RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

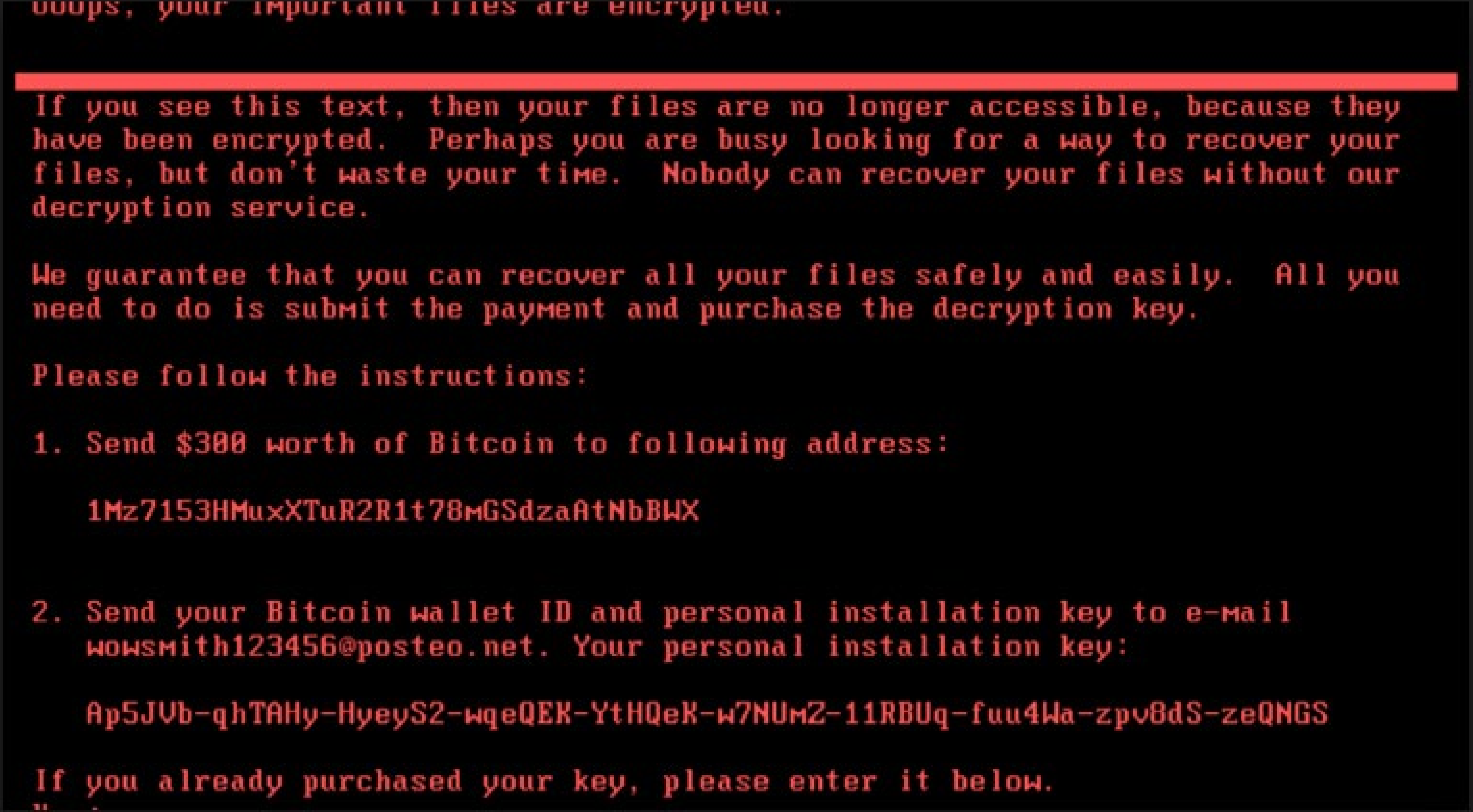
BETTER.

SESSION ID: MLAI-W02

Automating Security Controls Using Models and Security Orchestration

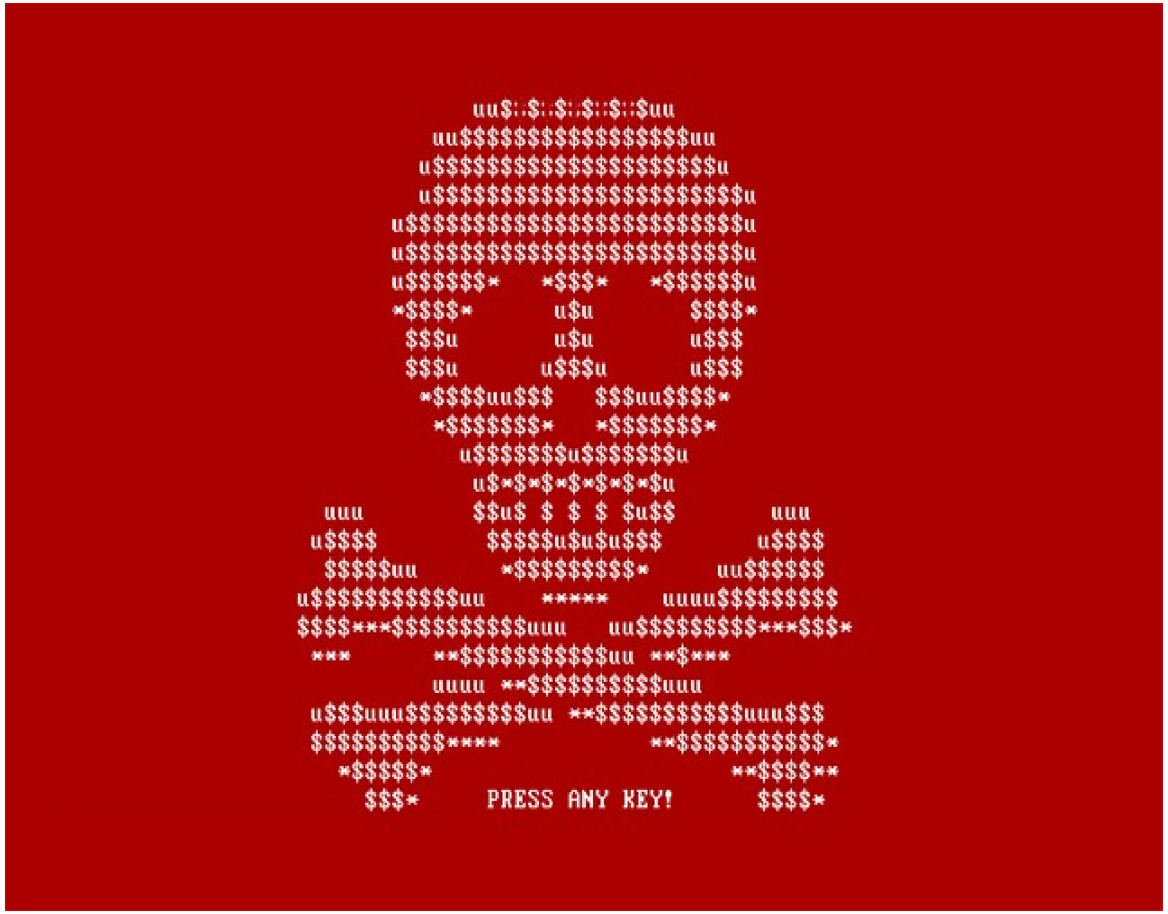
Kurt Lieber

Chief Information Security Officer
CVS Health/Aetna



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   Ap5JVb-qhTAHy-HyeyS2-wqeQEK-YtHQeK-w7NUmZ-11RBUq-fuu4Wa-zpv8dS-zeQNGS

If you already purchased your key, please enter it below.
