SEGURANÇA SEM GESTÃO É CORREÇÃO

Integrações de Práticas de Segurança no Desenvolvimento de Software

Cristiano Siqueira Israel
Fatec Assis
cristiano.israel@fatec.sp.gov.br

Dr. Fabio Eder Cardoso
Fatec Assis
fabio.cardoso6@fatec.sp.gov.br

RESUMO

Este artigo apresenta a teoria aos principais padrões e normas de segurança implementados na gestão do desenvolvimento de software. O foco está nos *frameworks* OWASP SAMM, SBOM, Security by Design e na cultura SecDevOps, amplamente aceitos no setor de segurança da informação. O objetivo do estudo é avaliar, teoricamente, a eficácia da gestão desses padrões, com base em pesquisas acadêmicas e práticas documentadas. A implementação prática desses *frameworks* será abordada em estudos futuros, com o intuito de fornecer suporte à gestão de desenvolvimento seguro, aplicando melhores práticas obtidas a partir da teoria aqui apresentada. A aplicação desses *frameworks* ao longo do ciclo de vida do software é fundamental para assegurar a conformidade e demonstrar a eficácia da segurança contínua. Além disso, entrevistas técnicas com especialistas da área foram conduzidas e serão apresentadas em um trabalho futuro, com o objetivo de complementar a análise teórica com dados práticos e oferecer uma visão mais completa sobre a aplicabilidade dos padrões discutidos.

Palavras-chave: Desenvolvimento. Segurança. SecDevOps.

ABSTRACT

This article presents the theory of the main security standards and norms implemented in software development management. The focus is on the OWASP SAMM, SBOM, Security by Design frameworks, and the SecDevOps culture, widely accepted in the information security sector. The aim of the study is to theoretically assess the effectiveness of managing these standards, based on academic research and documented practices. The practical implementation of these tools will be addressed in future studies, with the intention of providing support for secure development management, applying best practices obtained from the theory presented here. The application of these frameworks throughout the software lifecycle is essential to ensure compliance and demonstrate the effectiveness of continuous security. Additionally, technical interviews with specialists in the field were conducted and will be presented in a future work, with the objective of complementing the theoretical analysis with practical data and offering a more complete view of the applicability of the discussed standards.

Keywords: Development. Security. SecDevOps.

1 INTRODUÇÃO

Nos últimos anos, a segurança no desenvolvimento de software emergiu como uma questão estratégica para grandes corporações, principalmente devido à crescente sofisticação das ameaças cibernéticas, que afetam diretamente a continuidade dos negócios, a reputação corporativa e o cumprimento das exigências regulatórias (Jones, 2018). O desenvolvimento de software sem as devidas práticas de segurança pode comprometer operações críticas e expor as organizações a ataques cibernéticos que resultem em interrupções de negócio.

Desde os primeiros incidentes de segurança cibernética, como os experimentos de autorreplicação de John von Neumann e o vírus Creeper, o cenário da segurança digital tem evoluído consideravelmente. O rápido avanço tecnológico, incluindo a popularização da Internet na década de 1990, aumentou drasticamente a interconectividade global, ampliando os vetores de ataque e criando novas vulnerabilidades (Neumann, 1966; Schneier, 2015). O modelo tradicional de defesa, baseado em firewalls e perímetros de segurança, revelou-se ineficaz para combater as ameaças cada vez mais avançadas da era digital. Vulnerabilidades crescentes em cadeias de suprimentos e componentes de software de terceiros se tornaram alvos fáceis para crackers (hackers maliciosos) e outros grupos mal-intencionados, o que torna imperativo adotar uma abordagem proativa de segurança (Ramanathan et al., 2019).

O SecDevOps, prática emergente que integra segurança desde as fases iniciais do ciclo de desenvolvimento de software, tem se consolidado como uma abordagem fundamental para mitigar riscos de forma contínua e escalável. Dada a crescente complexidade das infraestruturas tecnológicas modernas, as organizações precisam adotar uma postura gerencial proativa, que integre segurança em todas as etapas de desenvolvimento e operação dos sistemas (Vehent, 2018; Sehgal, 2023). Para os CISOs (Chief Information Security Officers), a adoção de *frameworks* robustos vai além de atender a exigências regulatórias; é parte fundamental de uma estratégia abrangente para proteger operações críticas e garantir a resiliência digital das organizações (Kim et al., 2018).

