RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-T07

MODEL-DRIVEN SECURITY: IT'S CLOSER THAN YOU THINK

Jim Routh

CSO
Aetna
@jmrouth1

Session objectives

1

Share some examples of model-driven security

2

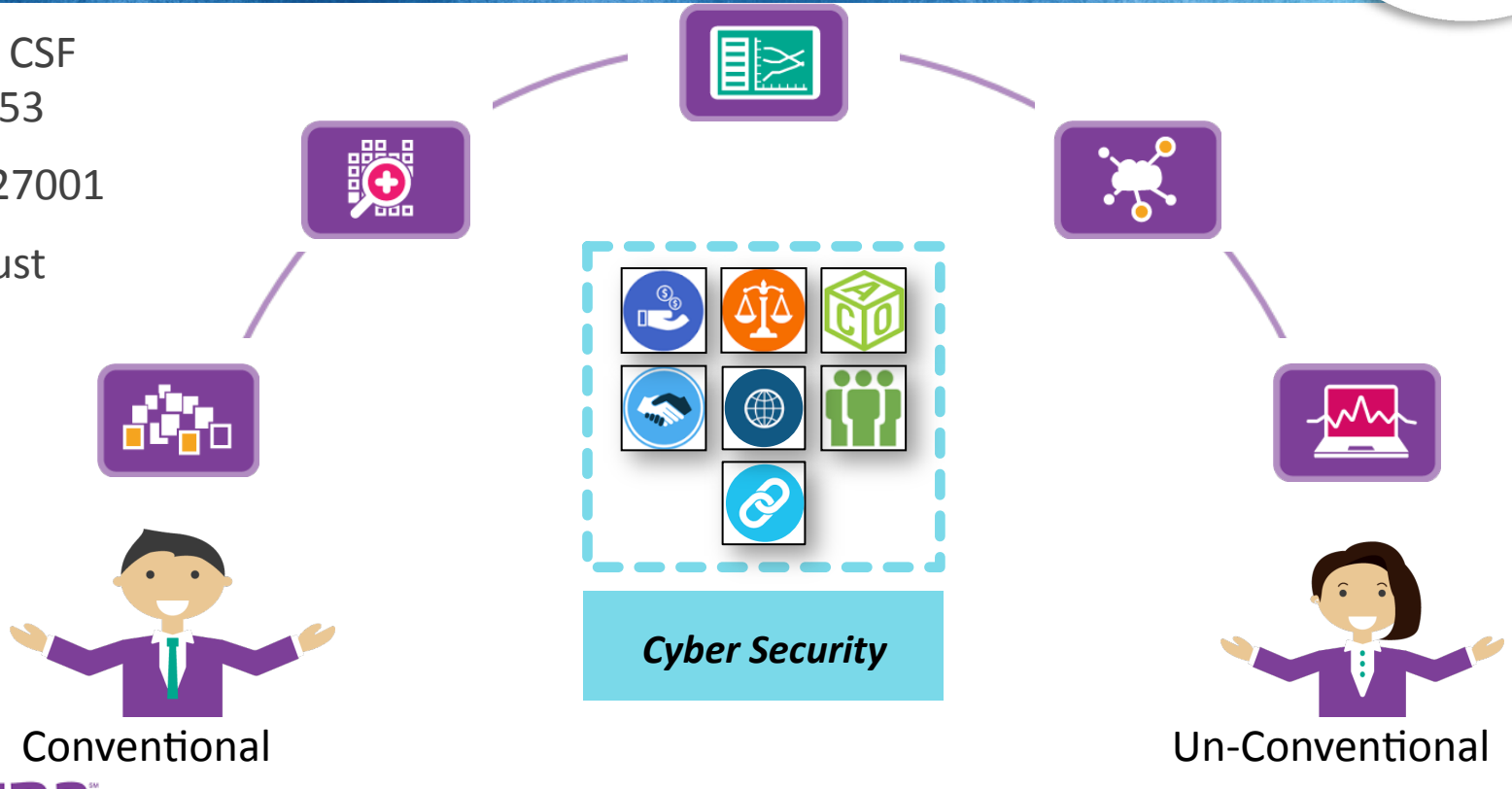
Introduce you to the world of unconventional controls

3

Identify talent development challenges

Evolution from conventional to unconventional controls

- NIST CSF 800-53
- ISO 27001
- HiTrust



The #1 Threat Vector today

#1 CYBER THREAT VECTOR

CONVENTIONAL CONTROL

UN-CONVENTIONAL CONTROL EVOLVING TO CONVENTIONAL

This is the reason that **phishing**, spear-**phishing**, and whaling attacks are directed against individuals. ... Almost all national and industry **phishing** laws and **regulations** include a stipulation that businesses and organizations must create, implement, and maintain a **security awareness training program.**

http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-laws-regulations

NIST SP 800-177
SEPTEMBER, 2016

Domain based Message Authentication, Reporting and Conformance **(DMARC)** was conceived to allow email senders to specify policy on how their mail should be handled, the types of security reports that receivers can send back, and the frequency those reports should be sent. Standardized handling of SPF and DKIM removes guesswork about whether a given message is authentic, benefitting receivers by allowing more certainty in quarantining and rejecting unauthorized mail.