```

Petya/Not Petya

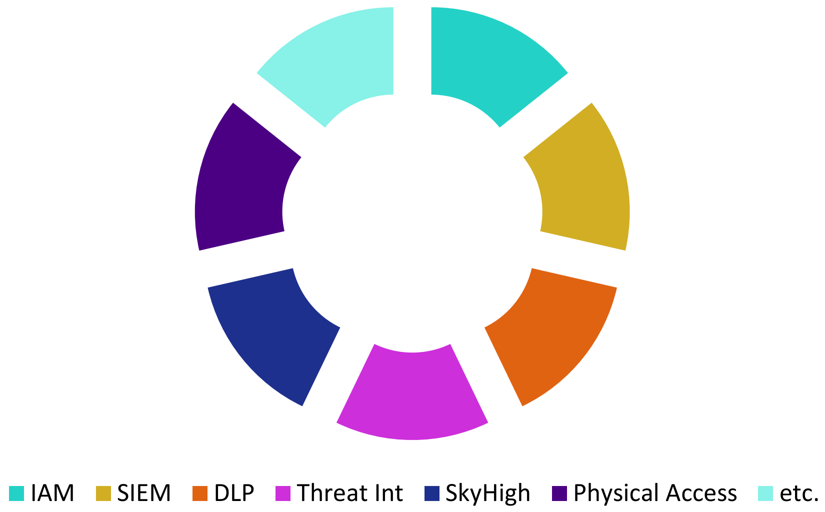


```
             uu$::$::$::$::$::$uu
          uu$$$$$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
           uuuu **$$$$$$$$$$uuu
  u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
  $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!       $$$$*
```

Year of Not Petya, in 2017, a major pharmaceutical company lost 15k servers in less than 90 seconds as a results of the NotPetya.

Static security controls are no longer sufficient. Security programs need to be moving at machine speed in order to protect against emerging threats.

Model Driven Security

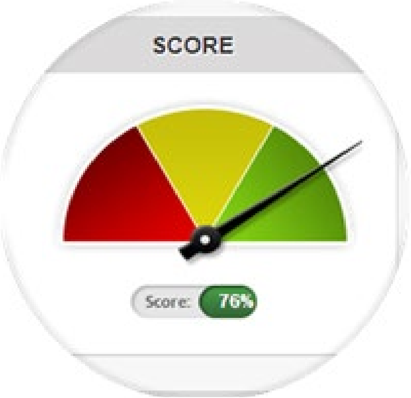


Collect Enterprise Risk Intelligence based on all available data

- Historical behavior pattern analysis
- Peer group analysis
- Geographic location
- Policies & known exceptions (e.g. Separation of Duty policies)

Individual Risk Scores

- Similar to a credit score
- Individualized to each user
- Adjust dynamically based on user behavior

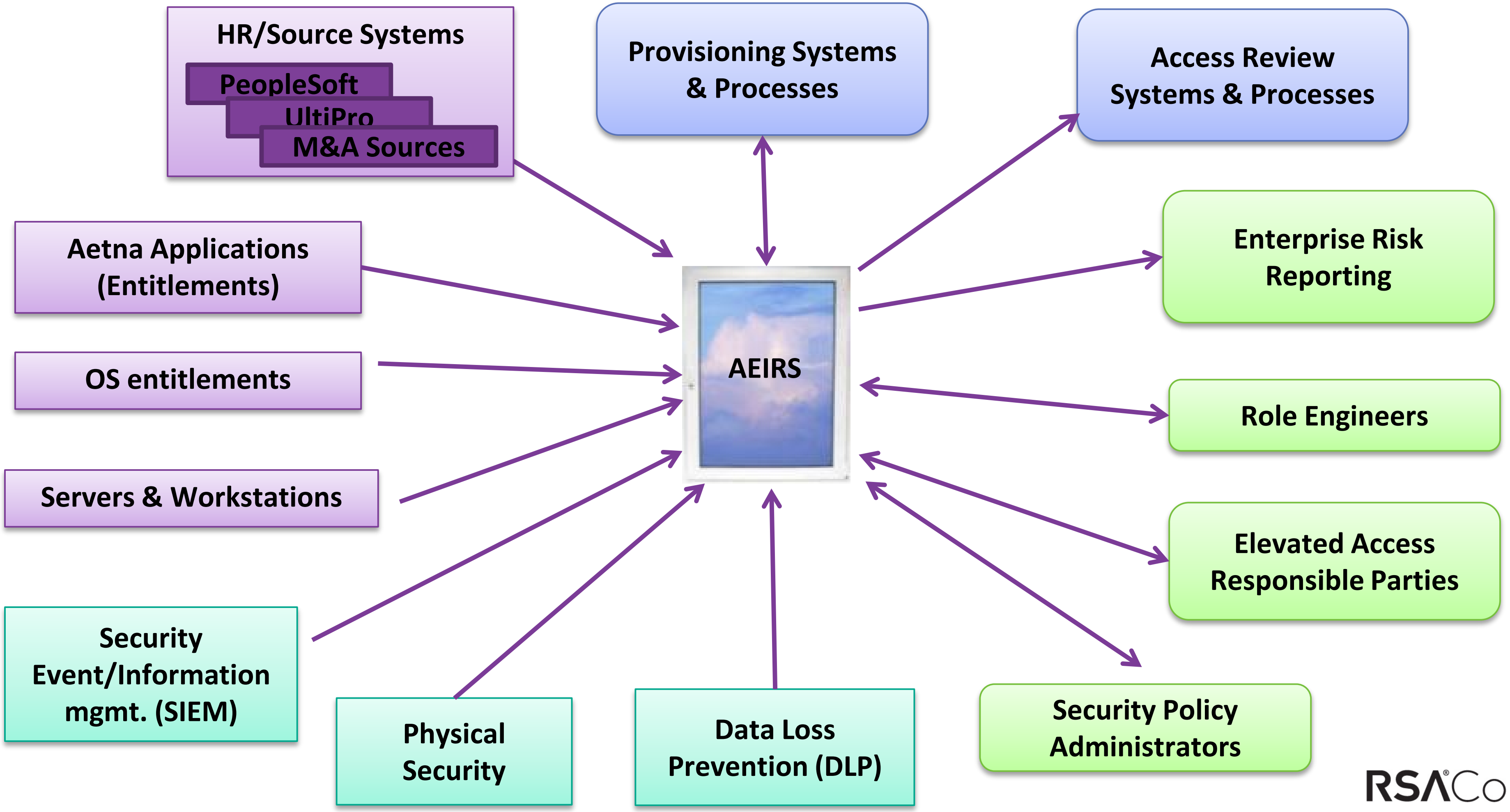


Behavioral based risk scores are the foundation of model driven security.

