

Compliments of:  
**ManageEngine**

# Detecting Insider Threats & Attacks

for  
**dummies**<sup>®</sup>  
A Wiley Brand



Monitor/alert  
attacks in real time

Reduce false  
positive alerts

Apply user behavior  
analytics

**ManageEngine**  
**Special Edition**

**Derek Melber, MVP**

# About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan, and China.



# Detecting Insider Threats & Attacks

ManageEngine Special Edition

**by Derek Melber, MVP**

for  
**dummies**<sup>®</sup>  
A Wiley Brand

# Detecting Insider Threats & Attacks For Dummies®, ManageEngine Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

[www.wiley.com](http://www.wiley.com)

Copyright © 2020 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, Dummies.com, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. ManageEngine and the ManageEngine logo are trademarks or registered trademarks of Zoho Corp. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY:** THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact [info@dummies.biz](mailto:info@dummies.biz), or visit [www.wiley.com/go/custompub](http://www.wiley.com/go/custompub). For information about licensing the *For Dummies* brand for products or services, contact [BrandedRights&Licenses@Wiley.com](mailto:BrandedRights&Licenses@Wiley.com).

ISBN 978-1-119-65686-9 (pbk); ISBN 978-1-119-65685-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

**Project Editor:** Martin V. Minner

**Acquisitions Editor:** Ashley Coffey

**Editorial Manager:** Rev Mengle

**Business Development**

**Representative:** Karen Hattan

**Production Editor:**

Mohammed Zafar Ali

# Introduction

---

**S**tudies, reports, and results show that insider threats and attacks still outnumber attacks from outside the organization. The obvious reason is that the insider has immediate access to the network, with credentials to access the network. Both of these are requirements to perform an attack, and insiders have both by default.

Then why can't insiders be detected when performing an attack? The answer lies in the default access. If a user has credentials and access to the network, how is it possible to delineate between good behavior and bad behavior? Security professionals and administrators have been trying to solve this dilemma for years.

The good news is that some distinct attacks can be monitored and alerted in real time. These attack detections are 100 percent accurate and can help organizations against insider attacks. However, without additional technologies, most attacks can't be 100 percent verified. Many organizations use security information and event monitoring (SIEM) solutions, which provide technologies such as thresholds, rules, and correlation, but are not always 100 percent precise in their detections.

# About This Book

Many organizations are turning to user and entity behavior analytics (UEBA) and user behavior analytics (UBA) to help their SIEM detect attacks with a broader scope and with more precision. UEBA/UBA can detect what a traditional SIEM can't by looking for strange behavior of the user, referred to as *anomalies*, that can indicate clear attacks.

In this short book, I look at use cases on how you can detect, with 100 percent accuracy, insider threats and attacks using traditional SIEM technologies, as well as UEBA/UBA technologies and concepts.

## Icons Used in This Book

I sometimes use icons to call attention to important material. Here's what to expect:



TIP

This icon points to advice and other helpful, useful tidbits of information.



REMEMBER

When you see this icon, I'm giving a friendly reminder of useful information.

- » Knowing the foundation for attacks
- » Monitoring user accounts
- » Recognizing changes that indicate attacks

# Chapter 1

## Detecting Logon Attacks

**M**any organizations track logon failures. The tracking of the logon failure can assist in forensics and in the detection of a brute force attack. However, I find that most organizations are missing one of the most powerful indicators of an insider attack.

Before you can begin detecting the attack, you must understand the foundation for this attack. I focus on Microsoft Active Directory (AD) because it's the most-used network operating system for identity and access management around the world.

Every employee who has an Active Directory user account has the capability to get a list of all other user accounts in the database. In the same manner, every employee can get a listing of every AD group and its members. This includes Domain Admins, Enterprise Admins, Schema Admins, and Administrators groups.



TIP

Any Lightweight Directory Access Protocol (LDAP) or PowerShell call can obtain the list of users and group members.