Different tactics require different controls

Sender

Impostor

Spoof

Look-Alike Domain

Display Name Deception

Authentic

Compromised Account

Account Owner

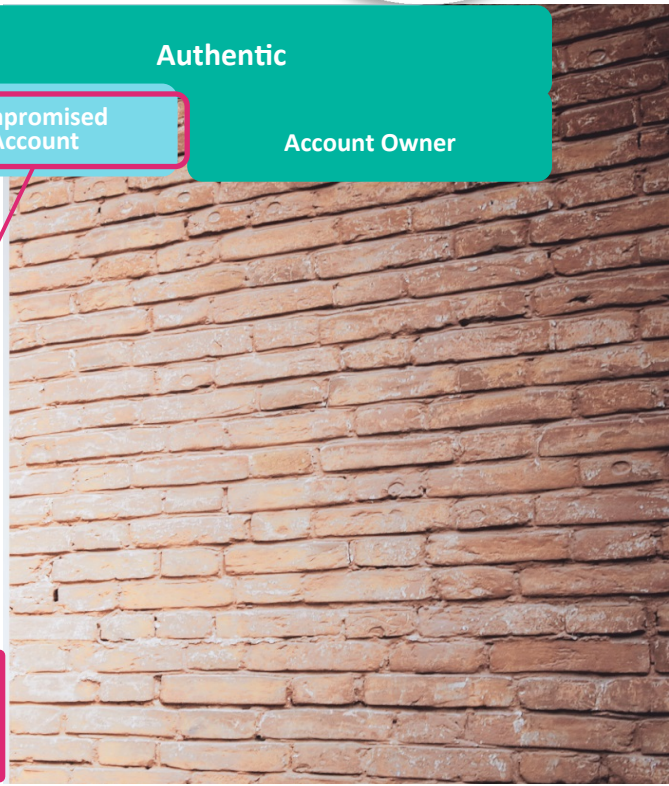
DMARC

Sinkhole newly registered domains

Apply domain attributes to inbound filters

Brand protection services

End user education TBD

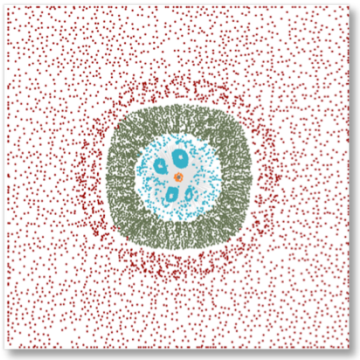


Inbound email protection- Domain Attributes

Using email traffic data, the system learns the **unique fingerprint** of all email senders into your enterprise

29,231 servers sent email for an enterprise on a single day

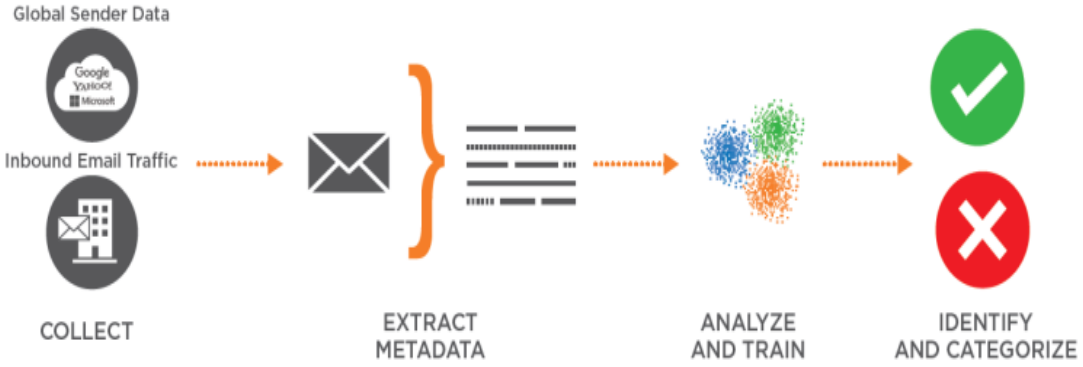
This durable **identity trust model** is used to stop all messages that do not prove they should be trusted



312 servers for the enterprise
4,641 servers owned by service providers
9,732 benign email forwarders
14,526 malicious senders

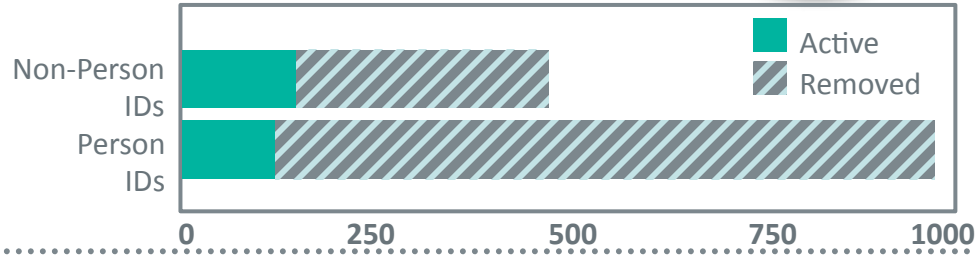
Enabled by models

Comparing Aetna in-bound email and correlating it with billions of emails every day from the largest email providers using machine learning models applied in real time enables filtering of email based on sending domain attributes to divide the mail stream into trusted and untrusted streams.

