AEIRS

AEIRS – What is it?

Jonathan M Backus

Senior Security Advisor

Identity & Access Management

AEIRS – What is it?

- The acronym AEIRS stands for
  - **A**etna **E**ntitlements, **I**dentity, & **R**isk **S**ystem
- It is a User Behavior Analytics (UDA) solution, built using
  - The latest technology (50+ Linux servers)
  - Big Data (Hadoop, Crate, and relationship MySQL)
  - The latest Technics (Models and Machine Learning)

AEIRS – What is it?

T.E.N. - ISE® West Project Winner 2018

(August 16, 2018 – San Francisco, CA)

aetna

AEIRS – What is it?

AEIRS is a made up of "Building Blocks".

Identities: A unique identifier of all the humans (employee and contingent) that have access to any of Aetna's electronic systems.

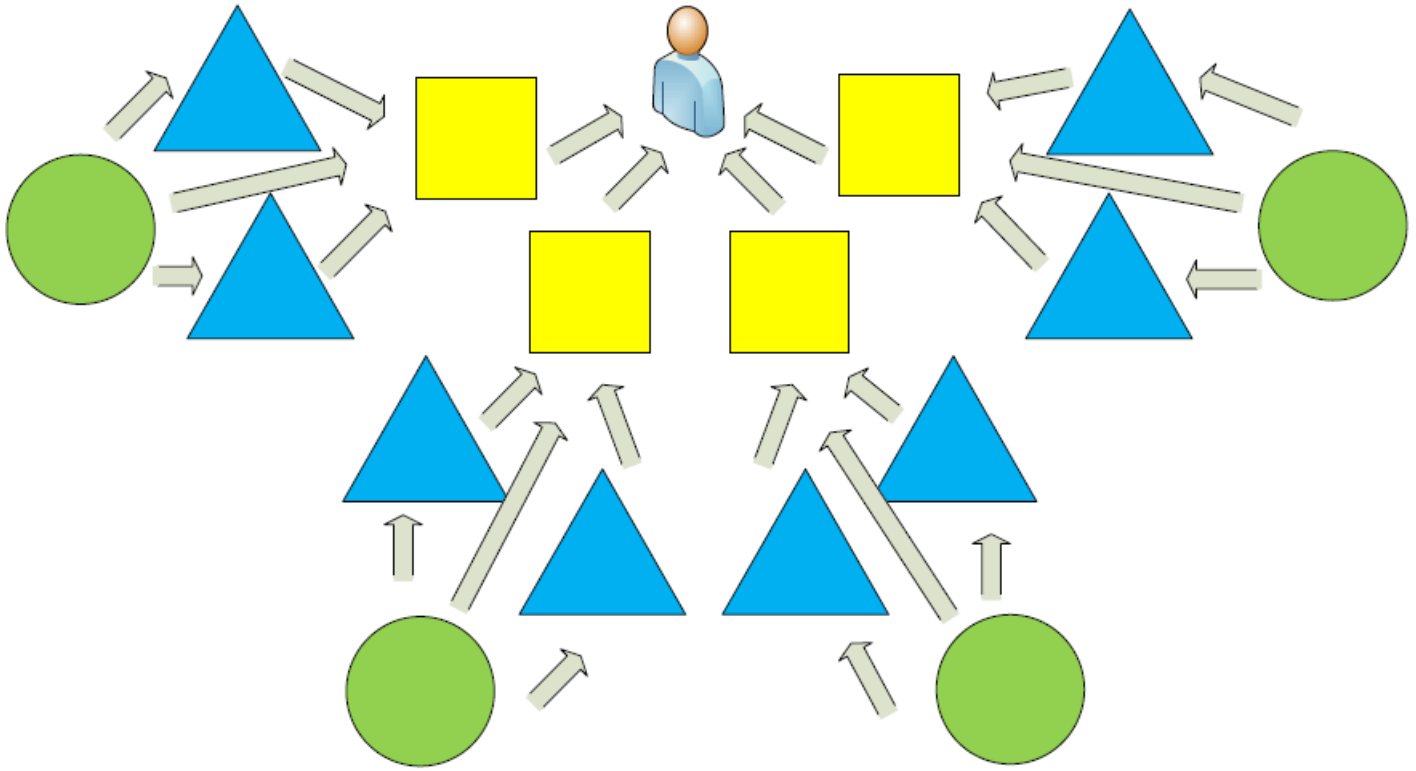
Accounts: A complete collection of all accounts or credentials an Identity has to any of Aetna's electronic systems. "Keys to the Aetna Kingdom"

