Transforming Intel's Security Posture with Innovations in Data Intelligence

Jac Noel
Security Solutions Architect | Intel Corporation

splunk> .conf19

Transforming Intel's Security Posture with Innovations in Data Intelligence

Aubrey Sharwarko
Security Data Scientist | Intel Corporation

Jerome Swanson
Security Data Scientist | Intel Corporation

splunk> .conf19

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.

Notices and Disclaimers

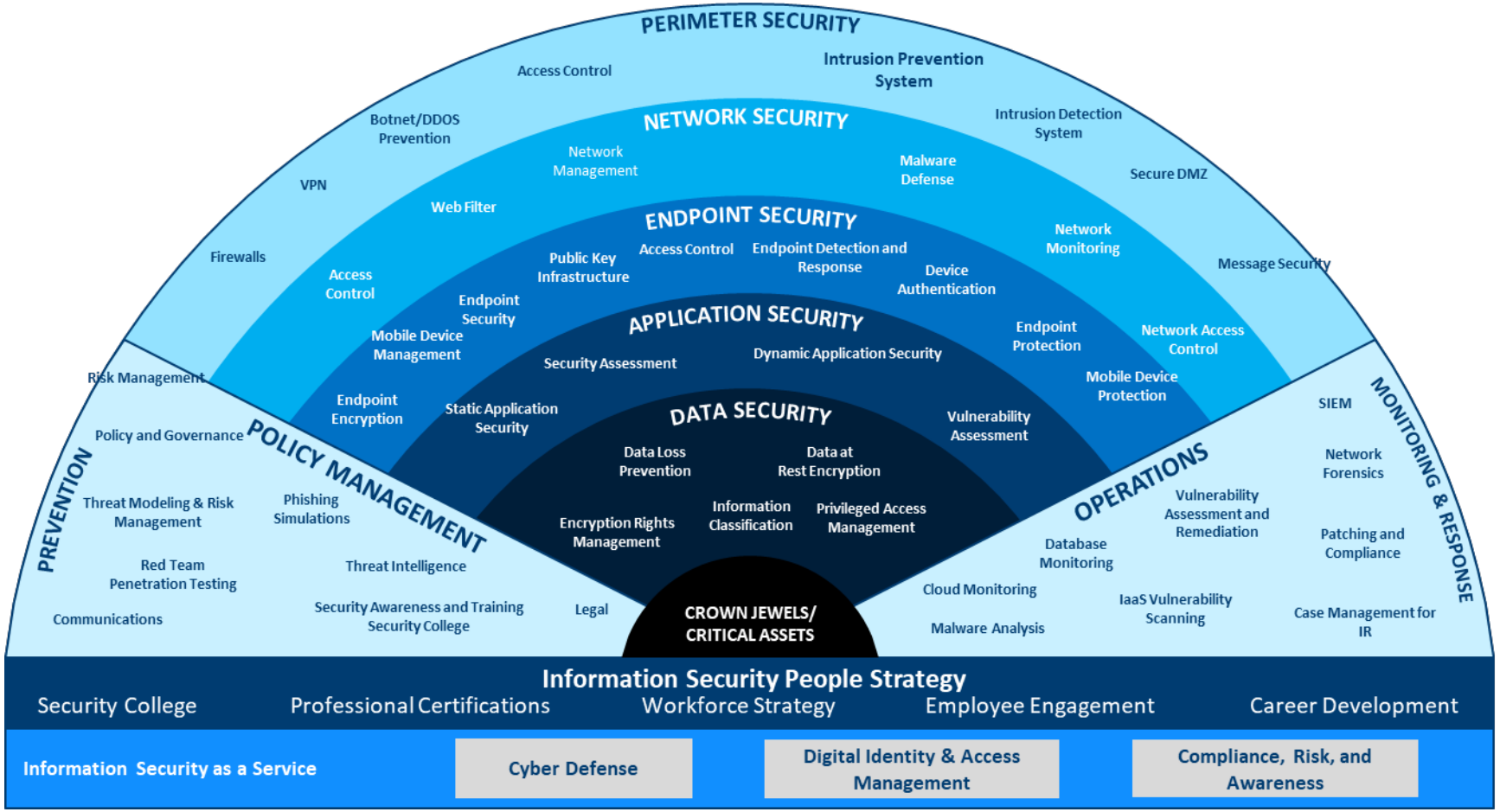
This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

For more complete information about performance and benchmark results, visit www.intel.com/benchmarks