Entre os *frameworks* mais destacados está o OWASP SAMM (Software Assurance Maturity Model), que oferece uma metodologia para analisar e melhorar as práticas de segurança ao longo do ciclo de desenvolvimento de software. Outro modelo fundamental é o SBOM (Software Bill of Materials), que promove transparência na cadeia de suprimentos de software, especialmente em um cenário onde bibliotecas de código aberto e componentes de terceiros são amplamente utilizados (OWASP, 2020; Veracode, 2021). A implementação do SBOM assegura que as organizações mantenham um inventário detalhado de todos os componentes de software, o que permite respostas rápidas a vulnerabilidades conhecidas.

Eventos recentes, como o ataque à cadeia de suprimentos da SolarWinds, ilustram os perigos da falta de rastreabilidade de componentes, que expuseram milhares de organizações ao risco de segurança (Schneier, 2024). A ordem executiva do presidente Joe Biden tornou obrigatória a adoção do SBOM por todos os fornecedores de software do governo dos Estados Unidos, visando fortalecer a segurança da cadeia de suprimentos. A medida estabelece padrões rigorosos de rastreamento e transparência nos componentes de software, com sanções previstas para o descumprimento, como a desqualificação de contratos. Para os CISOs, essa regulamentação não apenas alinha programas de segurança às exigências legais, mas também oferece uma oportunidade para fortalecer a resiliência cibernética das organizações através de cultura e melhores práticas (United States, 2022; NIST, 2022).

Soluções como o Dependency Track, suportadas pelo projeto OWASP, facilitam o monitoramento contínuo de riscos e vulnerabilidades na esteira de desenvolvimento, automatizando a correção de falhas em bibliotecas de terceiros e promovendo a colaboração eficaz entre as equipes de desenvolvimento e segurança (OWASP, 2021). A integração dessas soluções com práticas de SecDevOps e Security by Design cria um ambiente seguro e mais colaborativo, com monitoramento contínuo e uma resposta proativa a vulnerabilidades.