## Detecting Attacks on Accounts

Ideally, attackers want to gain access to the network as a privileged user account. It makes sense that the attacker in this scenario will try to log on as one of the user accounts that are located in the privileged groups.

Now that you understand the foundation for the attack, here are some ways to detect the attack.

### Administrator accounts

Administrators are keen on knowing where they are and when they are logging on. Thus, simply monitoring for when his or her own user account fails to log on gives an administrator a clear indication of being under attack.



Here are indicators that an administrator user account is under attack:

- » If an administrator is typing an e-mail and receives an alert that his or her user account failed to log on.
- » If an administrator is out of the office attending an event and receives an alert that his or her user account failed to log on.

## Privileged accounts

*Privileged accounts* are those accounts that can do more than a standard user account. These accounts are typically used for database administration, e-mail administration, server administration, and so on. These accounts are not “admin”-level administrators but clearly have the ability to manage key aspects of the network.

In the same light as the administrators from the previous example, these user accounts have limited times during which they log on; this especially includes when they experience failed logons. Continuing the approach from the preceding use case, here are some examples of when one of these accounts is clearly under attack:

- » When the SQL database administrator is on leave, and an alert is triggered that his or her user account has a failed logon.

- »» When an administrator is working at the New York office, and a failed logon attempt registers on a desktop located in the London office.

## Service accounts

Another type of user account that can show clear indications of attacks are the service accounts. *Service accounts* are user accounts used to help services authenticate in order to access the network, other servers, and even other services. Most network services require service accounts, such as SQL, Exchange, SharePoint, and so on.

## Best practices for safeguarding accounts

Here are a few best practices for service accounts:

- »» Service accounts are not human and therefore can't change their own passwords. Ideally, you should set the service account to not be able to change its password.
- »» Service accounts are configured to function within the service itself. Therefore, the service account does not need the ability to interactively log on

(from the keyboard). Ideally, configure the service account to not be able to log on interactively.

- » Don't use the built-in Administrator account.

Even if you don't have these best practices configured, you can still get clear indications that a service account is under attack. The following are clear indications that your service account is under attack:

- » You have limited the service account to log on to Server10 only, but a logon failure registers from Workstation100.
- » You have an alert indicating that a service account failure has registered from Workstation9.
- » The service account is configured for the ACME Service running on Server50 located in the New York office, but a logon failure registers from a workstation in London.

## Monitoring Non-Privileged User Accounts for Failed Logons

Ideally, you want to monitor as many user accounts as possible for failed logons. The core requirement is that

there must be some knowledge of the parameters for the user account logons. If you monitor all user account logon failures and attempt to receive an alert for any failed logon, this results in too many alerts that do not provide a clear indication of an attack.

For example, if Sally's user account has a logon failure at 8 a.m. Monday, what indicates whether this is Sally failing to type her password correctly, or an actual attack? With no better information regarding Sally's user account, the alert is potentially a false positive indication of an attack.

In this case, for non-privileged user accounts, a better plan might be to use thresholds to help indicate an attack. For example, if a user has four failed logon attempts in 15 seconds, most administrators would want to be notified of this activity.



TIP

Ensure that your logon failure threshold is below your account lockout threshold. If your lockout threshold is set to three and your failed logon attempt threshold is four, you will never receive an alert that the user account has received four failed logon attempts because the account will be locked out first.

# Detecting Domain Privileged Group Changes

Another area within a Windows Active Directory enterprise where it's easy to spot attacks is related to privileged groups. Every AD installation has the same privileged groups installed out of the box (OOB), so attackers know where to target. However, organizations need to look beyond these OOB privileged groups to ensure they're monitoring all privileged groups that might be compromised.

Privileged groups can be divided into three categories: built-in, service/application, and custom.

