4ª EDIÇÃO Science & Business Connection by colmeia

TECNOLOGIA BLOCKCHAIN PARA GARANTIA DA INTEGRIDADE DE LOGS EM INCIDENTES DE SEGURANÇA CIBERNÉTICA

Ana Livia dos Santos Lopes[1]; Jacquys Barbosa da Silva[2]; Wesley Novaes Fioreze Costa[3]; Anderson Adelson de Matos[4]

[1]Faculdade de Tecnologia SENAI Félix Guisard; ana.livia.santos.lopes@gmail.com
[2]Faculdade de Tecnologia SENAI Félix Guisard; jacquys0801@gmail.com
[3]Faculdade de Tecnologia SENAI Félix Guisard; wesley.fioreze@docente.senai.br
[4]Faculdade de Tecnologia SENAI Félix Guisard; anderson.matos@sp.senai.br

Resumo: A integridade dos registros de eventos em incidentes de segurança cibernética é um pilar fundamental da cadeia de custódia no processo de gerenciamento dos vestígios, sendo essencial para a resposta a incidentes e auditoria forense. No entanto, em cenários de comprometimento de servidores, invasores frequentemente alteram ou apagam esses registros para ocultar ações maliciosas, invalidando a trilha de evidências e impossibilitando a reconstrução dos fatos. Neste contexto, o presente estudo propõe e avalia experimentalmente uma arquitetura de proteção de logs baseada na imutabilidade da tecnologia Blockchain permissionada e no uso de métodos criptográficos com o algoritmo Secure Hash Algorithm 256-bit (SHA-256). O projeto, de forma exploratória e quantitativa, utiliza uma abordagem descentralizada onde o valor hash de arquivos de log é gerado e registrado de forma indelével em um contrato inteligente desenvolvido em linguagem Solidity, dentro do ecossistema Blockchain. A implementação foca na criação de um script de monitoramento contínuo que vincula o hash ao registro temporal, garantindo que qualquer modificação posterior no arquivo original seja detectada na verificação que confronta o estado atual do log com o registro imutável em blockchain, permitindo a rastreabilidade e a não perda de dados sensíveis para equipes de Resposta a Incidentes. Para assegurar a capacidade inerente contra invasores e o registro seguro de transações, o modelo foi validado em um ambiente de testes experimental estruturado com Docker, uma plataforma que permite empacotar, distribuir e executar aplicações em ambientes isolados, para a orquestração de microsserviços, garantindo isolamento e escalabilidade controladas. A rede blockchain escolhida foi Hyperledger Besu, por sua eficiência em ambientes corporativos e de testes. A arquitetura é integrada ao Gerenciamento de Eventos e Informações de Segurança (SIEM) Wazuh, que atua como o motor de monitoramento de integridade, disparando alertas automáticos sempre que uma discrepância entre o log local e o registro em blockchain for identificada. Os principais stakeholders deste projeto incluem equipes de Resposta a Incidentes, especialistas em segurança cibernética, administradores de sistemas de Tecnologia da Informação e empresas que lidam com dados sensíveis. Os resultados indicam que o modelo proposto mitiga a perda de dados e aumenta a confiabilidade das organizações, consolidando-se como um método eficaz de proteção de ativos digitais. Além disso, a solução apresenta requisitos de implementação que incluem a compatibilidade com sistemas operacionais diversos e o alinhamento estratégico com o ODS 9 (Indústria, Inovação e Infraestrutura), ao fortalecer a resiliência da infraestrutura digital corporativa.

Embora existam riscos tecnológicos, como a escalabilidade da blockchain frente a grandes volumes de dados e o desempenho em tempo real, a inovação é do tipo incremental, aprimorando sistemas de log tradicionais com uma camada descentralizada de prova de integridade capaz de suportar as ameaças cibernéticas em constante evolução.

Palavras-chave: Segurança Cibernética; Blockchain; Integridade de Dados; Forense Digital;

4ª EDIÇÃO Science & Business Connection by colmeia

BLOCKCHAIN TECHNOLOGY FOR ENSURING LOG INTEGRITY IN CYBERSECURITY INCIDENTS

Ana Livia dos Santos Lopes[1]; Jacquys Barbosa da Silva[2]; Wesley Novaes Fioreze Costa[3]; Anderson Adelson de Matos[4]

[1]Faculdade de Tecnologia SENAI Félix Guisard; ana.livia.santos.lopes@gmail.com
[2]Faculdade de Tecnologia SENAI Félix Guisard; jacquys0801@gmail.com
[3]Faculdade de Tecnologia SENAI Félix Guisard; wesley.fioreze@docente.senai.br
[4]Faculdade de Tecnologia SENAI Félix Guisard; anderson.matos@sp.senai.br

Abstract: The integrity of event logs in cybersecurity incidents is a fundamental pillar of the custody chain in the process of managing evidence, being essential for incident response and forensic auditing. However, in server compromise scenarios, attackers frequently alter or delete these logs to conceal malicious actions, invalidating the trail of evidence and making it impossible to reconstruct the facts. In this context, this study proposes and experimentally evaluates a log protection architecture based on the immutability of permissioned Blockchain technology and the use of cryptographic methods with the Secure Hash Algorithm 256-bit (SHA-256). The project, in an exploratory and quantitative manner, uses a decentralized approach where the hash value of log files is generated and indelibly recorded in a smart contract developed in Solidity language, within the Blockchain ecosystem. The implementation focuses on creating a continuous monitoring script that links the hash to the temporal record, ensuring that any subsequent modification to the original file is detected in the verification that compares the current state of the log with the immutable record on the blockchain, allowing traceability and preventing the loss of sensitive data for Incident Response teams. To ensure inherent protection against intruders and secure transaction logging, the model was validated in an experimental test environment structured with Docker, a platform that allows packaging, distribution, and execution of applications in isolated environments for microservice orchestration, ensuring controlled isolation and scalability. The chosen Blockchain network was Hyperledger Besu, due to its efficiency in corporate and testing environments. The architecture is integrated with the Wazuh Security Information and Event Management (SIEM) system, which acts as the integrity monitoring engine, triggering automatic alerts whenever a discrepancy between the local log and the blockchain record is identified. The main stakeholders in this project include Incident Response teams, cybersecurity specialists, IT system administrators, and companies that handle sensitive data. The results indicate that the proposed model mitigates data loss and increases organizational reliability, establishing itself as an effective method for protecting digital assets. Furthermore, the solution presents implementation requirements that include compatibility with diverse operating systems and strategic alignment with SDG 9 (Industry, Innovation and Infrastructure), strengthening the resilience of corporate digital infrastructure. Although technological risks exist, such as the scalability of Blockchain in the face of large data volumes and real-time performance, the innovation

is incremental, enhancing traditional logging systems with a decentralized integrity proof layer capable of supporting constantly evolving cyber threats.

Keywords: Cybersecurity; Blockchain; Data Integrity; Digital Forensics;