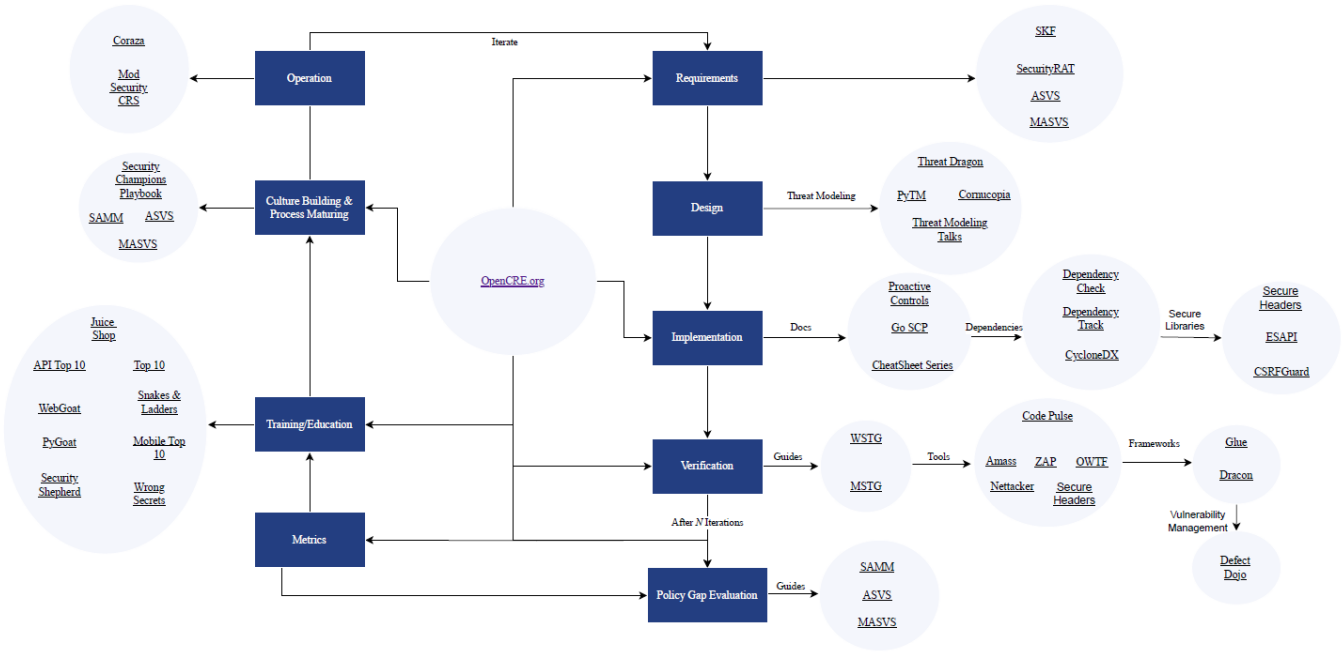
2 DESENVOLVIMENTO

A evolução da segurança da informação e a gestão de desenvolvimento de software têm acompanhado o aumento da complexidade das aplicações web e o crescimento das ameaças cibernéticas. Com o tempo, essas ameaças tornaram-se mais sofisticadas e prejudiciais, exigindo mudanças profundas nas abordagens de segurança. Inicialmente, a segurança era vista como uma preocupação secundária, concentrada principalmente em defesas tradicionais, como firewalls e proteção de perímetros (Kim et al., 2018). De acordo com dados do CERT.br, as crescentes ameaças cibernéticas forçaram as organizações a adotar estratégias proativas, incorporando segurança no ciclo de desenvolvimento de software (CERT.br, 2024).

Uma das mudanças mais significativas foi a necessidade da adoção de práticas como Security by Design e SecDevOps, que defendem a integração da segurança no início do desenvolvimento. Essas abordagens provaram ser eficazes na mitigação de vulnerabilidades, uma vez que permitem a identificação e a resolução de problemas nas fases iniciais, reduzindo drasticamente os custos e os impactos operacionais que surgiriam nas fases finais (Shostack, 2014). Além disso, a estimativa de custos de software, quando alinhada com práticas de segurança, demonstra uma correlação clara entre a identificação precoce de vulnerabilidades e a economia de recursos nas fases

posteriores do desenvolvimento, conforme destacado por Jones (2007). A mudança cultural nas organizações reflete uma compreensão mais profunda sobre a importância de uma segurança integrada e contínua durante todo o ciclo de desenvolvimento (Smith, 2020).

Figura 1 - Software Development LifeCycle.



Fonte: OWASP (2024).

O SecDevOps reflete essa mudança de mentalidade. Organizações que antes viam a segurança como uma prática isolada agora reconhecem sua importância como um processo contínuo (Kim, Behr & Spafford, 2016). A adoção dessa metodologia permite que as empresas otimizem seus investimentos em segurança e minimizem os riscos ao integrar a segurança nas operações diárias de desenvolvimento. A colaboração entre as equipes de desenvolvimento, operações e segurança mostrou-se fundamental para agilizar a identificação e correção de vulnerabilidades, aumentando a eficiência no combate às ameaças cibernéticas com menor custo (Veracode, 2021).

O OWASP SAMM oferece uma estrutura abrangente para medir e aprimorar a maturidade da segurança no desenvolvimento de software. Conforme descrito pelo OWASP (2024), o SAMM permite que os gestores de segurança alinhem suas práticas aos objetivos estratégicos da organização, considerando o nível de maturidade das práticas de proteção e o perfil de risco aceito. Dividido em quatro áreas principais Governança, Design, Implementação e Verificação, o SAMM facilita a adoção incremental

de práticas de segurança, adaptando-se conforme as necessidades específicas de cada empresa (OWASP, 2022).

A flexibilidade do OWASP SAMM é uma de suas maiores vantagens, especialmente para grandes corporações, onde o aumento das ameaças e vulnerabilidades acompanha o crescimento da organização. Empresas que implementaram o SAMM relatam melhorias substanciais na detecção de ameaças e mitigação de riscos, devido à sua capacidade de adaptação a diferentes perfis de risco e necessidades organizacionais. Com a introdução de regulamentações rigorosas, como a Lei de Melhoria da Segurança Cibernética dos EUA, as empresas que adotam o SAMM demonstram maior capacidade de resposta a incidentes e melhor alinhamento com padrões de segurança cibernética globais (Optiv, 2023; OWASP, 2024).

A crescente complexidade das cadeias de suprimentos de software demanda maior transparência na gestão de seus componentes. Para suprir essa necessidade, o SBOM (Software Bill of Materials) foi desenvolvido, fornecendo um inventário detalhado de todos os componentes de software utilizados, associados a versões e vulnerabilidades específicas. O SBOM ganhou destaque após a promulgação da Lei de Melhoria da Segurança Cibernética dos EUA, que exige sua utilização por fornecedores de software que atuam com o governo, garantindo a rastreabilidade e a segurança dos componentes críticos (Optiv, 2023; Schneier, 2024).

