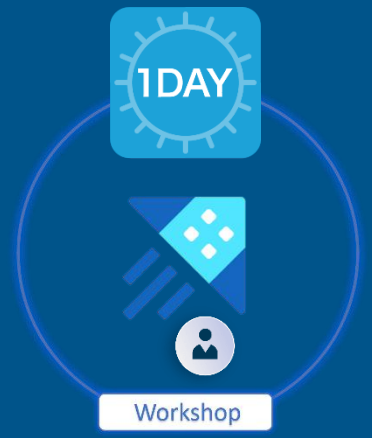
Executive Leadership Series

User and Entity Behavior Analytics for Cybersecurity Professionals

TLC Education & Training Services



- CXO's
- Business Leaders
- Technology Leaders
- Cybersecurity Professionals
- Digital Leaders
- Project Managers
- Strategic Planners
- Enterprise Architects

User and Entity Behavior Analytics for Cybersecurity Professionals

Skills and expertise to help you increase your knowledge in the field of digital technologies

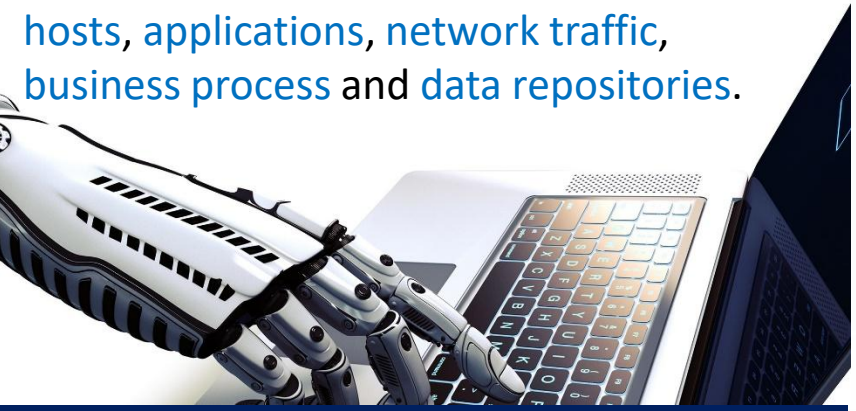
TLC Education & Training Services

Executive Leadership Series

About this Workshop

In a nut-shell, the concept of a User and Entity Behavior Analytics has been around for more than nine years, but adoption did not really begin to take hold until the past couple of years. UEBA is a behavioral solution for securing organizations in the cloud, on-premises and mobile world that asserts that no user or application should be trusted by default. Following a key zero trust principle, least-privileged access, trust is established based on context (e.g., user identity and location, the security posture of the endpoint, the app or service being requested) with policy checks at each step are what we are exploring in this one-day workshop.

UEBA solutions analyze activity from network users and other **entities**, such as hosts, applications, network traffic, business process and data repositories.



According to multiple threat intelligence resources, roughly 20% of all internet traffic originates from bad bots. These bots engage in activities like scraping, scanning, and searching for vulnerabilities in web applications. In this workshop we will see how UEBA is the most effective solution to combat various types of cyber threats.

Target Audience

- CXO's, Business Executives, Technology Executives, Entrepreneurs, Digital Leaders, project Managers, Strategic Planners, and Enterprise Architects.

User and Entity Behavior Analytics (UEBA) is a critical risk management solution that leverages machine learning (ML) algorithms and behavior analytics to provide comprehensive insights into user and entity activities within a network. By analyzing patterns and anomalies, UEBA helps security teams identify potential threats and take appropriate measures to mitigate their impact.

Unlike traditional signature-based detection methods, which rely on known threat signatures, UEBA focuses on behavior analysis and covers both users and entities (such as network devices, routers, and databases). For example, if a company's network experiences an unexpected surge in data requests, UEBA would promptly recognize this irregularity and notify administrators.

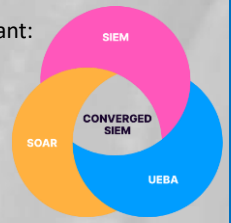
If you're interested in exploring UEBA solutions, then this one-day workshop is something that you can consider. Additionally, UEBA software uses artificial intelligence (AI) and ML to analyze user and device actions on a network, helping to identify potential threats.

Workshop Contents

- Understanding the Bigger Challenge.
- The need for having a UEBA Solution.
- Understanding Cognitive Computing.
- UEBA – User and Entity Behavior Analytics Defined.
- Understanding UEBA Engines.
- Three pillars of UEBA – Use Cases, Data Sources, and Analytics.
- Exploring main components of UEBA.
- Convergence of UEBA and SIEM.
- High-level Comparison between UEBA and SIEM.
- UEBA integration with SIEM.
- Similarities and Dissimilarities between SIEM and UEBA solution.
- Why do organizations need UEB.
- How UEBA works
- Understand UEBA Threat Workflow.
- Generic UEBA Architecture Deployment Models.
- Threat Remediation Workflow Process.
- Enterprise Data Sources analyzed by UEBA.
- Facts for a successful implementation of UEBA solution.
- UEBA for Enterprise Security – A layered-wise approach.
- UEBA Risk Scoring and Threat Indicator Signs.
- UEBA for Enterprise Security for threat hunting and incident investigation.
- Critical Devices of UEBA Systems.
- Best Practices for building a baseline of User Behavior.
- Understanding Disadvantages of using UEBA solution.
- UEBA Consideration for Success.
- Key Specifications for selecting a good UEBA Solution.
- UEBA Solution Providers.
- UEBA Conclusion.
- Unit 1 Assessment.

