ANÁLISE BIBLIOGRÁFICA: PADRÕES E NORMAS DE CIBERSEGURANÇA NO CICLO DE DESENVOLVIMENTO DE SOFTWARE

Thales Frazão Leite(IC)[1], Otávio de Souza Gomes(PQ)[1]
[1]*Universidade Federal de Itajubá*

Palavras-chave: Cibersegurança, SDLC, Normas e Padrões, Model Checking, Análise Bibliométrica

Introdução

A cibersegurança tem se tornado um tema central no desenvolvimento de software para sistemas críticos, à medida que as infraestruturas conectadas enfrentam um número crescente de ameaças cibernéticas sofisticadas. No contexto de sistemas como redes elétricas inteligentes (smart grids), veículos autônomos e infraestruturas industriais (como SCADA), a implementação de práticas de segurança robustas ao longo do Ciclo de Vida de Desenvolvimento de Software (SDLC) é crucial. O objetivo deste trabalho é investigar a aplicação de normas e frameworks de cibersegurança no SDLC, com destaque para a ISO/IEC 27001, identificando suas limitações e o impacto nas organizações que implementam esses padrões.

O estudo também explora o uso de ferramentas de verificação formal, como o model checking, que oferecem uma forma rigorosa de validar as propriedades de segurança em software crítico. Utilizando uma abordagem de revisão bibliográfica e análise bibliométrica com o VOSviewer, buscamos mapear as tendências e lacunas na literatura sobre cibersegurança aplicada ao SDLC, identificando os principais desafios e oportunidades para melhorias na segurança de sistemas críticos.

Metodologia

A metodologia aplicada consiste em uma revisão sistemática da literatura e análise bibliométrica. As publicações foram extraídas da base de dados Web of Science e cobrem um período de dez anos, com foco em palavras-chave como "Ciclo de Vida de Desenvolvimento de Software" (SDLC), "Normas de Cibersegurança" e "ISO/IEC 27001".

Em um primeiro momento, uma pesquisa preliminar foi realizada utilizando os termos “Software Development Life Cycle” e “Cybersecurity Standards”. Esta busca resultou em 6760 artigos, dos quais foram selecionados e analisados os mil mais relevantes, classificados por ordem de impacto. Esses artigos foram processados no software VOS Viewer, que permitiu a criação de mapas de coautoria e cocitação, revelando as principais conexões entre os autores e os temas de pesquisa. No entanto, essa abordagem inicial se mostrou ampla demais, já que muitos artigos tratavam de temas fora do escopo da pesquisa, como metodologias de desenvolvimento que não envolviam sistemas críticos ou não abordavam a cibersegurança de maneira direta. A presença de publicações com foco em áreas distantes do objetivo principal levou à necessidade de um refinamento na pesquisa para garantir a relevância dos artigos analisados.

A análise incluiu artigos que discutem a aplicação de normas de segurança cibernética em sistemas críticos, como as infraestruturas SCADA (Supervisory Control and Data Acquisition) e smart grids, assim como frameworks de segurança, como o NIST Cybersecurity Framework e o DevSecOps. Foram consideradas contribuições que abordam desafios específicos na adoção de normas, como a implementação da ISO/IEC 27001 em ambientes industriais e o uso de modelagem formal para verificação de segurança em sistemas embarcados.

Na segunda fase, foi adotada uma estratégia mais específica, com o uso das palavras-chave “Software Development Life Cycle” e “Cybersecurity”, associadas a termos adicionais, como “Critical System”, “DevSecOps”, “ISO/IEC 27001”, “OWASP” e “Security Tests”. Essa busca refinada resultou em um total de 159 artigos, que foram analisados mais detalhadamente. Para a seleção final, foram considerados critérios como a relevância dos artigos publicados nos últimos dez anos, sua pertinência direta ao tema de cibersegurança em sistemas críticos, e o impacto acadêmico medido pelo número de citações.

A fim de ilustrar a evolução da produção acadêmica nessa área, foi elaborado um gráfico de barras que apresenta a quantidade de artigos publicados anualmente na última década. Esse gráfico permite visualizar de forma clara o crescimento do interesse por este tema ao

longo dos anos.

Figura 1 - Gráfico Publicações da Última Década

Adicionalmente, o estudo explorou o uso de ferramentas de verificação formal, com foco no ESBMC (Bounded Model Checker para C/C++), para garantir a segurança de sistemas críticos. O ESBMC traduz as propriedades de segurança e o comportamento do código-fonte em C/C++ para fórmulas lógicas, que são analisadas por SMT solvers (Satisfiability Modulo Theories), como Z3, Boolector e CVC4. Esses solvers são capazes de resolver essas fórmulas em diversas lógicas, permitindo verificar propriedades complexas, como a conformidade de tempo real e a ausência de deadlocks ou violações de integridade.

Resultados e discussão

A análise da literatura mostrou que grande parte dos estudos sobre cibersegurança no SDLC se concentra nas fases de design e codificação, onde técnicas de análise estática e dinâmica são utilizadas para identificar vulnerabilidades. Segundo Núñez et al. (2020), a aplicação de um modelo de desenvolvimento seguro baseado em normas, como a ISO/IEC 27001, em fábricas de software permite a prevenção de ameaças cibernéticas, desde que os requisitos de segurança sejam integrados desde o início do ciclo de vida do software [1]. Essa integração antecipada permite uma mitigação proativa de riscos, reduzindo os custos relacionados à correção de falhas de segurança nas fases finais de desenvolvimento.