Entitlements: A complete collection of all "things" an Identity is entitlement or able to do when they use a specific Account. "What are they able to do when they use a key to unlock a door"

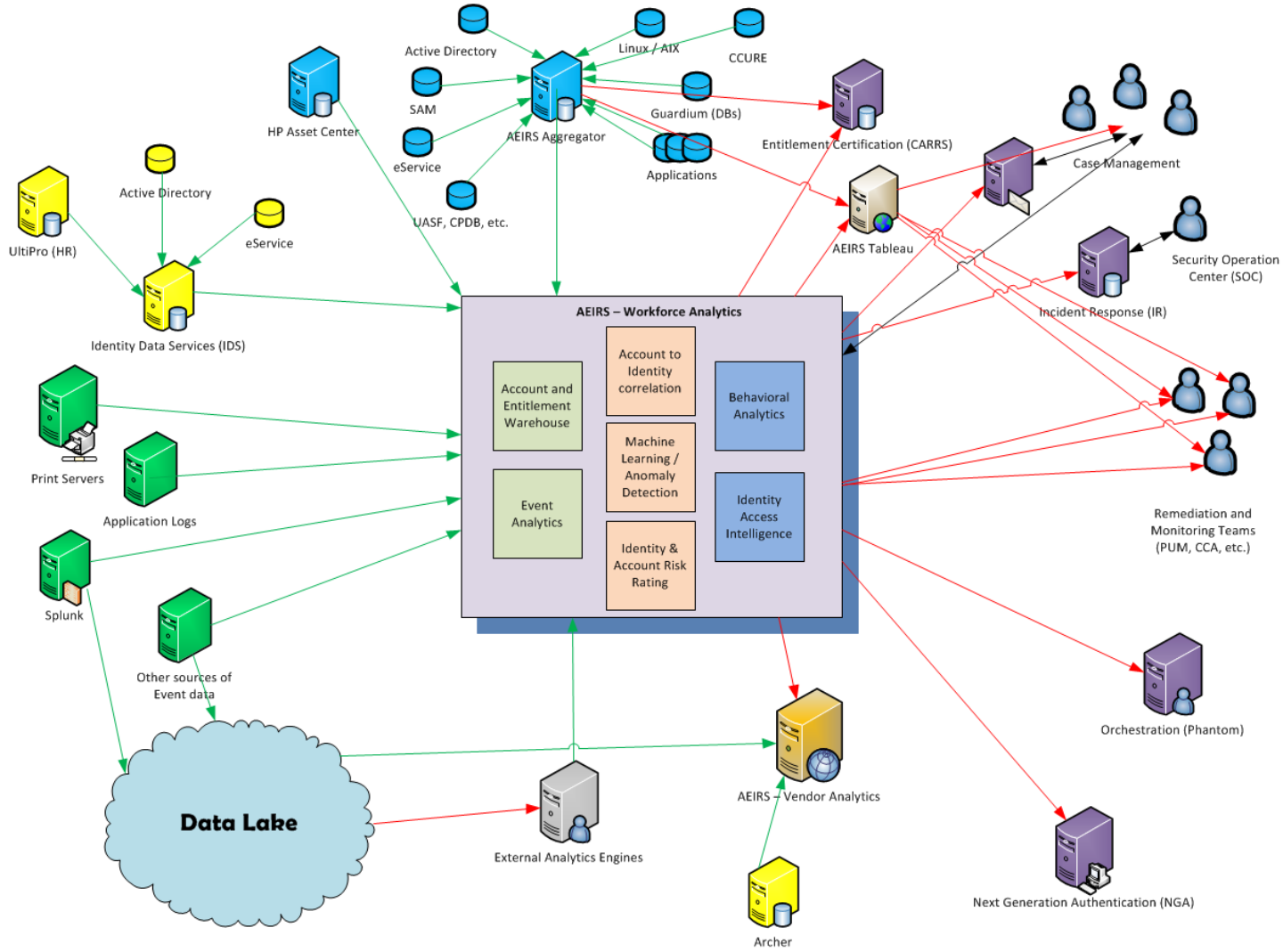
Events: The things a Identity (human) actually does when they log into an Account and take actions, permitted via their Entitlements.

AEIRS – What is it?

AEIRS is a made up of "Building Blocks".



AEIRS – What is it?



aetna

AEIRS – What is it?

Now that AEIRS is being fed all of this data on a daily basis, what are the next steps?