## Built-in privileged groups

These are groups installed at the time AD is initially installed. The list of built-in privileged groups that must be monitored include:

- » Administrators
- » Domain admins
- » Enterprise admins
- » Group policy creator owners

## Service and application groups

Service and application groups can vary widely from organization to organization. This is due to some organizations needing more services and applications to run their business than other organizations might need. The key, however, is that the groups created to manage and administer the installed services and applications must be documented and monitored for changes. Examples of these groups might include:

- » Exchange admins
- » SQL admins
- » SharePoint admins

## Custom groups

Administrators often rely on groups they create manually to set permissions and to restrict or allow access for administration. Yes, built-in groups exist for this purpose, but nearly all organizations create custom groups related to their business instead of relying solely on the Microsoft groups. In nearly all cases, these custom groups are members of the built-in groups, but the custom groups are used by the administrators to grant permissions and privileges. These groups also must be documented and monitored for group changes.

# Detecting Domain Privileged Group Attacks

Now that you understand the different types of privileged groups, all you need to do is monitor the groups for changes. Yes, you also need to know the group membership to be sure an unknown change is an attack, but any administrator should desire that. If the current group members are not known, these steps can help you verify the group members and ensure they're correct:

- 1. Get a listing of each group's members, down to the user level.**
- 2. Give the list to the group owner to have him or her verify the correct members.**
- 3. Update the group with the correct members.**



**TIP**

To get a listing of each group down to the user level, you can either use a command line tool like PowerShell or a graphical tool like ADManager Plus.

With the group membership correct, your next step is to monitor for changes and be alerted when a change occurs, as shown in Figure 1-1. Here are some use cases that clearly indicate an attack:

- » Your organization has only three domain administrators, and you are alerted that a user account

from finance was just added to the Domain Admins group.

- » A group has been created that only contains service accounts, and then an alert is generated indicating that the head of HR's user account has just been added to this group.
- » The company decided only two users should administer Exchange, and then an alert indicates a user account from the sales force has been added to the Exchange Admins group.

WHEN ▾	WHERE	ACCOUNT NAME	ACCOUNT DOMAIN	CALLER USER NAME	MESSAGE
Jun 20, 2019 11:41:37 AM	WINDOWS7	Administrators	ADSOLUTIONS.DEMO	derek	Member 'Domain Admins' was added to Domain Local Security Group 'Administrators' by 'ADSOLUTIONS\derek'.

**FIGURE 1-1:** A local group change.

## Detecting Local Administrators Group Changes

In a similar fashion to the domain privileged groups, a local privileged group, Administrators, is on every workstation and non-domain controller server in the Windows enterprise. The local Administrators group is a default group. All members of this group can control the



computer on which it is located and have full control over any aspect of the computer.

As with the domain privileged groups, the membership of the local Administrators group on each computer should be known. If the membership is known and the best practices for the membership are upheld, then any change to this group helps indicate an attack.

Here are some best practices for the local Administrators group on each computer:

- » Membership should only include domain admins and the local administrator account.
- » No user account, local or domain, should have membership in this group.
- » In rare cases, if an enterprise application is used to manage computers, a service account for this application can have membership in this group.

- » Reviewing SIEM rules, thresholds, and correlations
- » Knowing what SIEM won't detect
- » Checking out UBA use cases

# Chapter 2

## Utilizing and Expanding SIEM Technologies

**N**ow that the local Administrators group is restricted to Domain Admins, other service accounts, and the local Administrator account (see Chapter 1), the membership of these groups should not change unless an “admin” makes the change. Therefore, if any alert is triggered from monitoring changes to any local Administrators group on any Windows computer, it is a clear indication of an attack.

In this context, *Windows computer* includes all domain-joined Windows computers, minus domain controllers. This includes all your member servers and workstations. Because the membership of the local Administrators group should not change, alerts will be rare. If alerts occur, they will stand out from other alerts, and the IT staff can take immediate action.

## What SIEM Rules Work Well and Where They Can Fail

Security information and event management (SIEM) *rules* are the most basic of what a SIEM solution evaluates, monitors, and alerts on. SIEM rules typically look at single events to set off triggers that inform IT about a possible issue.