Para os CISOs, a implementação do SBOM pode garantir visibilidade e rastreabilidade dos componentes de software utilizados em suas aplicações. Essa transparência facilita a detecção e a correção ágil de vulnerabilidades, reduzindo os riscos de ataques cibernéticos em aplicativos web. Além disso, o uso de SBOMs facilita a conformidade com regulamentações como o NIST Cybersecurity Framework, que se tornou uma referência global em práticas de segurança cibernética (NIST, 2022).

O Dependency Track, uma solução amplamente utilizada, permite o gerenciamento eficaz de componentes de software de terceiros, analisando-os em tempo real. Essa ferramenta automatiza a detecção de vulnerabilidades e possibilita a correção proativa de falhas, promovendo maior eficiência e segurança (OWASP, 2021). Empresas que utilizam o Dependency Track relataram melhorias consideráveis na identificação de vulnerabilidades, possibilitando que as falhas fossem corrigidas antes de chegar à produção (Veracode, 2021). Em um cenário de ameaças cibernéticas em constante evolução, a gestão contínua e proativa de vulnerabilidades é essencial para manter a segurança das operações (Schneier, 20204).

A gestão proativa de vulnerabilidades é crucial para a segurança no ciclo de desenvolvimento de software. Para Jones (2018), a adoção de um programa robusto de gestão de vulnerabilidades deve incluir tanto a identificação antecipada de riscos quanto a rápida aplicação de correções. O uso de ferramentas como o SBOM e o Dependency Track fortalece a segurança contínua, especialmente em ambientes regulados ou de alto risco (Erich et al., 2017).

3 METODOLOGIA

Para alcançar os objetivos propostos, que visam fornecer uma base teórica sólida sobre a aplicação de normas e *frameworks* de segurança no desenvolvimento de software, adotou-se uma abordagem qualitativa. Essa metodologia combina análise documental com estudo de caso, permitindo uma investigação detalhada das práticas de segurança adotadas por grandes corporações. O foco da análise está na validação dos padrões OWASP SAMM, SBOM, Security by Design e SecDevOps, cuja relevância é amplamente respaldada por diretrizes governamentais, como o "Annual Intellectual Property Report to Congress" (Governo dos EUA, 2022).

A primeira etapa da pesquisa consistiu em uma revisão abrangente da literatura sobre o desenvolvimento seguro de software e a gestão contínua de vulnerabilidades. Foram analisados artigos científicos, relatórios técnicos e diretrizes emitidas por instituições renomadas como o OWASP e a NTIA (Administração Nacional de Telecomunicações e Informação). A escolha dessas fontes assegura que os dados sejam fundamentados em evidências sólidas, alinhando-se às melhores práticas de segurança.

Além da análise documental, foram examinados casos de empresas que já implementaram os padrões OWASP SAMM, SBOM e SecDevOps. Essas empresas foram escolhidas por atuarem em setores críticos e pela maturidade de seus programas de segurança. Os estudos de caso forneceram exemplos concretos sobre os desafios enfrentados, as soluções adotadas e os impactos que a implementação desses padrões teve na gestão de vulnerabilidades e na segurança operacional contínua. A análise desses exemplos práticos foi essencial para contextualizar a aplicação teórica dos padrões e alinhá-los às diretrizes internacionais de cibersegurança (Ramanathan et al., 2019).

Outra etapa importante da pesquisa envolveu entrevistas com especialistas da área de segurança da informação e desenvolvimento de software. Esses profissionais, que já utilizam *frameworks* como OWASP SAMM, SBOM e SecDevOps, compartilharam percepções valiosas sobre a eficácia dessas práticas na mitigação de vulnerabilidades. As entrevistas revelaram tanto as dificuldades encontradas durante a implementação e gestão desses padrões quanto os