Intel's Defense in Depth Strategy

Provides prevention, detection, and response to 99% of threats

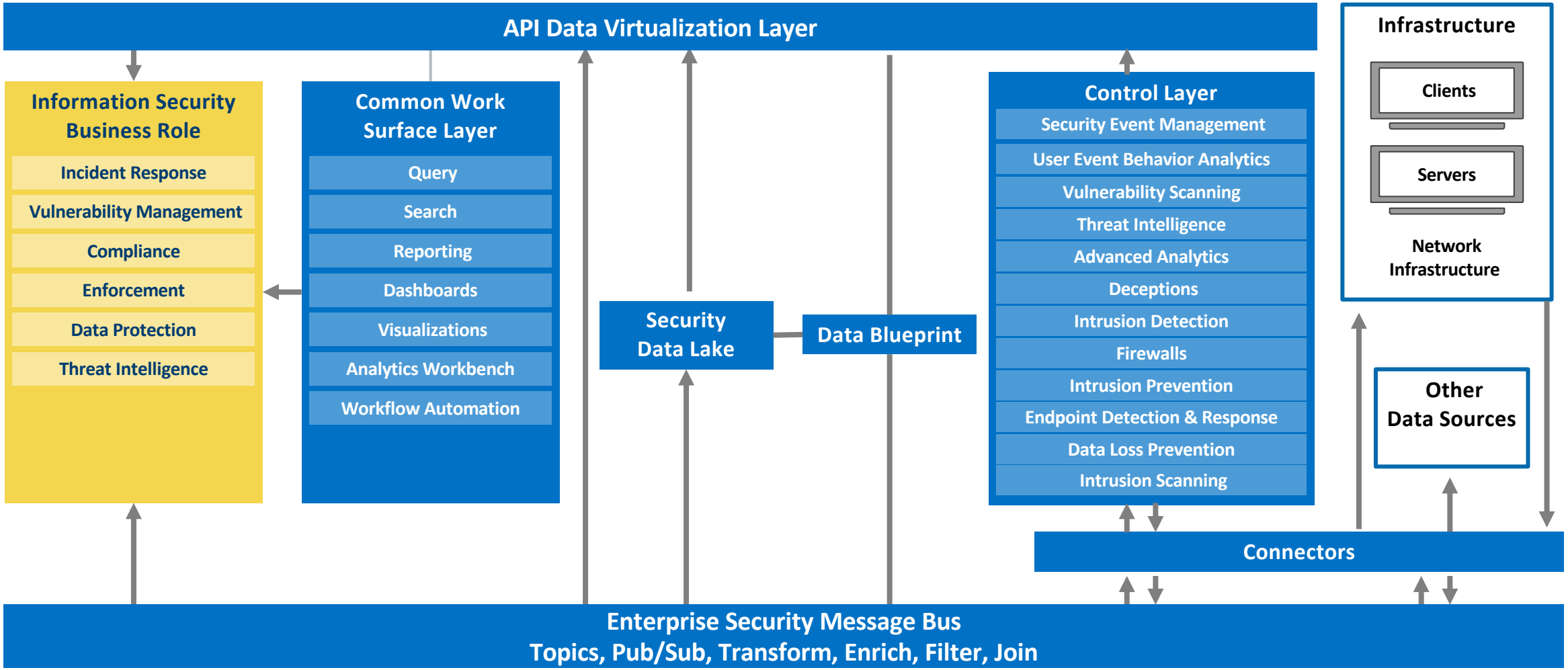
- Our defense in depth model is supported by a vast array of tools and capabilities.
- But advanced cyber security threats continue to grow in frequency and sophistication.



splunk> .conf19

Reference Architecture

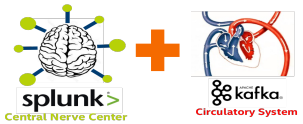
A platform that supports the entire organization