As an example, consider failed logons for users within your Active Directory (AD) domain. Assume you're at an event and out of the office for the day. During the event, you receive an email from your SIEM solution indicating that your user account has had a failed logon attempt from a computer on your corporate network.

This logon failure has only one possible cause: The reality is, you're under attack.

You can now take action by looking at the details of the attack, where the attack originated from, and if there are any other logon failures.



REMEMBER

All privileged accounts should be monitored for logon failures. Any logon failure for a privileged account that isn't accounted for is clearly an attack.

This rule for failed logons falls short if you monitor all failed logons and set up the SIEM to send alerts for any user account having a failed logon. Users often forget their password one or more times, so receiving failed logon alerts for standard users wouldn't provide much information.

## What SIEM Thresholds Work Well and Where They Can Fail

SIEM solutions also come with *thresholds*. These give you the ability to set up the system to look for a repeated event, which then can trigger an alert. In many cases on a typical network, a single event doesn't mean much. However, the same event triggered multiple times in a short time might indicate an attack.

If I take the example from the previous section on SIEM rules and expand on it, you can see how SIEMs can utilize thresholds. The previous example regarding failed logons

came up short when you looked at standard users. However, what if there were four failed logons in 15 seconds? This could surely indicate the user account is under attack.

Being able to set up a SIEM to look for repeated events for the same user account or device can give you additional information where a standard rule would not.



TIP

Don't set the threshold so low it triggers false positives. However, don't set the threshold so high it misses the alert because the threshold is never reached. This might happen if the lockout threshold of the password policy is set to five, and you set the logon failure threshold in your SIEM to six.

This SIEM feature fails if the user account is accessed in fewer failures than the threshold. If the account is truly under attack, and the attacker accesses the user account successfully after only three attempts, but you have the threshold set to four, the alert would never be triggered.

## What SIEM Correlations Work Well and Where They Can Fail

SIEM solutions provide another useful feature. *Correlation* is an advanced technique that does not look at a single event, nor even repeated events like thresholds. Instead,

correlation is capable of looking at events in sequence, across many devices.

Correlation is a reverse-engineered sequence of events organized in the SIEM, so the SIEM can look for the pattern of events representing the attack.

These events can be logon failures or successes, installation of applications, starting of a service, creation of a user account, modification of permissions, and so on. Here's an example where correlation might clearly indicate an attack:

1. A standard user account shows four failed logons within 15 seconds, followed by a successful logon in the next 15 seconds.
2. Within a minute, the user accesses a file server and installs a service.
3. After installing the service, the user account is added to a local group that has privileges, and then the user is added as the service account for the newly installed service.
4. The final event is when the service is started.

If your SIEM notices this series of events, you would have a clear indication of a potential attack using the service to collect and send information.

This SIEM feature might fail if the actions created are all correct. Often in a small company, user accounts for

employees are configured to run as services. The user could have forgotten his or her password, and then logged in successfully to install and configure the service.



TIP

This is why automatic actions — such as shutting down the server — are often not configured to not disrupt the normal processing of a server in cases where your SIEM might “think” there’s an attack due to correlation events being found.

## An Example of What Traditional SIEM Would Miss

Traditional SIEM solutions do a good job of looking for single events, repeated events, and even complex arrays of events to detect attacks. However, in many cases, a SIEM solution is not designed to look for certain events and situations that clearly indicate an attack.

For example, if a malicious user on your network attempts to log on to every standard user account with just a single password, traditional SIEM solutions fail to notice this.



REMEMBER

Single logon failures for standard user accounts occur all the time, so most SIEMs are not configured to look for them.

# What Is UEBA/UBA?

*User and entity behavior analytics* (UEBA) is a technology that uses machine learning to analyze voluminous amounts of security event data in order to detect anomalous behavior of a user or device.

With that definition, you might wonder how this differs from any other SIEM solution. UEBA works with SIEM solutions but analyzes the information at a different level.

