IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45ISM/2025/4547025/
Vol. 2025 (13), Article ID 4547025

Advancing Computer Security Incident Response: Global Standards and Best Practices*

Lukasz BARANIEWICZ

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Lukasz BARANIEWICZ, lbaraniewicz@outlook.com

* Presented at the 45th IBIMA International Conference, 25-26 June 2025, Cordoba, Spain

Abstract

As organizations expand their digital ecosystems, the security landscape is shifting from isolated breaches to a constant state of exposure. Financial losses are only one dimension of the problem – damage to trust, reputation and operational stability often carries even greater weight. This escalating challenge is not accidental; it stems from the accelerating pace of technological innovation, the global push toward cloud-native infrastructures, the decentralization of corporate IT environments and the growth of connected devices that extend the attack surface far beyond traditional perimeters.
Against this backdrop, the role of cybersecurity teams have become indispensable. Modern IT environments are increasingly complex, making effective monitoring and protection a significant challenge. The effectiveness of these teams depends on threat intelligence, the wisdom and experience of cybersecurity professionals and also on the adoption of advanced technologies enabling proactive detection, real-time threat analysis, automated responses, AI and resilient incident management.
This paper provides a comprehensive review of global standards, methodologies and best practices shaping the current landscape of computer security incident response. It surveys key challenges faced by cybersecurity teams, highlights opportunities for leveraging automation and intelligence-driven tools and examines reference architectures for reliable log collection and analysis. By synthesizing insights from literature and practice, the paper underscores the importance of harmonizing global approaches, adopting cutting-edge technologies and defining future research directions to advance the maturity and effectiveness of incident response worldwide.

Keywords: cybersecurity, threat detection, incident handling, AI

Cite this Article as: Lukasz BARANIEWICZ, Vol. 2025 (13) "Advancing Computer Security Incident Response: Global Standards and Best Practices," Communications of International Proceedings, Vol. 2025 (13), Article ID 4547025, https://doi.org/10.5171/2025.4547025