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.

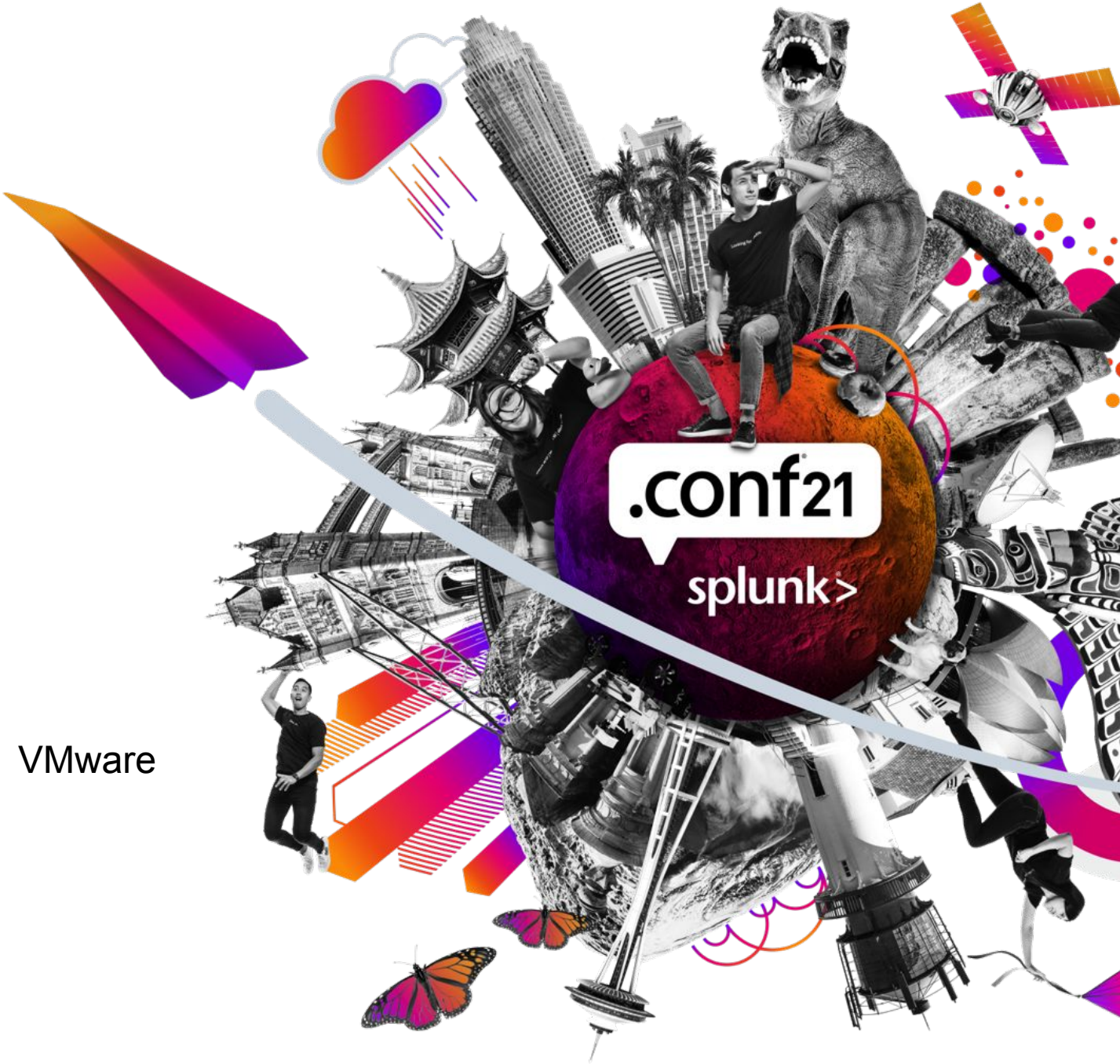
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Proactive Risk Based Alerting for Insider Threats