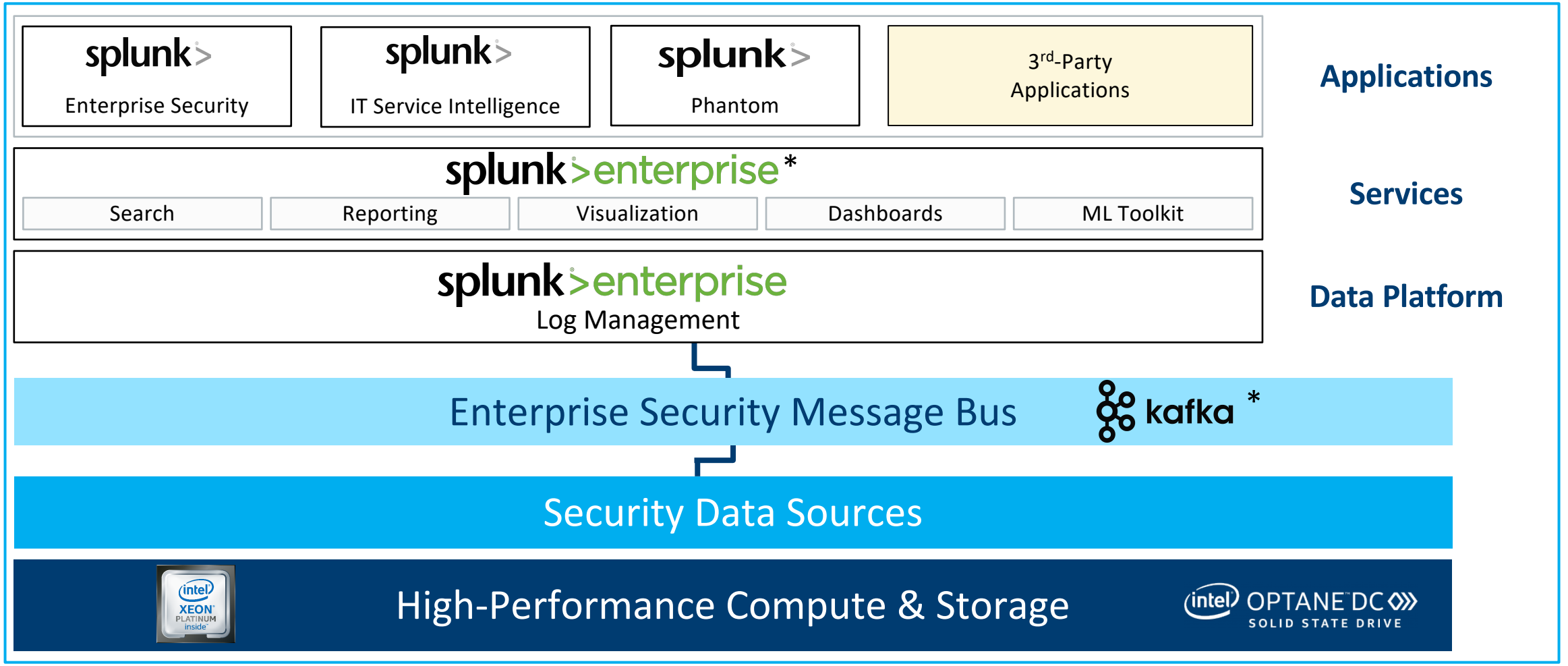


splunk> .conf19

Cyber Intelligence Platform Architecture

Focus on identifying and responding to sophisticated adversaries





*Other names and brands may be claimed as the property of others.

Information Security's Cyber Intelligence Platform

Transforming how Information Security works with a data advantage

A context-rich data platform

Built with industry-leading technologies

Reducing risk to intel's brand

Benefits to Intel

Easy Implementation and Fast Ramp of Human Talent

A Common Work Surface Across All of InfoSec

Data Taxonomy Common Language & Search on the Fly

Key Cyber Terrain InfoSec Org is DevOps Ready

Schema on Demand with Automated Data Normalization

Complete Threat Categorization and Kill Chain Visibility

Simple Integration of Curated Third-Party Security Tools

Connection to Open Source Machine Learning Libraries

*Other names and brands may be claimed as the property of others.

Practical Example: Machine Learning for E-Mail Phishing Analysis

Aubrey Sharwarko

splunk> .conf19

Machine Learning for Email Phishing Analysis

InfoSec analyst's report:

- "Email as a threat vector is the #1 cause of all breaches"
- "Top entry point for threat actors into your environment"
- "Suspected phish is reported to our SOC every 5 min"
- "Single largest resource drain on our teams"

* Verizon 2019 Data Breach Investigation Report

2018 FIFA WORLD CUP
RUSSIA -YOU WON LOTTO!

FIFA WORLD CUP
RUSSIA 2018

Dear Lucky Winner,

We Russia 2018 FIFA World Cup Organizing Committee (RFWCOC) in conjunction with Microsoft–Euro Online lottery Award team officially announce to you the raffle draw held the Month JANUARY 2018 in LONDON, UNITED KINGDOM. Your E-mail address was among the 500,000.00 e-mail raffle draw, which your e-mail was randomly picked up by the computer during the 3rd Quarter Raffle draws held in United Kingdom.

We therefore wish to inform you that your e-mail address has won you the total sum of **(£1,000,000,000.00)** One Million Great Britain Pounds Sterling. Participant's email addresses were sorted out globally (Powered by Microsoft) from Companies, Individuals, Government's Agencies, Co-operate bodies, Charity homes etc and computed "RANDOMLY" Via E-sorting balloting to select respective winners around the globe.

Be inform that this Internet Raffle Draw (IRD)was organized by Microsoft –Euro lottery Award team and Russia 2018 FIFA World Cup Organizing Committee (RFWCOC) to create awareness to the world as Russia is busy Finalizing their preparation for the hosting of the 2018 FIFA World Cup. Note: Winners shall be paid in accordance with his/her Settlement Centre and must be claimed not later than 30 Days from the date of draw notification, any Prize not claimed within this period will be forfeited.

