| [**Paper**](https://jems.sbc.org.br/ListPapers.cgi?c=4511&sortby=paper&showreviewer=0&topic=&category=&track=&papergroup=&excel=3&fieldList=paper&fieldList=papertitle&statusList=accepted) | [**Title**](https://jems.sbc.org.br/ListPapers.cgi?c=4511&sortby=papertitle&showreviewer=0&topic=&category=&track=&papergroup=&excel=3&fieldList=paper&fieldList=papertitle&statusList=accepted) |
| --- | --- |
| 240614 | *Vulnerabilidades de Segurança Cibernética em Dispositivos de Medição Avançada de Energia Elétrica* |
| 240700 | *Uso do TF-IDF na Comparação de Dados para Detecção de Ransomware* |
| 240764 | *Abrindo a Caixa-Preta - Aplicando IA Explicável para Aprimorar a Detecção de Sequestros de Prefixo* |
| 240767 | *Cross-Site Script Inclusion: um estudo das estratégias de mitigação e atual prevalência da vulnerabilidade em navegadores* |
| 240768 | *SAPO-BOI: Pulando a Pilha de Rede no Desenvolvimento de um NIDS Baseado em BPF/XDP* |
| 240800 | *Impacto de ataques de evasão e eficácia da defesa baseada em treinamento adversário em detectores de malware* |
| 240810 | *SECAdvisor: a Tool for Cybersecurity Planning using Economic Models* |
| 240851 | *Lattice Base Reduction Attack on Matrix NTRU* |
| 240859 | *Cutting dimensions in the LLL attack for the ETRU post-quantum cryptosystem* |
| 241289 | *A study on user-specific threshold configuration for keystroke dynamics in the context of adaptive biometric systems* |
| 241370 | *Uma Arquitetura baseada em Inteligência Artificial Explicável (XAI) para Sistemas de Detecção de Intrusões em Smart Grids* |
| 241371 | *Kill Chain Catalyst for Autonomous Red Team Operations in Dynamic Attack Scenarios* |
| 241372 | *Case Study: Parallel Network Topologies Between Redundant OT Networks Implemented with Different Protocols* |
| 241377 | *Gerenciamento de Conexões usando Firewall Automatizado a partir de Dados de Inteligência sobre Ameaças* |
| 241410 | *Detecção de Intrusão e Análise Cyberfísica em Redes Industriais* |
| 241416 | *Impacto do Aprendizado de Máquina Adversário contra Detectores de Anomalias em Séries Temporais* |
| 241419 | *Análise comparativa de IAs generativas como ferramentas de apoio à programação segura* |
| 241421 | *Modelos Interpretáveis com Inteligência Artificial Explicável (XAI) na Detecção de Intrusões em Redes Intra-Veiculares Controller Area Network (CAN)* |
| 241431 | *DogeFuzz: A Simple Yet Efficient Grey-box Fuzzer for Ethereum Smart Contracts* |
| 241433 | *Caracterização de conhecimentos e comportamentos de cibersegurança: Estudo exploratório com dados predominantes do extremo norte brasileiro* |
| 241435 | *Obsolescência não-Programada: Análise do Uso de Software Desatualizado em Ambiente de Produção* |
| 241445 | *Detecção de Ataques de GPS em Veículos Aéreos Não Tripulados com Classificação Multiclasse* |
| 241449 | *Modified versions of ML-KEM based on Brazilian government cryptographic resources* |
| 241466 | *Automatização da Seleção de Modelos Não Supervisionados na Predição de Ataques DDoS* |
| 241469 | *Utilizando Estratégias de Monitoramento Leve em Ambientes Conteinerizados para Detecção de Anomalias via HIDS* |
| 241472 | *Avaliação de algoritmos de machine learning para detecção de malware IoT no dataset IoT-23* |
| 241475 | *O Impacto de Software Anti-cheat na Privacidade do Usuário* |
| 241483 | *Implementação e avaliação da cifra de fluxo Forro14 em hardware programável Tofino usando a linguagem P4* |
| 241485 | *Detecção de Intrusão Através de Redes Neurais Profundas com Saídas Antecipadas para Inferência Rápida e Confiável* |
| 241486 | *Detecção de Mídias Pornográficas em Dispositivos com Recursos Limitados para Controle Parental* |
| 241488 | *Construção de um Modelo Orientado a Dados para Detecção de Fraudes em Cartões de Crédito utilizando Dados Sintéticos* |
| 241490 | *Detecção Hierárquica Confiável de Malware de Android Baseado em Arquiteturas CNN* |
| 241511 | *Descriptografando: Experimento em Análise de Memória Volátil Aplicada à Defesa Contra Ransomware* |