Traditional SIEM solutions and rules look at the incoming events as a singular event or in correlation with other events. When an event or sequence of events is determined, action can be taken. Of course, the action can be running a script, triggering an application, sending an email, or throwing a message up on a computer. This event monitoring is ideal for some situations, such as:

- » Security group membership modifications
- » Privileged user failed logons
- » Service account logons from an unapproved computer
- » An administrator attempting to log on to a non-privileged account workstation (PAW)



User behavior analytics (UBA) doesn't look at events individually. Instead, UBA first looks at each user and myriad behaviors to determine baselines. Behaviors might include failed logons, logon time, logoff time, volume of files accessed in a day, and so on, as shown in Figure 2-1. The baseline becomes the “normal activity” for the user.

Usual Activity Volume based on User

Q Advanced Search 1-12 of 12 25 Add/Remove Columns

USER NAME	ACTIVITY TYPE	TYPE	DOMAIN NAME	12-1 AM	1-2 AM	2-3 AM	3-4 AM	4-5 AM	5-6 AM	6-7 AM	7-8 AM	8-9 AM	9-10 AM	10-11 AM	11AM-12PM	12-1 PM	1-2 PM
derek	Logon Failure Count (Based on User)	Threshold	ADSOLUTIONS.DEMO	1	0	1	0	0	0	0	0	1	0	0	0	0	0
derek	User Management Activity Count	Threshold	ADSOLUTIONS.DEMO	3	9	14	15	3	1	39	9	40	3	3	2	4	2
derek	File Activity Count (Based on User)	Mean	ADSOLUTIONS.DEMO	0	22	0	0	0	0	3	0	18	0	0	0	0	0

**FIGURE 2-1:** Establishing a baseline for normal activity.



**TIP**

Most UBA baselines take 30 days to develop a valid “normal behavior.”



**REMEMBER**

UBA is user behavior analytics, and UEBA is user and entity behavior analytics. *Entity* can represent a computer, switch, router, file server, and so on. In this book, I shorten UBA and UEBA to just *UBA*.

Once you establish a baseline, any additional events that fall under that baseline are evaluated against the baseline. Any new event that falls outside the “normal range”

of the baseline is considered an *anomaly*. Anomalies are triggers for actions to be run, applications to start, emails to be sent, and so on.

## Examining Use Cases for UBA

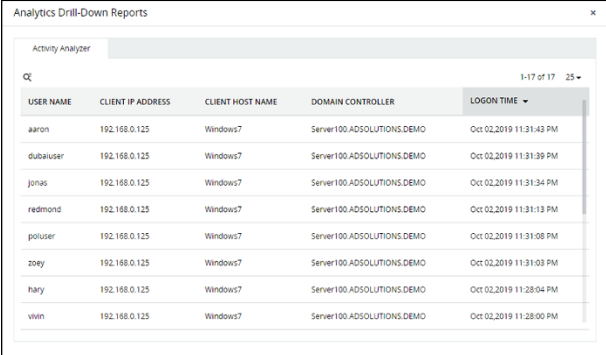
Earlier sections of this chapter explain what your SIEM does well and where your SIEM might not monitor the attacks that are occurring. By adding UBA to your SIEM, you can get more in-depth and widespread information about attacks as they occur. Just like the previous SIEM examples, some are clear indicators of an attack, and others are only indications of a potential attack.

Similarly, UBA has both levels of attack indicators. In this section, I cover two clear indications that an attack is occurring. Having the ability to detect attacks using UBA can alter the way you secure your environment.

### An attack on internal AD user accounts

The first example is an attack on your internal Active Directory user accounts. The attack tries one password against every user account and is referred to as a *password spray attack*. To show the full breadth of the attack and the inability to detect this attack, I cover all aspects of what's required for the attack, how the attack can go

undetected, and how UBA easily detects this attack in real time, as shown in Figure 2-2.