Stated below are your winning Details:
WINNING NUMBER: 20, 14, 30,45,18,50
REFERENCE NUMBER: REF2018/44.B2.
SECURITY CODE: BUK/4490.

Please note that your winning numbers falls within our Afro Booklet representative office in South Africa therefore, your fund will be released to you through our paying bank in " SOUTH AFRICA" Kindly contact fund processing Manager **Mr. Alex**

CONTACT DETAILS
Contact Person: **Mr. Alex**
E-mail: @yahoo.com
Phone: +277

SCAM

You're requested to send the following information's to **Mr. Alex**, to enable him facilitate the release of your winning fund to you. Also remember to place this security code **"BUK/4490"** on your subject for easy location of your file.

1. Full Name:
2. Residential Address:
3. Country:
4. Mobile /Fax number:
5. Occupation:
6. Age:
7. Male/Female:
8. Marital Status:
9. Attached Copy of International passport:
10. Winning Numbers:

Regards,

Mrs. Michelle

(FIFA 2018 Microsoft Online Lottery Coordinator)

APPROVED

Difficult to Extract Insights

Time Intensive

Subjective Results

splunk> .conf19

Email Phishing Classifier: A Recipe for Success

Ingredients

- MLTK
- NLP Text Analytics
- Wordcloud Custom Visualization
- Parallel Coordinates Custom Visualization
- Force Directed App For Splunk
- Halo - Custom Visualization
- Sankey Diagram - Custom Visualization

Algorithms

- Linear SVC
- ExtraTrees
- Nearest Neighbor

Accuracy, Precision, & Recall

Classification	Results
False Positive	Bad
True Positive	Excellent!!
False Negative	Very Bad!

SPL Used

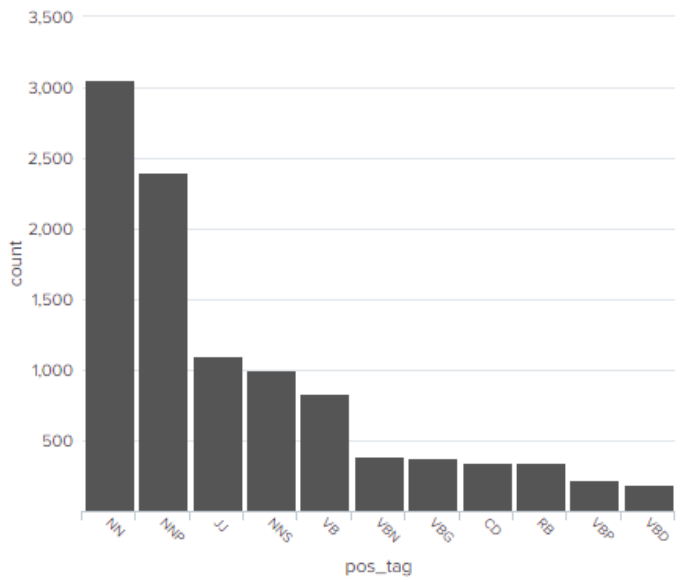
```
index=email sourcetype=suspicious_msg | table Body, Response | cleantext textfield=Body base_type=lemma_pos mv=f custom_stopwords="xxxx, xxxxs"| fields Response Body
| sample partitions=10 seed=2222 | search partition_number > 7 | apply nlp_tfidf_model | fields Response Body_tfidf* | apply nlp_mms | fields - MMS_Response* Body*
| apply nn AS prediction
```

Dashboard: Phishing Emails Example Results

Total # Terms	Total # Unique Terms	Total # Body	Avg Terms Per Body
10,529	2,765	120	87.7

Total # ngrams	Total # Unique ngrams
10,413	6,158

Top Parts-of-Speech Tags (+)



Top Terms (+)

term	count
account	97
email	94
message	93
please	69
plant	63
information	60
may	52
work	52
use	48
package	46

« prev 1 2 next »

Top ngrams (+)

ngrams	count
verify account	27
term condition	25
american express	17
first advantage	15
receive email	15
make following	13
medical coding	13
accord term	12
account access	12
account detail	12

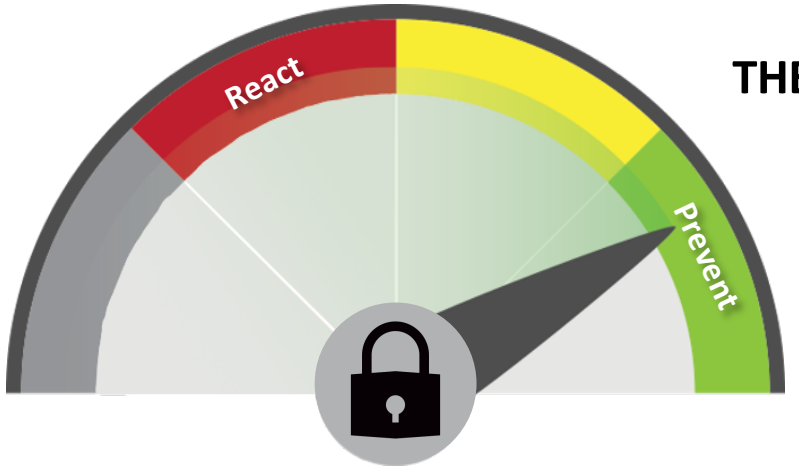
« prev 1 2 next »