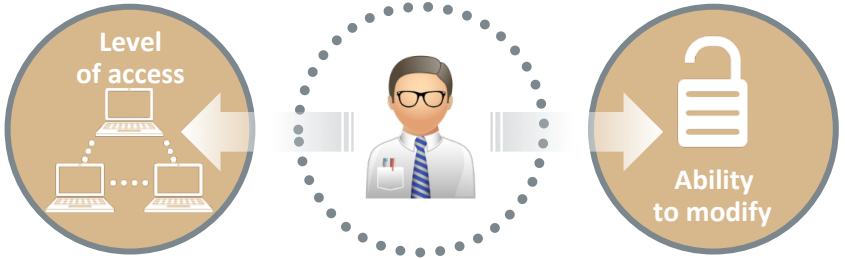


Privilege user & activity management activity

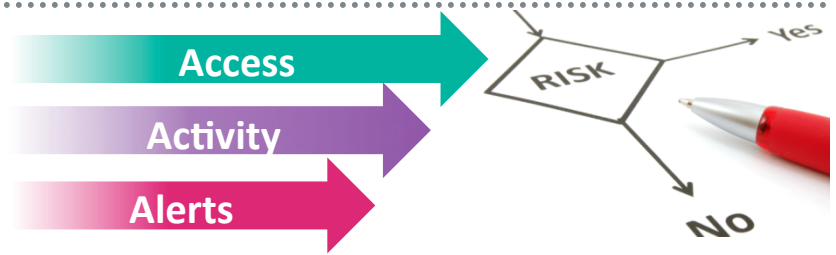
1 Reduce the number of privilege users



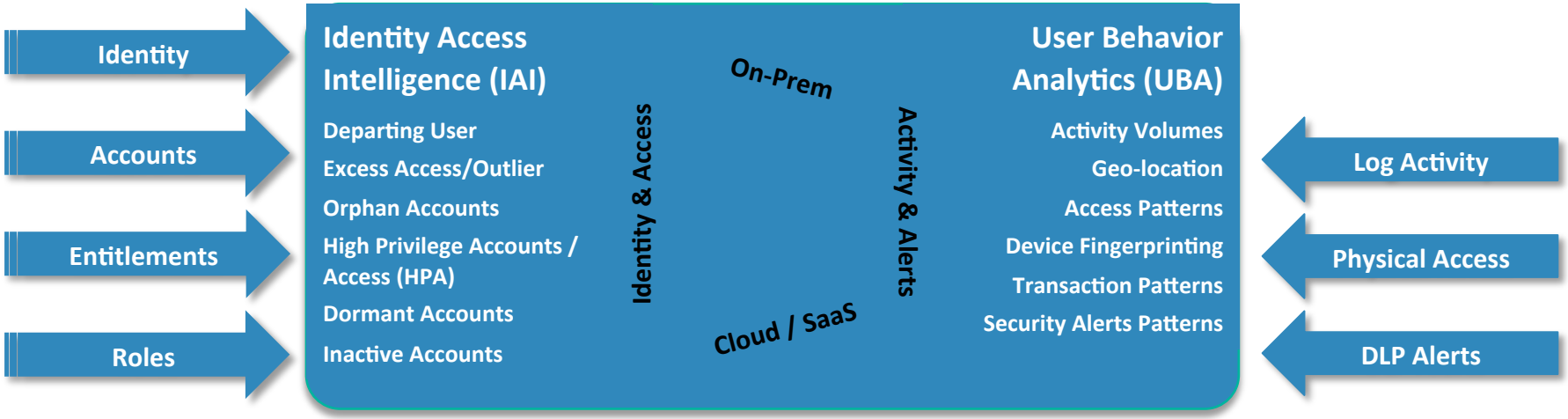
2 Provide context to monitoring and change admin tool choice



3 Implement data analytic techniques to determine behavioral patterns



Behavioral analysis is the cornerstone



Example of an event email

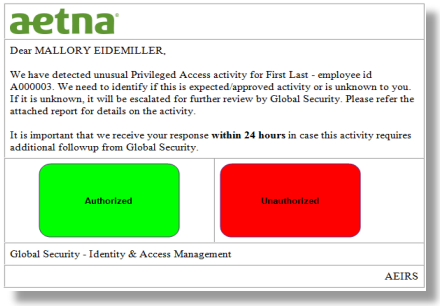
Privileged Access Management (PAM)

Implement and consolidate access monitoring, alerting, and response utilizing all available access and identity data (policy and event) to identify anomalies:

- Provide clear understanding of privileged access
- Ensure appropriate access is not being misused
- Target investigations & follow up

Event email is sent:

- When unusual activity is detected within a 24-hour period
- To the employee's manager
- And contains attachment of Anomalous Activity Report


aetna

Dear MALLORY EIDEMILLER,

We have detected unusual Privileged Access activity for First Last - employee id A000003. We need to identify if this is expected/approved activity or is unknown to you. If it is unknown, it will be escalated for further review by Global Security. Please refer the attached report for details on the activity.

It is important that we receive your response **within 24 hours** in case this activity requires additional followup from Global Security.

Authorized

Unauthorized

Global Security - Identity & Access Management

AEIRS

This results in a substantial 'false-positive' reduction, as well as an increased business awareness of privileged access.

Over 3 billion user IDs and passwords were stolen in 2016

Source: Shape Security

Criminals use credentials for account takeover

40%

In 2016, data breaches increased by

3 Billion

In one breach- Yahoo 2013

51%

of consumers suffered some kind of security incident in 2016, including a stolen password or breached account

81%

of hacking related breaches leveraged stolen or weak passwords

Sources: 2017 Verizon DBIR Report; Identity Theft Resource Center (ITRC) and CyberScout

The trouble with passwords…

Most people use less than 5 passwords for all accounts

50%

of those **haven't changed** their password in the last **5 years**

Reuse makes them easy to compromise

39%

of adults use the **same password** for many of their online accounts

They are difficult to remember

25%

of adults admit to using less secure passwords, because they are **easier** to **remember**