Aetna’s Entitlement, Identity, and Risk System (AEIRS)

AEIRS is populated with ‘single pane of glass’ view of all workforce access across all systems

- Including ability to risk rate all users, applications, systems and individual entitlements


HR/Source Systems
PeopleSoft
UltiPro
M&A Sources
Provisioning Systems & Processes
Access Review Systems & Processes
Aetna Applications (Entitlements)
Enterprise Risk Reporting
OS entitlements
AEIRS
Role Engineers
Servers & Workstations
Elevated Access Responsible Parties
Security Event/Information mgmt. (SIEM)
Physical Security
Data Loss Prevention (DLP)
Security Policy Administrators

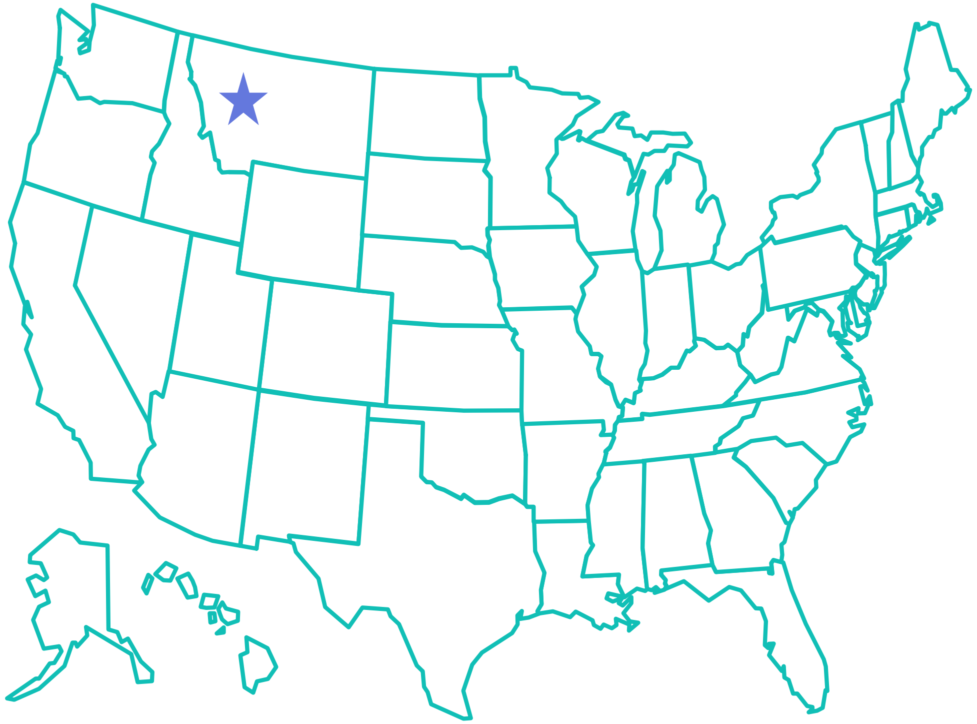
RSAConference2019

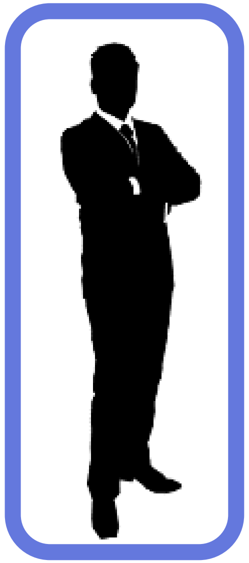
So What?

RSA Conference2019

Correlating the Logical and Physical Worlds

Risk Based Authentication





User badges in from Montana

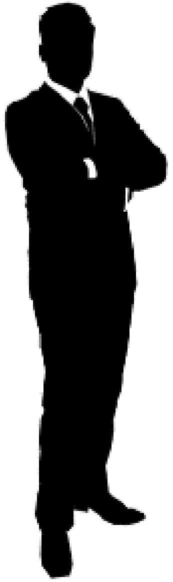
VPN is coming from Spain

User's risk automatically is changed to HIGH.

RSA®Conference2019

Using Risk Scores as a Dynamic Security Control

Password Vaulting Example



User attempts to check out a vaulted password

VERY LOW
LOW
MODERATE
HIGH
VERY HIGH

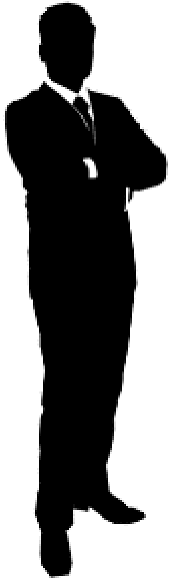
Risk score is evaluated

Approved

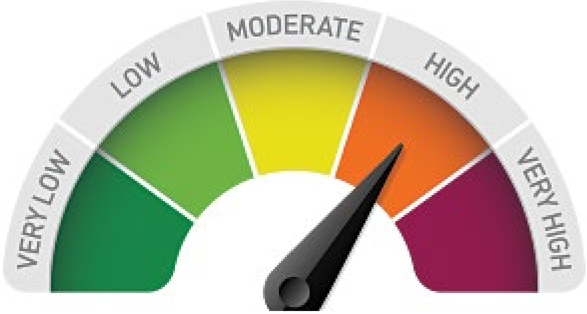
Denied/Call HelpDesk

Example of Fine Grain Policy Control

Using Data Loss Prevention (DLP)



User gives two-week notice



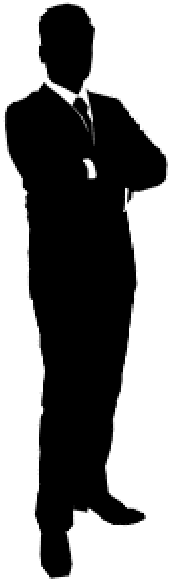
The risk to the enterprise has changed. This user is now considered HIGH risk.

Monitor the user more closely

Change the lens

This allows us to switch lenses and look at the employees from a different point of view based on the risk profile.

Using Security Orchestration



User's risk score all of sudden is HIGH

Alerts are sent

ip address

124.456.789.123

my-web-host-url.myhostsdomain.net

ip.skattertech.com // powered by Skatter Tech

Block ip address

Restrict all traffic via DLP

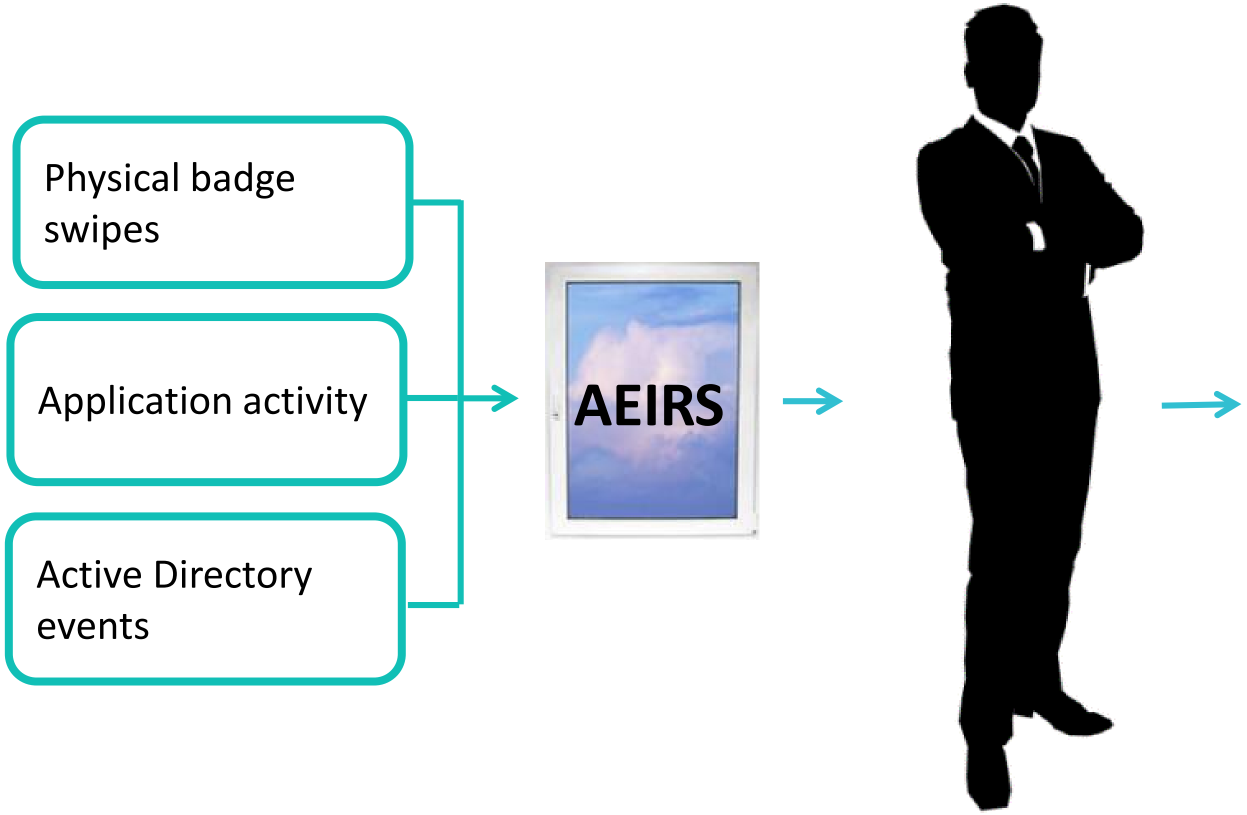
Disabled Account

▾ My account has been disabled.