SEC1163A

Matt Snyder

Program Lead - Advanced Security Analytics | VMware



Matt Snyder

Program Lead - Advanced Security Analytics | VMware

splunk> .conf21

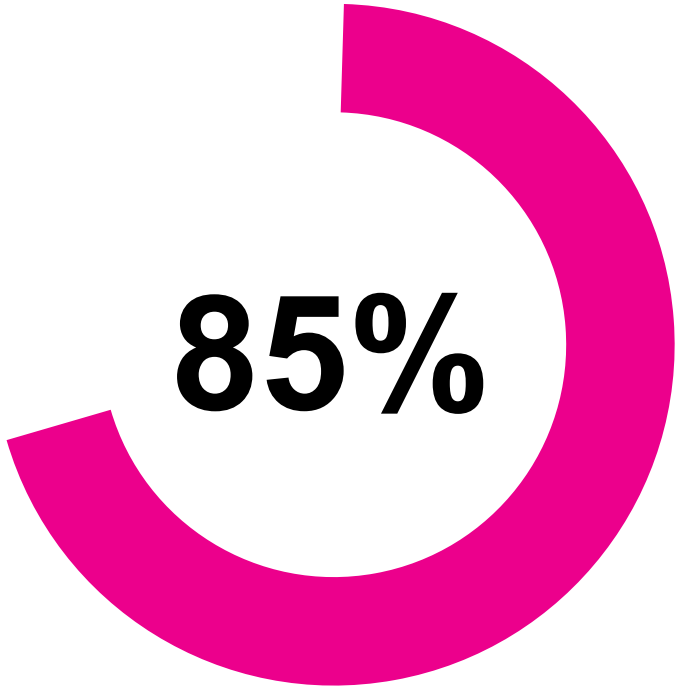
A Little About Me...

- Over the last 16 years I've been responsible for:
  - Investigations
  - System Admin/Support
  - Digital Forensics
  - Incident Response
  - Security Engineering/Consulting
- Been using Splunk since 2013
- This is my 4th in person .conf (Orlando .confs are the BEST!!!!)
- Fun Fact: I collect Koozies (little things for drinks to keep them cold)

Everyone Has an Insider Threat Problem

No matter what industry you are in or the size of your company, you face challenges from Insider Threats.

% of Employees likely to leak data post COVID-19



Source: https://www.code42.com/resources/report-2021-data-exposure/

Remote work has accelerated risks

With workforces around the world shifting to remote/work from anywhere models, employees now have greater access to data than ever before.

Now it’s time to build a team!

splunk> .conf21

You Need Support

Building strong partnerships is key!

Legal

What issues are they concerned with, biggest threats they see.

HR/ER

What are you going to do when you have a case? How do they report a potential issue?

Privacy

What can and can't your program do?