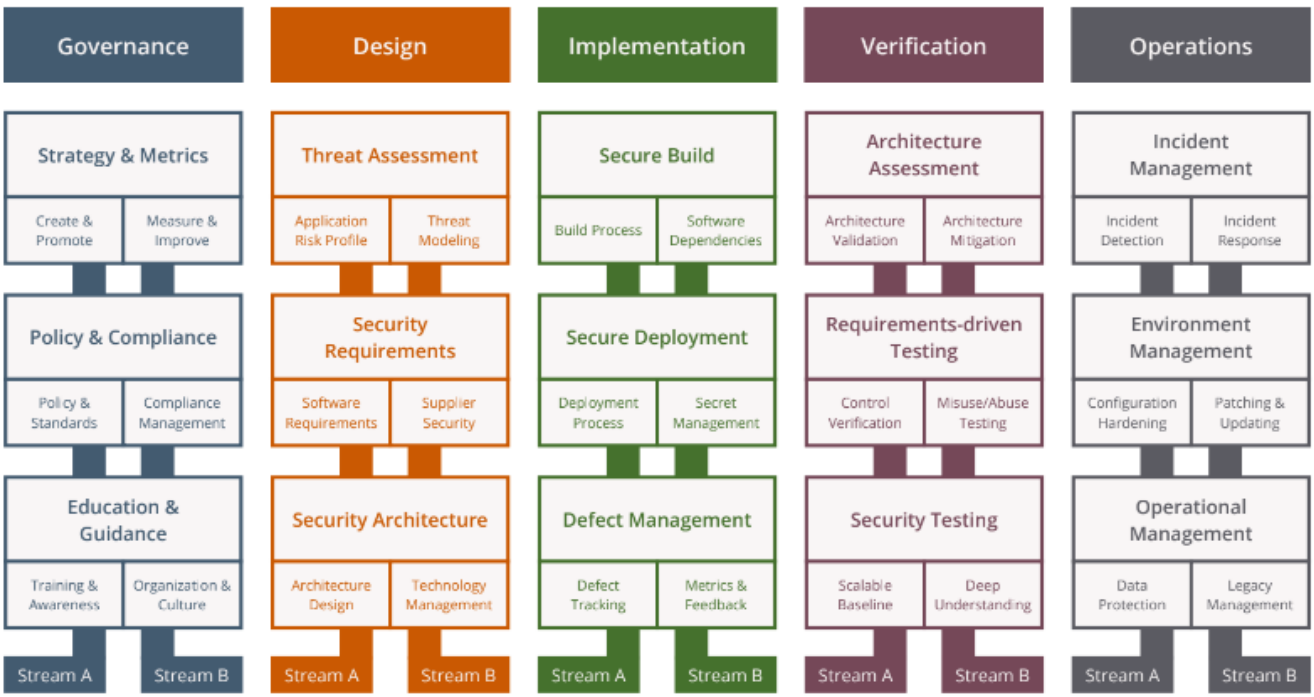
benefícios observados ao longo do tempo. Os dados coletados das entrevistas e dos estudos de caso foram analisados qualitativamente, utilizando técnicas de análise de entrevistas e questionários que serão apresentadas em um trabalho futuro do docente.

4 ANÁLISE DE RESULTADOS E DISCUSSÃO

Os resultados obtidos na pesquisa evidenciam a teoria da importância de uma abordagem estratégica e gerencial para a segurança no desenvolvimento de software. A adoção de padrões como OWASP SAMM, SBOM e cultura SecDevOps mostrou-se essencial para garantir a resiliência das aplicações web e mitigar os riscos ao longo de todo o ciclo de vida do software. Esses *frameworks* fornecem uma base robusta para que os CISOs e gestores de segurança adotem uma postura estruturada e eficiente na gestão de vulnerabilidades e na conformidade com regulamentações emergentes.

Organizações que implementaram o OWASP SAMM relataram melhorias substanciais na capacidade de identificar, mitigar e corrigir vulnerabilidades ainda nas fases iniciais do desenvolvimento de software. Permitiu que essas empresas alinhassem suas práticas de segurança com suas estratégias de negócios, proporcionando agilidade no desenvolvimento e reduzindo a probabilidade de interrupções causadas por incidentes (OWASP, 2020).

Figura 2 - OWASP Software Assurance Maturity Model (SAMM).



Fonte: OWASP SAMM (2024).

O SBOM, por sua vez, trouxe benefícios significativos para a gestão das cadeias de suprimentos de software, com visibilidade detalhada dos componentes utilizados. A maior transparência apresentada no SBOM permiti que as empresas respondessem rapidamente a incidentes, minimizando o impacto de falhas críticas, como as que ocorreram no ataque à cadeia de suprimentos da SolarWinds (Schneier, 2024). Empresas que adotaram o SBOM relataram uma redução no tempo de resposta a vulnerabilidades detectadas em bibliotecas de terceiros e conformidade com regulamentações, como a Lei de Melhoria da Segurança Cibernética dos EUA (NIST, 2022).

