WHITE PAPER

10 REASONS TO AUGMENT YOUR SIEM WITH BEHAVIORAL ANALYTICS

User and Entity Behavior Analytics (UEBA) is one of the fastest-growing areas within enterprise security, growing at a compound annual growth rate of 48% per year, according to Gartner. Modern enterprise IT security solutions use this technology to detect and remediate advanced threats that are unable to be addressed by traditional solutions. UEBA solutions ingest operational data from many sources, and use analytics such as machine learning and behavior analysis to determine what is "normal" behavior by users and entities on an enterprise network. Entities may include IT assets such as hosts, applications, network traffic and data repositories. The solution builds standard profiles of behavior across peer groups and over time in order to create a baseline. As anomalous activity is identified, it is assigned a risk score. The score rises with increasing amounts of anomalous behavior until it crosses a predefined threshold. Upon this escalation, UEBA sends an alert to Security Operations Center analysts who use the data for appropriate remediation of threats.

WHY BEHAVIORAL ANALYTICS SHOULD BE PART OF YOUR ORGANIZATION'S SECURITY FRAMEWORK

Today's attacks are increasingly sophisticated, and often invisible to traditional rule based security solutions. You read about these successful breaches almost on a daily basis. Security analysts do what they can with incumbent tools, but these tend to swamp analysts with alerts that lack context and are useless in the rapid detection and remediation of compromised credentials and lateral movement of attackers.

The advanced analytics of a modern UEBA solution employ a different approach by using variations of artificial intelligence and machine learning, data enrichment, and data science to effectively combat advanced threats. This modern UEBA solution combines all the data sources together for analysis and automatically synthetizes results. Analysts get a lower volume but higher fidelity feed instead of drowning in alerts.

The organization gets a future-proof solution that looks for abnormalities instead of a limited, predetermined set of activities. Augmenting your SIEM with behavioral analytics is the only way to effectively address the use cases described below.

TOP 10 USE CASES FOR AUGMENTING YOUR SIEM WITH BEHAVIORAL ANALYTICS

1. DETECT COMPROMISED USER CREDENTIALS

User account credentials are keys to legitimate access, and stolen credentials are second only to phishing attacks for data breaches, according to the 2020 Verizon Data Breach Investigations Report (DBIR). When a hacker uses stolen credentials, traditional security tools cannot identify unauthorized access. This scenario allows the attacker to proceed at will to access sensitive data or internal resources. Clearly, the result of compromised user credentials can be devastating, which makes this use case mandatory for augmenting your SIEM with the advanced analytics of a modern UEBA. It's irrelevant how the attacker obtained the credentials – security tools must be able to detect unauthorized access across the combination of a user's account credentials, devices or IP addresses. The capability to easily detect compromised credentials of any employee or contractor within the organization is a foundational requirement for UEBA.

2. DETECT PRIVILEGED-USER COMPROMISE

A privileged user has authorized access to high-value resources, such as a sensitive database, a user-rights management system, or an authentication system. When a hacker obtains privileged-user credentials, the attack can proceed directly to those high-value assets with impunity. The result can be devastating – especially if the incumbent security system is unable to detect the initiation and follow-on actions of a privileged-user compromise. Hackers are aware of this benefit, which makes privilege abuse one of the top tactics used in reported data breaches (Verizon 2020 DBIR). Detection is challenging because a privileged user's work patterns may not occur in regular, predictable patterns. For example, responses to emergencies may produce totally unrelated actions by the privileged user. The ability to accommodate these variables and reliably detect any privileged-user compromise is an essential use case requirement for augmenting a SIEM with the advanced analytics of a modern UEBA.

3. MONITOR EXECUTIVE ASSETS

Getting access to executive computing assets such as the CEO's or CFO's laptop are obvious targets for hackers. These systems may contain data about sensitive earnings, mergers and acquisitions, budget planning, product and services planning, or competitive information. An effective UEBA solution must be able to augment your SIEM by automatically building asset and behavior models that identify executive assets and monitor them for unusual access and usage. A legitimate executive user's abuse of these assets is addressed in Use Case 5: Insider Access Abuse.

4. DETECT COMPROMISED SYSTEMS/ HOSTS/DEVICES

It is very common for attackers to take control of systems, hosts or devices within an organizational network, and operate undetected for months or years. This timeline underscores the importance of the compromised system/host/device use case for augmenting your SIEM with a behavioral analytics solution to detect and stop attacks quickly. In addressing this use case, a modern UEBA solution should monitor several vectors, including: user accounts to identify anomalous activity and alert analysts with the data they need to understand if a privileged user account was breached; servers for detecting deviations from baseline activity; network devices to monitor traffic over time and detect unusual spikes, non-trusted communication sources, insecure protocols, and other signs of malicious behavior; and anti-virus/malware monitoring to detect protection disablement or removal, or status of threat updates.

5. DIFFERENTIATE NORMAL BEHAVIOR FROM MALICIOUS BEHAVIOR

While many of the most well-known breaches have been caused by malicious outsiders, it is the insider (malicious or well intentioned) that continues to be a major source of sensitive data loss. Insider threat detection is challenging because “trusted” behavior doesn’t set off alerts in most security tools; the threat actor appears to be a legitimate user. Potential bad actors include the malicious insider, which is a security threat originating from the organization’s employees, former employees, contractors, business partners, or associates; and compromised insiders – persons for whom an external entity has obtained legitimate access credentials. In this case, the UEBA solution must be able to detect when a user (privileged or not) is performing risky activities that are outside of their normal baseline. A behavioral analytics solution can help discover insider threat indicators via behavioral analysis, which helps security teams to identify and mitigate attacks. Some of the techniques used by a modern UEBA include detecting logins from unusual locations, at unusual hours, at unusual frequency, or accessing unusual data or systems; changes or escalation of privileges for critical systems; correlating network traffic with threat intelligence to discover malware communicating with external attackers; and discovering data exfiltration by correlating seemingly unrelated events such as insertion of a USB thumb drive, use of a personal email service, or unauthorized cloud storage or excessive printing. Other discoveries of insider abuse may include detecting and stopping encryption of large amounts of data or lateral movement.