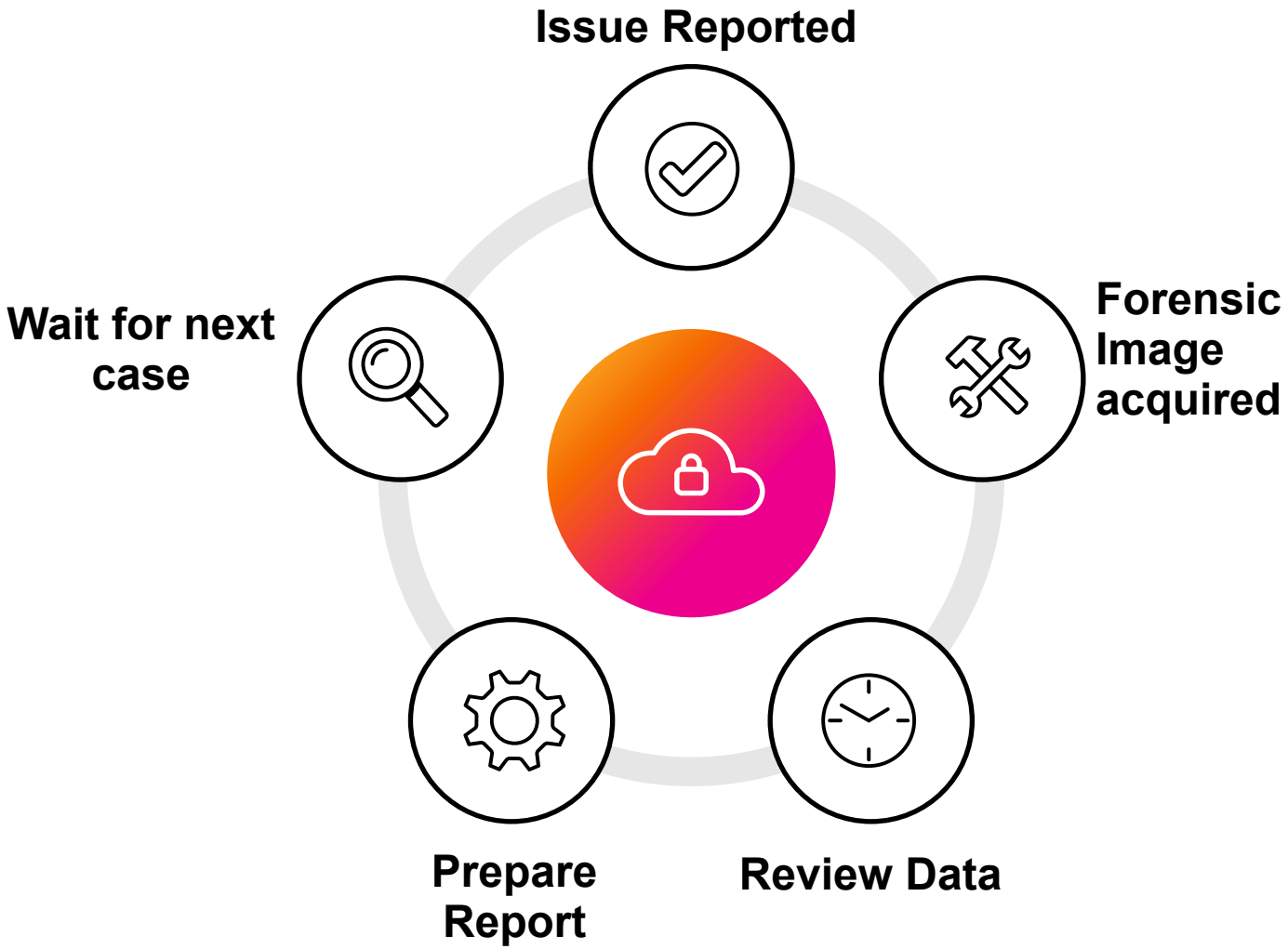
Physical Security

Who are you going to call if things get ugly?

Why Use Splunk For Insider Threats?

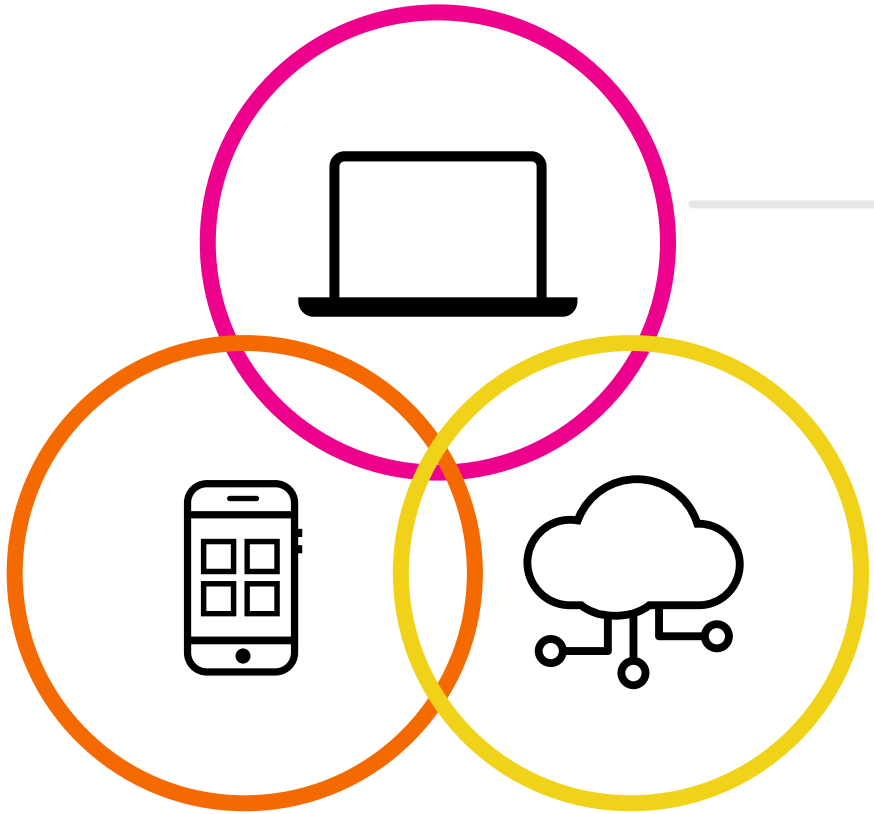
Life Cycle of Investigation

Before Splunk and RBA, the process was slow, time consuming, and reactive!



