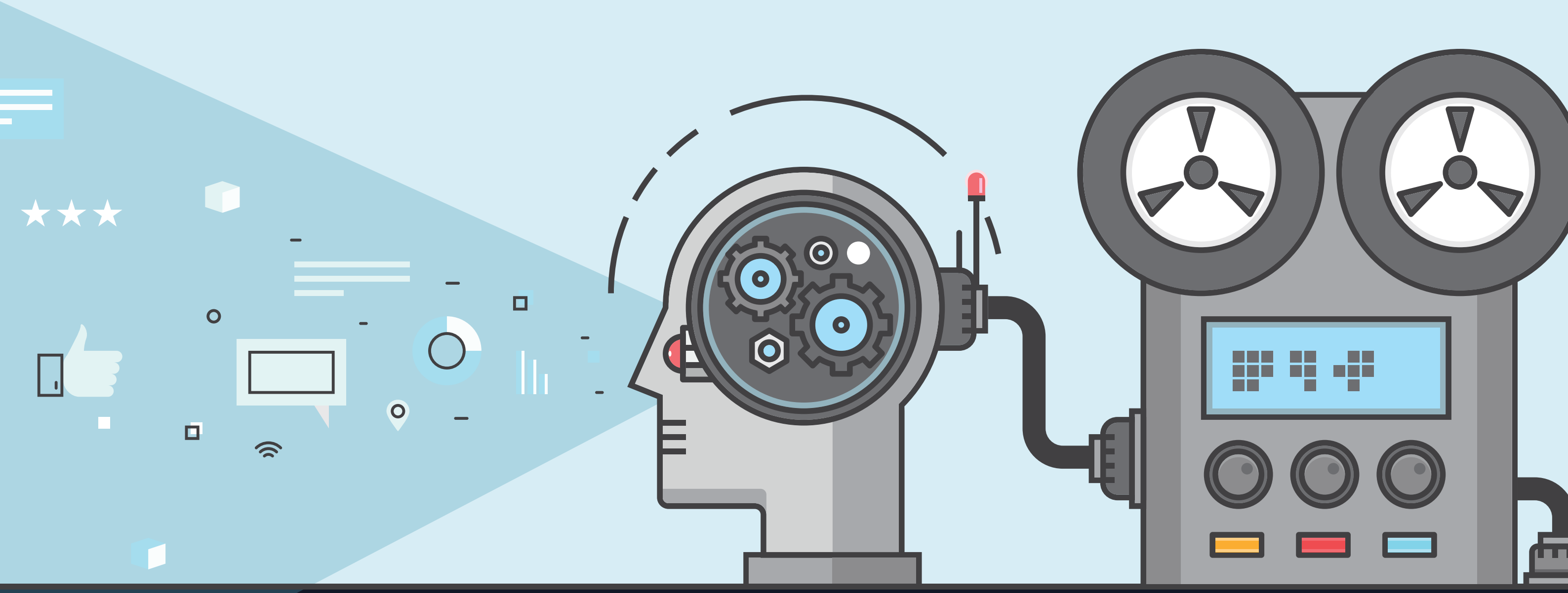
ManageEngine
ADAudit Plus

5 THINGS YOU SHOULD KNOW ABOUT

User Behavior Analytics (UBA)



www.adauditplus.com

As the threat landscape continues to evolve at an alarming rate, Gartner predicts that the market for user behavior analytics (UBA) will grow at a steep 48 percent CAGR between 2015 and 2020. So if you're not familiar with UBA already, it's about time you got acquainted. The following five topics will tell you everything you need to know about UBA.

1. What UBA has to offer

Behavioral analytics was first applied in the field of marketing to help companies understand and predict consumer buying patterns. Today, behavioral analytics is used to detect potential threats in the cybersecurity space. Two key findings from the 2018 Verizon Data Breach Investigation Report reveal why UBA has become so popular:

- **Twenty-eight percent of all breaches involved internal actors.** Existing security solutions are predominantly designed to protect enterprises against external threats, not trusted employees. By focusing on external threats, enterprises often overlook rogue insiders abusing access, as well as attackers who have become very good at looking like ordinary employees once they're inside the corporate network. This is where a UBA solution differs from traditional security tools; by focusing on the behavior of users within an enterprise, UBA provides defense from internal threats.

- **Sixty-eight percent of all breaches took a month or longer to discover.** This delay in detecting threats is because of the large number of false positives that existing security solutions create, resulting in security professionals missing out on a critical alert in a haystack of insignificant warnings. Caught between setting lower threshold values for alerts and triggering a lot of false positives, or configuring higher threshold values and missing a threat, security professionals more often than not choose the former. UBA solutions reduce the number of false positives and buy ample time for security professionals to focus on the real indicators of compromise.