Sources: Pew research; Telesign research

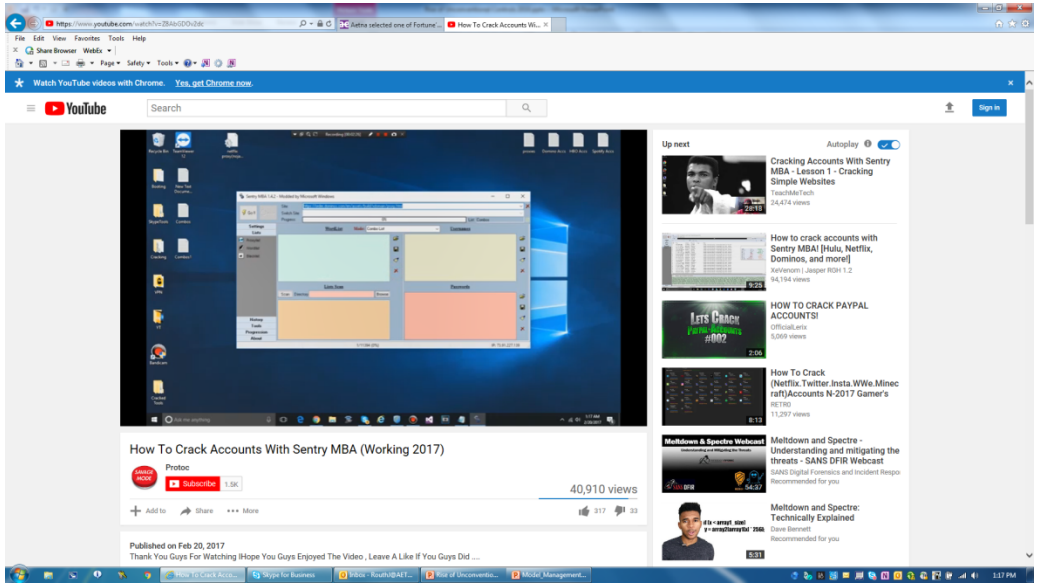
If I were a criminal…

I would use **Sentry MBA** for credential stuffing. I'd take log in credentials and try them on different domains. I'd get a 2% hit, meaning 2% of the credentials I use will give me control of the account.

I can get a 4% return by using the domain name in front of the password.

10,000 credentials = 200 or 400 accounts that I own.

https://www.youtube.com/watch?v=Z8AbGDOv2dc



https://sentry.mba/

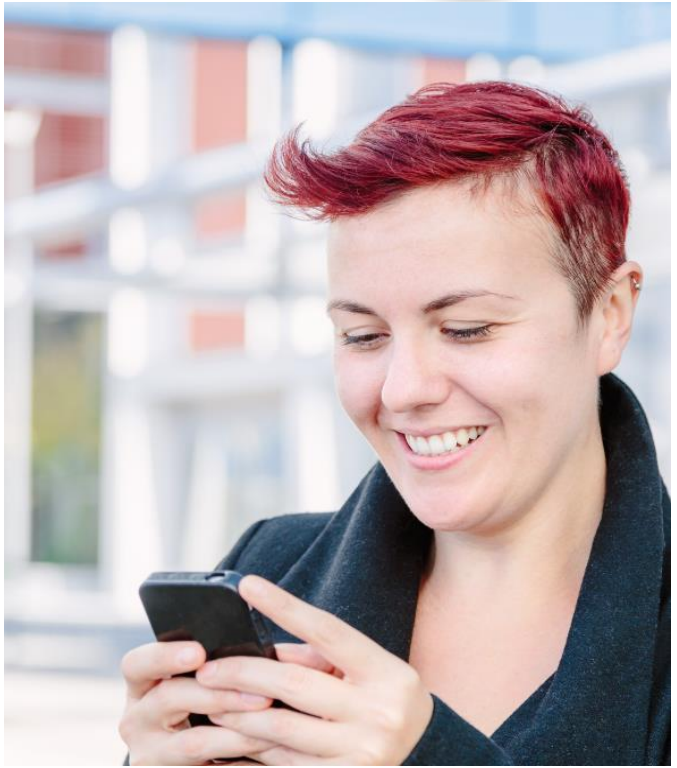
Sources: https://krebsonsecurity.com/tag/sentry-mba/
https://blog.shapesecurity.com/2016/03/09/a-look-at-sentry-mba/

It’s time for something better

A simpler and more secure experience

Aetna is leading the way in introducing advanced authentication methods into the health care sector.

- Our consumers no longer need to rely on traditional usernames and passwords when logging into Aetna applications
- Authentication, once a single event, is now integrated into the application transparently and continuously
- We’re adjusting controls and analytic capabilities to create friction for the threat adversaries while reducing friction for our **users**

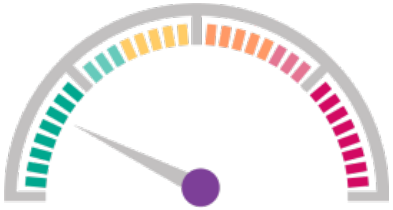


Continuous risk-based authentication

30-60 user attributes assessed

Continual authentication

without impacting the user experience

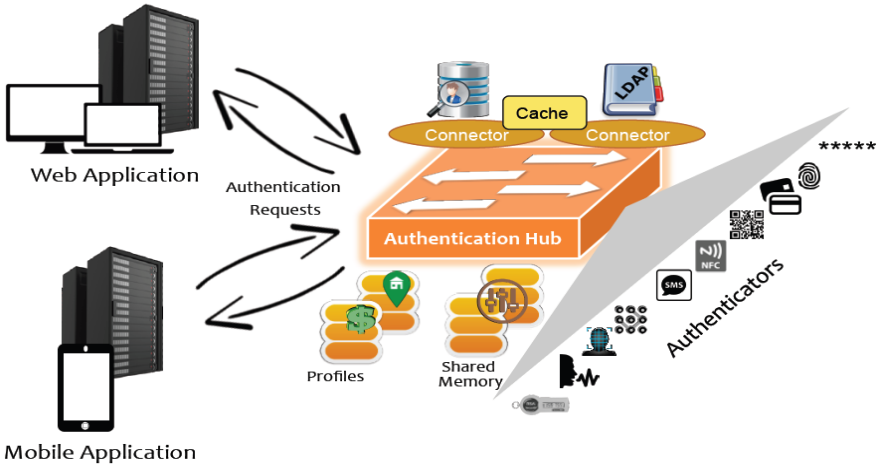


Risk score calculated

Risk score determines how much and what access to provide

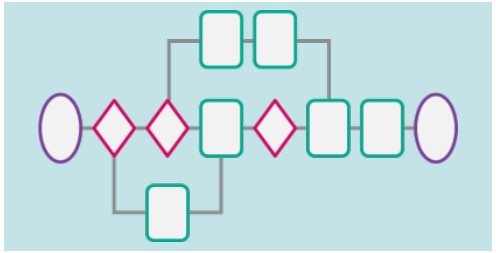
Authentication framework for mobile & web