Enter the Tools!

The Sales Rep promised this product would solve all our problems!!



Endpoint/Agents

Policies will stop bad activity

IDM

Access Control fixes everything!

DLP

Miracle device to detect everything

Too Many False Positives!!!

False Positive

Missed Events

False Positive

False Positive

False Positive

False Positive

Missed Events

We deserve better!

So we are going to build it ourselves....

Using the existing infrastructure in Splunk Enterprise Security, we are going to build better detections.

splunk> .conf21

RBA is simple and elegant...

All organic ingredients with no artificial flavors...

Data

You probably already have the data you need, if not, go get it!

Build Correlation Searches

These will have the Risk Analysis action attached and events will be written to the “risk” index

Create Notable Event Searches

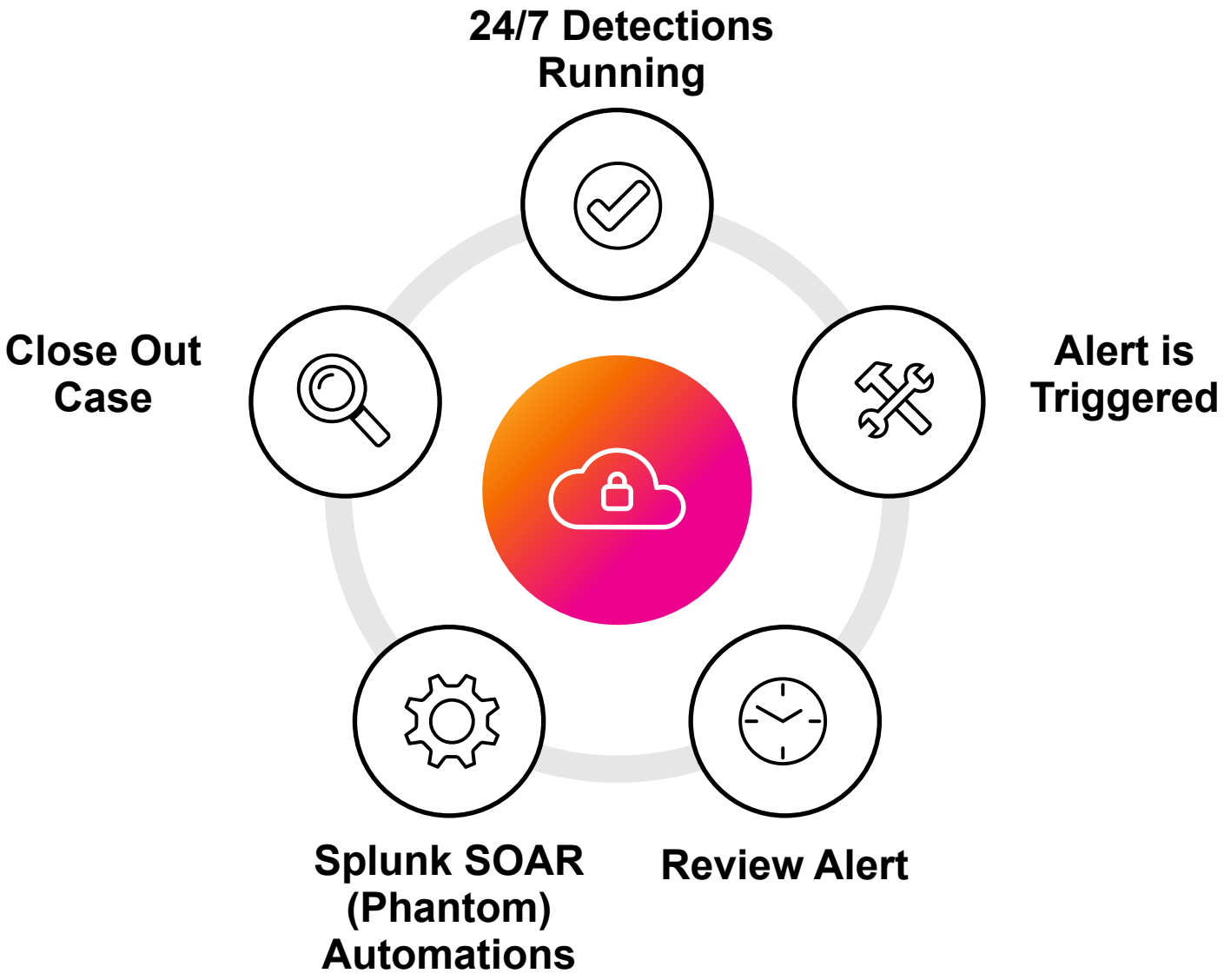
These correlation searches run against the “risk” index or data model and have a Notable Event action attached.

