OVERVIEW
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 legacy 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 UEBA SHOULD BE PART OF YOUR ORGANIZATION’S SECURITY FRAMEWORK
Attacks have become increasingly sophisticated, and often are invisible and undetectable by legacy security solutions. You read about these successful data breaches (it seems) almost on a daily basis. Security analysts do what they can with legacy tools, but these tend to swamp analysts with alerts that are difficult to understand and are often useless for rapid detection and remediation of advanced threats.

UEBA solutions employ a different approach by using variations of artificial intelligence and machine learning, advanced analytics, data enrichment, and data science to effectively combat advanced threats. The 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. UEBA is valuable to the enterprise because it has a low maintenance overhead. The ML system tunes itself via behavioral modeling. The organization gets a future-proof solution for unknown attacks that looks for abnormalities instead of a limited, pre-determined set of activities. UEBA is the only way to effectively address the Top 10 Use Cases described below.
TOP 10 USE CASES FOR UEBA

The rest of this paper presents the Top 10 Use Cases for UEBA. Each describes the unique operational requirement and how a UEBA solution helps to improve enterprise security.

1. COMPROMISED USER CREDENTIALS

User account credentials are keys to legitimate access, and stolen credentials are the Number One vector for data breaches, according to the Verizon 2018 Data Breach Investigations Report (DBIR) (p.8). When a hacker uses stolen credentials, legacy 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 a UEBA solution. It’s irrelevant how the attacker obtained the credentials – UEBA 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. 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 a legacy 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 the fourth highest tactic used in reported data breaches (Verizon 2018 DBIR, p. 8). 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 UEBA. The UEBA solution should monitor suspicious activity by departed employees or contractors, and identify human errors dealing with or overexposure to sensitive data.

3. EXECUTIVE ASSETS MONITORING

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. Another insidious risk vector is fooling the executives themselves. For example, hundreds of millions of dollars are stolen each year via wire transfers driven by webmail schemes that
trick company executives into approving these transfers. An effective UEBA solution must be able to automatically build asset and behavior models that identify executive systems 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. COMPROMISED SYSTEM/HOST/DEVICE DETECTION

It is very common for attackers to take control of systems, hosts or devices within an organizational network, and carry out attacks stealthily for months or years. In terms of breach timelines, the average time companies took to detect a data breach was 562 days, according to the Verizon DBIR (p. 10). This astonishing timeline underscores the importance of the compromised system/host/device use case for UEBA to detect and stop attacks quickly. In addressing this use case, the 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. INSIDER ACCESS ABUSE

While many of the most well-known breaches have been caused by malicious outsiders, the rogue insider continues to be a major source of sensitive data loss. Top internal actors in reported breaches have included system administrators, end users, developers, managers and executives, according to the Verizon DBIR (p. 9). 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. The UEBA 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 UEBA include detecting logins 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. LATERAL MOVEMENT DETECTION
IA 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 legacy 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 UEBA use case 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. DATA EXFILTRATION DETECTION
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 UEBA solution detects network traffic to command and control centers and identifies infected systems transmitting data to unauthorized parties. UEBA monitors 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. UEBA detects emails forwarded or sent to other entities other than stated recipient. It also monitors data from the mobile workforce to identify anomalies that might indicate information leakage via a mobile device.
8. ACCOUNT LOCKOUTS

An account lockout disallows access to a user. This is a security feature that aims to protect an account from anyone or anything trying to guess the username and password. Lockout occurs after a login failure exceeds a set parameter of permitted attempts. Typically, the user must wait for a set amount of time before being able to log into the account; in some cases, the user must appeal to an administrator to be re-granted the right to log into the account. Account lockouts consume a surprisingly large amount of administrative time. It is common for larger organizations to use an entire fulltime 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 UEBA use case helps to automate the risk assessment process and quickly render a verdict on account risk. Done effectively, the UEBA solution could save up to a full headcount annually at a larger organization.

9. SERVICE ACCOUNT MISUSE

A service account is used in lieu of a normal system 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 UEBA. By employing its behavioral analytics capabilities, the UEBA solution will automatically identify service accounts and flag any abnormal behavior within them.

10. SECURITY ALERT INVESTIGATION

Security alert investigation is the primary role of a Security Operations Center analyst. Security alerts are indicators of a potential threat; a red-level security alert demands immediate attention and usually signifies an attack in process. From a practical perspective, security alert investigation using legacy security tools is an onerous 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 manual correlation of various log files, interpreting meaning, manually culling 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 UEBA can dramatically improve the productivity of SOC analysts. UEBA, in conjunction with a modern Security Information and Event Management solution, uses machine-built timelines that offer a better interface for threat hunting even by a junior analyst. Instead of presenting discrete events, a machine-built timeline presents the results with context and risk scoring to help rapidly distil the essence of a threat – and how to quickly fix it if needed.
CONCLUSION

UEBA 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 UEBA use cases 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 Security Management Platform 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

Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation.

With the Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com or follow us on Twitter @exabeam.