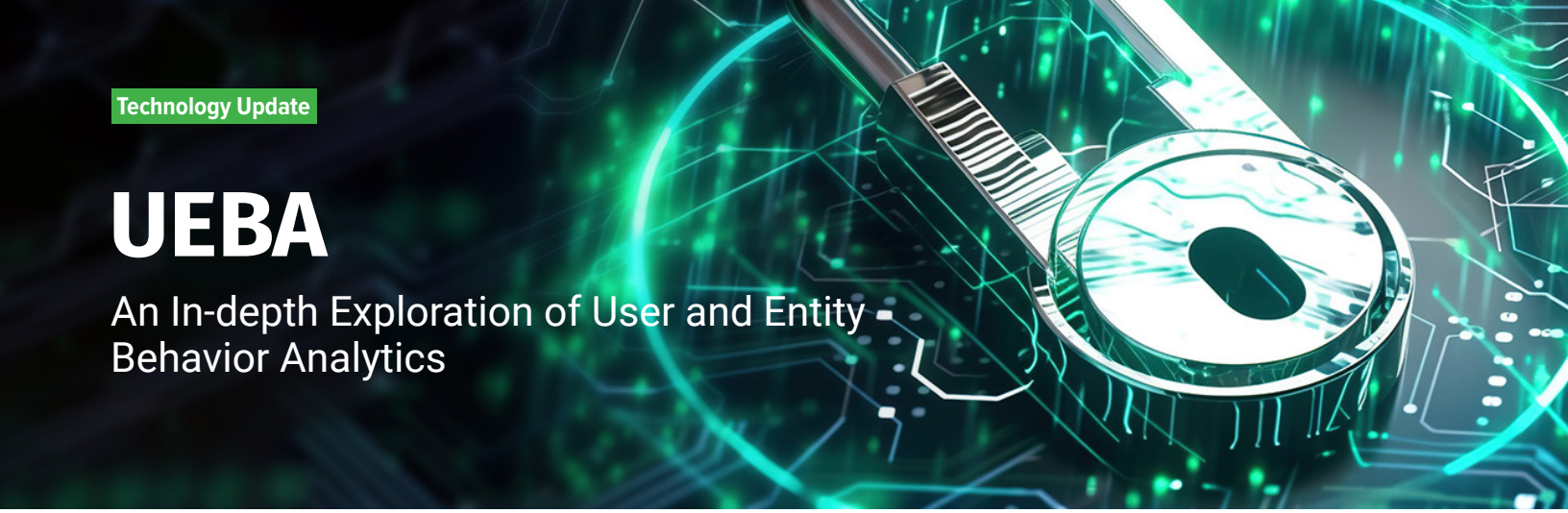


Technology Update

UEBA

An In-depth Exploration of User and Entity Behavior Analytics

In today's rapidly evolving cybersecurity landscape, organisations confront a perpetual challenge: safeguarding their digital assets against an array of potential risks. While traditional security measures offer some level of protection, they often fall short in detecting and countering insider threats, targeted attacks, and other sophisticated cyber assaults. In response to this imperative need for more robust security solutions, User and Entity Behavior Analytics (UEBA) emerges as a critical component within modern cybersecurity frameworks.

UEBA signifies a paradigm shift in security analytics, providing organisations with a proactive approach to threat detection and mitigation. Unlike conventional security tools that primarily focus on perimeter defence and signature-based detection methods, UEBA delves deep into the behavioural patterns of users and entities within an organisation's network environment. By harnessing advanced analytics, machine learning algorithms, and behavioural modelling techniques, UEBA solutions analyse extensive data sets to establish baseline behaviour and pinpoint deviations indicative of potential security threats.

The concept of UEBA extends beyond traditional user behaviour analysis to include monitoring various entities, such as applications, devices, and systems. This holistic approach empowers organisations to gain deeper insights into the activities occurring within their digital ecosystems, enabling them to detect anomalous behaviour that might evade conventional security measures.