Tune and Repeat

Keep reviewing your detections, make adjustments, then do it again.

Life Cycle of Investigation

With the RBA approach and relevant logs, we can proactively address issues that would never have been discovered, in a way that is scalable and efficient.



Does it work?

Real stats from a real program

Pre Splunk	Pre RBA	RBA	Program Dev	Total Detections
1 Week	1-2 Days	10 Minutes	3 Weeks	52 +
Average time to complete investigation	Average time to complete investigation	Average time to complete investigation	Time to roll out detections and built alerts, all done by 1 person	Number of searches populating Risk index

Where are your Risks?

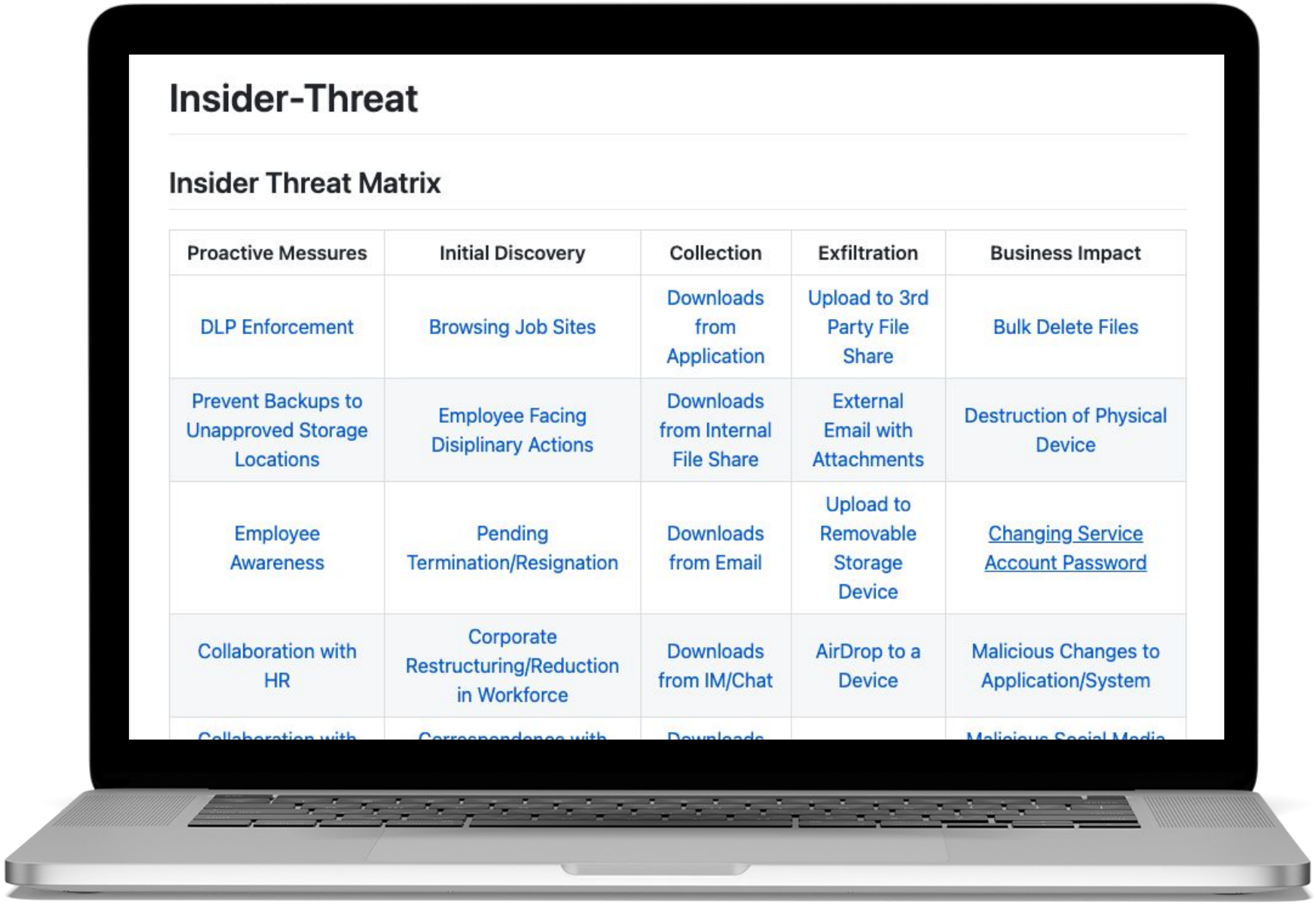
There are 9 Risks in the photo, can you spot them all?