2. How UBA works

- UBA solutions first collect information on what users across the organization are doing over an extended period of time. They then create a **baseline of "normal" activities** specific to every single user. And finally, whenever there is a deviation from that norm, the solution notifies the concerned personnel.

- While existing solutions use static threshold values defined by humans to differentiate between what is normal and what is not, **UBA solutions use an analytical approach (read: a combination of data analytics and machine learning) to define dynamic thresholds based on real-world user behavior.**

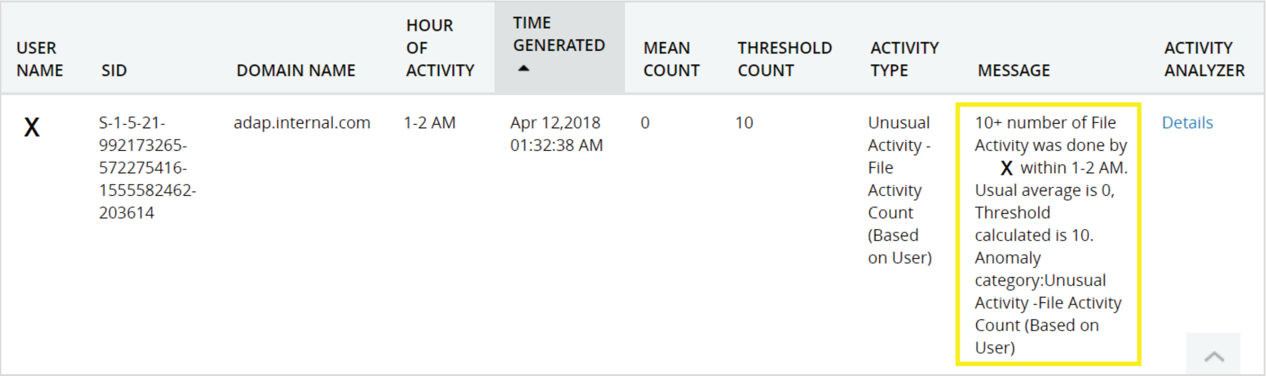
- The cornerstone of UBA solutions is the premise that **human behavior is hard to mimic.** So, even when an external entity does manage to break into a network, it's going to be hard for them to mimic another person's daily behavior.

By looking at how UBA solutions detect common breach scenarios that fly below the radar of existing security solutions, we can gain a better understanding of UBA. The following breach scenarios cover the entire threat spectrum: from an insider gone rogue, to an attacker who has just gained a foothold within the network using compromised credentials, to an all-out external threat.

3. UBA vs. rogue insiders

- **A common scenario**
  A disgruntled employee departing from the organization decides to exfiltrate data. They know the location of critical documents and decide to copy a handful of only the most important files, careful not to trigger the organization's alerting system based on file activity volume.
- **Indicator of compromise: Unusual file activity count**
- **How UBA helps**

Because of the low volume of file activity, this breach would go undetected if not for a UBA solution. The UBA solution, though, knows how many files the user usually accesses at that particular time of day based on their past behavior. Since there will clearly be a spike in file activity compared to past behavior, the UBA solution notifies the concerned security personnel.



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

4. UBA vs. compromised accounts

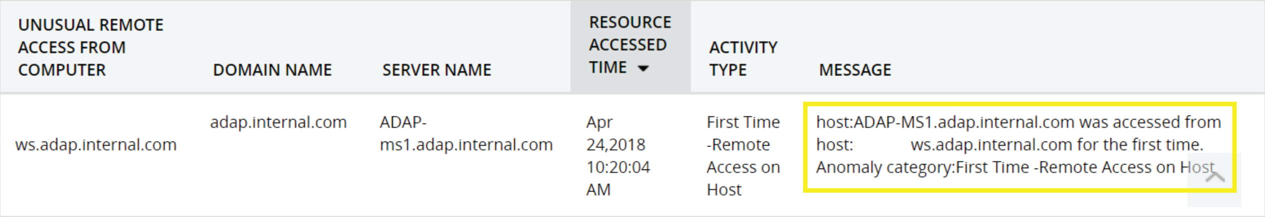
- **A common scenario**

  An attacker with stolen credentials wants to widen his control within the network, so he targets other systems using RDP to gain remote access to other hosts on the network. The attacker knows that administrators typically check for a high volume of failed logins to detect such attacks, so he's careful not to cause many failed logons and in the process trigger a logon failure volume-based alert.