Disable accounts

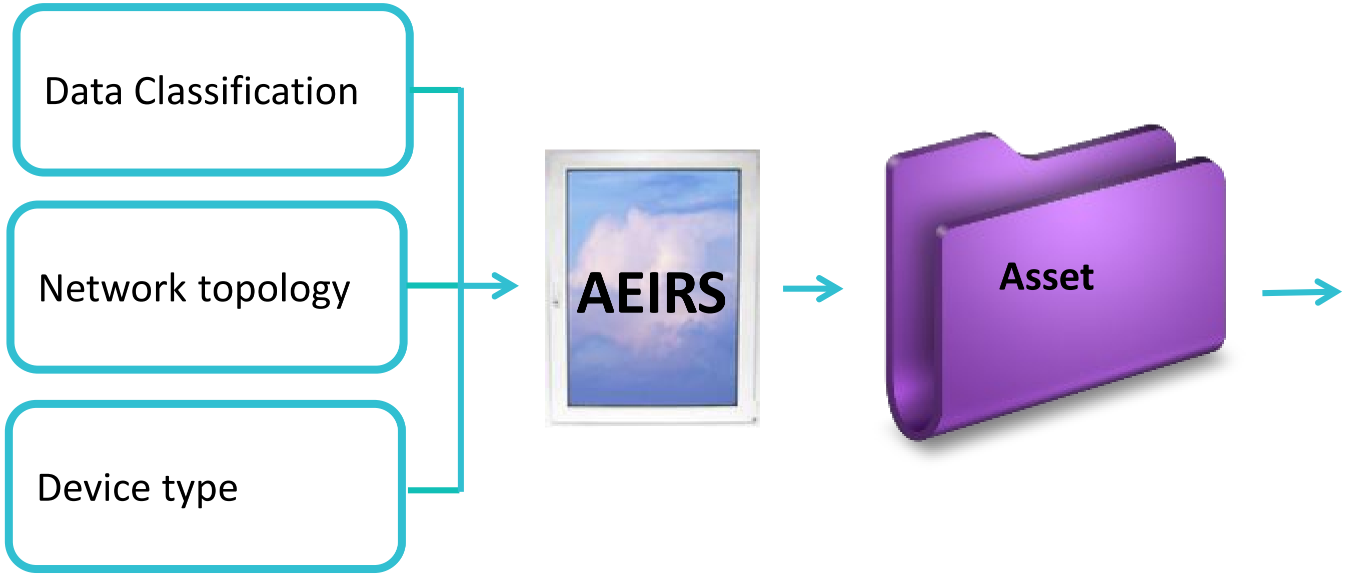
Dynamic Provisioning

Risk Measures - Users



User Risk Score
Low
Medium
High

Risk Measures - Assets



Data Classification

Network topology

Device type

AEIRS

Asset

User Risk Score
Low
Medium
High

Tomorrow Using Dynamic Provisioning

Dynamic Provisioning looks at the risk of the user, combined with the risk of the asset being requested and makes a real-time decision on whether or not to grant access.

Risk Score = Low

Asset

Risk Level = Medium

Notification sent

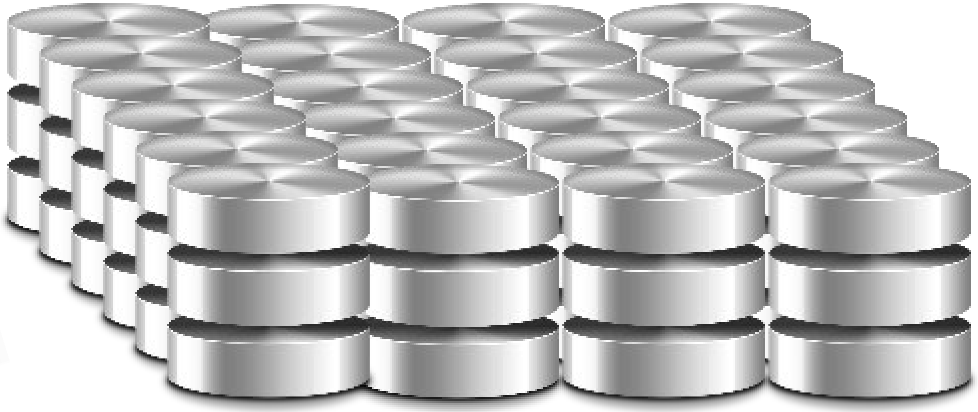
User Risk Score	Asset Risk Score	Action Required By Employee	Notification
Low	Low	Access granted automatically	None
Low	Medium	Access granted automatically	Informational notification sent to the manager
Medium	Low	Access granted automatically	Informational notification sent to the manager
High	Any	Normal request process	Formal approval required
Any	High	Normal request process	Formal approval required

Dynamic Provisioning allows us to use operational risk indicators to automatically provision access without a user first having to request it.

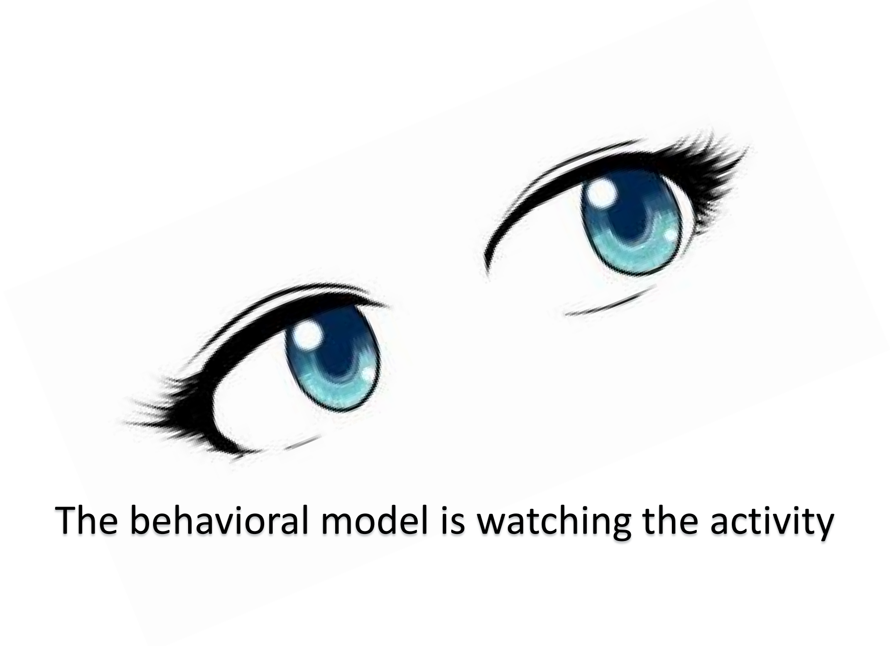
RSAConference2019

But What About NotPetya?

