

CoReTM

O artigo aborda a importância de abordagens colaborativas na modelagem de ameaças, especialmente diante do aumento do número de sistemas de informação, funcionários e ativos críticos que necessitam de proteção. Destaca-se que a inclusão de diversos especialistas, dependendo do tipo de ativo em modelagem, é essencial para uma análise abrangente.

As ferramentas existentes não suportam adequadamente a colaboração em processos modernos, como metodologias ágeis e DevSecOps, pois estão vinculadas a metodologias subjacentes específicas. Em resposta a essa limitação, a implementação prototípica do CoReTM oferece:

1. **Editor Colaborativo Baseado em Anotações:** Facilita a contribuição síncrona e assíncrona de múltiplos colaboradores.
2. **Relatórios Automatizados de Ameaças:** Gera documentação sistemática das ameaças identificadas.
3. **Integração com DevOps:** Suporta a modelagem de ameaças em diversas combinações de estilos de reuniões, adaptando-se a diferentes fluxos de trabalho.

O artigo também revisa metodologias existentes de modelagem de ameaças, como STRIDE, CAPEC, ATT&CK, OWASP e Attack Trees, discutindo suas categorias de ameaças, abordagens e limitações em contextos colaborativos. Destaca-se que metodologias como PASTA e Trike apresentam complexidades adicionais ao buscar uma análise de riscos mais detalhada.

Relevância para a Pesquisa:

- **Modelagem de Ameaças:** CoReTM exemplifica uma abordagem que facilita a colaboração na modelagem de ameaças, alinhando-se com a necessidade de participação distribuída em estruturas organizacionais horizontais.
- **Governança e Segurança:** A integração com DevOps e a flexibilidade para diferentes estilos de reuniões refletem a adaptabilidade necessária para governanças horizontais.
- **Frameworks de Segurança:** A análise comparativa com metodologias como STRIDE e PASTA fornece insights sobre a combinação de diferentes frameworks para fortalecer a modelagem de ameaças em organizações não-hierárquicas.