- **Indicator of compromise: Unusual logon activity—First time remote access on host**

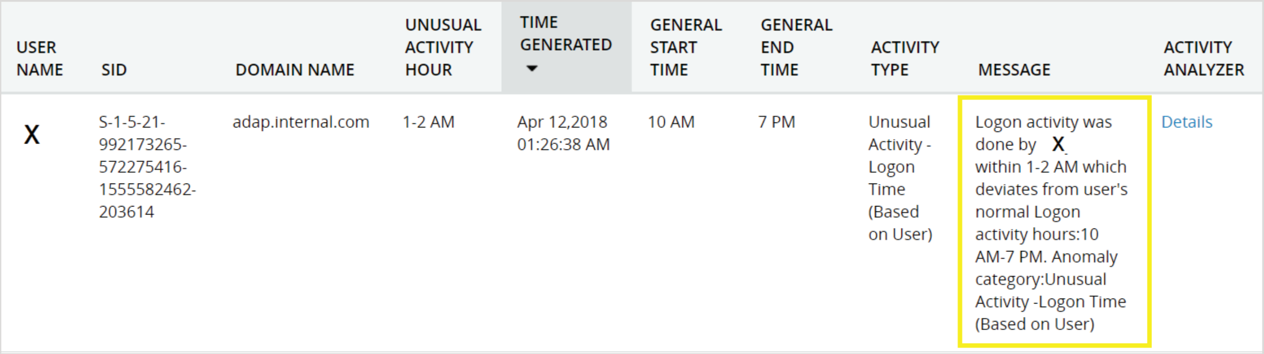
- **How UBA helps**

Because of the low volume of logon failure activity, this breach would fall under the radar of existing security solutions. The UBA solution, however, raises an alert because hosts on the network were accessed for the first time by a remote logon from the attacker's client machine.



UNUSUAL REMOTE ACCESS FROM COMPUTER	DOMAIN NAME	SERVER NAME	RESOURCE ACCESSED TIME ▾	ACTIVITY TYPE	MESSAGE
ws.adap.internal.com	adap.internal.com	ADAP-ms1.adap.internal.com	Apr 24,2018 10:20:04 AM	First Time -Remote Access on Host	host:ADAP-MS1.adap.internal.com was accessed from host: ws.adap.internal.com for the first time. Anomaly category:First Time -Remote Access on Host

What's more, unaware of when the insider whose credentials they're using usually logs on, the attacker also triggers an unusual logon activity alert.



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

5. UBA vs. external threats

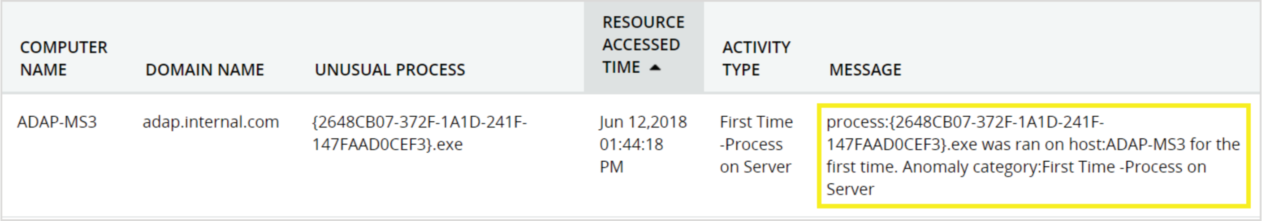
- **A common scenario**

  An employee clicks on a malicious link, immediately downloading malware that encrypts their data and starts spreading across the network.

- **Indicator of compromise: Unusual process—New process on host**

- **How UBA helps**

While existing solutions could detect ransomware once data encryption starts, the UBA solution detects ransomware before files are even encrypted. Immediately after the malicious program is downloaded, the UBA solution detects a new process on the host and triggers an alert. Faster ransomware detection thanks to UBA enables admins to better mitigate the impact of the attack.



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

ADAudit Plus' UBA module helps detect all three of the above breach scenarios and more.

Schedule a one-on-one demo now.

ManageEngine ADAudit Plus is an IT security and compliance solution listed in Gartner's Magic Quadrant as a part of the Log360 suite. With over 200 event-specific reports and real-time alerts, ADAudit Plus provides comprehensive information on changes to both the content and configuration of Active Directory (AD), Azure AD, and Windows servers. Additionally, it provides thorough access intelligence for workstations and file servers (including NetApp and EMC).

$ Get Quote

Download

☎ Toll Free
+1 844 245 1101

Direct Dialing Number
+1-408-916-9891

✉ support@adauditplus.com

www.adauditplus.com