Identify what matters most

Stop hunting blindly

Insider Threats are not singular events, they are like external threat actors, they follow a similar “attack” chain.

Source: https://github.com/Insider-Threat/Insider-Threat



Insider-Threat

Insider Threat Matrix

Proactive Messures	Initial Discovery	Collection	Exfiltration	Business Impact
DLP Enforcement	Browsing Job Sites	Downloads from Application	Upload to 3rd Party File Share	Bulk Delete Files
Prevent Backups to Unapproved Storage Locations	Employee Facing Disiplinary Actions	Downloads from Internal File Share	External Email with Attachments	Destruction of Physical Device
Employee Awareness	Pending Termination/Resignation	Downloads from Email	Upload to Removable Storage Device	Changing Service Account Password
Collaboration with HR	Corporate Restructuring/Reduction in Workforce	Downloads from IM/Chat	AirDrop to a Device	Malicious Changes to Application/System
Collaboration with	Correspondence with	Downloads		Malicious Social Media

Now it’s time to build stuff!!

Calculated Fields

- High Risk File – keyword-based list to help find files that might be sensitive
- SPL:
  - if(match(file, "CONFIDENTIAL, Sensitive, Important_Stuff_In_Here"), "1”, "0")
- Competitors List – keyword based list to help find files related to Competitors
- SPL:
  - if(match(file, ”Other_Company, Not_as_Good, Product_Stinks"), "1”, "0")
- More Info: https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/CreatecalculatedfieldswithSplunkWeb

Lookups

- High Risk User – this is used for users that have been identified as:
  - Behaving suspiciously
  - Part of a reduction in force (RIF)
  - Working on a sensitive project
- Fields:
  Username | Date added | Status - active or not_active | Notes
- SPL:
  index=risk | lookup high_risk_user.csv user as user OUTPUT hru_status notes date_added | search hru_status="active"
- Pro Tip - keep list access to the lookup limited!
- Easy to update with the Lookup Editor app
- More Info:
  https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/Usefieldlookupstoaddinformationtoyourevents

splunk> .conf21

eventstats

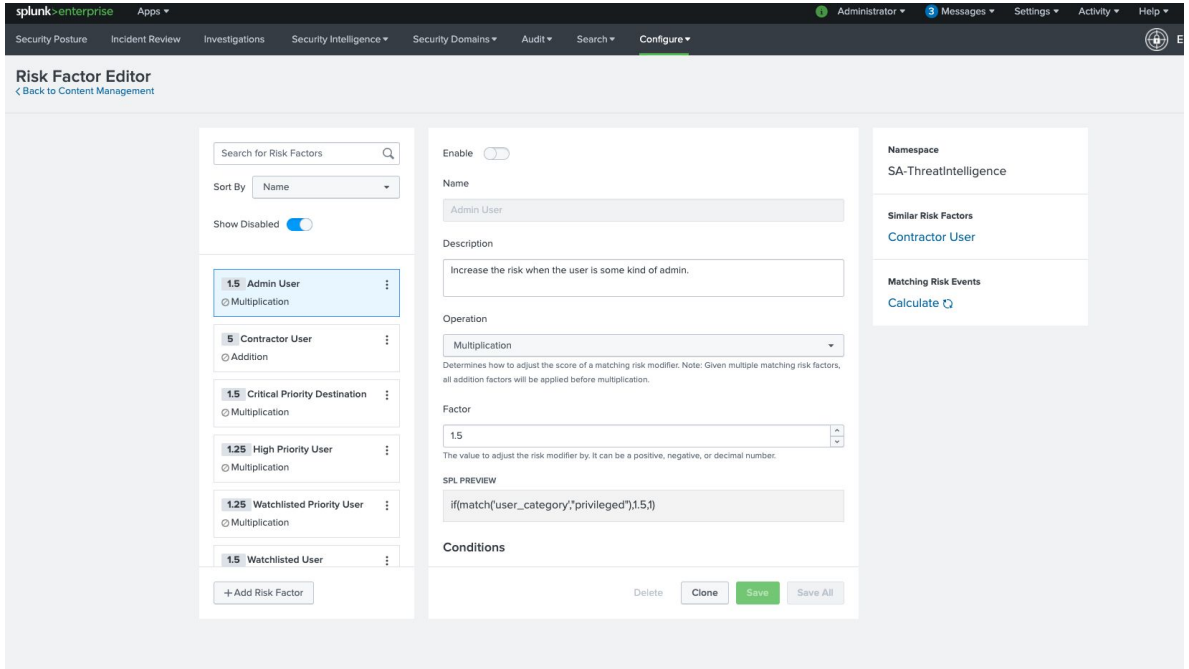
- eventstats - Generates summary statistics from fields in your events and saves those statistics in a new field.
- SPL:
  | eventstats avg(risk_score) as avg_risk stdev(risk_score) as stdev_risk
- Get average risk scores and see how they compare with other users.
- High Risk scores are great but don't always capture everything
- More Info:
  https://docs.splunk.com/Documentation/SplunkCloud/latest/SearchReference/Eventstats

