User Behavior Analytics (UBA)

Short UBA Best Practices Guide

"User and Entity Behavior Analytics (UEBA) successfully detects malicious and abusive activity that otherwise goes unnoticed..." - Gartner

Challenges for securing the modern IT environment:

- Companies lack visibility into employee activity and application usage across critical IT systems.
- Legacy defense strategies are typically focused on the perimeter, so they fail to identify insider threats or attacks in progress within the network.
- Security teams are often overwhelmed by the huge volume of audit logs generated every day, increasing the risk that important actions can be missed.
- Most legacy security applications, such as SIEM solutions, are time-consuming to use.

Best practices:

- Identify the existing sources of data on user behavior, including logs, data warehouses, network flow data, etc. The more data you have, the better.
- Integrate data from other monitoring systems, such as advanced threat management and HR customer relationship management (CRM) systems.
- Enable Active Directory auditing to track who is doing what across your critical systems.
- Enable auditing for all systems that contain sensitive information, including your file servers, SharePoint, SQL servers, etc.
- If you are using SaaS applications, enable access and user activity logging.
- Track account creation and account logons, because such activity can reveal account takeovers and other attacks.
- Enable journaling on your e-mail server and use e-discovery software for e-mail flow analytics.
- Regularly review effective permissions and enforce a least-privilege model.
- Track and control your users' internet traffic via web filtering software.
- Provide your UBA solution with all the data mentioned above. Fine-tune its rules, alerts, reports and thresholds to reduce noise and false-positive anomalies.
- Review UBA reports on anomalous activity regularly and investigate incidents promptly.

Corporate Headquarters:
300 Center Drive, Suite 1100, Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social