Targeted Behavioral Analytics: Prioritizing High Privileged Accounts to Mitigate Risk
As part of a unified security system, user behavior analytics offer a powerful way for organizations in financial services, utilities, telecommunications, pharmaceuticals, government and other industries that handle high risk and confidential information to proactively identify and counteract internal and external threats. The key to mitigating these risks is to intelligently prioritize the data collection process for high privileged accounts—using automation combined with human interaction to focus on the accounts that pose the biggest risk.
Introduction

Organizations routinely monitor user accounts in an attempt to improve their security posture. However, it can be difficult to collect the right amount of data: too little and the company cannot effectively inform security professionals’ decisions; too much and the company quickly reaches data overload. This turns the search for meaningful security events into “needle in the haystack” scenarios. To compound the challenge, many organizations make decisions in the data collection stage that limit their abilities to use complex algorithms because of large compute times. In other words, it takes too long to analyze and model collected data at massive scales to produce actionable results.

Leading enterprises are taking a more strategic and systematic approach to this security challenge by preemptively addressing compromised accounts and insider threats using automation and advanced analytics. The first step is to evaluate which employees have been granted high privileged accounts (HPA) in the organization. These “golden key holders” have access to sensitive information, processes, data sets or services—thus they can inadvertently or maliciously introduce the highest potential impact and risk to an organization. The second step is to deploy user behavior analytics focused on the high privileged accounts to more quickly identify and respond to security concerns.

Concentrate on highest-risk profiles

Unlike normal accounts with standard access to enterprise systems, high privileged accounts pose additional risk because of the higher levels of access to information and potential capabilities they can enact if an external threat actor (i.e., individual outside the organization) or insider threat actor (i.e., employee) compromises them.

Insider threats, in particular, are extremely dangerous because their familiarity with internal systems makes it possible to do more damage across the enterprise—and to do it more quickly. Additionally, insiders may be provisioned access that a malevolent outsider would have to take additional steps to obtain. By targeting high privilege account holders, malicious actors may be able to shorten or skip steps in the attack chain, specifically in gaining footholds and reconnaissance. This makes timely detections even more critical in the case of insider threats.

Profile of high privileged accounts

Examples of high privileged accounts may include but are not limited to:

- C-suite leadership and management with more access to enterprise systems due to level in organization.
- IT organization accounts such as administrator accounts, shared service accounts or infrastructure configuration accounts.
- Marketing or Finance team accounts with access to personally identifiable information (PII).
- R&D accounts belonging to innovative project teams.
Monitor high privileged accounts with user behavior analytics

Increasingly these algorithms are being embedded into user behavior analytics (UBAs) from vendors such as Securonix, Bay Dynamics or Splunk. Organizations can incorporate user behavior analytics into their security processes to automate portions of the detection and remediation process. These specialized analytics form models of user behavior—in this case high privileged accounts—and help to detect deviations from patterns that security professionals might miss.

Since user behavior analytics can operate autonomously in near real time, organizations can rely on them to provide an early warning system for accounts that begin to act abnormally. In the event that the anomalous accounts are contiguous with steps in the attack kill chain, the security team can take additional steps to neutralize the account and threat.

Applying user behavior analytics across industries

Enterprises can secure the locations, dates and times of access, among other variables, of infrastructure configuration accounts and systems administrator accounts through user behavior analytics. Additional industry-specific examples include:

**Software**
- Protect source code, making it easier to quickly identify potential malicious access or use of developer accounts to access source code repositories.

**Pharmaceutical**
- Safeguard confidential intellectual property.

**Utilities**
- Secure national infrastructure assets by monitoring configuration accounts for control systems and responding quickly to anomalous accounts.

**Retail**
- Protect PII by applying analytics to identify attempts by actors to use customer service accounts to extract information from databases.
Steps to seize a security advantage

In order to implement a full-scale high privileged account monitoring program, organizations must have a strong foundation in security with clearly defined processes for performing data identification and classification activities (i.e., What data is being collected? Where are the logs stored?) and identity and access management assessments (i.e., Who owns high-risk accounts? Who can access them?).

Using the outcomes from these processes, companies can follow these steps to implement user behavior analytics:

1. **Identify**
   - Identify and tag high privileged accounts via computer and human classification. (Take into account reference data for organization—directory data, application metadata, HR metadata and role membership.)
   - Establish a common identifier to link accounts from different applications owned by the same high privileged account user.
   - Expand monitoring set to all accounts owned or associated with each common identifier.

2. **Collect**
   - Establish centralized logging or SIEM to collect application and activity data associated with each account in the monitoring set.
   - Log source data can include: system alerts, access events, user activity, firewall activity, data loss prevention activity, network traffic or application log data.
   - Collect varied log data sources in a centralized SIEM system for easy access and centralized manipulation.

3. **Score**
   - Set up user behavioral models to leverage the log sources, characterize anomalous behavior based on risk score and aggregate risk(s) associated with each common identifier to a composite risk score.
   - Regularly review and tune the models to keep the false positive rate low.

4. **Remediate**
   - Use the generated composite risk scores to issue an investigation workflow ticket for any common identifiers that receive risk scores above a certain threshold.
   - Investigate and remediate generated workflow tickets and validate/alert on any exceptions.
Conclusion

Selectively monitoring high privileged accounts through user behavior analytics not only reduces the noise associated with account monitoring, but also targets accounts that insider threat actors are likely to use and external threat actors will attempt to compromise to achieve their goals. Organizations that take this strategic and vital step can empower their cyber defenders and substantially improve their security posture. (To learn more about Accenture's perspective on key technology trends in the security industry, see our Security Technology Vision 2016.)
Contacts

Are you ready to learn more about behavior analytics to better protect your organization? Please contact these members of the Accenture Labs Security R&D group for more information:

**Louis DiValentin**
louis.divalentin@accenture.com

**Josh Patterson**
joshua.patterson@accenture.com

**Lisa O’Connor**
lisa.oconnor@accenture.com

About Accenture Labs

Accenture Labs invents the future for Accenture, our clients and the market. Focused on solving critical business problems with advanced technology, Accenture Labs brings fresh insights and innovations to our clients, helping them capitalize on dramatic changes in technology, business and society. Our dedicated team of technologists and researchers work with leaders across the company to invest in, incubate and deliver breakthrough ideas and solutions that help our clients create new sources of business advantage.

Accenture Labs is located in six key research hubs around the world: Silicon Valley, CA; Sophia Antipolis, France; Arlington, Virginia; Beijing, China; Bangalore, India, and Dublin, Ireland. The Labs collaborates extensively with Accenture’s network of nearly 400 innovation centers, studios and centers of excellence located in 92 cities and 35 countries globally to deliver cutting-edge research, insights and solutions to clients where they operate and live. For more information, please visit www.accenture.com/labs.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 375,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.