eval

- eval – one of the most powerful Splunk commands.
- SPL:
  | eval risk_score=if(in(user_prop, "CEO", "CFO", "COO", "Executive Vice President"), risk_score+20,risk_score)
  | eval risk_score=if(total_hvf >=1 AND total_hvf <=50, risk_score+10,risk_score)
- Great way to apply dynamic scores based on your needs.
- In ES 6.4, see Risk Factors https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Createriskfactors
- More Info: https://docs.splunk.com/Documentation/SplunkCloud/latest/SearchReference/Eval

Risk Factors

- Great way to apply dynamic scores based on your needs.



- https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Createriskfactors

where

- where – The where command uses eval-expressions to filter search results.
- SPL:
  | where (risk_score>=75 AND total_hvf>=10 AND (tactic_exfil_value >=100 OR tactic_delete_value>=100))
- Awesome way to help set your threshold and filter out noise
- More Info: https://docs.splunk.com/Documentation/Splunk/Latest/SearchReference/Where

splunk> .conf21

Risk Notable - Threshold

- Risk Notable – A correlation search with a Notable Event attached.

```
index=risk

| lookup high_risk_user.csv user as user OUTPUT hru_status notes date_added

| search hru_status=”active”

| eval risk_score=if(in(user_prop, "CEO", "CFO", "COO", "Executive Vice President"),
risk_mod_count+20,risk_score)
| eval risk_score=if(total_hvf >=1 AND total_hvf <=50, risk_mod_count+10,risk_score)
| eval aa_tactic_exfil_value=case(aa_tactic == "Exfiltration", "1", aa_tactic == "Collection", "0",
aa_tech == "Data_Destruction", "0")
| eval aa_tactic_delete_value=case(aa_tactic == "Exfiltration", "0", aa_tactic == "Collection",
"0", aa_tech == "Data_Destruction", "1")

| eventstats avg(risk_score) as avg_risk stdev(risk_score) as stdev_risk

| stats dc(file) as file_count sum(hvf) as total_hvf values( aa_tactic) as aa _tactic
values(aa_tech) as aa_tech by user

| where (risk_score>=75 AND total_hvf>=10 AND (tactic_exfil_value >=100 OR
tactic_delete_value>=100))
```

Risk Notable - Multi Tactic

```
index=risk

| lookup high_risk_user.csv user as user OUTPUT hru_status notes date_added

| search hru_status=”active”

| eval risk_score=if(in(user_prop, "CEO", "CFO", "COO", "Executive Vice President"),
risk_mod_count+20,risk_score)
| eval risk_score=if(total_hvf >=1 AND total_hvf <=50, risk_mod_count+10,risk_score)
| eval aa_tactic_exfil_value=case(aa_tactic == "Exfiltration", "1", aa_tactic == "Collection", "0",
aa_tech == "Data_Destruction", "0")
| eval aa_tactic_delete_value=case(aa_tactic == "Exfiltration", "0", aa_tactic == "Collection",
"0", aa_tech == "Data_Destruction", "1")

| eventstats avg(risk_score) as avg_risk stdev(risk_score) as stdev_risk

| stats dc(file) as file_count sum(hvf) as total_hvf values(aa_tactic) as aa _tactic
values(aa_tech) as aa_tech dc(aa_tactic) as aa_tactic_count dc(aa_tech) as aa_tech_count
by user

| where (aa_tech_count > 2 OR aa_tech_count >3)
```