A cultura e prática de SecDevOps também foi destacada entre as empresas pesquisadas. Empresas que integraram essa metodologia relataram melhor desempenho na detecção precoce e correção de vulnerabilidades em comparação com aquelas que ainda utilizam modelos tradicionais de desenvolvimento.

A colaboração contínua entre as equipes de desenvolvimento, operações e segurança permitiu uma mitigação proativa dos riscos, eliminando falhas antes que fossem exploradas por agentes maliciosos em produção (Kim et al., 2018). A abordagem de segurança mostrou-se eficaz em ambientes dinâmicos, onde a agilidade no ciclo de desenvolvimento é crucial para a competitividade de mercado e para o cumprimento das exigências regulatórias.

Também trouxeram benefícios financeiros, reduzindo os custos associados à correção de falhas. Empresas que integram a segurança desde o início do ciclo de vida do software conseguem minimizar o retrabalho causado por vulnerabilidades detectadas nas fases finais de produção, resultando em um retorno sobre o investimento em segurança (Shostack, 2014).

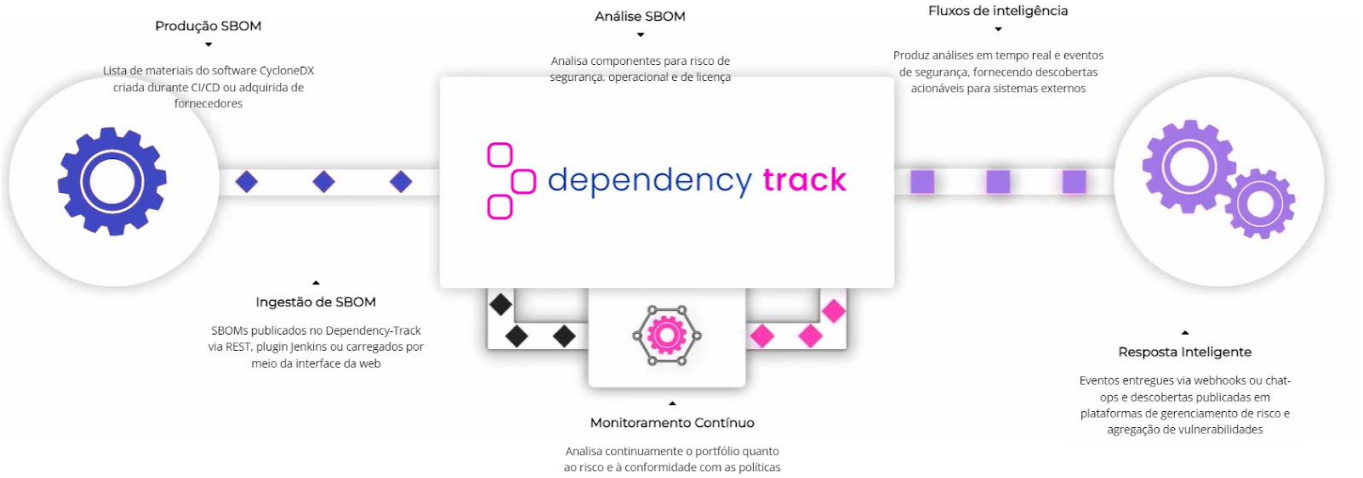
Incidentes recentes, como a descoberta de vulnerabilidades críticas no protocolo HTTP/2, reforçam a importância de práticas robustas de segurança desde as fases iniciais do ciclo de desenvolvimento de software.

A falha "CONTINUATION Flood", que afetou diversas implementações do protocolo HTTP/2, demonstrou a necessidade de monitoramento contínuo e atualizações regulares para manter a integridade dos sistemas web (Microsoft, 2023). Empresas que implementaram revisões constantes de segurança e atualizações automáticas baseadas nos padrões OWASP reduziram significativamente sua exposição a ataques, mitigando o tempo de inatividade e os impactos causados (OWASP, 2022).

A adoção do Dependency Track, em conjunto com o SBOM, também foi destacada como uma solução eficaz para monitorar e gerenciar componentes de software em tempo real. Empresas que utilizam essa ferramenta relataram melhorias consideráveis na resposta a falhas em bibliotecas de código aberto e componentes de terceiros, facilitando a correção de vulnerabilidades antes de entrarem em produção.

