

DREADful

No artigo "DREADful _ Microsoft Learn", são discutidas as metodologias de modelagem de ameaças **STRIDE** e **DREAD**, ambas desenvolvidas e implementadas pela Microsoft. As principais observações e críticas apresentadas incluem:

- **Críticas às Metodologias STRIDE e DREAD:**
 - **Falta de Rigor Acadêmico:** Ambas as metodologias foram alvo de críticas por não terem sido desenvolvidas com rigor acadêmico, o que compromete sua robustez do ponto de vista científico.
 - **Intercorrelações em STRIDE:** A metodologia STRIDE apresenta várias intercorrelações entre suas categorias de ameaças. Por exemplo, a elevação de privilégio (Elevation of Privilege - E) pode implicar spoofing e perda de não-repúdio, além de potencialmente indicar tampering, information disclosure e denial of service. Essa sobreposição resulta em uma classificação menos rigorosa e mais complexa.
 - **Utilidade Prática vs. Rigidez Científica:** Apesar das limitações acadêmicas, STRIDE e DREAD são considerados úteis na prática, especialmente para focar debates e discussões sobre problemas específicos de segurança. Essas metodologias são valorizadas no ambiente corporativo por sua capacidade de organizar e categorizar ameaças de maneira acessível, mesmo que não atendam a padrões acadêmicos rigorosos.
- **Desenvolvimento e Aplicação de DREAD:**
 - **Origem do DREAD:** DREAD surgiu a partir de iniciativas de segurança no Visual Studio e foi uma das primeiras metodologias de segurança antes da implementação da segurança no Windows Server 2003.
 - **Avaliação do DREAD:** Embora o modelo DREAD seja considerado razoável, o principal desafio identificado é a implementação de um escore geral para as ameaças. A dificuldade em atribuir pontuações consistentes compromete a eficácia do modelo.
- **Conclusões Gerais:**
 - **Utilidade Prática:** Mesmo sem rigor acadêmico, as metodologias STRIDE e DREAD são úteis para profissionais de segurança na identificação e categorização de ameaças.
 - **Limitações:** A principal limitação observada é a alta intercorrelação entre categorias em STRIDE e a dificuldade de escore no DREAD, o que pode levar a inconsistências e subestimação de ameaças importantes.

Relevância para a Pesquisa

A avaliação crítica das metodologias **STRIDE** e **DREAD** apresentada no artigo é altamente relevante para a pesquisa em modelagem de ameaças em **organizações não-hierárquicas**, alinhando-se com o objetivo de desenvolver um protocolo que valorize a **horizontalidade organizacional** como um ativo estratégico. As principais considerações incluem:

- **Limitações das Metodologias Existentes:** A falta de rigor acadêmico e as intercorrelações nas categorias de STRIDE indicam que essas metodologias podem não capturar todas as nuances e complexidades presentes em estruturas organizacionais horizontais. Em ambientes

descentralizados, onde as responsabilidades e funções são distribuídas, uma categorização rígida e inter-relacionada de ameaças pode levar a lacunas na identificação de riscos específicos.

- **Necessidade de Metodologias Adaptáveis e Consistentes:** A dificuldade em implementar um escore geral no DREAD ressalta a necessidade de metodologias que ofereçam consistência e precisão na avaliação de ameaças. Para organizações não-hierárquicas, onde a colaboração e a distribuição de responsabilidades são essenciais, uma abordagem que permita uma avaliação mais granular e adaptável das ameaças é crucial.
- **Integração com Abordagens Complementares:** Dado que STRIDE e DREAD têm suas limitações, a pesquisa pode se beneficiar da integração dessas metodologias com outras abordagens mais criativas e colaborativas, como **Security Cards** e **Persona Non Grata**. Essas metodologias podem complementar STRIDE e DREAD, oferecendo uma visão mais abrangente e adaptável das ameaças, alinhada com a governança horizontal e a confiança distribuída.
- **Desenvolvimento de um Protocolo Personalizado:** Considerando as críticas às metodologias existentes, há uma oportunidade significativa para desenvolver um protocolo de modelagem de ameaças que combine a estrutura organizada de STRIDE com a criatividade e adaptabilidade de outras abordagens. Esse protocolo personalizado deve atender às necessidades específicas de organizações não-hierárquicas, garantindo uma identificação e mitigação de ameaças mais eficazes e contextualmente relevantes.
- **Foco na Consistência e Completude:** A alta taxa de ameaças omitidas em STRIDE destaca a importância de garantir que o protocolo de modelagem de ameaças desenvolvido para organizações horizontais seja capaz de identificar uma ampla gama de ameaças de maneira consistente. Isso é essencial para evitar vulnerabilidades que podem ser exploradas em ambientes onde a supervisão centralizada é mínima.