3m ago

splunk> .conf19

No Matter the Progress, Security Never Sleeps

Hunting the 1% -
More Sophisticated Threats



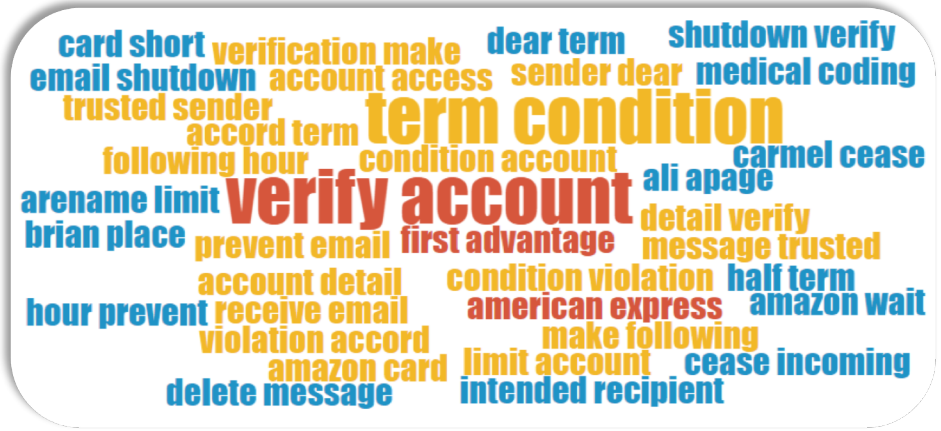
SHIFT THE NEEDLE

Security Incidents

Classification Report On Data Not Seen

See how well the model performs on new data

class	accuracy
Weighted Average	0.98



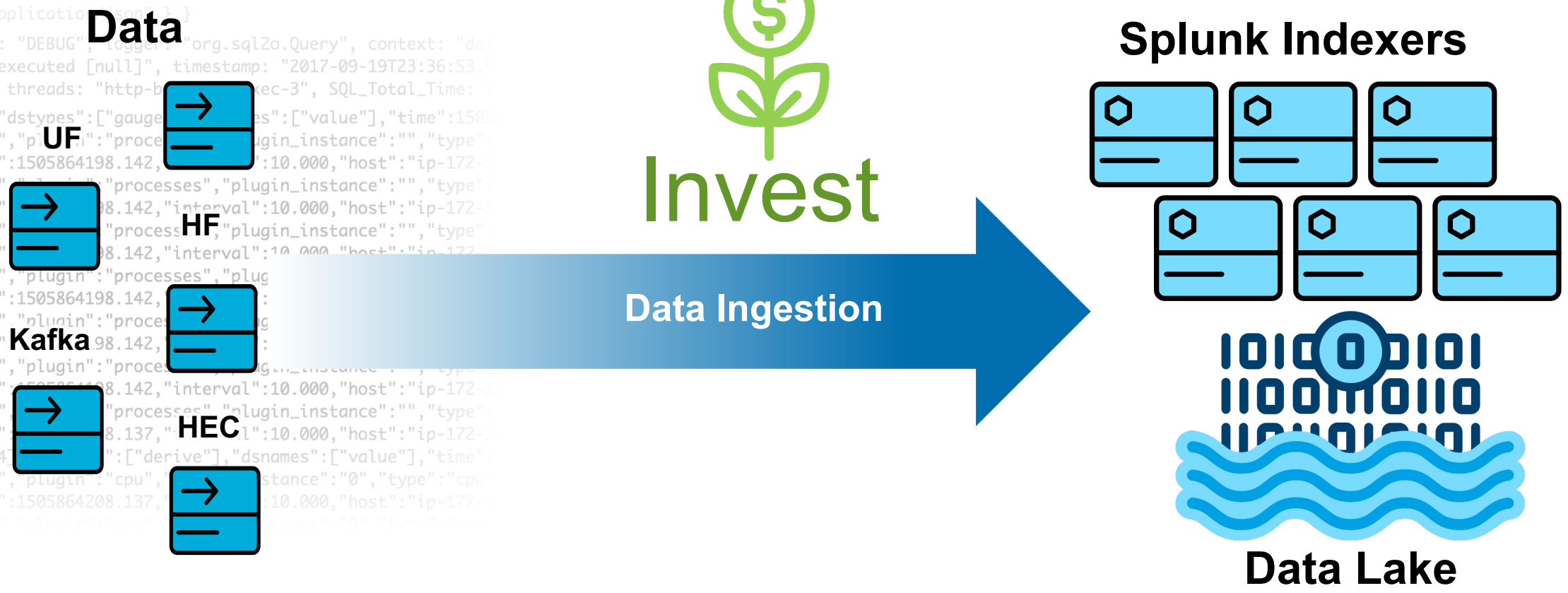
Practical Example: Cybersecurity Data Insights

