extensible and require fewer of them

action ↕	rule_confidence_fine ↕	rule_impact_fine ↕	signature ↕
allowed	High	Critical	Hacktool*
blocked	High	High	Hacktool*
deferred	High	Critical	Hacktool*
allowed	High	Low	PUA*
blocked	High	Low	PUA*
deferred	High	Low	PUA*
allowed	High	Critical	Heur*
blocked	High	Medium	Heur*

...

Art of Detection - Ideas

The New Rules

SCF118737 - The Art of Detection Using Splunk Enterprise Security

SEC1039 – Detection Technique Deep Dive

Doug Brown

*May need to watch a few times...or 7

The New Rules

Hunting Lab

ShadowHawk - Hunting Lab - Data Model Based


Dashboard for testing threat models based on data models

Target Data Model: Malware X Target Dataset: Malware_Attacks X Primary Field: file_name X

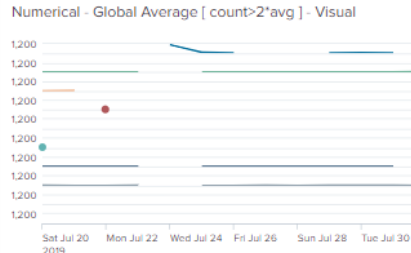
Factor - Averaging: 2 X Factor - Deviation: 2 X Factor - Large Increase: 2 X Factor - Differential: 2 X Last 30 days Submit

filter

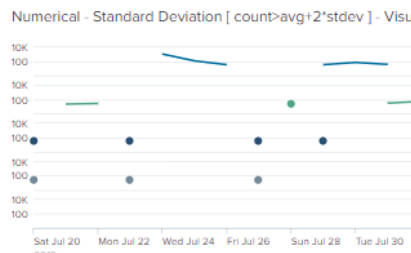
- Malware_Attacks
- __time
- action
- category
- date
- dest
- dest_bunit
- dest_category
- dest_nt_domain
- dest_priority
- dest_requires_av
- file_hash
- file_name
- file_path
- host
- is_Allowed_Malware
- is_Blocked_Malware
- is_Deferred_Malware
- is_not_Allowed_Malware
- is_not_Blocked_Malware
- is_not_Deferred_Malware
- sender



Numerical - Global Average [count>2*avg] - Visual



Numerical - Standard Deviation [count>avg+2*stdev] - Visual



Numerical - Global Average [count>2*avg] - Table

No results found.

Numerical - Standard Deviation [count>avg+2*stdev] - Table

file_name	__time	count	avg	stdev
EFSUpdateLS.exe	2019-07-24	1093	9.74413646055437	36.57186304008252
EFSUpdateLS.exe	2019-07-25	119	9.74413646055437	36.57186304008252

Statistics Driven NOT Signature

Rounds Out Detection Program

Rapid Prototyping

Dynamic To Data Models

The New Rules

Effective Base Searches

Non-Standard Ports - Web Traffic

```
index=web_proxy dest_port!="80" dest_port!="443"
```

Scripting UserAgent Strings – Web Traffic

```
index=web_proxy (http_user_agent="*WinHttp.WinHttpRequest*" OR http_user_agent="*Microsoft-WebDAV-MiniRedir*")
```

Data-Exfil From Snipping Tool – Email

```
index=email_proxy attachment="" sender="*@acme.com" recipient!="*@acme.com" message_subject="*Sent from Snipping Tool*"
```

Potential Phish from Raw IP - Email

```
index=email_proxy | regex email_dns_name="^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?).){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"$"
```

“One more thing...”

Steve Jobs

One More Thing

Alert Modeling Tool

ShadowHawk - Alert Model - Composite Score

Dashboard for modeling composite score scenarios with whitelist and test risk rules. This page utilizes calculations across large datasets so there may be some processing time for the searches.

Time Frame: Exclude White List Entries: Yes No Use Test Rules: No Yes Test Rules:

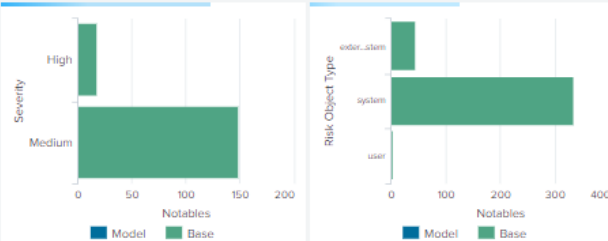


0

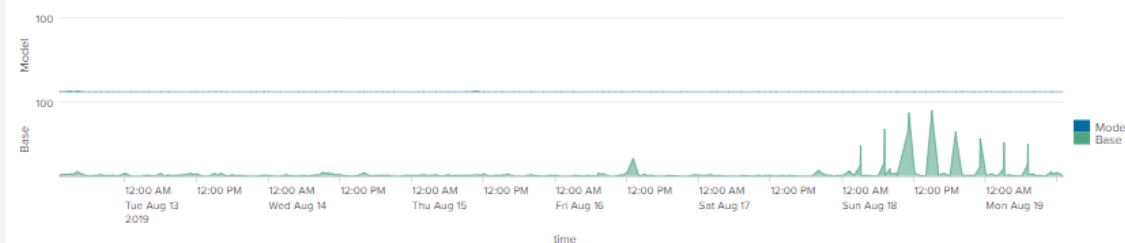
Notable Total

330

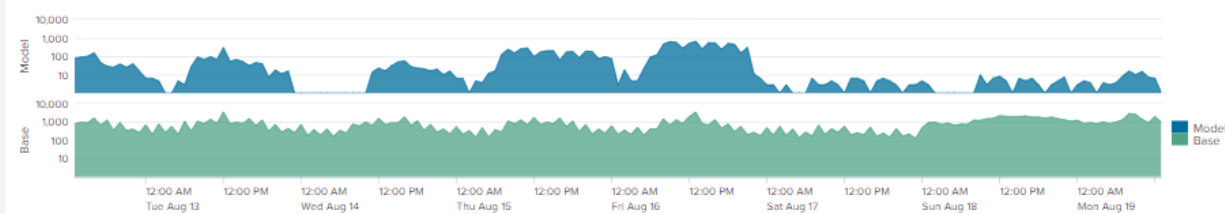
Risk Objects



Notables - Over Time



Risk Attribution - Over Time



- ▶ Simulate Timing And Throttling
- ▶ Models Impact of Test Risk Rules
- ▶ Shows What Notables Would Look Like



Q&A

Stuart McIntosh | Outpost Security

.conf19 – RBA Sessions

SEC1556 - [Building Behavioral Detections: Cross-Correlating Suspicious Activity with the MITRE ATT&CK™ Framework](#)

Tuesday, October 22, 01:45 PM - 02:30 PM

SEC1803 - [Modernize and Mature Your SOC with Risk-Based Alerting](#)

Tuesday, October 22, 03:00 PM - 03:45 PM

SEC1538 - [Getting Started with Risk-Based Alerting and MITRE](#)

Wednesday, October 23, 12:30 PM - 01:15 PM

SEC1908 - [Tales From a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach](#)

Wednesday, October 23, 03:00 PM - 03:45 PM

Birds of a Feather – [RBA Community – Slack Channel](#)

TBD



splunk>

Thank

You!

Go to the .conf19 mobile app to

RATE THIS SESSION

