ManageEngine
Log360

Securing business data by integrating UEBA and Zero Trust

www.manageengine.com/log360

Table of contents

Executive Summary

Since the start of the pandemic, organizations worldwide have faced an increasing number of IT security challenges. Cyberattacks targeting employees are now more common, and the threat actors' tactics are now more sophisticated.

Globally, we've seen persistent insider attacks that are difficult to detect because the users have already been granted legitimate access to an organization's sensitive and critical data. Traditional rule-based and signature-based attack detection systems often fail to uncover many insider attacks, and this is complicated by the human element often now associated with them.

Cybersecurity frameworks, like user and entity behavior analytics (UEBA), leverages machine learning (ML) and artificial intelligence (AI) techniques to analyze user behavior and establish a baseline of normal behavior. This is used to detect any anomalies and differentiate them from normal behavior, giving organizations enhanced capabilities to thwart sophisticated insider attacks. When UEBA is combined with Zero Trust architecture, an identity-based security hardening technique, it can be used to circumvent most attacks that originate from within the network.

01 Rising insider threats and attacks

Insider threats or attacks are a cybersecurity risk by current and former employees, or anyone within the organization who exploits their legitimate user credentials. The impacts are serious as these individuals evade the defense system with their legal access to the organization's sensitive and critical data.

Insider threats can lead to:

1. Data breaches that can result in loss of critical or sensitive data
2. Legal or compliance issues due to data breaches
3. Serious financial impacts on the organization
4. Repercussions to an organization's reputation and a negative impact on customer loyalty

Types of insider attack

Insider attack can be broadly classified based on the intent of the user or insider involved.

1. **Compromised insider:**
   These are users whose credentials have been compromised or whose computer has been infected, with malware, for example. A common attack vector, or hacker exploitation strategy, is a phishing attack where the compromised insider clicks on a malicious link or links.

2. **Negligent insider:**
   Negligent insiders are those who do not follow proper cyber hygiene practices and IT procedures. For example, these can be employees who do not lock their computers while stepping away, or an IT administrator who failed to apply a security patch.

3. **Malicious insider:**
   Malicious insiders are the employees who steal information and disrupt normal activities on purpose. These might be employees who look for financial gains, or a disgruntled employee taking it out on the organization.

Anatomy of an insider attack

Let's take the example of a negligent employee, Edna, who works in a managerial position but doesn't lock her computer when she is away. Lately, working out of a cafe during the pandemic as a break from her mundane remote working routine, she happened to make a friend, Ryan. During one of their conversations, she mentioned that she handles critical information for her team. Ryan accurately guessed that Edna has privileged access to this information. When Edna stepped away, Ryan noticed that she does not lock her system, and schemed to take advantage of this neglectful security practice. Waiting for the perfect opportunity, Ryan had a USB drive handy, copied the critical data to it when Edna was away, and arranged to sell it to an external agent for a lump sum.

02 Need to account for the human element

Organizations are looking at investing in technologies that can help combat cyberthreats. But malicious entities often succeed when executing cyberattacks due to human ignorance, laziness or misjudgment, and this is not generally considered while devising a security strategy.

Let's take Edna's case as an example.

She shouldn't have left her computer unlocked during her time away. She shouldn't have discussed the nuances of her work with Ryan. Even after Ryan gained access to the data, he shouldn't have been able to use a portable storage device. If use of an USB device cannot be avoided in an organization, Edna's computer drive should be encrypted, which would make it almost impossible to access the files.

If continuous monitoring and appropriate cyber solutions were in place, the IT admins would've been notified about this suspicious activity so that the attack could've been deflected.

As attackers exploit human imperfection and carelessness to launch their attacks, it is necessary for cybersecurity professionals to factor in the human element while deploying cybersecurity frameworks. The strategies can be educating people about good cyber hygiene practices, regularly analyzing normal human behavior to detect deviations, and implementing authentication models that verify the identity every time before granting access.

03 The role of UEBA in cybersecurity

UEBA leverages the predictability of human behavior to detect and identify anomalous behavior of users in machines and other entities in the network, which can indicate an insider attack. For example, an employee attempting to download a large amount of sensitive data outside of their normal working hours could be a potential threat, and the IT admin can take the necessary actions to tackle it. Activities of the users are monitored to create a baseline of normal behavior. Any deviations denote possible malicious activity within the network. Organizations can prioritize high-risk threats based on the score assigned to denote the intensity of the threat.

UEBA solutions also address other entities, such as routers, servers, and endpoints in the network which traditional UBA solutions lack. This provides a considerable edge over using UBA solutions in the current cybersecurity landscape, since machine identities are growing in volume and outnumbering human or user identities within the network. UEBA solutions can also help detect a broader range of attacks including DDoS attacks, brute-force attacks, data exfiltration, and a wide range of insider attacks.