6. IDENTIFY AND TRACK LATERAL MOVEMENT

A breach through the most innocuous entry point of an organization’s network may quickly become a proverbial hole in the dyke with undetected lateral movement. The process of lateral movement entails systematically moving through a network in search of sensitive data and assets. Perhaps the attack began by compromising a low-level employees account. Once inside, the hacker probes other assets for vulnerabilities in order to switch accounts, machines and IP addresses. Opportunity knocks once the attacker secures administrative privileges. Lateral movement is extremely difficult to detect by traditional security tools because parts of the attack are scattered across the IT environment, spread among different credentials, IP addresses and machines; the seemingly unrelated events all appear to be normal. The Lateral Movement Detection use case for augmenting your SIEM with behavioral analytics is critical for detecting these breaches. The UEBA solution uses behavioral analysis to connect the dots between “unrelated” activity and stops these attacks before damage occurs.

7. DETECT INSTANCES OF DATA EXFILTRATION

Data exfiltration happens when sensitive data is illicitly transferred outside an organization. It can happen manually, when a user transfers data over the internet or copies it to a physical device and moves it outside the premises. Exfiltration may also be automatic, which often occurs as the result of malware infecting local systems. In this use case, the behavioral analytics solution detects network traffic to command and control centers and identifies infected systems transmitting data to unauthorized parties.

Modern UEBA solutions monitor for unusual amounts of network traffic over protocols that facilitate large data transfer compared to the baseline of a user or machine transferring the data. It monitors usage of organizational web applications by outsiders, or inside usage of external web applications, which might involve downloads or browser access to sensitive data, and detects emails forwarded or sent to other entities other than the stated recipient. It also monitors data from the mobile workforce to identify anomalies that might indicate information leakage via a mobile device.

8. PROVIDE CONTEXT TO FAILED LOGIN ATTEMPTS & ACCOUNT LOCKOUTS

An account lockout disallows access to a user. This is a security feature that aims to protect an account from a brute force attack or dictionary attack to guess and crack the user's password. Failed login attempts and corresponding account lockouts consume a surprisingly large amount of administrative time. It is common for larger organizations to use an entire full time headcount during the year, just to analyze user account lockouts to determine whether the lockout was due to a simple "fat fingered" mistake or was a sign of an attempted account takeover. To determine risk, administrators often spend four or five hours looking at conditions and accounts related to each lockout. This use case for augmenting your SIEM with behavioral analytics helps to automate the risk assessment process and quickly render a verdict on account risk.

9. IDENTIFY SERVICE ACCOUNTS & MISUSE

A service account is used in lieu of a normal s ystem account to run specific application services. Service accounts are used to improve security; if it is compromised, losses will be limited as opposed to compromise of a general system account.

Typical security tools provide limited or no visibility into service accounts. This limitation is somewhat bizarre because service accounts have high privileges – and are high-value targets for attackers. For example, the SAP "Firefighter" account often has significant privileges within that critical application. Service Account Misuse is a valuable use case for a behavioral analytics solution. By employing its behavioral analytics capabilities, a modern UEBA solution will augment your SIEM by automatically identifying service accounts and flag any abnormal behavior within them.

10. AUTOMATE DETECTION, TRIAGE AND INVESTIGATIONS

Security alert investigation is the primary role of a Security Operations Center analyst. From a practical perspective, security alert investigation using traditional security tools is an onerous manual process. Alerts typically consist of arcane data in raw log files that defy comprehension – even for seasoned security analysts. Alerts may scream "time is of the essence!" but the investigation itself demands correlation of various log files, interpreting meaning, manually analysing ancillary data sources for clues, and spending considerable time trying to determine the root cause of an alert incident. The Security Alert Investigation use case is another way an advanced behavioural analytics solution augments your SIEM to dramatically improve the productivity of SOC analysts. Modern UEBA solutions automate the detection, triage and investigation of the alert lifecycle and instead of presenting discrete events, a machine-built timeline of a users session presents the results with context and risk scoring to help rapidly distil the essence of a threat – and how to quickly resolve it.

exabeam

CONCLUSION

A behavioral analytics solution addresses the top issues in security that are frequently missed by traditional tools incapable of detecting advanced, complex threats. The detection capability and advanced notice to attacks provided by modern UEBA solutions is a huge, incalculable benefit to organizations because it enables security teams to stay in front of danger and quickly remediate active threats. The UEBA capabilities in Exabeam Advanced Analytics address all of the Top 10 Use Cases described above. If these benefits are attractive to your organization, we invite you to learn more by contacting Exabeam or one of our services partners.

ABOUT EXABEAM

From the CISO to the analyst, Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes and hundreds of other business and security products. Out-of-the-box use case coverage delivers repeatable outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. And alert enhancement and automated timeline creation help overcome staff shortages by minimizing false positives and reducing the time it takes analysts to detect, triage, investigate and respond to incidents by 51 percent. For more information, visit https://www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.