The screenshot shows a window titled "Analytics Drill-Down Reports" with a close button (X) in the top right corner. Inside the window, there is a tab labeled "Activity Analyzer". Below the tab is a search bar with a magnifying glass icon and a dropdown menu showing "1-17 of 17" and "25". Below the search bar is a table with the following columns: "USER NAME", "CLIENT IP ADDRESS", "CLIENT HOST NAME", "DOMAIN CONTROLLER", and "LOGON TIME". The table contains eight rows of data.

USER NAME	CLIENT IP ADDRESS	CLIENT HOST NAME	DOMAIN CONTROLLER	LOGON TIME
aaron	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:31:43 PM
dubauser	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:31:39 PM
jones	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:31:34 PM
redmond	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:31:13 PM
poluser	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:31:08 PM
zoey	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:31:03 PM
hary	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:28:04 PM
vlvin	192.168.0.125	Windows7	Server100.ADSOLUTIONS.DEMO	Oct 02, 2019 11:28:00 PM

**FIGURE 2-2:** Using UBA to detect a password spray attack.

The password spray attack first requires that the attacker first obtain the full list of user account names from Active Directory.



**TIP**

Every user who has an AD user account can get a full list of all user accounts from Active Directory. This is possible because all users have read access to the directory to obtain this information. The simple command: `net group /domain "domain users"` gives you a list of all usernames in the domain.

Once the full list of user account names is obtained, a small batch file is created to try each username against a

single password. This is an ideal attack that most SIEMs fail to catch for the following reasons:

- » Single failed logons don't trigger alerts.
- » Failed logons aren't checked across many user accounts.
- » Failed logons aren't tracked per device.

However, when UBA is incorporated with your SIEM, this attack is found quickly, and an alert is sent to all administrators notifying them of the attack — because UBA is looking for failed logons for a device, which is out of the normal failed logons.

A typical workstation doesn't receive many failed logons in a single day because most users fail to log on a few times a day, at most. However, when the same device has many failed logons during the password spray attack, UBA sees this behavior is outside the normal baseline and causes an alert to be triggered.

## Combining UBA anomalies

A second example is more complex but also indicates a clear attack. This UBA technique involves the concept of combining UBA anomalies into an *over risk score*.

The purpose is to not look at individual anomalies, but to look at the same user or entity having many anomalies in

a short amount of time. A single anomaly might not indicate malicious intent; when many anomalies from the same user or entity occur in a short time, the chances that this is an attack are very good.

In the example, assume the user performs the following actions, all causing anomalies compared to the baselines:

- » Four failed remote logons at 2 a.m. (This causes three anomalies.)
- » A successful remote logon at 2 a.m. (This causes two anomalies.)
- » Installation of a service to the workstation.
- » Starting the local service on the workstation.
- » Accessing more than 1,000 files on a file server.
- » Modification of a registry entry on the local workstation.

Each of these anomalies individually would not trigger any issue with a traditional SIEM. However, when you look at the behavior of the user — accessing the network in the middle of the night, over a remote connection (which is rare for this user), and then accessing ten times as many files as usual — the actions are not normal and likely constitute an attack.

- » Recognizing malicious behavior
- » Preventing future insider attacks

# Chapter 3

## Ten Key Takeaways

Identifying incidents as potential insider attacks is important to stopping those attacks and preventing future ones. To properly identify attacks as such, you must be able to recognize what is truly malicious behavior (indicating a potential attack) and what might be a normal occurrence, like a user forgetting his or her password.

Here are ten key takeaways for keeping your organization safe from insider threats and attacks:

- » **Default access trips up attack detection.**
- » **Privileged account monitoring for failed logons is essential.**

- » User and entity behavior analytics (UEBA) and user behavior analytics (UBA) find anomalies that traditional SIEM technologies don't.
- » User account failed logons must be monitored.
- » Attackers want network access via a privileged user account.
- » Secure service accounts with best practices.
- » Groups must be monitored for changes.
- » Best practices for local Administrators groups must be followed.
- » Service accounts must be monitored.
- » Doing nothing opens the network to successful attacks.