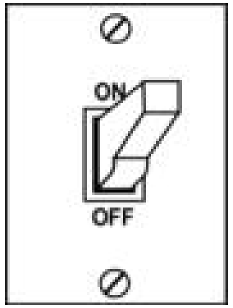
Authentication Cut Off



15k Servers



The behavioral model is watching the activity



Access is turned off

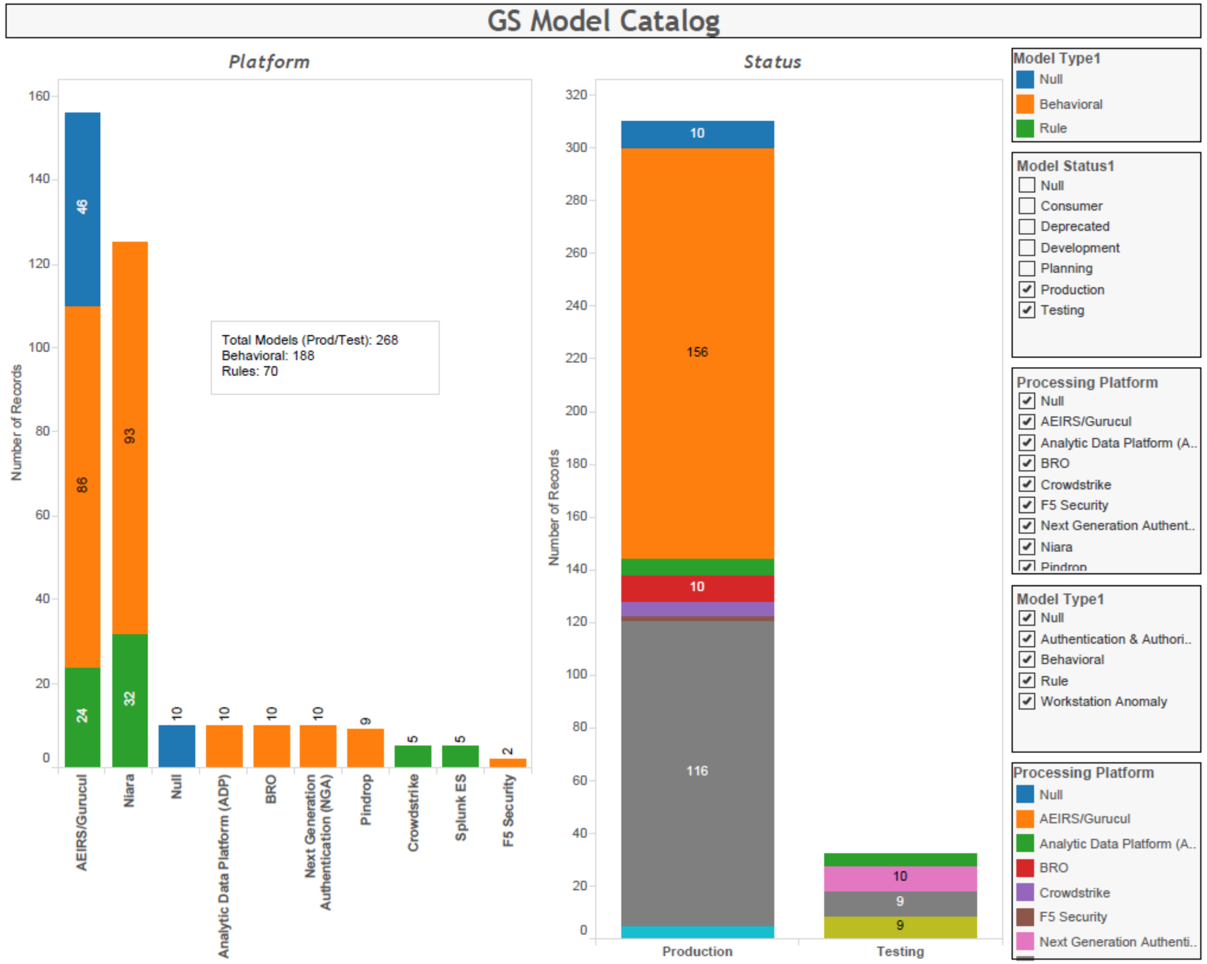
Knowing Your Environment

Privileged Users logging in

100+ Servers

Behavioral Models

Model Inventory Management



GS Model Catalog

Total Models (Prod/Test): 268
Behavioral: 188
Rules: 70

Model Type1

- 🟦 Null
- 🟧 Behavioral
- 🟩 Rule

Model Status1

- ☐ Null
- ☐ Consumer
- ☐ Deprecated
- ☐ Development
- ☐ Planning
- ☑ Production
- ☑ Testing

Processing Platform

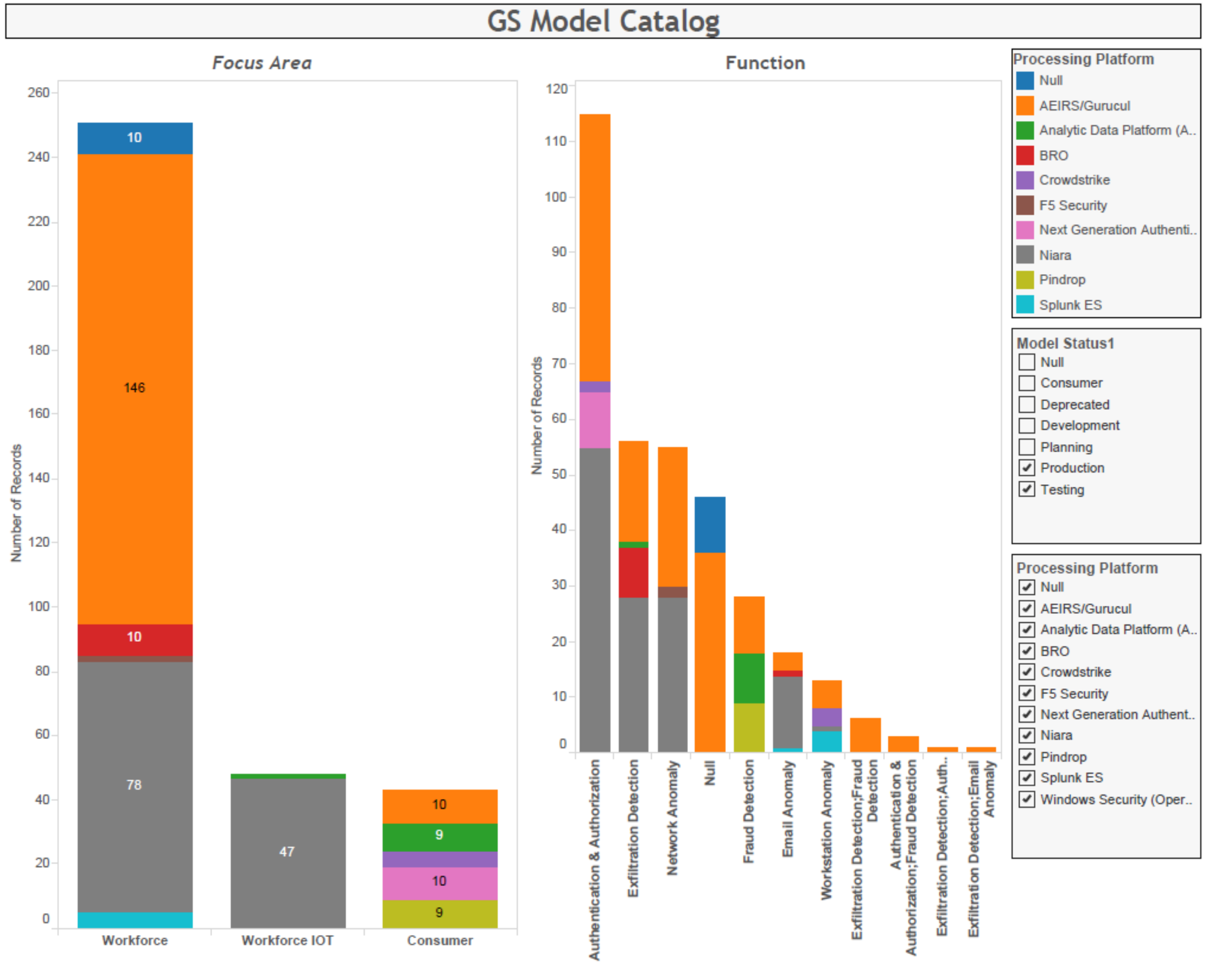
- ☑ Null
- ☑ AEIRS/Gurucul
- ☑ Analytic Data Platform (A..
