ManageEngine
ADAudit Plus

Streamlining threat detection through user behavior analytics

www.adauditplus.com

Introduction

Recent high-profile breaches and global ransomware attacks have proved that traditional security tools are not sufficiently equipped to deal with the constantly evolving threats haunting the IT landscape. The 2018 **IBM X-Force Threat Intelligence Index** states that 60 percent of cyberattacks were caused by insider threats, and that two-thirds of total data records compromised were due to inadvertent insiders. Risk factors included excessive access privileges, an increasing number of devices with access to sensitive data, and the increasing complexity of information technology. On top of that, the **Verizon 2018 Data Breach Investigations Report** states nearly 68 percent of all breaches in 2017 took a month or longer to discover. These findings clearly point to the limitations of traditional security tools.

Businesses need to incorporate security solutions bolstered by the latest technologies to stay ahead of the game. **Gartner** predicts that the market for user behavior analytics (UBA) will grow a steep 48 percent by 2020. This growth will be fueled by the demand for insider threat and compromised account detection capabilities that traditional security systems lack. UBA solutions use data analytics and machine learning algorithms to create a baseline of behavior specific to each user. Deviations from this baseline can indicate a potential threat, which means monitoring user behavior can help you quickly detect anomalous activity in your network.

This white paper will discuss the importance of implementing a security solution that incorporates UBA. It will further look at real-world scenarios and how UBA solutions can help detect anomalies in user behavior that traditional security tools miss.

Why UBA is so important

The common thread across various forms of insider attacks is the deviation from a user's normal behavior. These changes to behavior—or anomalies—indicate potential threats. UBA can detect these anomalies and trigger alerts to administrators, even if anomalies rarely occur.

The threat detection capabilities UBA offer:

Efficiency:

Improve detection speed, analyze the impact of security incidents, and respond quickly to them.

Precision:

Move beyond simple rules, and utilize targeted attack detection capabilities for user credential theft and abuse to detect events early in the attack.

Reduced false positives:

With false positive alerts being a source of distraction that delay breach detection, dynamic alert thresholds—which are specific to each user in the organization—become important. UBA calculates the threshold value for each user based on their level of activity instead of using a blanket threshold across all users.

Better threat detection:

UBA solutions rely on the baseline activities of users to identify unusual user behavior that points to potential attacks.

UBA in action

While existing security solutions use static threshold values to differentiate between what is normal and what is not, UBA solutions use an analytical approach—a combination of data analytics and machine learning—to implement dynamic thresholds based on real-world user behavior.

UBA collects information on what users across the organization are doing over an extended period of time. It then creates a baseline of "normal" activities specific to each user. Whenever there is a deviation from the established baseline, the UBA solution considers this abnormal and alerts the administrator.

The cornerstone of UBA solutions is the premise that humans are creatures of habit. So, when an external entity does try to break into the network, it's going to be easy to spot.

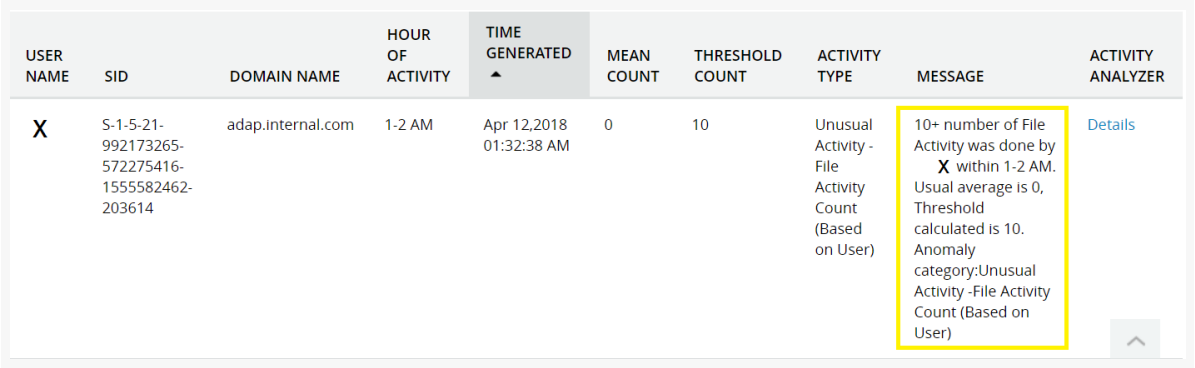
The various stages of UBA are:

- **Collect** information on users over an extended period of time.
- **Model** a baseline of normal activities specific to each user.
- **Define** dynamic thresholds based on real-world user behavior.
- **Find** deviations from the norm.
- **Notify** the concerned security personnel.
- **Update** thresholds continuously based on recent data.

Real-world scenarios

1. Monitoring rogue users

A disgruntled employee departing from the organization wants to steal critical financial information. The employee copies 200 documents containing corporate financial data. Since the user normally accesses around 10 documents a day, this behavior is abnormal. The UBA solution recognizes this abnormal behavior and triggers an alert to the administrator. See Figure 1.