Outro aspecto relevante é a dificuldade enfrentada por organizações que operam sistemas críticos em adaptar as diretrizes da ISO/IEC 27001 às suas necessidades específicas. Longras et al. (2018) identificam que, em muitos casos, a implementação da norma requer ajustes para se adequar à natureza do ambiente operacional,especialmente em setores industriais, como sistemas SCADA e redes de energia [3]. A complexidade desses ambientes exige flexibilidade na adoção das práticas de segurança e uma abordagem mais personalizada, baseada na modelagem de ameaças e vulnerabilidades específicas.

O estudo de Ten et al. (2008) sobre a segurança de sistemas SCADA demonstra que, embora as normas de segurança forneçam uma estrutura sólida para a proteção de infraestruturas críticas, existem vulnerabilidades inerentes que exigem a adoção de práticas complementares, como a verificação formal de software e a integração de modelagem de ameaças no SDLC [4]. Ferramentas de verificação formal, como o ESBMC e o CBMC, permitem a verificação de propriedades complexas de segurança, utilizando solvers SMT para validar se o software está em conformidade com as regras definidas. A LTL (Linear Temporal Logic) e a CTL (Computation Tree Logic) têm sido eficazes na verificação de sistemas embarcados, garantindo que esses sistemas operem dentro dos limites de segurança previamente estabelecidos [5].

Os resultados obtidos a partir da análise bibliométrica utilizando o VOS Viewer revelam que há uma dispersão significativa entre os autores que pesquisam a aplicação de normas de cibersegurança no desenvolvimento de software. Os gráficos de coautoria indicam que há poucos esforços colaborativos sistemáticos, o que sugere a necessidade de maior integração entre pesquisadores e profissionais da indústria para abordar os desafios da implementação de segurança em sistemas críticos [6]. A falta de uma colaboração estruturada entre academia e indústria pode resultar em soluções de segurança desatualizadas ou inadequadas para certos ambientes operacionais, reforçando a necessidade de padrões adaptáveis e flexíveis.

Conclusões

Este estudo confirma a importância da aplicação de normas e frameworks de cibersegurança no SDLC, especialmente em sistemas críticos. O uso de ferramentas de visualização bibliométrica, como o VOS Viewer, proporcionou uma visão clara das principais tendências e lacunas na literatura. A análise mostrou que, embora a ISO/IEC 27001 seja amplamente adotada, há desafios significativos na sua implementação em ambientes industriais e sistemas críticos, como SCADA e smart grids.

Concluímos que, para mitigar as ameaças cibernéticas emergentes, as organizações devem adotar uma abordagem mais integrada, que combine as melhores

práticas das normas existentes com técnicas avançadas de verificação de segurança e modelagem de ameaças. Além disso, é necessário promover maior colaboração entre a academia e a indústria, a fim de desenvolver metodologias mais eficazes e adaptáveis às necessidades específicas dos ambientes de desenvolvimento de software.

Agradecimentos

Gostaria de expressar minha profunda gratidão a todos que, de alguma forma, contribuíram para a realização deste trabalho. Primeiramente, agradeço ao meu orientador, Otávio de Souza Gomes, por sua orientação precisa, paciência e incentivo ao longo de toda esta jornada. Sua expertise e dedicação foram fundamentais para o desenvolvimento desta pesquisa.

Agradeço também à Universidade Federal de Itajubá pela oportunidade de participar do programa de iniciação científica, e ao CNPq, pelo apoio financeiro que tornou este projeto possível.

Por fim, meu agradecimento especial à minha família e amigos, cujo apoio incondicional foi essencial em cada etapa deste processo.

Referências

[1] NÚÑEZ, J. C. S., LINDO, A. C., and RODRÍGUEZ, P. G. (2020). "A preventive secure software development model for a software factory: A case study." IEEE Access, 8:77653–77665.

[2] KHAN, R. A., KHAN, S. U., ALZAHRANI, M., and ILYAS, M. (2022). "Security assurance model of software development for global software development vendors." IEEE Access, 10:58458–58487.

[3] LONGRAS, A., PEREIRA, T., CARNEIRO, P., and PINTO, P. (2018). "On the track of ISO/IEC 27001:2013 implementation difficulties in Portuguese organizations." In 2018 International Conference on Intelligent Systems (IS), pages 886–890

[4] TEN, C.-W., LIU, C.-C., and MANIMARAN, G. (2008). "Vulnerability assessment of cybersecurity for SCADA systems." IEEE Transactions on Power Systems, 23(4):1836–1846.

[5] HUMAYUN, M., JHANJHI, N. Z., and ALMUFAREH, M. F. A. M. I. K. (2022). "Security threat and vulnerability assessment and measurement in secure software development." Computers, Materials & Continua, 71(3):5039–5059.

[6] LONGRAS, A., PEREIRA, T., CARNEIRO, P., and PINTO, P. (2018). "On the track of ISO/IEC 27001:2013 implementation difficulties in Portuguese organizations." In 2018 International Conference on Intelligent Systems (IS), pages 886–890.