| 241518 | *Um Framework Baseado na Pilha ELK Para Análise Pós-Intrusão de Ataques de DDoS* |
| 241567 | *Desafios e oportunidades de pesquisa na adoção de criptografia pós-quântica em redes veiculares* |
| 241574 | *k-DynMix: Um Mecanismo de Proteção Dinâmica de Privacidade em Mix-Zones* |
| 241619 | *Um Framework Gerador de Tráfego para Detecção de Intrusões em Redes CAN* |
| 241630 | *Análise de ocorrência de falso positivos em recuperação de dados formatados* |
| 241632 | *MH-1M: One of The Most Comprehensive and Up-to-Date Dataset for Advanced Android Malware Detection* |
| 241637 | *DoH Deception: Evading ML-Based Tunnel Detection Models with Real-world Adversarial Examples* |
| 241645 | *Análise de Vulnerabilidades da Plataforma Moodle com base no Top 10 da OWASP* |
| 241677 | *Practical algorithms and parameters for modification-tolerant signature scheme* |
| 241680 | *Federated Learning under Attack: Improving Gradient Inversion for Batch of Images* |
| 241681 | *Identificação de Endereços IP Dinâmicos com Dados Públicos* |
| 241682 | *SIM-Ciber: Uma Solução Baseada em Simulações Probabilísticas para Quantificação de Riscos e Impactos de Ciberataques Utilizando Relatórios Estatísticos* |
| 241684 | *Detecção de Ataques de Negacão de Serviço Distribuídos com Algoritmos de Aprendizado de Máquina* |
| 241689 | *Bifocal Agent: Identificando automaticamente funções maliciosas para aumentar o foco do analista de malware* |
| 241693 | *Comprehensive Ransomware Detection: Optimization of Feature Selection through Machine Learning Algorithms and Explainable AI on Memory Analysis* |
| 241712 | *A Triad of Defenses to Mitigate Poisoning Attacks in Federated Learning* |
| 241721 | *Identificação de Serviços e Dispositivos em Dados de Motores de Busca para o Enriquecimento de Análise de Vulnerabilidades* |
| 241728 | *Uma Análise Compreensiva e Exaustiva de Métodos de Seleção de Características para Detecção de Malware Android* |
| 241730 | *ECO-SA: Estratégia de Contenção Otimizada da Propagação em Câmaras de Eco utilizando Simulated Annealing* |
| 241731 | *Geração de dados sintéticos tabulares para detecção de Malwares Android: um estudo de caso* |
| 241733 | *Best Cryptanalysis of Lightweight cipher FUTURE* |
| 241757 | *ToID: Reputação Baseada em Identificadores Descentralizados Para Aplicações Distribuídas* |
| 241759 | *Um esquema baseado em blockchain por Proof-of-Download para gerenciamento de direitos digitais e detecção de traidores* |
| 241760 | *Automação de Autenticação para Testes de Segurança em Aplicações Web no OWASP ZAP* |
| 241763 | *PTP Flood: ataque cibernetico de DoS em cliente PTP* |
| 241765 | *Trust, but Verify: Evaluating Developer Behavior in Mitigating Security Vulnerabilities in Open-Source Software* |
| 241766 | *D-NAC: Controle de acesso distribuído para redes de dados nomeados* |
| 241769 | *Detecção de Varreduras de Portas pela Análise Inteligente de Tráfego de Rede IoT* |
| 241772 | *MAV: Metodologia de Análise de Ameaças e Vulnerabilidades em um framework integrado multiplataforma* |
| 241778 | *Observação de Ataques contra a Memória do Kernel Android: Desafios e Soluções* |
| 241780 | *IWSHAP: Um Método de Seleção Incremental de Características para Redes CAN baseado em Inteligência Artificial Explicável (XAI)* |
| 241781 | *Firewalls de Próxima Geração (NGFW): Funcionalidades, Aplicações e Vulnerabilidades* |
| 241782 | *Classificação de Risco de Vulnerabilidades de Segurança via Processos Gaussianos e Aprendizado Ativo* |
| 241786 | *Exploring Digital Signatures Secrecy in Web-Platform: a Client-Side Cryptographic Operations.* |
| 241787 | *Além do Sinal: Autenticação Biofísica com Wi-Fi CSI e Raspberry Pi* |
| 241788 | *On-Device Network Intrusion Detection for Resource-Constrained Devices of the Internet of Things* |
| 241843 | *Requirements for a hybrid TPM based on optimized ML-DSA post-quantum signature* |