Dado o aumento das interdependências entre componentes de software, a gestão contínua e proativa de vulnerabilidades é crucial para manter a segurança das operações (Veracode, 2021).

Figura 3 - OWASP Software Bill of Materials (SBOM).



Fonte: Dependency Track (2024).

Em março de 2022, a Check Point Research revelou uma vulnerabilidade crítica em chips da AMD, que poderia permitir a execução remota de código malicioso em sistemas corporativos. A resposta rápida a essa vulnerabilidade, possibilitada pela implementação de normas de segurança desde a fase de desenvolvimento, foi essencial para mitigar os riscos de exploração em larga escala (Check Point Research, 2022). De forma semelhante, o ataque realizado pelo grupo de hackers DarkHalo em 2023 destacou a relevância de práticas preventivas no desenvolvimento de software, como o uso dos padrões OWASP SAMM e Security by Design, para evitar a exploração de falhas por novas ameaças (FireEye, 2023).

Essas vulnerabilidades reforçam a importância da integração contínua de normas de segurança, permitindo que as empresas não apenas cumpram regulamentações, mas também protejam seus ativos digitais e garantam a continuidade de suas operações em um ambiente dinâmico com ameaças cibernéticas cada vez mais sofisticadas.

E, é importante ressaltar que os dados detalhados sobre a implementação dos padrões e as entrevistas com especialistas serão apresentados em um próximo artigo, produzido pelo mesmo docente em um contexto acadêmico futuro. Esses dados fornecerão uma análise prática aprofundada sobre a eficácia na prática de gestão dos padrões OWASP SAMM, SBOM e cultura SecDevOps na mitigação de vulnerabilidades e gestão aplicada ao fortalecimento da segurança das aplicações web nas organizações.

5 CONSIDERAÇÕES FINAIS

As teorias desta pesquisa evidenciam a importância da gestão estratégica da segurança no desenvolvimento de software, especialmente em um cenário digital complexo e suscetível a ameaças. A adoção de *frameworks* como OWASP SAMM, SBOM e a cultura de SecDevOps desde o início do ciclo de desenvolvimento tem se mostrado fundamental para garantir a resiliência das aplicações web e a proteção dos ativos digitais das organizações.

Ao integrar a segurança em todas as fases do ciclo de vida do software, as empresas podem gerenciar e reduzir as chances de sofrer ataques cibernéticos e, simultaneamente, assegurar a conformidade com regulamentações emergentes. A implementação contínua de práticas de segurança desde no início do desenvolvimento é uma estratégia eficaz da gestão para mitigar vulnerabilidades e aumentar a confiabilidade das aplicações web.

Para os CISOs e gestores de segurança, o uso de soluções como o Dependency Track mostrou-se eficaz na gestão de componentes de software de terceiros. A visibilidade das vulnerabilidades proporcionada pela solução facilita a correção antecipada de falhas e fortalece a governança. Essa governança se torna ainda mais essencial à medida que as organizações enfrentam demandas complexas e desafios operacionais, garantindo que a eficiência não seja comprometida por medidas de segurança.

Por fim, este estudo reafirma que a gestão contínua e proativa da segurança, aliada às práticas de SecDevOps, garante a proteção e conformidade das aplicações ao longo do tempo. A adoção de uma abordagem contínua de monitoramento e correção permite que as empresas não apenas mitiguem riscos de forma preventiva, mas também adaptem suas estratégias de segurança conforme as ameaças cibernéticas evoluem. A relevância dessa abordagem se torna ainda mais evidente diante de incidentes recentes que destacam a fragilidade das cadeias de suprimento de software em um mundo cada vez mais interconectado. Nesse contexto, fica claro que segurança sem gestão é apenas correção uma postura que, em vez de prevenir, apenas reage aos problemas, muitas vezes com consequências significativas para as operações.

6 REFERÊNCIAS

CERT.br. Incidentes Notificados ao CERT.br. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 24 out. 2024.

CHECK POINT RESEARCH. Critical Vulnerability in AMD Chips. 2022. Disponível em: https://www.checkpoint.com/research/. Acesso em: 01 out. 2023.

CISA. Cybersecurity & Infrastructure Security Agency. Disponível em: https://www.cisa.gov/. Acesso em: 09 out. 2024.