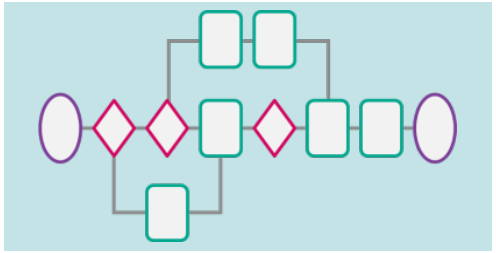
- One framework
- Multiple authentication tools
- Change controls without changing applications
- Across mobile and web
- Policy-driven authentication model



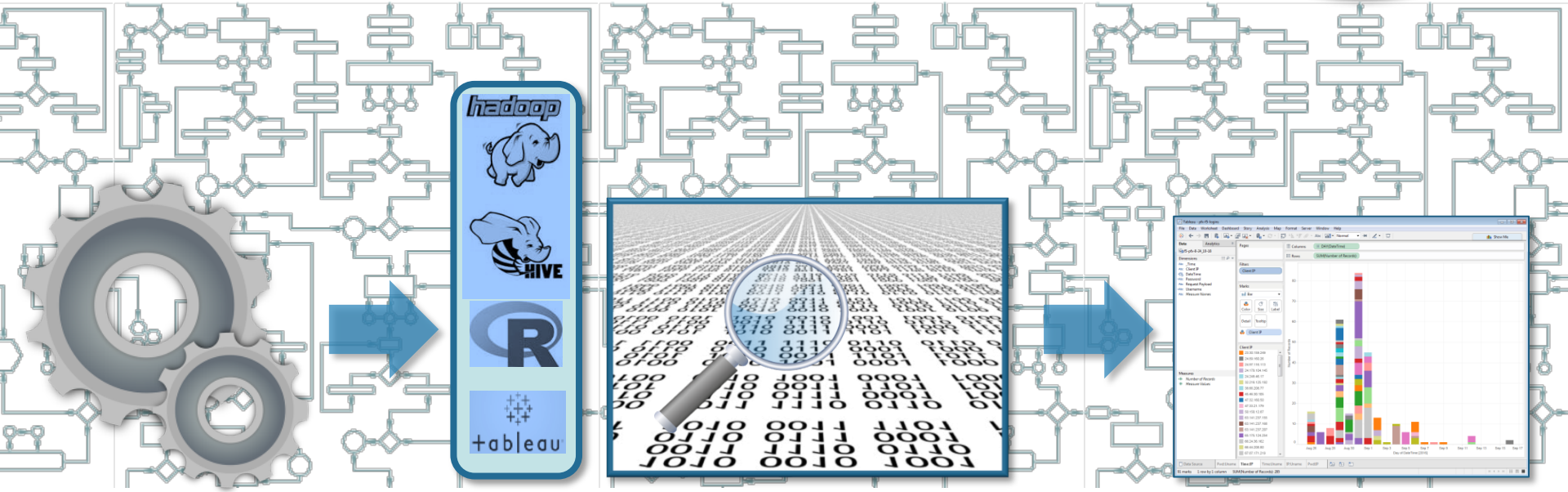
Model-driven security controls have arrived

- Inbound email protection
- Continuous behavioral based authentication
- Privileged User Monitoring
- High risk user monitoring
- Endpoint protection using Machine Learning
- Fraud management models
- Dynamic access provisioning
- Voice biometrics for fraud detection