Jerome Swanson

splunk> .conf19

Data Investment

Indexed Data is a Corporate Asset

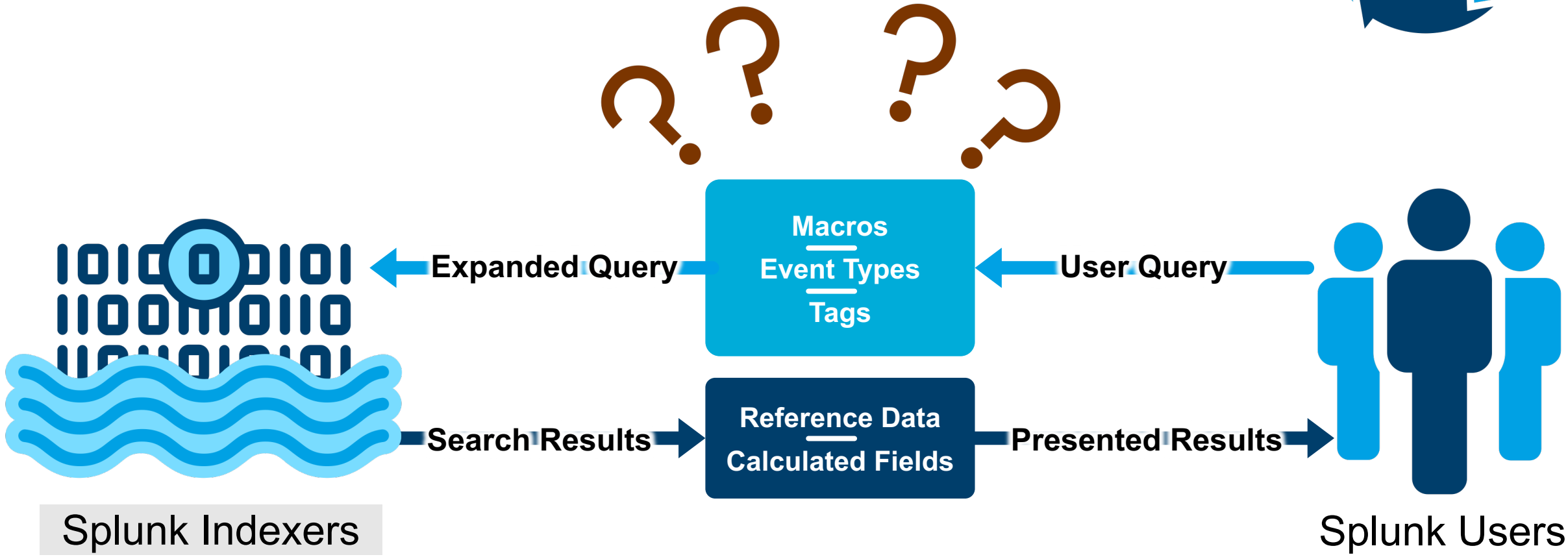


Measure Data Usage

Search Utilization is a Quantifiable Measure of ROI

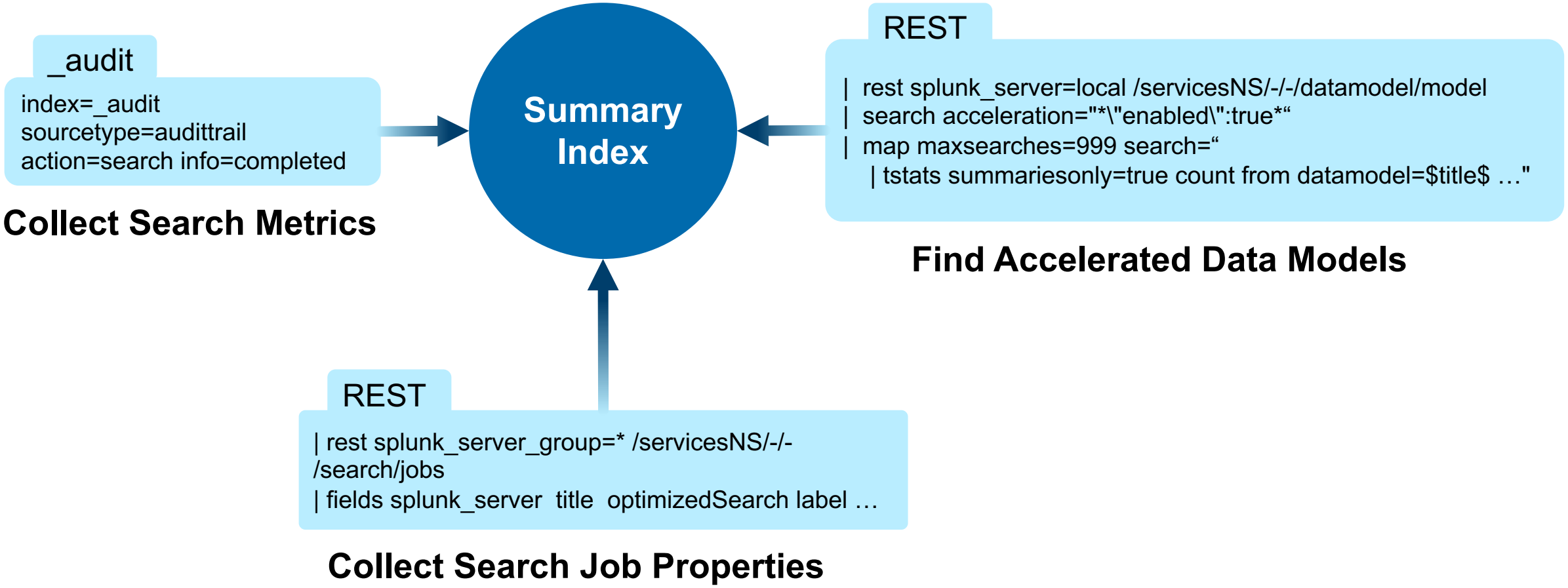
Calculate ROI

