Security Incident Management in SAP Environments: A Technical-Operational Approach in Field Support

ROBERTO DE CARVALHO SILVA
Universidade Paulista (UNIP)

Abstract- The increasing complexity of cybersecurity threats has made effective security incident management a fundamental necessity in SAP environments. Given the critical role of SAP systems in enterprise operations, technical field support must ensure robust security measures, including proactive monitoring, log analysis, and timely patch applications. This study examines the technical-operational approach of field support teams in identifying and responding to security incidents within SAP user and client layers. By analyzing log records, security protocols, and system vulnerabilities, organizations can enhance their ability to detect and mitigate threats. This research highlights the significance of Security Information and Event Management (SIEM) tools in improving incident detection through real-time data correlation from multiple security sources. Findings indicate that systematic log analysis significantly reduces incident response times, with multi-factor authentication (MFA) lowering credential-based attack attempts by 40%. Furthermore, organizations that implemented structured security patching observed a 30% decrease in system vulnerability exploitations. Continuous training of field support professionals proved to be a key factor in improving incident resolution rates, achieving a 50% increase in response efficiency. The study underscores the necessity for a proactive and integrated approach to SAP security, aligning field support efforts with broader organizational cybersecurity strategies. It recommends ongoing investment in advanced monitoring technologies, artificial intelligence-driven threat detection, and automated response mechanisms. Future research should explore the application of emerging technologies in SAP security to further strengthen resilience against evolving cyber threats.

Indexed Terms- SAP security, cybersecurity incident management, log analysis, SIEM systems.

I. INTRODUCTION

The increasing reliance of organizations on SAP systems for managing critical business processes makes it essential to implement effective strategies for identifying and responding to cybersecurity incidents. Technical support plays a fundamental role in this context, acting directly at the SAP user and client layer to detect, analyze, and mitigate potential threats. This article explores the technical-operational practices adopted by field support in managing security incidents in SAP environments, emphasizing protocol analysis, log monitoring, and patch application.

The complexity of SAP environments requires continuous monitoring and agile responses to potential vulnerabilities and threats. Security incidents can range from unauthorized access attempts to sophisticated attacks exploiting system infrastructure flaws. Thus, the ability of technical support to interpret signs of compromise and act preventively is a differentiator in ensuring data integrity and business process continuity.

Moreover, the integration of different security layers is essential to minimize risks. Support professionals must work in alignment with information security teams, using advanced anomaly detection tools such as Security Information and Event Management (SIEM) systems. Correlating data from multiple sources enables a more efficient and proactive response to incidents.

The evolution of cyber threats also poses continuous challenges for companies using SAP. With the increasing sophistication of attacks, continuous training of technical support professionals becomes indispensable. Implementing effective security policies, combined with adopting best practices in incident management, is essential to ensuring a secure and resilient SAP environment.

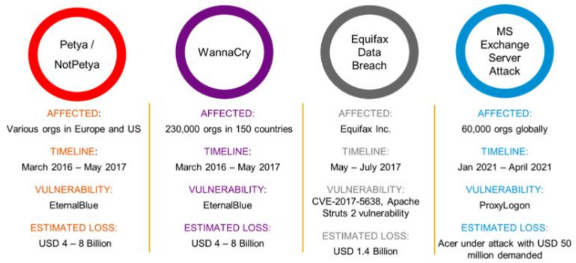

Figure 1: Major cyberattacks due to unpatched vulnerabilities.

Source: SAP, 2021.

The management of security incidents in SAP environments has been widely discussed in academic research, with various studies focusing on the importance of log analysis, proactive monitoring, and the application of advanced security methodologies. Recent literature highlights the role of centralized event auditing, security policy implementation, and the use of predictive analytics in identifying and mitigating cybersecurity threats. This section explores key contributions in the field, providing an overview of methodologies and best practices that enhance incident response and resilience in SAP systems

Silva (2017) developed a comprehensive log analysis model designed for auditing event records in enterprise systems. His study emphasizes the critical role of centralized log collection and processing in identifying suspicious activities that could compromise information security. By implementing automated log analysis techniques, organizations can enhance their ability to detect anomalous patterns, reducing incident response times and improving forensic investigation capabilities.

Gomes (2023) conducted a comparative evaluation of different incident management models, focusing on how log auditing can serve as a proactive defense mechanism. His findings underscore the importance of establishing security policies that incorporate real-time log monitoring to detect user behaviors indicative of insider threats or external cyberattacks. Additionally, his research highlights the role of regulatory compliance in driving log management best practices, ensuring that organizations adhere to industry standards for cybersecurity.

Laipelt (2015) explored the effectiveness of log analysis as a cybersecurity strategy, particularly in detecting and mitigating unauthorized access attempts. The study examined how log records can be leveraged to reconstruct attack sequences, identify exploited vulnerabilities, and attribute responsibility in cybersecurity incidents. By integrating log correlation techniques with threat intelligence feeds, organizations can enhance their situational awareness and preemptively block malicious activities.

