ManageEngine
ADSolutions

Exposing attackers using AI and UBA

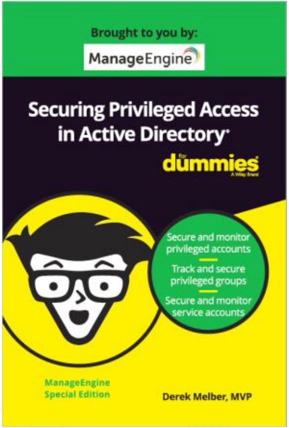
Derek Melber

derek@manageengine.com

About Your Speaker

About Derek Melber

- Derek Melber
  - Chief Technology Evangelist
  - MVP (AD and Group Policy)
  - derek@manageengine.com
  - LinkedIn
- Online Resources
  - ManageEngine Active Directory Blog
  - Security Hardening Site
  - Download free Dummies book
- 2019 World Tour

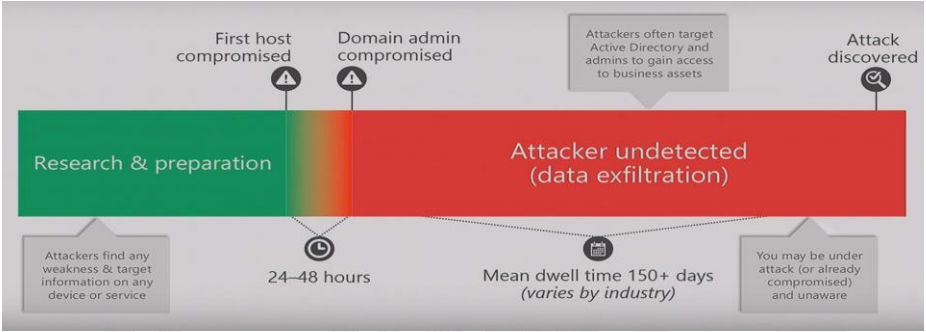

Brought to you by:
ManageEngine
Securing Privileged Access in Active Directory
for dummies
A Wiley Brand
Secure and monitor privileged accounts
Track and secure privileged groups
Secure and monitor service accounts
ManageEngine Special Edition
Derek Melber, MVP

Agenda

- Why SIEM and UBA is needed!
- Logical approach to detecting attacks
- Traditional SIEM approach to detect attacks
- What is AI and UBA?
- UBA approach to detecting attacks
- UBA: Logons
- UBA: User management
- UBA: Resource access
- UEBA: Risk score

WHY SIEM AND UBA IS NEEDED!

Attack timeline: According to Microsoft



First host compromised

Domain admin compromised

Attackers often target Active Directory and admins to gain access to business assets

Attack discovered

Research & preparation

Attacker undetected (data exfiltration)

Attackers find any weakness & target information on any device or service

24–48 hours

Mean dwell time 150+ days *(varies by industry)*

You may be under attack (or already compromised) and unaware

Why SIEM and UBA is needed: Lessons learned

- Current processes are failing to catch changes
- Current processes are failing to detect an intrusion
- Example: Marriott breach
  - 500,000,000 accounts affected
  - Initial breach: 2014
  - Discovery of breach: September 2018
  - Determination of breach: Late November 2018
  - 4 years from breach to determination!!!!!!!!

LOGICAL APPROACH TO DETECTING ATTACKS

Logical approach to detecting attacks

- Focus on what attackers do
  - Utilize network access
  - Focus on endpoints for access
  - Need to achieve privileged access
  - Attack weak security
- Harder to detect “allowed” attackers
  - Users that have access to data
  - Privileged users (local and in AD)

TRADITIONAL SIEM APPROACH TO DETECT ATTACKS

ManageEngine

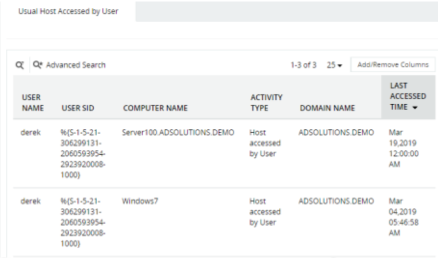
Traditional SIEM approach to attacks

- Sift through voluminous event logs
- Look for changes that might be related to an attack
  - Groups
  - Security settings
  - Failed logons
- Thresholds can help reduce false-positives
- Correlation can help splice different events, from different computers, together
  - X failed logons
  - Success logon
  - Installed service
  - Connection to file server
- Auto-action based on behavior and events (hard for admins to implement)

WHAT IS AI AND UBA?

What is AI and UBA?