ERICH, F. M. A.; AMRANI, A.; SNYDER, C.; STRÜBER, D. Secure Software Engineering: The Role of SBOMs in Large Corporations. Journal of Secure Software Practices, 2017.

FIREEYE. DarkHalo Exploits Print Management Software Vulnerabilities. 2023. Disponível em: https://www.fireeye.com/blog. Acesso em: 01 out. 2023.

JONES, Capers. Estimating Software Costs: Bringing Realism to Estimating. 2. ed. New York: McGraw-Hill, 2007.

JONES, B.; SMITH, C. Secure by Design: How to Create Security-Enhanced Software Design. Wiley, 2018.

KIM, G.; BEHR, K.; SPAFFORD, G. The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win. IT Revolution Press, 2018.

MESQUITA, Michelle. Vamos conversar sobre OWASP SAMM! Medium, 2023. Disponível em: https://michelleamesquita.medium.com/vamos-conversar-sobre-owasp-samm-c0b4e38f88cd. Acesso em: 11 ago. 2024.

MICROSOFT. Microsoft Security Development Lifecycle (SDL). 2022. Disponível em: https://www.microsoft.com/security/sdl/. Acesso em: 05 out. 2023.

NEUMANN, John von. Theory of Self-Reproducing Automata. Urbana: University of Illinois Press, 1966.

NÍCOLAS, P. Alerta de Segurança: Vulnerabilidades "CONTINUATION Flood" no HTTP/2 Expõem Riscos Significativos. LinkedIn, 2023. Disponível em: https://www.linkedin.com/feed/update/urn:li:activity:7182180104804909056/. Acesso em: 11 out. 2024.

NIST. NIST Cybersecurity Framework. 2022. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 06 out. 2023.

NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018. Disponível em: https://www.nist.gov/. Acesso em: 06 out. 2023.

OPTIV. Improving Application Security Using OWASP SAMM. Disponível em: https://www.optiv.com. Acesso em: 24 out. 2024.

OWASP. The Model. Disponível em: https://owaspsamm.org/model/. Acesso em: 24 out. 2024.

OWASP. OWASP Top Ten. 2022. Disponível em: https://owasp.org/top10/. Acesso em: 06 out. 2023.

OWASP. Top 10 Vulnerabilities. Open Web Application Security Project, 2020. Disponível em: https://owasp.org/. Acesso em: 06 out. 2023.

OWASP. Dependency Track Project. 2021. Disponível em: https://dependencytrack.org/. Acesso em: 06 out. 2023.

OWASP. Software Assurance Maturity Model (SAMM). 2022. Disponível em: https://owaspsamm.org/. Acesso em: 06 out. 2023.

RAMANATHAN, R. et al. A Survey of Secure Software Development Lifecycle Methodologies. Journal of Information Security and Applications, v. 49, p. 102363, 2019. Disponível em: https://www.sciencedirect.com/journal/journal-of-information-security-and-applications. Acesso em: 07 out. 2023.

SCHNEIER, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company, 2015.

SCHNEIER, B. Secrets and Lies: Digital Security in a Networked World. Indianapolis: Wiley, 2000.

SCHNEIER, B. On the CSRB's Non-Investigation of the SolarWinds Attack. Disponível em: https://www.schneier.com/blog/archives/2024/07/on-the-csrbs-non-investigation-of-the-solarwinds-attack.html. Acesso em: 05 out. 2024.

SHOSTACK, A. Threat Modeling: Designing for Security. Wiley, 2014.

SMITH, A. DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations. IT Revolution Press, 2020.

SMITH, C. The Evolution of Security Paradigms in Software Development. Journal of Information Security, v. 9, n. 3, p. 126-135, 2018.

THE WHITE HOUSE. The White House. Washington: U.S. Government. Disponível em: https://www.whitehouse.gov/. Acesso em: 07 out. 2023.

UNITED STATES. Annual Intellectual Property Report to Congress. Washington: U.S. Government, 2022. Disponível em: https://ustr.gov/sites/default/files/Annual_Intellectual_Property_Report_to_Congress.pdf. Acesso em: 07 out. 2023.

VERACODE. State of Software Security Report, 2021. Disponível em: https://www.veracode.com/security/state-of-software-security-report. Acesso em: 06 out. 2023.

VEHENT, Julien. Securing DevOps: Security in the Cloud. 1. ed. Shelter Island: Manning Publications, 2018.