Avtar Singh
Scientist - D
avtarsingh@nic.in

Sumit Vimal
Scientist - B
sumit.vimal@nic.in

UEBA revolutionises cybersecurity by scrutinising the behaviour of users and entities within a network. Through advanced analytics and machine learning, UEBA identifies anomalies in real time, allowing organisations to detect potential security threats swiftly. By establishing baselines of normal behaviour and assigning risk scores, UEBA provides proactive threat detection and helps prioritise response efforts. Integrated with other security tools, UEBA enhances overall cybersecurity posture, empowering organisations to mitigate risks effectively and safeguard their digital assets against evolving threats.

In this article, we will explore the key components, functionalities, benefits, challenges, and implications of UEBA for modern cybersecurity operations. By gaining a comprehensive understanding of the foundational principles and capabilities of UEBA, organisations can enhance their security posture, mitigate risks, and proactively defend against a wide range of cyber threats.

Introduction

UEBA, first introduced in 2015, builds upon User Behavior Analytics (UBA) by extending its scope beyond end-user behaviour to encompass the monitoring of non-user entities such as servers, routers, and IoT devices for suspicious activity. This expansion enhances threat detection capabilities, particularly in identifying insider threats that mimic legitimate network traffic—a challenge for traditional security tools. Integrated into security operations centres (SOCs) and various enterprise security solutions such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Identity and Access Management (IAM), UEBA plays a pivotal role in bolstering defences against evolving cyber threats. Its effectiveness in detecting insider threats makes it an essential component of modern cybersecurity strategies.

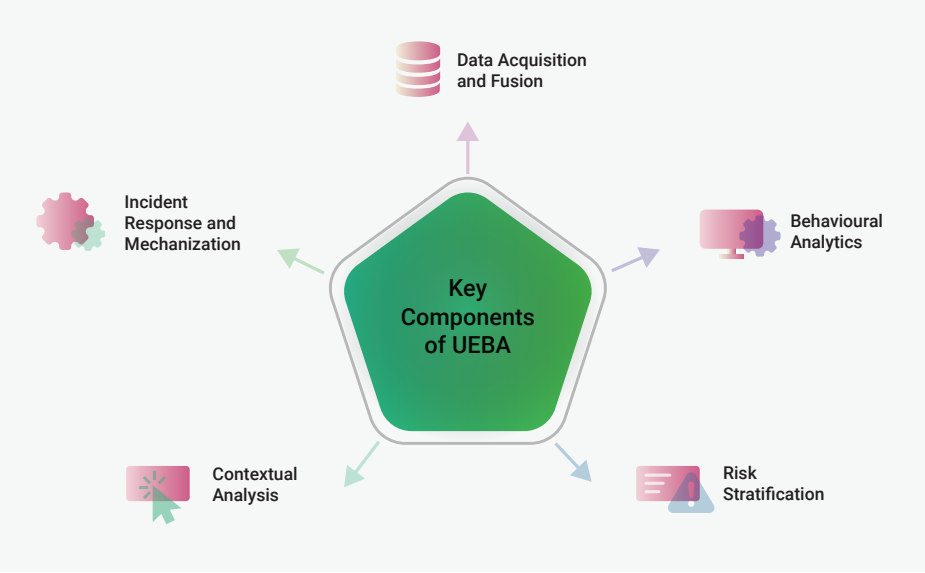
How UEBA Works

UEBA solutions leverage data analytics and machine learning to provide security insights. These tools analyse extensive data from various sources to establish a baseline of normal behaviour for privileged users and entities. Through machine learning, the baseline is continuously refined, requiring fewer samples over time for accurate assessment.

Once the baseline is established, UEBA employs advanced analytics and machine learning to detect deviations in real-time user and entity activity data. It draws from multiple enterprise sources, including network equipment, security tools, authentication databases, threat intelligence feeds, and ERP/HR systems, to assess behaviour comprehensively. UEBA identifies anomalous behaviour and assigns risk scores accordingly. For example, multiple failed authentication attempts or abnormal system access patterns may signal insider threats, resulting in low-risk alerts. Conversely, suspicious activities such as plugging in multiple USB drives and unusual download patterns may indicate data exfiltration, warranting higher risk scores. This scoring system enables security teams to prioritise threats effectively and monitoring low-level alerts.

UEBA Use Cases

UEBA aids organisations in identifying suspicious behaviour and fortifying data loss



prevention (DLP) strategies. In addition to its tactical applications, UEBA can also fulfil strategic roles, such as ensuring compliance with regulations pertaining to user data and privacy protection.