04 Cyber safety at the intersection of UEBA and Zero Trust

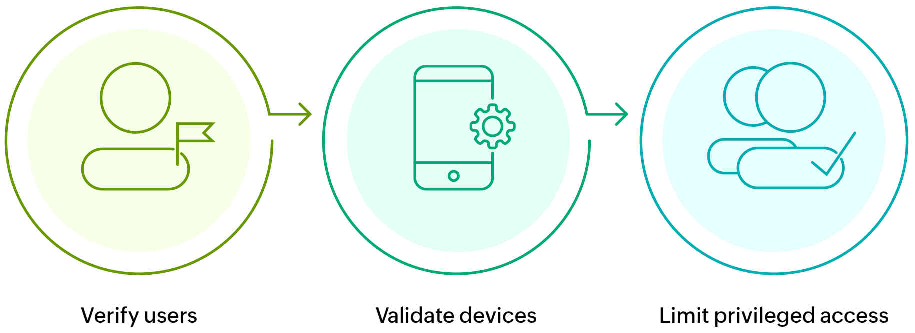
To close the human gap in cybersecurity, it is crucial to integrate the technological aspect of cybersecurity with the human element. To achieve this, it may be necessary to bring together another framework called Zero Trust architecture with UEBA.

Zero Trust

1. **Prevents unauthorized access to data, services, and application:**
   A Zero Trust approach eliminates the idea that trust is binary, and believes that attackers can be present both inside and outside the network perimeter.

2. **Access control and security decisions are made as granular as possible to ensure least privilege:**
   The policy of least privilege grants access only to the data and resources that are essential for carrying out a specific task. This requires access control and security decisions to be granular to prevent exposure to the sensitive and vulnerable parts of a network.

Zero Trust Security Model



How UEBA fits into a Zero Trust architecture

A solution that can defend the network against both internal and external attacks is the need of the hour for organizations. Zero Trust architecture focuses on eliminating the idea of implicit trust within the network. Providing a solution that can identify and thwart attacks originating within the network is required as attackers need not always come from outside the network. Continuous monitoring is a core aspect of Zero Trust and UEBA leverages this by continuously monitoring and collecting data from across the network to create a baseline of normal behavior. UEBA is also very effective since the collected data includes a wide variety of use cases and sources. This way, Zero Trust architecture can be customized to integrate UEBA and effectively close the human gap in cybersecurity.

05 Checklist for a good UEBA solution

Here are some core capabilities to evaluate for a UEBA solution:

a. Data collection and analysis
b. Gaining context to reduce false positives
c. Score-based risk assessment
d. Detect insider threats, data exfiltration, and account compromise
e. Automated alerts and threat response
f. Actionable reports

Data collection and analysis

The basic functions of any UEBA solution include collecting and analyzing data of users, machines, and other entities in a network, like event logs and packet capture data.Any anomalous behavior within the network can be detected by continuous monitoring and analysis of data from different sources.

Gaining context to reduce false positives

A UEBA solution gains the intelligence to detect threats with precision by correlating multiple actions of a user to uncover and identify suspicious patterns to draw a baseline of normal behavior, thereby reducing false positive alerts. Contextual data includes the user's identity information, geolocation, external threat intelligence, and other data which will ensure that the alerts are accurate.

Score-based risk assessment

UEBA makes it easy to prioritize incident responses to tackle the most dangerous threats with its score-based risk assessment. Since UEBA solutions flag a sizable number of suspicious activity within the network, the score-based risk assessment simplifies the prioritization with its risk score for every single user or entity profile within the network. The risk score increases every time there is a deviation from the normal behavior, which will help to prioritize high-risk incidents to attend to immediately and prevent potential security incidents.

Detect insider threats, data exfiltration, and account compromise

A UEBA solution is deployed to detect insider threats and create alerts for activities associated with data exfiltration, and account compromise.

Signs that indicate potential insider threats:

- Access at odd hours and unusual times
- Unauthorized file access and modification
- High frequency of authentication failures within a specific time period
- Abnormal or anomalous access patterns

Signs which indicate possible data exfiltration:

- Multiple USB drives and external storage devices plugged in by the user
- Suspicious commands executed by the user
- Logon activities from unusual locations
- Abnormal download patterns

Signs to identify compromised accounts:

- Multiple instances of software installed on a specific host
- Multiple login failures
- Irregularity in access locations
- Installation of unauthorized software

Automated alerts and threat response

A good UEBA solution must be able to send out automated alerts and notifications when malicious activity is detected so that the IT security team would be able to respond right away and defuse the threat. They can integrate AI and ML algorithms to automate alerts and the threat response. Leveraging ML techniques to deduce a pattern of user and entity behavior is a core feature of any UEBA solution. ML algorithms help a great deal in analyzing data from different sources, and draw a baseline of normal behavior based on patterns in the behavior of users and entities.

Actionable reports

Consolidating the gathered data into easy to view and actionable reports is another critical function of a UEBA solution. Regular review of reports helps spot false flagging within the network and provides insights on how to customize a UEBA solution to comply with an organization's security norms.

06 Conclusion

Zero Trust architecture is becoming a fundamental security requirement for most organizations as insider threats are becoming more prevalent. Accounting for the human element becomes a key aspect, since humans form the weakest link in the cybersecurity chain. Making UEBA part of your Zero Trust strategy will help your organization monitor what goes on within the network. Integrating UEBA into Zero Trust architecture can bridge the human gap in cybersecurity and secure businesses from attacks within and outside the organization.

ManageEngine

Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

Schedule a demo

Download