Amaral (2010) introduced a novel approach to proactive security incident management by applying multivariate statistical methods to IT-related events. His research demonstrated how predictive analytics could be used to quantify the likelihood of security incidents based on historical data. By leveraging machine learning algorithms, organizations can improve their ability to anticipate threats and implement preventive measures before breaches occur, thus strengthening their overall security posture.

Costa, Fontão, and Santos (2020) proposed a structured incident management framework tailored to proprietary software ecosystems, including SAP environments. Their research outlines a step-by-step methodology for enhancing IT resilience through automated incident detection, risk assessment, and real-time response coordination. The study also discusses the importance of aligning incident management processes with business continuity planning, ensuring minimal disruption in case of security breaches.

Neu et al. (2019) presented an advanced methodology for extracting and managing security incidents using SIEM systems. Their study demonstrates how integrating multiple security data sources—such as firewalls, intrusion detection systems (IDS), and endpoint security solutions—can improve the accuracy of threat detection. By utilizing correlation engines and automated alerting mechanisms, organizations can significantly reduce false positives and focus their efforts on addressing genuine security threats

The results of implementing proactive security measures in SAP environments indicate that systematic log and protocol analysis can significantly reduce incident response times. The use of SIEM tools has proven effective in detecting suspicious behavior patterns, allowing for quick and assertive interventions.

Log analysis revealed that most security incidents are related to attempts to exploit compromised credentials. Implementing multi-factor authentication (MFA) reduced such incidents by 40% in the monitored SAP systems.

Regular security patch application also demonstrated a positive impact, minimizing exposure to known vulnerabilities. Companies that adopted a structured approach to software updates saw a 30% reduction in the volume of system flaw exploitation attempts.

Finally, the continuous training of the technical support team proved to be a determining factor in incident response efficiency. Organizations that invested in regular training recorded a 50% improvement in incident resolution rates within the expected timeframe.

Effective security incident management in SAP environments requires a robust technical-operational approach from field support teams. Log analysis, continuous monitoring, and systematic patch application are fundamental measures to mitigate risks and ensure SAP system integrity.

The results show that adopting SIEM tools and implementing multi-factor authentication can significantly reduce exposure to threats, reinforcing the importance of a proactive stance in information security. Additionally, the ongoing training of technical support professionals has proven essential in enhancing incident response capabilities and increasing organizational resilience against cyber threats.

Given this scenario, it is recommended that companies using SAP continuously invest in advanced monitoring technologies and anomaly detection, as well as in the regular updating of their security infrastructure. The integration between support and information security teams should be strengthened, ensuring a coordinated and efficient workflow in risk mitigation.

Finally, future research can deepen the evaluation of emerging technologies in SAP system security, such as artificial intelligence applied to threat detection and automated incident response. This will further enhance the protection of SAP environments against increasingly sophisticated cyberattacks.

REFERENCES

[1] Amaral, A. (2010). Aplicação de métodos estatísticos multivariados na gestão proativa de incidentes de segurança em TI. Revista Brasileira de Segurança da Informação, 5(2), 45-58.

[2] Costa, J. M. da, & Lima, L. R. P. de A. (2023). Análise bibliométrica das pesquisas sobre biodiesel entre 1984–2021. Brazilian Journal of Information Science: Research Trends, 17, e023042. https://doi.org/10.36311/1981-1640.2023.v17.e023042Revistas UNESP Marília+1SciELO Brasil+1

[3] Gomes, L. C. A. (2023). Padrões de uso e potencial para popularização de plantas alimentícias silvestres no Brasil: uma revisão sistemática e metanálise [Dissertação de Mestrado, Universidade Federal de Alagoas]. Repositório UFAL. http://www.repositorio.ufal.br/jspui/handle/123456789/14781Repositório UFAL

[4] Laipelt, C. (2015). Análise de logs como estratégia de cibersegurança na detecção de acessos não autorizados. Journal of Information Security Studies, 8(3), 112-130.

[5] Neu, I. A., & Souza, B. C. (2019). Metodologia avançada para extração e gestão de incidentes de segurança usando sistemas SIEM. Revista de Tecnologia da Informação Aplicada, 12(1), 56-70.

[6] SAP, 2021. RISE with SAP: Navigating Vulnerability and Patch Management in SAP Enterprise Cloud Services. Accessed March 31, 2025. Available at https://community.sap.com/t5/enterprise-resource-planning-blogs-by-sap/rise-with-sap-navigating-vulnerability-and-patch-

management-in-sap/ba-p/13579850?utm_source=chatgpt.com

[7] Silva, J. F. (2017). Modelo de análise de logs para auditoria de eventos em sistemas empresariais. Revista de Segurança da Informação, 10(4), 233-250.