User and Entity Behavior Analytics (UEBA) software is crucial for business and technology decision makers because it provides an effective tool for identifying suspicious or abnormal behavior and activities within an IT environment.

Here are some reasons why UEBA solutions are important:



- Threat Detection and Prevention
- Insider Threat Mitigation
- Holistic Monitoring
- Customization and Flexibility
- Kill Chain Detection

In summary, UEBA solutions empower decision makers with insights, early threat detection, and the ability to proactively address security risks, making them essential for safeguarding business environments.

In a nutshell, if you are considering implementing UEBA, ensure you choose a right UEBA solution that aligns with your organization's key objectives and security requirements.

Detail Information

Course Code	: TN481
Course Duration	: 1 Day Workshop
Course Location	: TLC, Online and Customer On-site.
Terms & Conditions	:100% payment in advance.
Course Deliverable	: Comprehensive Student Guide and Course Certificate

For additional information,
please write to us at: info@tlc-pak.com

User and Entity Behavior Analytics for Cybersecurity Professionals

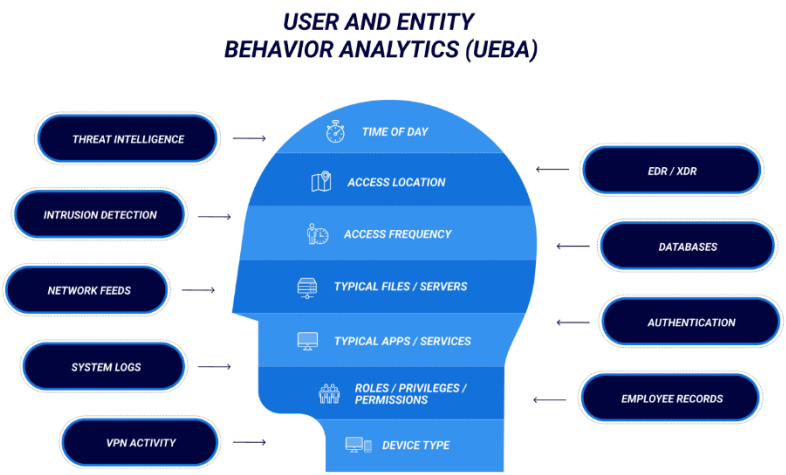
Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

In summary, UEBA provides a more comprehensive and context-aware approach to threat detection, making it an essential component for safeguarding mission-critical business operations.

UEBA and Advanced Analytics: UEBA solutions analyze activity from network users and other **entities**, such as hosts, applications, network traffic, business process and data repositories.

UEBA solutions apply advanced analytics methods to look for **anomalies** that indicate potentially suspicious or malicious activity and irregularities across an organization. For example: Insider threats, Identity Thefts, Account Take Over, Data Manipulation, Data Theft, Lateral Movement, Compromised Accounts, Potentially Dangerous Users, and Device Behavior.



Projected Market Size and Growth Rate of the User and Entity Behavior Analytics Software Market

User and Entity Behavior Analytics (UEBA) Software Market was valued at USD 373.37 Million in 2024 and is projected to reach USD 5469.49 Million by 2029, growing at a CAGR of 40.5% from 2025 to 2029.

Some of the Value-add for using UEBA for the Business: (User and Entity Behavior Analytics (UEBA) provides several significant value-adds for businesses. Following are some of the key features;

Advanced Threat Detection: UEBA solutions use artificial intelligence (AI) and machine learning (ML) to effectively combat advanced threats. By analyzing data from various sources, UEBA identifies anomalies and potential security risks. This proactive approach helps detect insider threats, compromised accounts, and other malicious activities.

Contextual Insights: UEBA shows both normal and anomalous behavior within a user session timeline. Understanding the context is crucial for effective threat detection. For example, it considers whether a user's actions align with their typical behavior or if they are engaging in unusual activities. This reduces investigation time and enhances accuracy.

Automatic Identity Linking: UEBA automatically connects hosts to IP addresses and user identities. This is essential because hostnames are often uninformative, and IP addresses change frequently. By positively attributing activity to specific individuals, UEBA improves threat detection and reduces manual investigative efforts.

Lateral Movement Detection: A compromised account often exhibits lateral movement—hopping between user credentials and devices to avoid detection. UEBA identifies such lateral movement patterns, helping security teams take timely remedial action.

Enhanced Zero Trust Security: UEBA aligns well with the principles of Zero Trust Security by continuously monitoring behavior and assessing risks, it contributes to a proactive security approach. Organizations can make informed decisions based on real-time insights, improving their overall security culture.

Additionally, UEBA extends beyond threat detection to impact various business functions. For instance:

- In financial services, it aids fraud management.
- In consumer operations, it enhances customer experience.
- In manufacturing supply chains, it provides partner value analysis.
- In sales and marketing, it assists with targeted strategies.
- Across the board, it contributes to efficient operations.

Overall, UEBA is a critical risk management solution that leverages ML algorithms and behavior analytics to provide comprehensive insights into user and entity activities, ultimately mitigating potential impacts.

UEBA security is imperative since user-based threats are on the rise

of organizations report incidents of attempted data theft — by internal threats

of breaches involve stolen or weak credentials.

report inadequate insider threat detection programs.

Opportunities are made, not found

Executive Leadership Series

We look forward serving you as one of your trusted education and training services partners.

www.tlc-pak.com