Search Utilization is a Quantifiable Measure of ROI



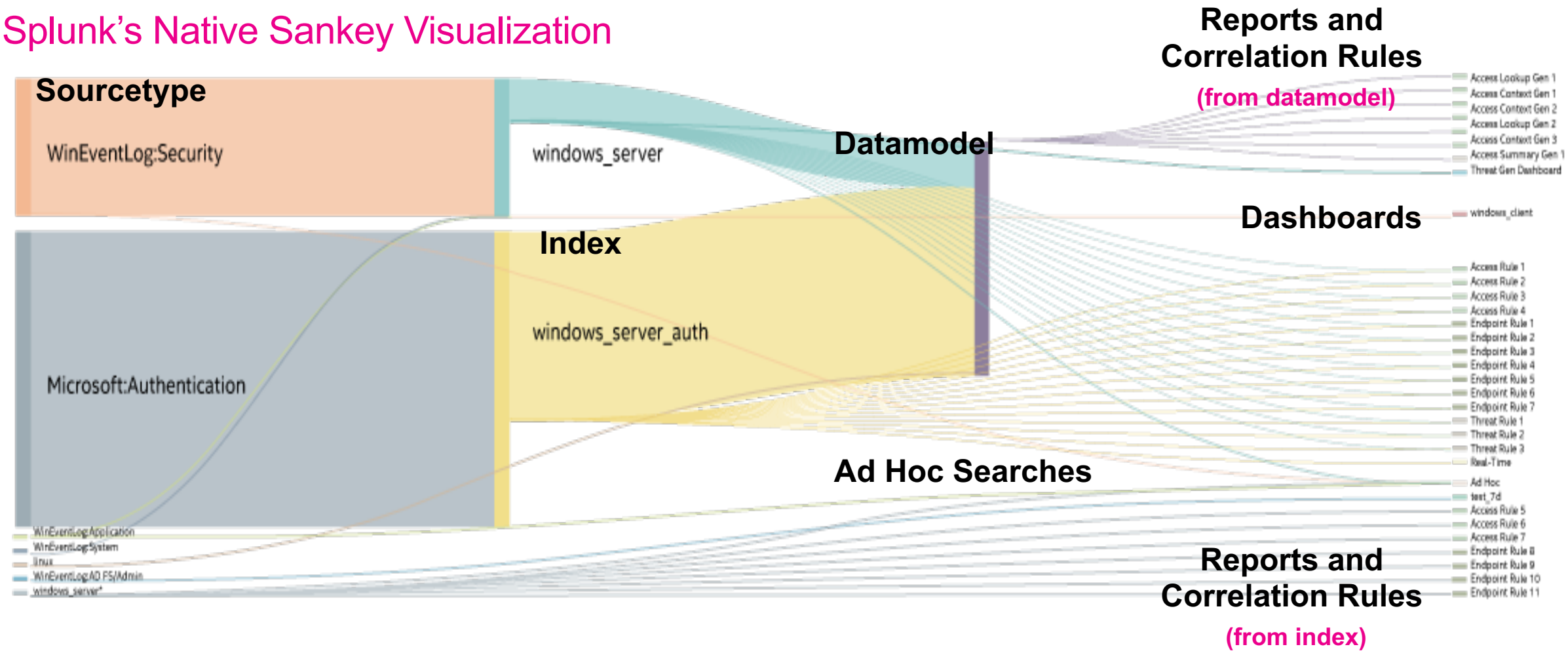
Solving with Splunk

A combination of _audit data and REST calls



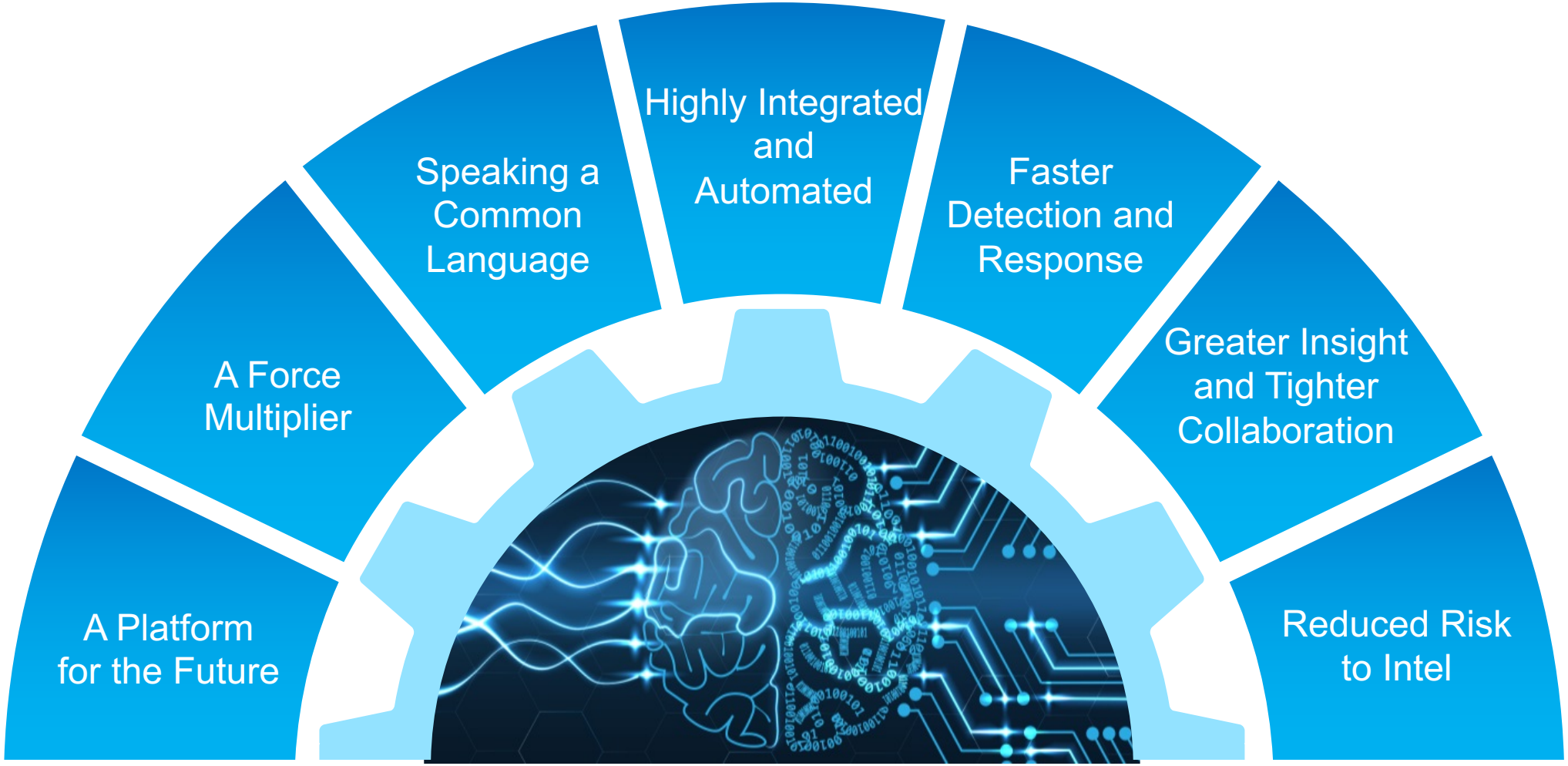
The Result

Splunk's Native Sankey Visualization



People + Technology + Data

Transforming How Information Security Works



IT@INTEL: Sharing Intel IT Best Practices with the World

Learn more about Intel IT's initiatives at: www.intel.com/IT

splunk> .conf19

Q&A

splunk> .conf19

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION