User-Entity Behavior Analytics (UEBA) – A Systematic Review of Literatures

Revanth Filbert Raj I
Department of Management
Amrita Vishwa Vidyapeetham University
Bangalore, 560035, India
revanthfilbertraj1995@gmail.com

Shekar Babu PhD
Department of Management
Amrita Vishwa Vidyapeetham University
Bangalore, 560035, India
sb@amrita.edu

Abstract

There are a lot of stories of security failures. In addition to attackers, lack of proper monitoring and controls implementation, and data breaches we are seeing these challenges and consequences. The security professionals are grappling to solve these issues. One of the biggest challenges with incident response is it is not the tool to identify them; it is the large amount of data that the environment has generated and how to accommodate and analyze the data. Analytics in the security sphere are working to creation of new rules, correlational aspects, trends and behavior patterns related to user behavior. In this regard, user-entity behavior analytics (UEBA) is one of the areas which researchers and practitioners are exploring solutions. UEBA can help in the security areas. UEBA focuses more on user actions and user behaviors and less on events. Behavior indicators and user-entity first access anomalies are popular and deployed for ease of interpretation with malicious activities. UEBA has approached as a viable approach in the area of security to detect anomalies of user behaviors by statistical analysis and machine learning. The paper aims to show how analytics and specifically UEBA can help in detection. The objective of this paper is to systematically review the literatures to identify published analytics and specifically UEBA. As part of the UEBA literatures the authors looked at research literatures and articles beyond research papers. Searches were made from digital library of Amrita University and through online library database sources and references of eligible papers. The authors created a review process as a method to review the various literatures. For the research design the authors developed a matrix which has aggregated the various use-cases, vendors, the various solutions. The authors through the developed matrix also focus on the best practices across the industry and the various policies that have been developed and used across various industries. The authors also explored the various risks, technologies, data and the tools used in UEBA space across industry. The authors aggregated the analysis of 150 recent empirical studies, published in the last 10 years, between 2008 and 2018, in the international literature on UEBA. The literature review analysis also focuses on ratifying and exploring the existing underlying theories related to UEBA. With the focus on user behaviors and the analytics related to user behaviors the authors look at the insights, benefits and the utilization of resources in the area of security.

Keywords

Security; Cyber security; Systematic Review of Literatures; UEBA; User Behavior;

Biographies

Mr. Revanth Filbert is a 2nd year student pursuing his MBA & MS Collaborative Dual-Degree program at Department of Management, Bangalore, India. He earned his B.Tech in Engineering from India.

Shekar Babu Ph.D. is the Founding Head, Department of Management, Bangalore Campus, AMRITA Vishwa Vidyapeetham University, Bangalore, India. Dr. Shekar holds a Bachelor of Engineering degree in Electronics and Communications from Bangalore University and a Master of Science (MS) degree in Electrical and Computer Science from California State University, Los Angeles and a Doctoral Degree in Strategic Management from Amrita University. He is a Management Consultant with over 25 years of experience in working with Price Waterhouse and Hewlett-Packard Co. His research areas are Corporate Social Responsibility (CSR), Corporate Governance (CG), Strategy and Social Development. He has taught courses in Marketing, Leadership, Management Consulting and Business Ethics.