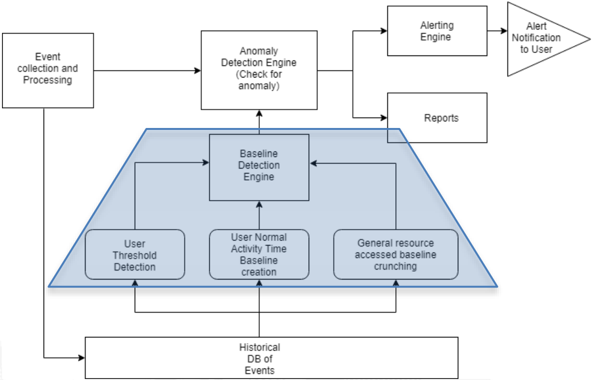
- User Behavior Analytics (UBA)
  - Uses machine learning
  - Creates a baseline of activity
  - Uses baseline to detect anomalies
- UBA focuses on what the user is doing
  - Apps launched
  - Logons
  - Files accessed
  - Administrative actions



Usual Host Accessed by User

USER NAME	USER SID	COMPUTER NAME	ACTIVITY TYPE	DOMAIN NAME	LAST ACCESSED TIME
derek	%{S-1-5-21-306299131-2060593954-2923920008-1000}	Server100.ADSOLUTIONS.DEMO	Host accessed by User	ADSOLUTIONS.DEMO	Mar 19,2019 12:00:00 AM
derek	%{S-1-5-21-306299131-2060593954-2923920008-1000}	Windows7	Host accessed by User	ADSOLUTIONS.DEMO	Mar 04,2019 05:46:58 AM

UBA flow chart


Event collection and Processing
Anomaly Detection Engine (Check for anomaly)
Alerting Engine
Alert Notification to User
Reports
Baseline Detection Engine
User Threshold Detection
User Normal Activity Time Baseline creation
General resource accessed baseline crunching
Historical DB of Events

UBA APPROACH TO DETECTING ATTACKS

UBA for attack detection

- Create baseline of normal behavior for all users and hosts
  - Logon time
  - Thresholds for logon failure
  - Usual host access
  - Remote access
  - Resource access volume
  - Processes running on host
- UBA then measures real-time events against baseline, checking for anomalies

UBA: LOGONS

UBA: Logons

- Use Cases
  - Employee attempts to logon to other AD accounts
    - This will generate many failed logons (but maybe only 1 per account)
    - The “per user” failed logon threshold will not be triggered
    - The “per host” failed logon threshold will be triggered
  - First time host accessed by user

UBA: Logons

- Users
  - Logon times
    - Normal logon times
    - Logons outside normal
  - Host access
    - Usual host accessed
    - First time host access
    - First time remote access to host
- Hosts
  - Logon times
    - Normal logon times
    - Logons outside normal
  - Unusual volume logon failures

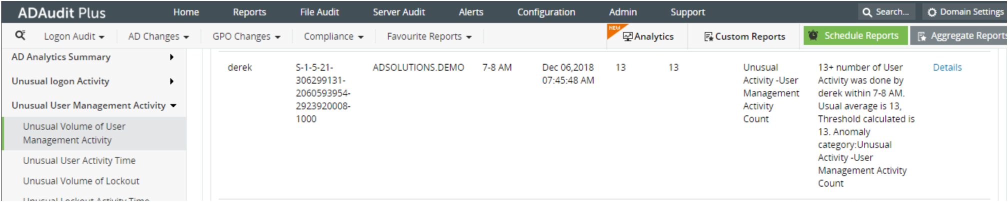
UBA: USER MANAGEMENT

UBA: User Management

- Use Cases
  - Administrator performs abnormal tasks, such as enabling user accounts
    - Hard to delineate good and bad admin behavior
    - Key is to know “normal” vs abnormal
    - If admin enables “many disabled user accounts”, this is abnormal

UBA: User management

- Abnormal volume of user management



derek	S-1-5-21-306299131-2060593954-2923920008-1000	ADSOLUTIONS.DEMO	7-8 AM	Dec 06,2018 07:45:48 AM	13	13	Unusual Activity -User Management Activity Count	13+ number of User Activity was done by derek within 7-8 AM. Usual average is 13, Threshold calculated is 13. Anomaly category:Unusual Activity -User Management Activity Count	Details

UBA: RESOURCE ACCESS

UBA: Resource Access

- Use Cases
  - User copies 100’s of files at one time
    - Users normally access 25 to 50 files in a day
    - If a user copies 100’s of files, this will trigger UBA!

UBA: Resource access

- File access – Exceeds normal volumes
  - Success
  - Failure
  - Modification
  - Delete
- File access – Outside normal time

UEBA: RISK SCORE

Summary

- Why SIEM and UBA is needed!
- Logical approach to detecting attacks
- Traditional SIEM approach to detect attacks
- What is AI and UBA?
- UBA approach to detecting attacks
- UBA: Logons
- UBA: User management
- UBA: Resource access
- UEBA: Risk score

ManageEngine

Thank you!

Derek Melber

derek@manageengine.com