- ☑ BRO
- ☑ Crowdstrike
- ☑ F5 Security
- ☑ Next Generation Authent..
- ☑ Niara
- ☑ Pindrop

Model Type1

- ☑ Null
- ☑ Authentication & Authori..
- ☑ Behavioral
- ☑ Rule
- ☑ Workstation Anomaly

Processing Platform

- 🟦 Null
- 🟧 AEIRS/Gurucul
- 🟩 Analytic Data Platform (A..
- 🟥 BRO
- 🟪 Crowdstrike
- 🟫 F5 Security
- 🟪 Next Generation Authenti..



GS Model Catalog

Processing Platform

- 🟦 Null
- 🟧 AEIRS/Gurucul
- 🟩 Analytic Data Platform (A..
- 🟥 BRO
- 🟪 Crowdstrike
- 🟫 F5 Security
- 🟪 Next Generation Authenti..
- ⬛ Niara
- 🟨 Pindrop
- 🟦 Splunk ES

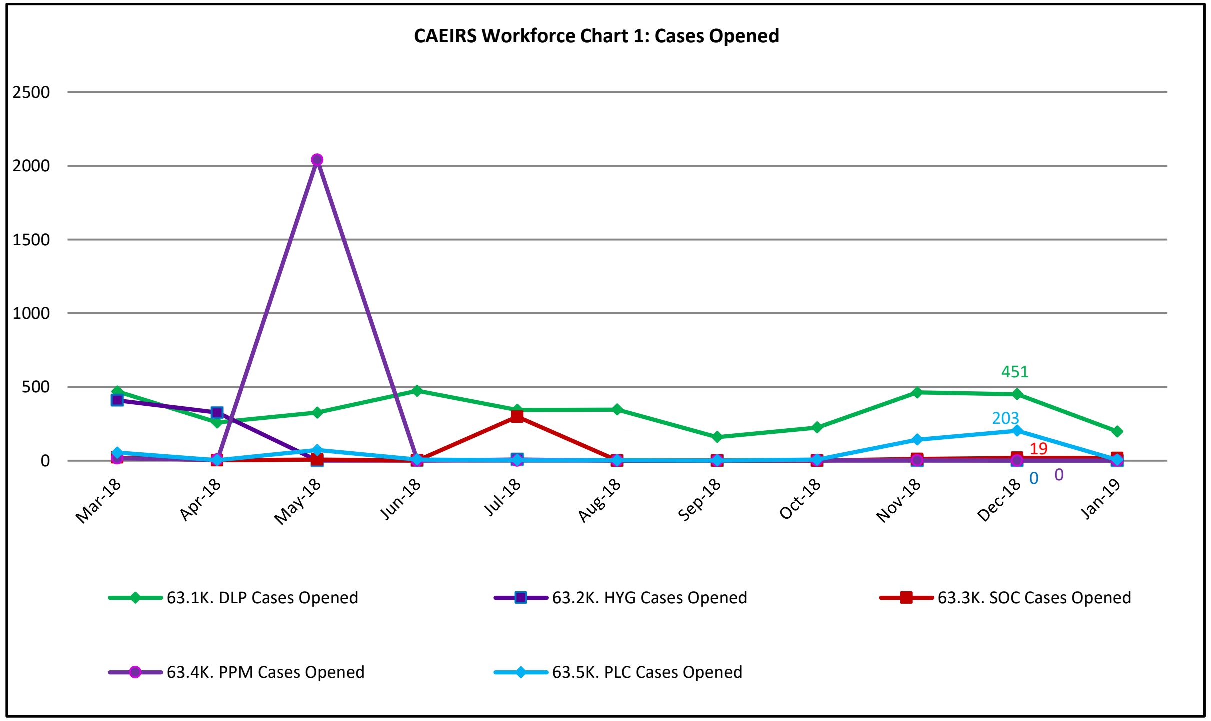
Model Status1

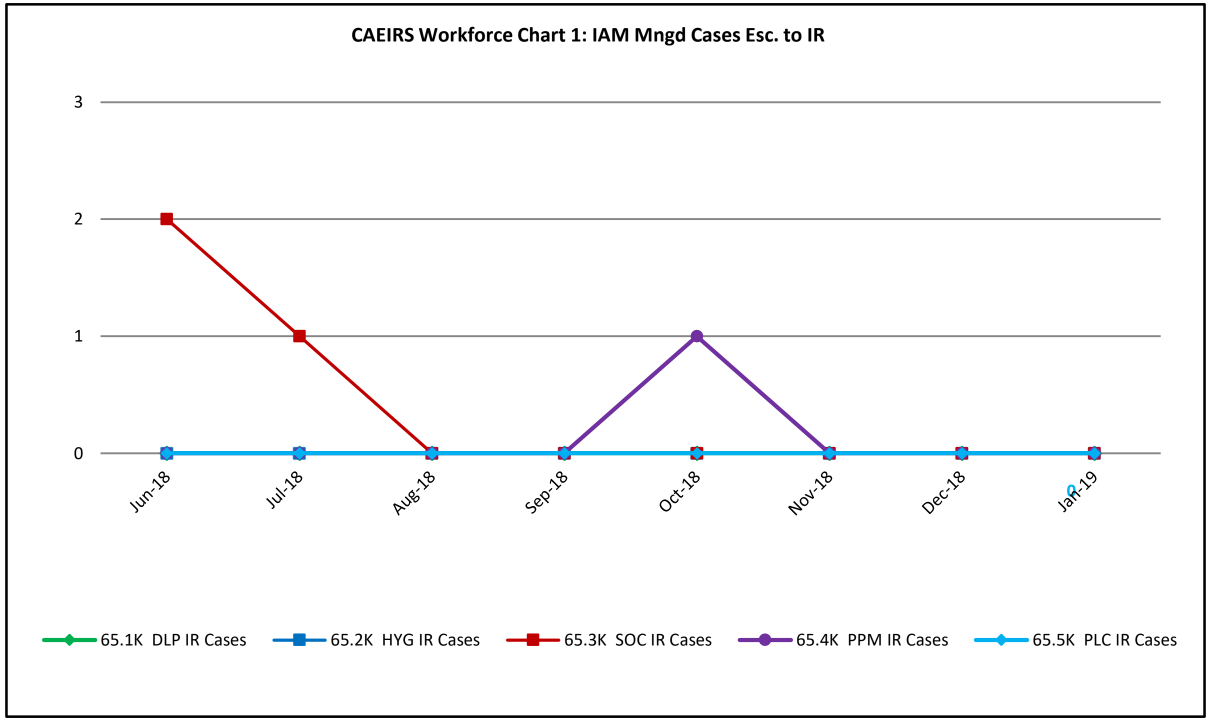
- ☐ Null
- ☐ Consumer
- ☐ Deprecated
- ☐ Development
- ☐ Planning
- ☑ Production
- ☑ Testing

Processing Platform

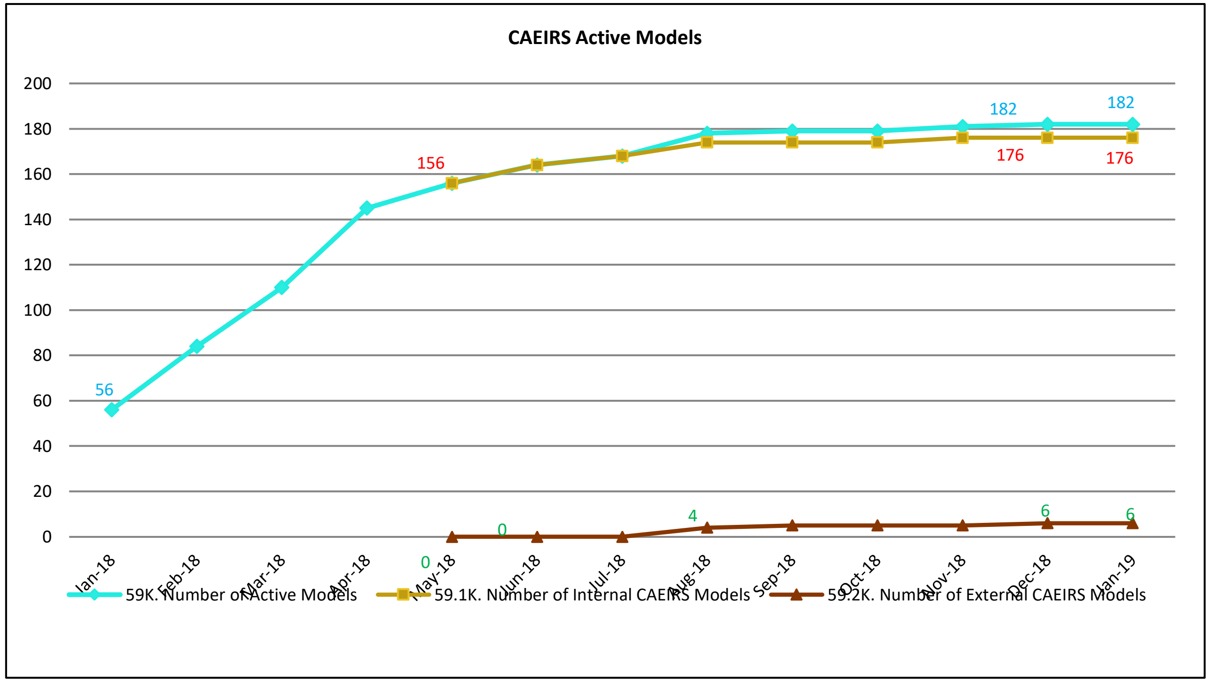
- ☑ Null
- ☑ AEIRS/Gurucul
- ☑ Analytic Data Platform (A..
- ☑ BRO
- ☑ Crowdstrike
- ☑ F5 Security
- ☑ Next Generation Authent..
- ☑ Niara
- ☑ Pindrop
- ☑ Splunk ES
- ☑ Windows Security (Oper..

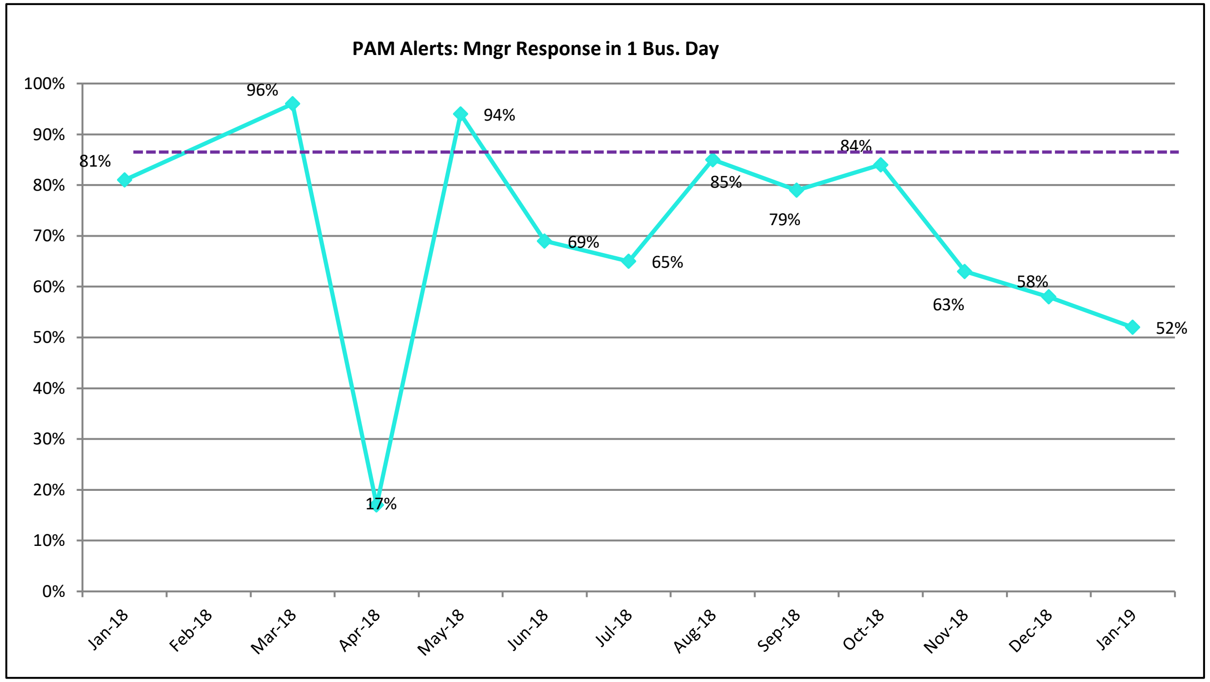
Measuring Success



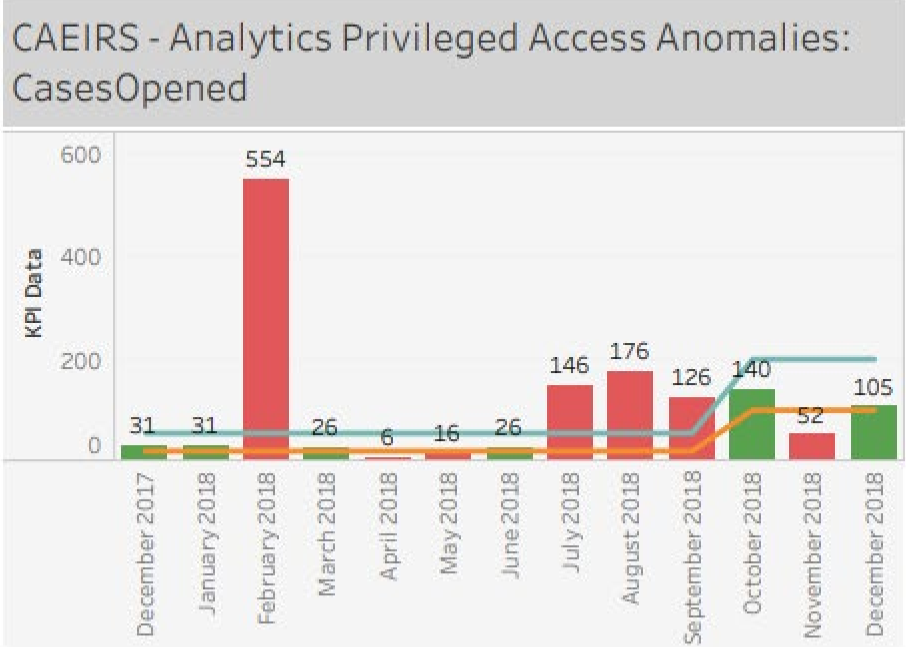


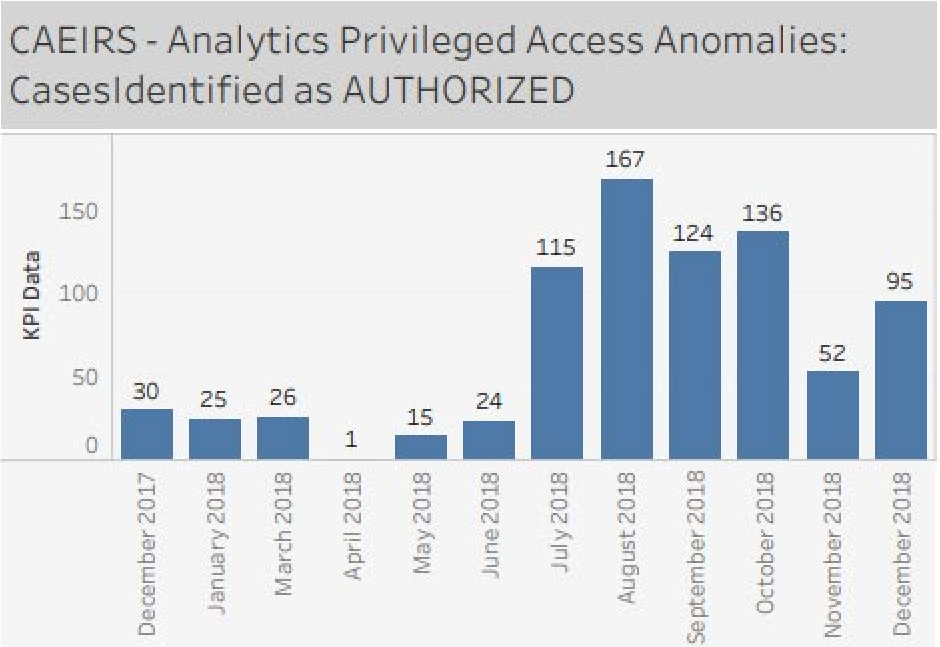
Measuring Success

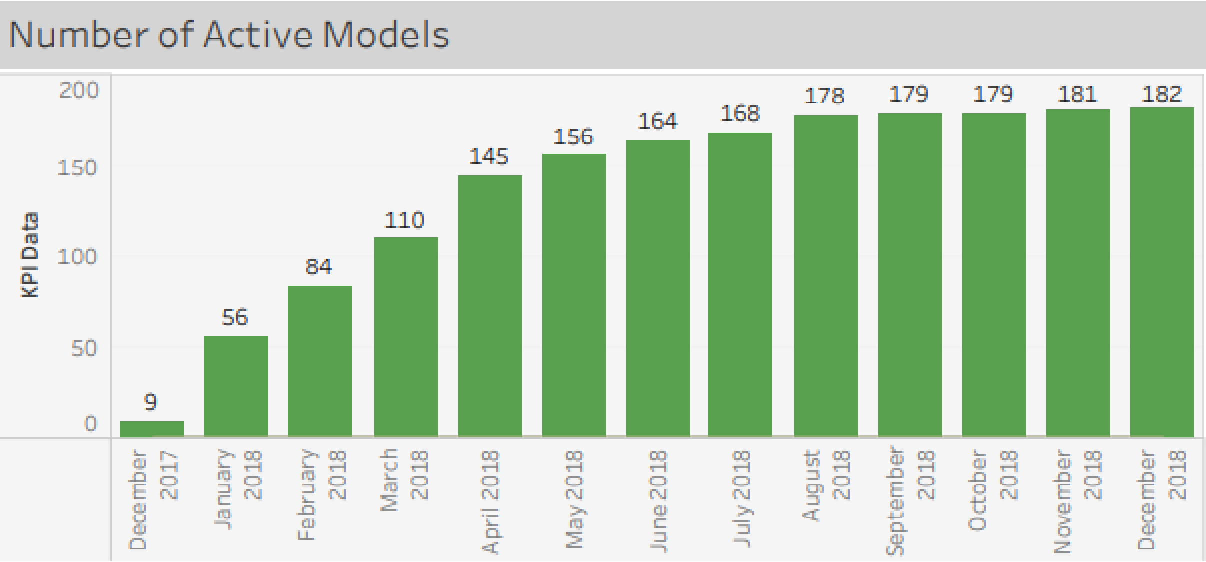