USER NAME	SID	DOMAIN NAME	HOUR OF ACTIVITY	TIME GENERATED	MEAN COUNT	THRESHOLD COUNT	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
X	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:32:38 AM	0	10	Unusual Activity - File Activity Count (Based on User)	10+ number of File Activity was done by X within 1-2 AM. Usual average is 0, Threshold calculated is 10. Anomaly category:Unusual Activity -File Activity Count (Based on User)	Details

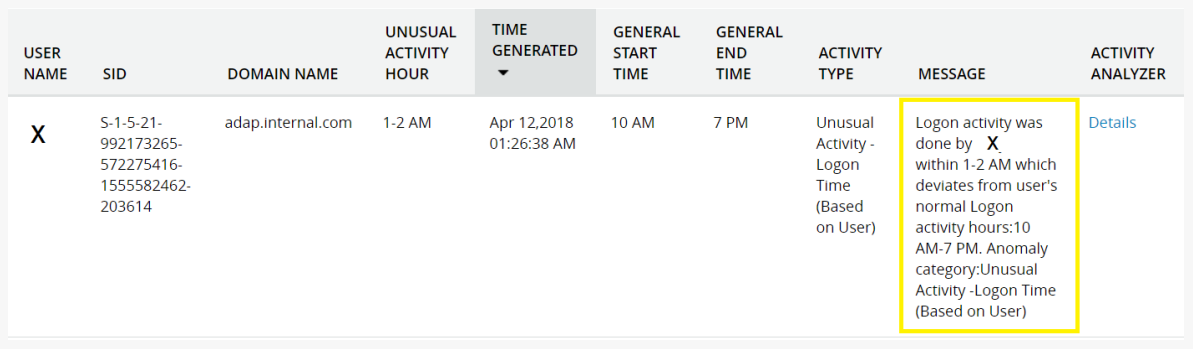
Figure 1. **Monitoring unusual file activity count.**

An auditing solution without UBA capabilities can't establish a baseline of normal user activity to spot abnormalities and would not see this level of file access as strange. However, this is a clear case where the user's activity is abnormal and requires an administrator's attention.

2. Checking for compromised accounts

A disgruntled employee wants to steal important information by using a coworker's credentials. After the coworker goes home for the day, the attacker attempts to log on from the coworker's computer to avoid flagging a logon event from the wrong computer. After several incorrect guesses at the coworker's password, the attacker successfully enters the correct password and logs on.

Having calculated the typical logon time of the coworker for the past months, the UBA solution detects an abnormal logon time. With UBA, not only is the unusual logon time detected, but an alert is raised and sent immediately to the administrator. See Figure 2.



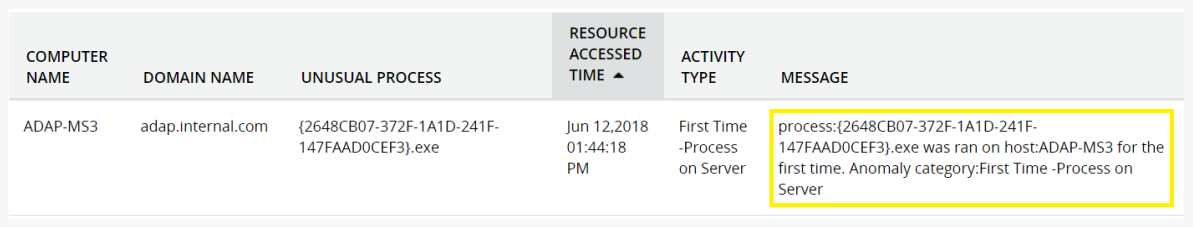
USER NAME	SID	DOMAIN NAME	UNUSUAL ACTIVITY HOUR	TIME GENERATED	GENERAL START TIME	GENERAL END TIME	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
X	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:26:38 AM	10 AM	7 PM	Unusual Activity - Logon Time (Based on User)	Logon activity was done by X within 1-2 AM which deviates from user's normal Logon activity hours:10 AM-7 PM. Anomaly category:Unusual Activity -Logon Time (Based on User)	Details

Figure 2. **Monitoring unusual logon activity time.**

Without a UBA solution, a traditional SIEM solution would not consider the logon abnormal, as it was a successful logon from the user's own computer.

3. Detecting unusual processes on member servers

An employee gets a malicious application installed when browsing the internet. He then connects to the server, where he has administrator privileges, to perform administrative tasks. The application moves laterally and installs on the server. The application launches a process in the background. The UBA solution detects this new process on the server and triggers an alert. More quickly detecting an attack enables administrators to mitigate its impact.



COMPUTER NAME	DOMAIN NAME	UNUSUAL PROCESS	RESOURCE ACCESSED TIME ▲	ACTIVITY TYPE	MESSAGE
ADAP-MS3	adap.internal.com	{2648CB07-372F-1A1D-241F-147FAAD0CEF3}.exe	Jun 12,2018 01:44:18 PM	First Time -Process on Server	process:{2648CB07-372F-1A1D-241F-147FAAD0CEF3}.exe was ran on host:ADAP-MS3 for the first time. Anomaly category:First Time -Process on Server

Figure 3. **Detecting first-time processes on member servers.**

Summary

UBA is one of the fastest-growing areas within enterprise security as it leverages existing normal user behavior to detect threats. UBA in ADAudit Plus can track normal behavior for users and devices to detect unusual file access, logon times, and even first-time processes starting on a server. Without UBA these attacks and breaches would go unnoticed, and the network would be compromised. **ADAudit Plus** gives organizations the advantage to react to threats faster and with better precision.