# Free Tools

The chapters of this book give insight into securing and monitoring privileged accounts. Before you begin that tracking and securing, however, you must know who and what has access in your environment. The tools listed in this appendix provide the means to help you accomplish these goals. The tools listed here come with a free 30-day trial:

### » AD Audit Plus

[www.manageengine.com/products/active-directory-audit/](http://www.manageengine.com/products/active-directory-audit/)

### » EventLog Analyzer

[www.manageengine.com/products/eventlog/](http://www.manageengine.com/products/eventlog/)

### » Log360

[www.manageengine.com/log-management/](http://www.manageengine.com/log-management/)

### » AD Manager Plus

[www.manageengine.com/products/ad-manager/](http://www.manageengine.com/products/ad-manager/)



## »» **ADSelfService Plus**

[www.manageengine.com/products/self-service-password/](http://www.manageengine.com/products/self-service-password/)

## »» **DataSecurity Plus**

[www.manageengine.com/data-security/](http://www.manageengine.com/data-security/)

## »» **Exchange Reporter Plus**

[www.manageengine.com/products/exchange-reports/](http://www.manageengine.com/products/exchange-reports/)

## »» **RecoveryManager Plus**

[www.manageengine.com/ad-recovery-manager/](http://www.manageengine.com/ad-recovery-manager/)

## »» **O365 Manager Plus**

[www.manageengine.com/office365-management-reporting/](http://www.manageengine.com/office365-management-reporting/)

# Comprehensive UEBA Solution

ManageEngine Log360 is a UEBA tool which enforces tighter security measures by detecting behavior anomalies, and strengthening your defenses against insider threats and data breaches.

**With over 1000 predefined report and alert profiles, Log360 uses machine learning to defend against:**



Insider  
Threats



Account  
Compromise



Data  
Exfiltration

Try Log360 now!  
[bit.ly/ManageEngine-Log360](https://bit.ly/ManageEngine-Log360)

ManageEngine<sup>®</sup>  
Log360



Scan QR Code



# Active Directory Security Solution

ADAudit Plus is the real-time change auditing and analytics component of Log360 that helps secure your Active Directory, Azure AD, file servers, and other Windows servers.

**ADAuditPlus leverages machine learning to notify security personnel in the event of:**



Malicious  
logins



Anomalous  
change activity



Data  
breaches

Start your 30-day free trial now!  
[bit.ly/ADAuditPlus](https://bit.ly/ADAuditPlus)

ManageEngine<sup>®</sup>  
ADAudit Plus



Scan QR Code



# Detect insider threats and attacks

Many organizations are turning to user and entity behavior analytics (UEBA) and user behavior analytics (UBA) to help their security information and event monitoring (SIEM) solutions detect attacks. UEBA/UBA can detect what a traditional SIEM can't by looking for strange behavior of the user, referred to as *anomalies*, that can indicate attacks. This book shows you how you can detect, with 100 percent accuracy, insider threats and attacks using traditional SIEM technologies as well as UEBA/UBA.

## Inside...

- Detect attacks on accounts
- Monitor/alert privileged user logons
- Track privileged group changes
- Understand SIEM rules, thresholds, and correlations
- Know what SIEMs can't detect
- Leverage user behavior analytics

Go to **Dummies.com™**  
for videos, step-by-step photos,  
how-to articles, or to shop!

**for**  
**dummies**  
A Wiley Brand

## ManageEngine

**Derek Melber** is a 15-time Microsoft MVP and the Chief Technical Evangelist at ManageEngine. He focuses on Active Directory, Group Policy, and security for corporate networks. Derek has written more than 15 books and published thousands of articles and blogs over the years. Derek educates and evangelizes Microsoft technologies to thousands of administrators around the world each year. You can reach him at [derek@manageengine.com](mailto:derek@manageengine.com).

ISBN: 978-1-119-65686-9

Not For Resale



9 781119 656869

# **WILEY END USER LICENSE AGREEMENT**

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.