Risk Notable - Anomaly

```
index=risk
| lookup high_risk_user.csv user as user OUTPUT hru_status notes date_added
| search hru_status=”active”
| eval risk_mod_count=0
| eval risk_score=if(in(user_prop, "CEO", "CFO", "COO", "Executive Vice President"),
risk_mod_count+20,risk_score)
| eval risk_score=if(total_hvf >=1 AND total_hvf <=50, risk_mod_count+10,risk_score)
| eval risk_mod_count=if(like(aa_tech,"Correspondence_with_Competitor"),risk_mod_count+30,risk_mod_count)
| eval risk_mod_count=if(like(aa_tech,"Pending_Resignation"),risk_mod_count+30,risk_mod_count)
| eval risk_mod_count=if(like(aa_tech,"Pending_End_of_Contract"),risk_mod_count+30,risk_mod_count)
| eval risk_mod_count=if(like(aa_tech,"Security_Tool_Alerts"),risk_mod_count+30,risk_mod_count)
| eval risk_mod_count=if(like(aa_tech,"Behavior_Based"),risk_mod_count+30,risk_mod_count)
| streamstats sum(risk_score) as risk_score
dc(file) as total_files
sum(high_value_file) as total_hvf
values(source) as source
dc(source) as source_count
values(aa_tactic) as "aa_tactic"
values(aa_tech) as "aa_tech"
dc(aa_tactic) as  count_aa_tactic
by user
| stats
dc(file) as total_files
sum(high_value_file) as total_hvf
values(source) as source
dc(source) as source_count
values(aa_tactic) as "aa_tactic"
values(aa_tech) as "aa_tech"
dc(aa_tactic) as  count_aa_tactic
max(risk_score) as risk_score
max(avgRisk) as avgRisk
values(stdevRisk) as stdevRisk
by user
| eventstats avg(risk_score) as avg_risk stdev(risk_score) as stdev_risk
| where risk_score>avgRisk+(2*stdevRisk)
```

High Risk User Monitoring

Spot Suspicious Activity

An easy-to-use dashboard to find suspicious activity and take action proactively.

Source: https://github.com/matt-snyder-stuff/.conf_2021/blob/main/Dashboards/High_Risk_Monitoring

splunk> .conf21

Lessons Learned

Get a head start on your program...

You need the business's support.

Alerts/Investigations that aren't actioned mean nothing.

Prioritize and Execute!

Start building things that will save you time first!

Automate the small things.

Grab files that need to be reviewed, generate email to manager, disable USB connections, etc.

RBA is the way!

Your alerts need to be accurate, you don't get second chances when you accuse an employee of wrongdoing.

But wait, there’s more…

How RBA Saved Christmas!

A true story.

splunk> .conf21

Helpful Links

- Insider Threat Matrix: https://github.com/Insider-Threat/Insider-Threat
- Code42 Insider Threat Report: https://www.code42.com/resources/report-2021-data-exposure/
- RBA Deck: https://deck.rbaallday.com/
- Alerts and Dashboards: https://github.com/matt-snyder-stuff/.conf_2021

splunk> .conf21

RBA 2021 .conf Talks

SEC1163A - Proactive Risk Based Alerting for Insider Threats

SEC1162A - Supercharge Your Risk Based Alerting (RBA) Implementation

SEC1249A - Accenture's Journey to RBA with Splunk Enterprise Security and Beyond

SEC1271 - What's New in Splunk Enterprise Security?

SEC1590C - Augmented Case Management With Risk Based Analytics and Splunk SOAR SEC1800A - Implementing Zero Trust: From Hype to Reality

SEC1466A - A Deep-Dive Into How Zoom Is Building Its World-Class Detection Pipeline in Response to the Zoom-Boom!

Thank You

Please provide feedback via the

SESSION SURVEY

splunk> .conf21