International Journal of Multidisciplinary Conference Proceedings
editor@ijmcp.com
https://www.ijmcp.com

AI Enabled SIEM with Self-Healing Capabilities

1st Bilal Sameer Khan, 2nd Affan Zahid, 3rd Maleeha Anwar, 4th Tehreem Rasheed & 5th Laiba Latif

1st, 2nd, 3rd, 4th & 5th Dawood University of Engineering and Technology, Pakistan

KEYWORDS

Security Information and Event Management (SIEM), Machine Learning (ML), Behavioral Analysis, Self Healing, Threat Detection.

ARTICLE HISTORY

Date of Publication:16-04-2025

Conference Organizer(s)

Research Consultancy on Social & Management Development
&
University of Karachi
DHA Suffa University

ABSTRACT

Cyber threats are revolutionizing and evolving day by day. As these threats are increasing rapidly, all an organization need is ideal solution to monitor their system and notify them by keeping system up to date and updating it. Traditional SIEM collects and analyzes log data from various devices and monitor whole system to detect potential security issues within the system. Traditional SIEM systems generates lot of alerts which are false positive which are disturbing for user. By using Machine Learning and behavioral analysis, AI system can monitor data in real time and detect anomalies within the system. AI-enabled SIEM systems can integrate with real time threat intelligence feeds to instantly detect new malware signatures. For many cyber attacks, AI-enabled SIEM systems would have been able to rapidly detect unusual behaviors such as communication between trusted systems and external, previously unknown IP addresses. If an unusual IP is detected or any other kind of suspicious activity is detected within the system, the system could automatically isolate the affected systems from the network. This paper explores analysis of AI enabled SIEM with self healing capabilities, why is AI enabled SIEM important, why traditional SIEM needs to be replaced, what is self healing, how efficient is self healing, examples of how in past AI enabled SIEM systems would be used to keep data safe and avoid organization from data breach.

Corresponding Email: bilaahmed@gmail.com

Volume-Issue-Page Number: 2(1) 38

Citation: Khan, B. S., Zahid, A., Anwar, M., Rasheed, T., & Latif, L. (2025). AI Enabled SIEM with Self-Healing capabilities. *Proceedings of the 1st International Conference on Innovation and Sustainability in Management and Social Sciences, *International Journal of Multidisciplinary Conference Proceedings, 2(1).*