Measuring Success


CAEIRS - Analytics Privileged Access Anomalies: CasesOpened


CAEIRS - Analytics Privileged Access Anomalies: CasesIdentified as AUTHORIZED

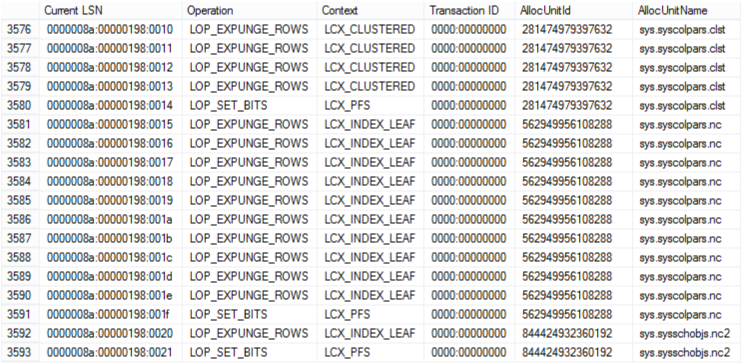

Number of Active Models

How do I get here?

"It's amazing to see the things that a mature security program can do, but our program could never get there."

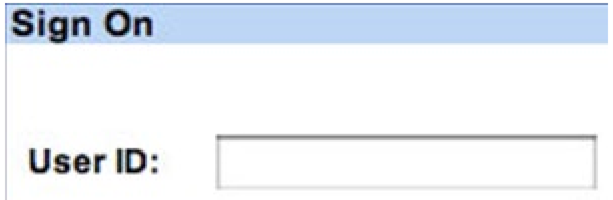
Things you should do to get here

The system is ***ONLY*** as good as the quality of your log data



	Current LSN	Operation	Context	Transaction ID	AllocUnitId	AllocUnitName
3576	0000008a:00000198:0010	LOP_EXPUNGE_ROWS	LCX_CLUSTERED	0000:00000000	281474979397632	sys.syscolpars.clst
3577	0000008a:00000198:0011	LOP_EXPUNGE_ROWS	LCX_CLUSTERED	0000:00000000	281474979397632	sys.syscolpars.clst
3578	0000008a:00000198:0012	LOP_EXPUNGE_ROWS	LCX_CLUSTERED	0000:00000000	281474979397632	sys.syscolpars.clst
3579	0000008a:00000198:0013	LOP_EXPUNGE_ROWS	LCX_CLUSTERED	0000:00000000	281474979397632	sys.syscolpars.clst
3580	0000008a:00000198:0014	LOP_SET_BITS	LCX_PFS	0000:00000000	281474979397632	sys.syscolpars.clst
3581	0000008a:00000198:0015	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3582	0000008a:00000198:0016	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3583	0000008a:00000198:0017	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3584	0000008a:00000198:0018	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3585	0000008a:00000198:0019	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3586	0000008a:00000198:001a	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3587	0000008a:00000198:001b	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3588	0000008a:00000198:001c	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3589	0000008a:00000198:001d	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3590	0000008a:00000198:001e	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	562949956108288	sys.syscolpars.nc
3591	0000008a:00000198:001f	LOP_SET_BITS	LCX_PFS	0000:00000000	562949956108288	sys.syscolpars.nc
3592	0000008a:00000198:0020	LOP_EXPUNGE_ROWS	LCX_INDEX_LEAF	0000:00000000	844424932360192	sys.sysschobjs.nc2
3593	0000008a:00000198:0021	LOP_SET_BITS	LCX_PFS	0000:00000000	844424932360192	sys.sysschobjs.nc2

You must be able to correlate back to a single user ID



Sign On

User ID:

Start small and build on your successes

RSAConference2019

Thank You