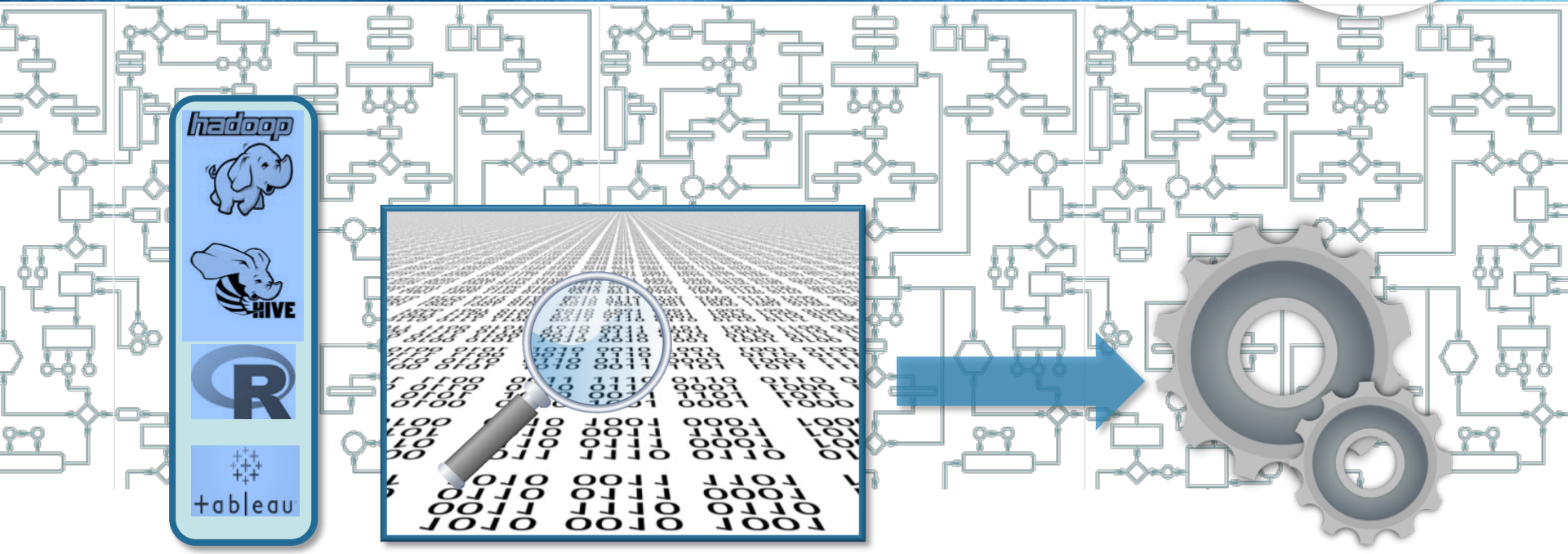


The Models are driving security



Security Controls ***Data Aggregation*** ***Data Analysis*** ***Results***

The Models are driving security



Data Aggregation

Data Analysis

Security Controls

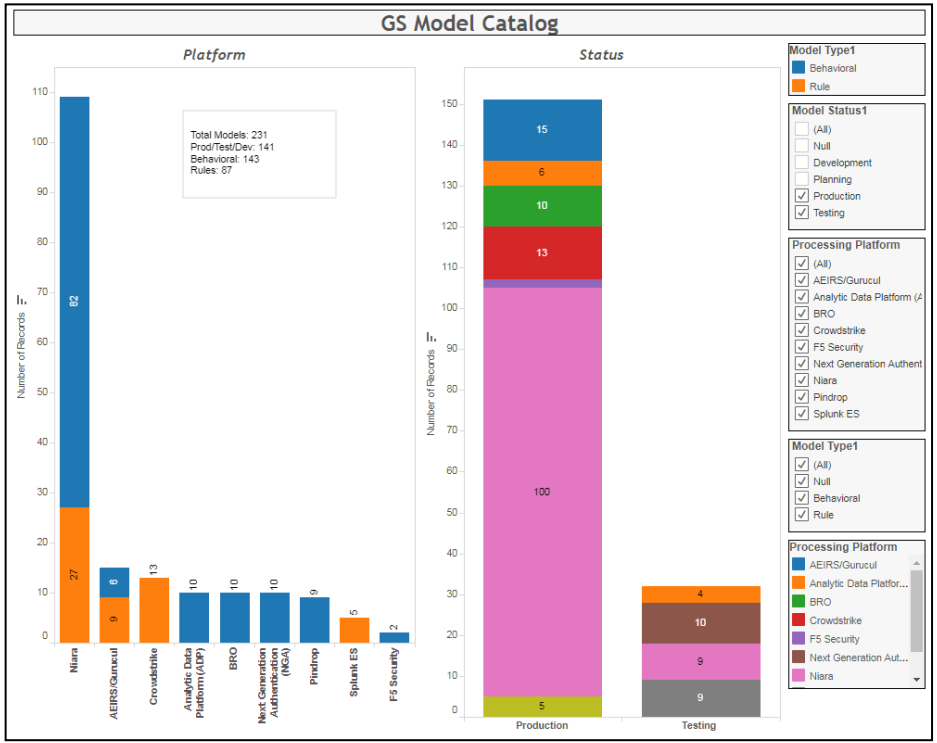
Model Inventory

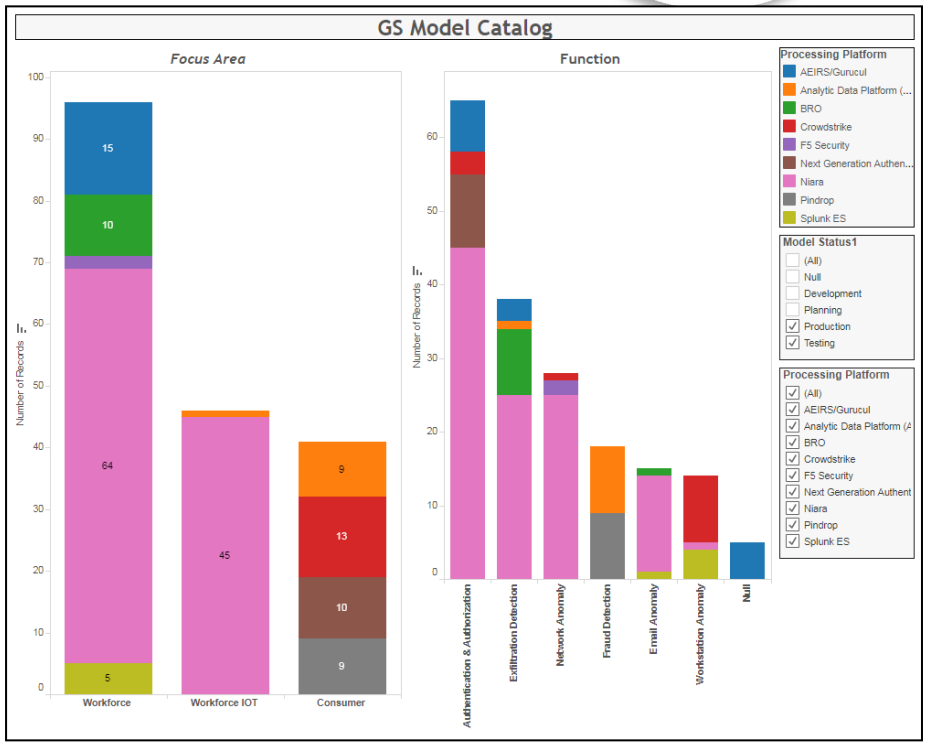
Model/Policy Name	Description	Effects
High Risk user - Departing User Sending self email	Users with future term date in UltiPro sending email to personal email accounts	Workforce
Restrict SSN email for High Risk users	Provide a daily list of all users with a risk score over 80 so they are restricted from sending email with SSN data.	Workforce
Events By Restricted Users	High volumes of privileged activity	Workforce
Off hours activities	Unusual evening privileged activity	Workforce
Week end login events	Unusual weekend privileged activity	Workforce
Unauthorized password changes	Vaulted accounts that have passwords changed by an unauthorized ID	Workforce
Self-Privilege Escalation	Admin granting privileges to themselves	Workforce
Account Compromise: Multiple Failed Logins/ Possible Configuration Issue	Multiple Failed Logins/ Possible Configuration Issue	Workforce
Unusual amount of password reset events	Unusual amount of password reset events	Workforce
Unusual amount of Failed Password changes	Unusual amount of Failed Password changes	Workforce
Purging of Audit Logs	A user purges an audit log from a server	Workforce