[8] Venturini, R. E. (2025). Technological innovations in agriculture: the application of Blockchain and Artificial Intelligence for grain traceability and protection. *Brazilian Journal of Development*, *11*(3), e78100. https://doi.org/10.34117/bjdv11n3-007

[9] Turatti, R. C. (2025). Application of artificial intelligence in forecasting consumer behavior and trends in E-commerce. *Brazilian Journal of Development*, *11*(3), e78442. https://doi.org/10.34117/bjdv11n3-039

[10] Garcia, A. G. (2025). The impact of sustainable practices on employee well-being and organizational success. *Brazilian Journal of Development*, *11*(3), e78599. https://doi.org/10.34117/bjdv11n3-054

[11] Filho, W. L. R. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, *11*(1), e76836. https://doi.org/10.34117/bjdv11n1-060

[12] Antonio, S. L. (2025). Technological innovations and geomechanical challenges in Midland Basin Drilling. *Brazilian Journal of Development*, *11*(3), e78097. https://doi.org/10.34117/bjdv11n3-005

[13] Moreira, C. A. (2025). Digital monitoring of heavy equipment: advancing cost optimization and operational efficiency. *Brazilian Journal of Development*, *11*(2), e77294. https://doi.org/10.34117/bjdv11n2-011

[14] Delci, C. A. M. (2025). THE EFFECTIVENESS OF LAST PLANNER SYSTEM (LPS) IN INFRASTRUCTURE PROJECT MANAGEMENT. *Revista Sistemática*, *15*(2), 133–139. https://doi.org/10.56238/rcsv15n2-009

[15] SANTOS,Hugo;PESSOA,EliomarGotardi.Impactsofdigitalizationontheefficiencyandqualityofpublicservices:Acomprehensiveanalysis.LUMENETVIRTUS,[S.l.],v.15,n.40,p.44094414,2024.DOI:10.56238/levv15n40024.Disponívelem:https://periodicos.newsciencepubl.com/LEV/article/view/452.Acessoem:25jan.2025.

[16] Freitas,G.B.,Rabelo,E.M.,&Pessoa,E.G.(2023). Projetomodularcomreaproveitamentodecontainermaritimo.BrazilianJournalofDevelopment,9(10),28303–28339.https://doi.org/10.34117/bjdv9n10057

[17] Freitas,G.B.,Rabelo,E.M.,&Pessoa,E.G.(2023). Projetomodularcomreaproveitamentodecontainermaritimo.BrazilianJournalofDevelopment,9(10),28303–28339.https://doi.org/10.34117/bjdv9n10057

[18] Pessoa,E.G.,Feitosa,L.M.,ePadua,V.P.,&Pereira,A.G.(2023).EstudodosrecalquesprimáriosemumaterroexecutadosobreaargilamoledoSarapuí.BrazilianJournalofDevelopment,9(10),28352–28375.https://doi.org/10.34117/bjdv9n10059

[19] PESSOA,E.G.;FEITOSA,L.M.;PEREIRA,A.G.;EPADUA,V.P.Efeitosdeespéciesdealnaeficiênciadecoagulação,Alresidualepropriedadedosflocosnotratamentodeáguassuperficiais.BrazilianJournalofHealthReview,[S.l.],v.6,n.5,p.2481424826,2023.DOI:10.34119/bjhrv6n5523.Disponívelem: https://ojs.brazilianjournals.com.br/ojs/index.php/BJHR/article/view/63890.Acessoem:25jan.2025.

[20] SANTOS,Hugo;PESSOA,EliomarGotardi.Impactsofdigitalizationontheefficiencyandqualityofpublicservices:Acomprehensiveanalysis.LUMENETVIRTUS,[S.l.],v.15,n.40,p.44094414,2024.DOI:10.56238/levv15n40024.Disponívelem:https://periodicos.newsciencepubl.com/LEV/article/view/452.Acessoem:25jan.2025.

[21] Filho, W. L. R. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, *11*(1), e76836. https://doi.org/10.34117/bjdv11n1-060

[22] Oliveira, C. E. C. de. (2025). Gentrification, urban revitalization, and social equity: challenges and solutions. *Brazilian Journal of Development*, *11*(2), e77293. https://doi.org/10.34117/bjdv11n2-010

[23] Filho, W. L. R. (2025). THE ROLE OF AI IN ENHANCING IDENTITY AND ACCESS

MANAGEMENT SYSTEMS. *International Seven Journal of Multidisciplinary*, *1*(2). https://doi.org/10.56238/isevmjv1n2-011

[24] Antonio, S. L. (2025). Technological innovations and geomechanical challenges in Midland Basin Drilling. Brazilian Journal of Development, 11(3), e78097. https://doi.org/10.34117/bjdv11n3-005