SISTEMA FORENSE DE ANÁLISE DE LOGS - DA CUSTÓDIA À TIPIFICAÇÃO DE AMEAÇAS AVANÇADAS

Congresso Catarinense de Ciências Forenses, 1ª edição, de 24/06/2026 a 26/06/2026
ISBN dos Anais: 978-65-5465-186-8

OLIVEIRA; Pablo Agnaldo Marques [1], LIMA; Eliomar Araújo de [2]

RESUMO

Introdução: A segurança digital enfrenta o desafio do Big Data Forense e a evolução de Ameaças Persistentes Avançadas (APTs) que empregam táticas furtivas Living off the Land (LotL). Ferramentas tradicionais geram fadiga de alertas ao focarem em análises atômicas isoladas, negligenciando a rastreabilidade jurídica da evidência [1]. **Objetivo(s):** Apresentar o Sistema Forense de Análise de Logs (SFAL), arquitetura air-gapped multicamadas para otimizar a detecção de ameaças complexas, garantir a cadeia de custódia criptográfica e materializar o modelo de Forense Digital e Tipificação de Incidentes (DFIT). **Método:** O SFAL emprega microsserviços (Rust e Python) orquestrados via Redis e DuckDB. Atua em camadas: atômica (regras MITRE ATT&CK [2]), comportamental e cognitiva (ML e Grafos). A integridade é garantida por Árvores de Merkle e laudos gerados por SLM. A validação, em ambiente com processador Ryzen 7 3750H, dividiu-se em: teste funcional com APT simulada (PHANTOM-0) via MITRE CALDERA e teste de carga processando 1.000.000 de eventos Windows EVTX em streaming. **Resultados:** No teste de carga, a arquitetura evitou estouros de memória, contendo o pico em 4,02 GB. A ingestão atingiu 15.748 Eventos Por Segundo (EPS), evidenciando o poder da linguagem Rust. O enriquecimento (2.533 EPS) e a correlação (2.469 EPS) cadenciaram o processamento para suportar a complexidade algorítmica. No teste funcional, o funil mitigou a fadiga de alertas, condensando os rastros do ataque em 16 descobertas de alta fidelidade: execução, persistência, evasão, acesso a credenciais e movimento lateral. **Considerações finais:** O SFAL comprova a viabilidade de harmonizar triagem de ameaças com a admissibilidade legal da evidência. Ao integrar nativamente cadeia de custódia e métodos validados [3] ao arcabouço jurídico brasileiro, a arquitetura materializa o paradigma DFIT na perícia computacional moderna. **Referências:** Lin X. Introductory Computer Forensics. Springer; 2018. Strom BE et al. MITRE ATT&CK. J Cybersecurity Privacy. 2020. ISO/IEC 27037:2012.

PALAVRAS-CHAVE: Informática Forense, Inteligência Artificial, Cadeia de Custódia, Tipificação de Incidentes, Big Data

[1] Universidade Federal de Goiás – Instituto de Informática, pablooliveira@discente.ufg.br
[2] Universidade Federal de Goiás – Instituto de Informática, eliomar.lima@ufg.br

[1] Universidade Federal de Goiás – Instituto de Informática, pablooliveira@discente.ufg.br
[2] Universidade Federal de Goiás – Instituto de Informática, eliomar.lima@ufg.br