Tactical Applications

Malicious Insiders: These individuals possess authorised access to corporate networks and attempt cyberattacks. While conventional data analysis may overlook them, UEBA's advanced analytics can pinpoint them by focusing on specific user behaviours rather than IP addresses.

Compromised Insiders: Attackers acquire legitimate user credentials through methods like phishing, making them appear authorised. UEBA detects their anomalous behaviour, aiding in thwarting their attacks.

Compromised Entities: With the proliferation of IoT devices lacking robust security measures, organisations become vulnerable to hackers who exploit these entities for data theft or disruptive activities. UEBA identifies signs of compromise in these entities, enabling proactive threat mitigation.

Data Exfiltration: Both insider threats and malicious actors target servers and devices to steal sensitive data. UEBA alerts security teams to unusual data access patterns in real-time, facilitating swift responses to potential breaches.

Strategic Applications

Zero Trust Security Implementation: UEBA plays a pivotal role in implementing a zero trust security approach by providing comprehensive visibility into all user and entity activities. This ensures continuous authentication, authorization, and validation to maintain network security.

GDPR Compliance: Compliance with the GDPR mandates meticulous tracking of personal data access and usage. UEBA tools aid in GDPR compliance by monitoring user behaviour and access to sensitive data, ensuring adherence to regulatory requirements.

Key Components

Data Acquisition and Fusion: UEBA platforms aggregate and correlate data from multiple sources to provide a comprehensive view of the organisation's digital landscape.

Behavioural Analytics: Machine learning algorithms analyse historical and real-time data to establish normative behaviour patterns for users and entities, facilitating the detection of deviations.

Risk Stratification: UEBA assigns risk scores to users and entities based on their behaviour, enabling security teams to prioritise response efforts.

Contextual Analysis: Consideration of contextual factors such as time, location, and user roles enhances the accuracy of behavioural analysis.

Incident Response and Mechanization: UEBA automates response actions to security incidents, streamlining the mitigation process and reducing response times.

Advantages

Preliminary Threat Detection: UEBA enables the early detection of potential security threats, minimising the impact of breaches.

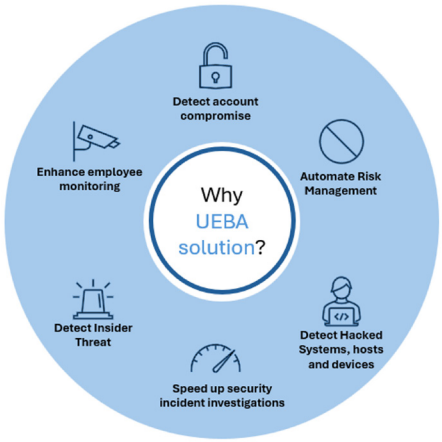
Insider Threat Recognition: By monitoring user activities, UEBA can identify both deliberate and inadvertent insider threats, enhancing internal security measures.

Mitigation of False Positives: Contextual analysis and risk scoring capabilities reduce false positives, allowing security teams to focus on genuine threats.

Sustained Monitoring: UEBA provides continuous oversight of user and entity behaviour, adapting to evolving threats and ensuring ongoing security vigilance.

Challenges and Considerations

Data Privacy: Concerns about user privacy necessitate transparent policies and adherence to regulatory frameworks.



Integration: Seamless integration with existing security infrastructure requires careful planning and coordination to avoid disruptions.

False Positives: Fine-tuning UEBA systems to minimise false positives requires ongoing adjustments and alignment with organisational dynamics.

Summary

In conclusion, UEBA stands as a pivotal tool in the modern cybersecurity arsenal, empowering organisations to proactively detect and respond to potential security threats. By harnessing the capabilities of advanced analytics and machine learning, UEBA enhances security posture, safeguarding critical assets against evolving cyber threats. As organisations navigate an increasingly complex threat landscape, the adoption of UEBA represents a proactive step towards fortifying digital defences and mitigating security risks.

Contact for more details

Avtar Singh
Scientist - D
1st Floor Block 3
DMRC IT Park, Shastri Park, New Delhi - 110053
Email: avtarsingh@nic.in, Phone: 011-24305862