Models to be scheduled

Model/Policy Name	Description	Effects	Order
Register new bank followed by transaction over threshold	If a person changes banking information and performs a financial transaction same day	Consumer	**1**
Account email address changed followed by password reset request	Account email address changed followed by password reset request	Consumer	**2**
Financial Activity greater than threshold	Financial Activity greater than threshold	Consumer	**3**
Brute Force Attack	high number of failed login attempts	Consumer	**4**
Prevent Vault Checkout for High Risk Users	**Require additional verification before allowing a vaulted ID to be checked out by a high risk user**	**Workforce**	**5**
Geographic Activity without Physical Access	Logical Account activity at Geo location where there is no Physical Account activity	Workforce	**6**
Physical/Geographic Location Mismatch	Logical Account Geo location not matching Physical Account Geo location.	Workforce	**7**
Accounts Creation and deletion in a day	Accounts created by the admin , used and then deleted in the same day	Workforce	**8**
Accounts Enable and Disable in a day	Accounts enabled by the admin , used and then disabled in the same day	Workforce	**9**
Potential Access Misuse Attempt (Wanderer) - Badge	User is getting failed access at multiple access point	Workforce	**10**
Abnormal Access using Multiple Cards - Badge	Person is using temporary badge and permanent badge in short timeframe	Workforce	**11**
Rare Badge Access Anomaly	User accesses badge outside his normal historical behavior	Workforce	**12**
Potential Access Breach Attempt - Badge Stats model	User is getting high number of failed access	Workforce	**13**

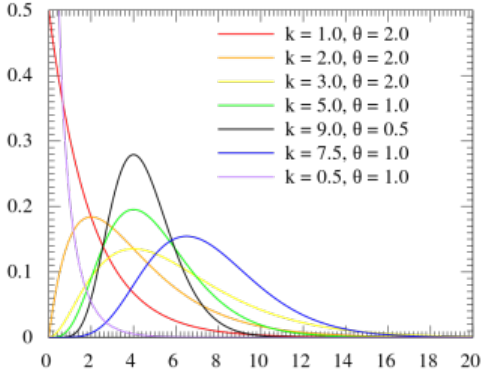
Model Inventory Management

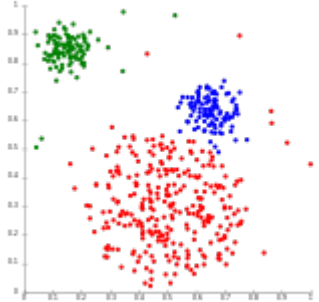


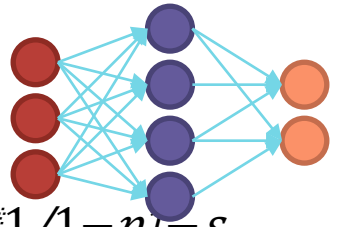


What are Models?

