(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :23/03/2023

(21) Application No.202311020558 A
(43) Publication Date : 19/05/2023

(54) Title of the invention : A NOVEL METHOD OF IoCs ACQUISITION, CYBER INCIDENT DETECTION RESULTING IN EFFECTIVE RESPONSE

(51) International classification :A61K 380000, A61K 480000, C12N 151130, C12Q 016886, G01N 335740
(86) International Application No :PCT// Filing Date :01/01/1900
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA Filing Date :NA
(62) Divisional to Application Number :NA Filing Date :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)Chitkara Innovation Incubator Foundation
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)KHOSLA, Praveen Kumar
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)KAUR, Prabhjot
Address of Applicant :Centre For Development of Advanced Computing (C-DAC), A-34, Sector 72, Phase 8, Industrial Area, Mohali, Punjab - 160071, India. Mohali ---------- ----------
3)CHACHRA, Prerna
Address of Applicant :Centre For Development of Advanced Computing (C-DAC), A-34, Sector 72, Phase 8, Industrial Area, Mohali, Punjab - 160071, India. Mohali ---------- ----------
4)CHAHAL, Navdeep Singh
Address of Applicant :Centre For Development of Advanced Computing (C-DAC), A-34, Sector 72, Phase 8, Industrial Area, Mohali, Punjab - 160071, India. Mohali ---------- ----------
5)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
6)PRIYA
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure relates to a system and a method of acquiring indicators of compromise (IoC), detecting cyber security incident using IoCs including a novel hashing technique, and detection of windows event logs tampering in an end point / host event logs, particularly detection of tampering in security and system event logs, network traffic logs. It involves obtaining, at acquisition unit 102, IoCs through email parsing module, TAXII client and server. A shipping unit 108-1 comprising of log read and shipping agents, which reads network and host event logs, format logs, filters logs and ship to the server. A monitoring unit 106 comprising a learning engine 104, which detects end-point / host and networking event log tampering, based on novel event log tempering detection technique, and incident mitigation and response, at the response unit 112. Communication with tampering IoC is blocked for protection against current and future incidents.

No. of Pages : 31 No. of Claims : 10