(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/07/2023

(21) Application No.202311045884 A
(43) Publication Date : 04/08/2023

(54) Title of the invention : SYSTEM OF GENERATING AND ANALYZING SECURITY ALERTS AND METHOD THEREOF

(51) International classification	:B08B 070000, G06F 215500, G06F 402000, G06Q 400000, H04L 675500
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)GILL, Rupali
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present invention discloses a system for generating and analyzing security alerts. The system includes a processor (102) to receive data from various sources such as logs, network traffic, system events, and user activities on multiple computing devices. The received data is then organized using data classification and structuring techniques, and the processor (102) evaluates the received data to determine if it indicates any threats, attacks, or breaches. Further, sorting of data being done and identifying relationships and patterns to detect and respond to potential threats, and correspondingly generating alerts and audits for the activities performed by multiple users, while also identifying irregularities in user activities, system behavior, and network traffic to address security issues. Organizations proactively identify and address potential security risks, enhance incident response capabilities, and safeguard their computing infrastructure from threats, breaches, and attacks, by using the system (100).

No. of Pages : 29 No. of Claims : 10