$$e^x = 1 + x/1! + x^2/2! + x^3/3! + \ldots$$







$$\zeta(s) = \sum n=1^{\infty} 1/n^s = \prod p^{} 1/1-p^{-s}$$

Mathematical formulation of observed events

Vendor Analytics Ecosystem

Acceptto

f5

pindrop security

AGARI

GURUCUL
PREDICTIVE SECURITY ANALYTICS

BRO

niara

splunk>

CROWDSTRIKE

nifi

TRANSMIT SECURITY

Phantom

aetna

Various models in production from a variety of vendors

Custom Fraud Analytic Models

HSA Burst Model

FSA Burst Model

Merchant Spike

HSA Employer Breach

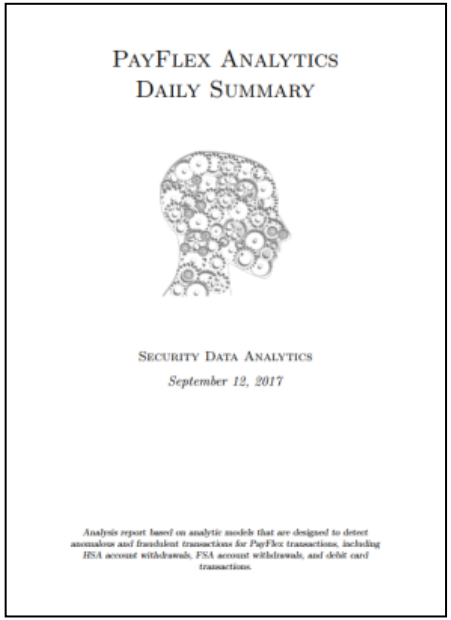
FSA Employer Breach

Cardholder Fraud

HSA Individual Fraud

FSA Individual Fraud

Targeted Merchant

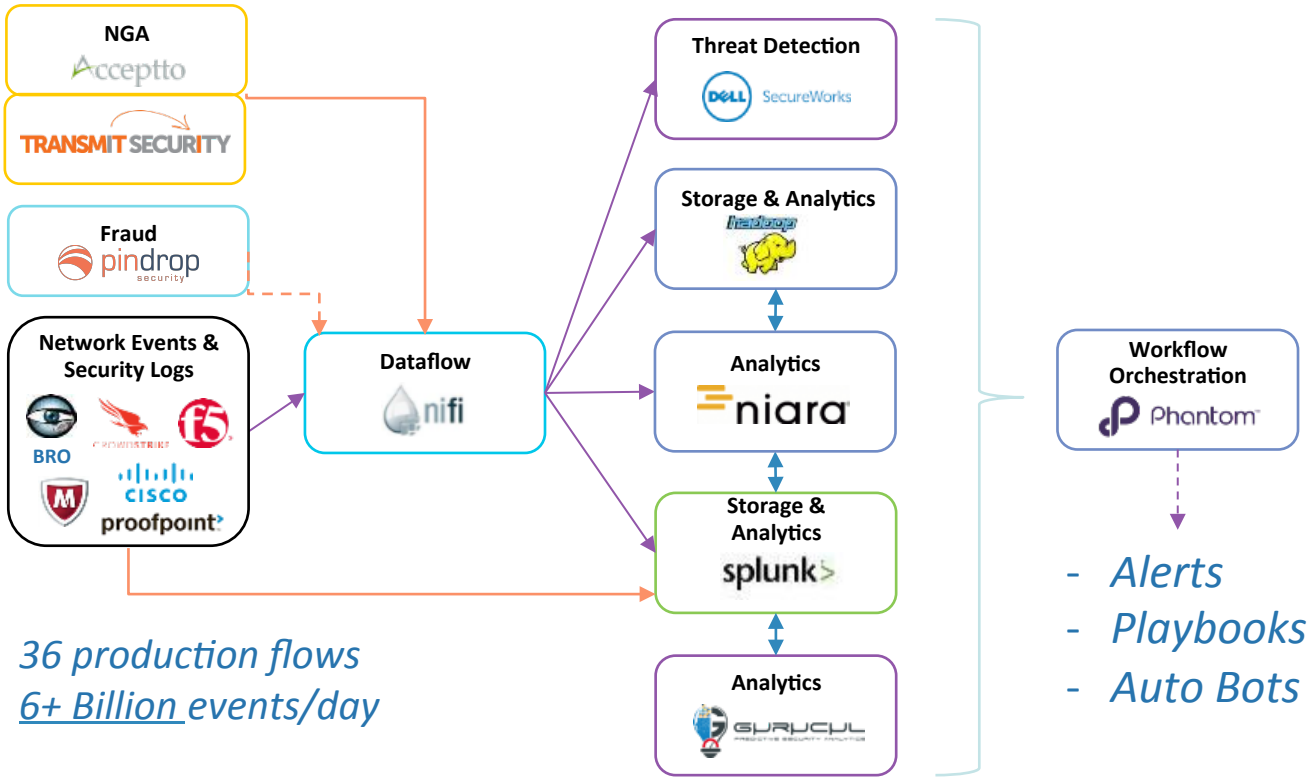

PayFlex Analytics
Daily Summary

Security Data Analytics
September 12, 2017

Analysis report based on analytic models that are designed to detect anomalous and fraudulent transactions for PayFlex transactions, including HSA account withdrawals, FSA account withdrawals, and debit card transactions.

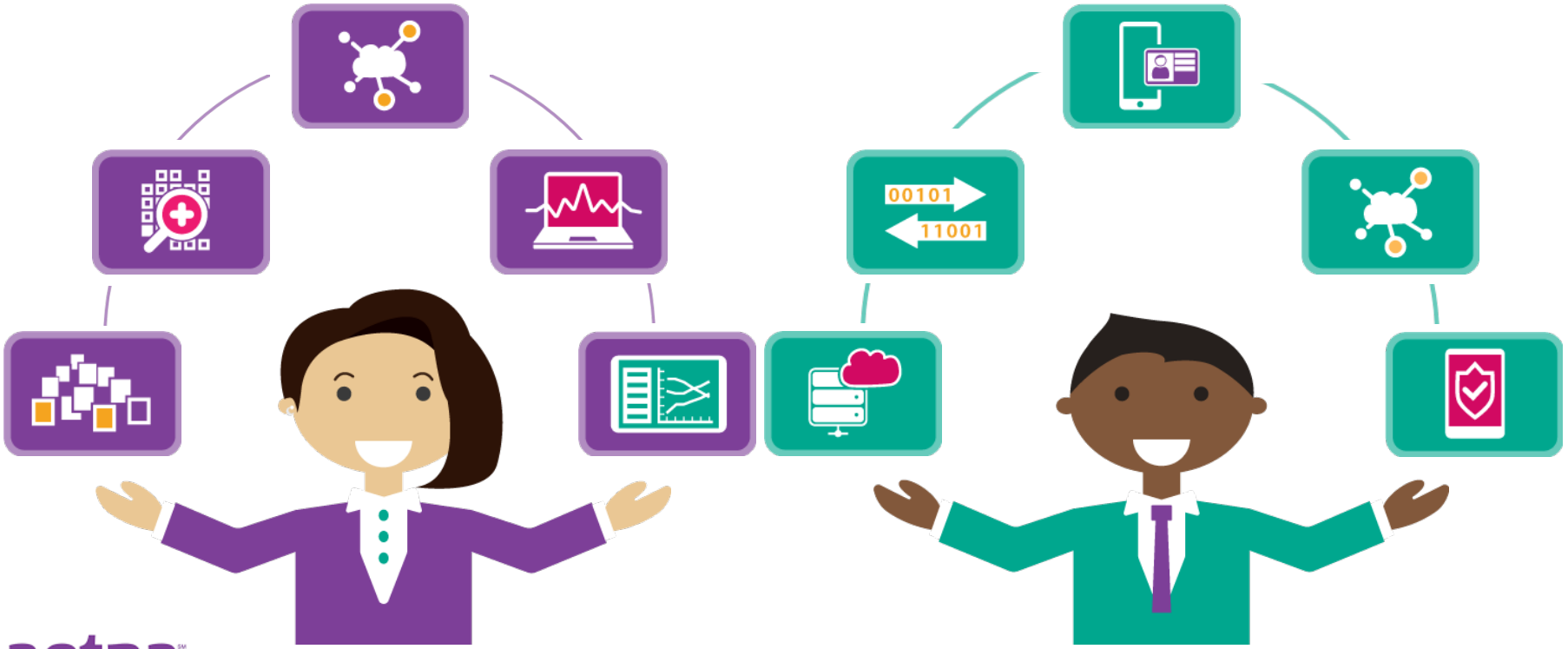
Daily Report

Model Data and Workflow



36 production flows
6+ Billion events/day

Data Scientist meet Security Professional



aetna

QUESTIONS?

routhj@aetna.com

https://www.linkedin.com/in/jmrouth/