1) After the data is fed into AEIRS, it applies "Machine Learning" to create / maintain a baseline of normal behavior for every Identity. It then stores this "meta data" about each Identity in a relational database.
2) Next AEIRS applies models to the data. Models are broken into three groups, Behavior based, Rule based, and External.
   - Behavioral Models use the normalized behavior for all Identities (outlined above) and looks for abnormal behavior or breaks from pattern.
   - Rule Models look for patterns or events in all the activity data that are never considered normal.
   - External Models are ones that run outside of AEIRS and when triggered data is fed to AEIRS for processing.
3) If a model is triggered, a case is created against the Identity that caused it, for investigation by a Case Management.

AEIRS – What is it?

Now that AEIRS is being fed all of this data on a daily basis, what are the next steps?

4) The “weighted” value of the model is applied in a calculation to determine the Identity’s new Risk Score.
5) The Case Manager ultimately decides an “end state” for the case.
    I. If the case is determined to be authorized, it is accepted and the individuals Risk Score is lowered by the effect of the case.
    II. If the case is determined to be unauthorized, further investigation and possible corrective actions are taken outside of AEIRS. The impact or increase in the Risk Score remains.
        i. The Case Manager would create an IR (Incident Response) ticket.

AEIRS – What is it?

Category	Description	Count
AIR	Airwatch	3
DBA	Database	34
DLP	Data Loss Prevention	18
HYG	IT Hygiene	2
PAM	Privilege Access Management	17
PFX	Payflex	19
PHS	Phishing	3
PLC	Physical / Logical Convergence	17
PPM	Privilege Password Management	3
PTR	Printer	4
SOC	Server / AD Monitoring	19
VPN	Virtual Private Network Connections	3
WEB	Web Proxy	30
WKS	Workstations	12
	Total Number of Models Deployed (to date):	**184**

aetna

AEIRS – What is it?

Now that we have a reliable and robust set of IAM data and Identity Risk Scores for our work force we can feed it down stream to other systems for further targeted analysis and/or actionable steps.

- Contingent worker risk scores into our AEIRS – Vendor Analytics system.
- High Risk users to DLP for automatic blocking for certain functions.
- Data feeds and/or reports:
  - CARRS (Centralized Access Review & Recertification Service) for ARR, eTAR, PAR, and NPA efforts.
  - PUM (Privileged User Management) for validation of all privileged entitlements and the accounts they are associated with.
  - AAP (Access, Analysis, & Provisioning) & CCA (Certification, Compliance, & Self-Assessment) for security policy review, management, and auditing.
  - Data Transformation for various data clean up and validation efforts.

AEIRS – What is it?

AEIRS Analytics

Hello Backus, Jonathan (a616784). Your risk score is 50.

HIGH RISK:

Risk Score from 80 to 100

MEDIUM RISK:

Risk Score from 21 to 79

LOW RISK:

Risk Score from 0 to 20

Aetna uses a "User Behavior Analytics" system (UBA) to monitor all electronic activity. This system is called AEIRS (Aetna Entitlements, Identity, & Risk System). AEIRS uses data modeling and machine learning to detect unusual activity that could be an indicator of compromise (IOC) or that a member of our workforce is simply doing something they should not be doing.Out of this process a risk score is calculated on each and every workforce member (employees and contingent/contract workers). The risk score will go up or down, depending on observed activities.A person's risk score can impact what they are allowed to do and/or how much validation is required for them to access certain systems. The area of activities includes, but is not limited to the following.

In many cases the models are designed to take into account combinations of activities that include two or more of these areas.

- Workstations – The frequency, location, and nature of usage, including VPN.
- Printing – The nature, volume, and location of printing activity.
- Mobile – The use of mobile applications that allow access to Aetna data.
- Email – The nature, content, and recipient of emails you send.
- Phishing – The likelihood of you falling for a false email, known as phishing.
- Badge – The frequency and location of badging into Aetna properties and/or secure areas.
- Applications – The nature and volume of activity within applications.
- Internet – The nature and volume of Internet activity.
- Database – The nature and volume of activity directly within a database.
- Servers – The nature and volume of activity directly logged onto a server.

AEIRS – Next Generation

So what is in the future for AEIRS?

- All Identities and their Risk Scores will be feed to Next Generation Authentication (NGA)
- “Watch List” – Used by Case Management to monitor specific Identities closer
- “Risk Profiles” – Policies that increase the impact of models on Identities based on some attribute.
- “Risk Clusters” – Grouping of models together for trending.
- “Automatic Assessment” – Triggered when an Identity becomes High Risk.
- “Peer Group Analysis” – Grouping Identities by attributes to review entitlements and activity.
- And of course, more data and more models…

Questions?

Jon Backus
JMBackus@aetna.com

aetna®