CyberThreatModeling
No artigo "Cyber Threat Modeling: An Evaluation of Three Methods", são avaliadas três metodologias distintas de modelagem de ameaças cibernéticas: **STRIDE**, **Security Cards** e **Persona Non Grata**. As principais observações e conclusões do estudo incluem:

- **STRIDE**:
    - **Desenvolvimento e Aplicação**: Desenvolvido pela Microsoft, o STRIDE é uma abordagem amplamente adotada que envolve a modelagem de sistemas e subsistemas, analisando como os dados fluem através deles. Utiliza uma abordagem baseada em checklists, categorizando ameaças em seis categorias (confidencialidade, integridade, disponibilidade, etc.).
    - **Vantagens**: Baixo número de falsos positivos e ideal para equipes com pouca expertise em segurança, pois a abordagem de checklist limita a geração de falsos positivos.
    - **Desvantagens**: Aplicar checklists a componentes variados de sistemas pode ser uma tarefa onerosa e pode levar a resultados inconsistentes, dependendo da composição e experiência das equipes.
- **Security Cards**:
    - **Desenvolvimento e Aplicação**: Desenvolvido pela Universidade de Washington, o Security Cards é um toolkit de brainstorming que utiliza 42 cartas divididas em quatro dimensões: Impacto Humano, Motivações do Adversário, Recursos do Adversário e Métodos do Adversário.
    - **Vantagens**: Promove maior criatividade e identificação de ataques incomuns ou sofisticados, resultando em maior eficácia na identificação de tipos variados de ameaças.
    - **Desvantagens**: Gera um alto número de falsos positivos e apresenta grande variabilidade nos resultados entre diferentes equipes, tornando-se ideal para cenários onde se valoriza uma gama mais ampla de resultados em detrimento da consistência.
- **Persona Non Grata**:
    - **Desenvolvimento e Aplicação**: Desenvolvido pela Universidade DePaul, o Persona Non Grata foca em identificar atacantes, suas motivações e capacidades. Envolve a criação de perfis de atacantes para guiar a identificação de vetores de ataque.
    - **Vantagens**: Reduz o número de falsos positivos e promove a consistência na identificação de ameaças, sendo ideal para análises onde se busca identificar ameaças prioritárias com alto grau de confiança.
    - **Desvantagens**: Pode não fornecer uma visão abrangente das ameaças, identificando apenas um subconjunto consistente de tipos de ameaças, o que limita a compreensão completa das possíveis vulnerabilidades.

Relevância para a Pesquisa

A avaliação comparativa das metodologias **STRIDE**, **Security Cards** e **Persona Non Grata** é extremamente relevante para a pesquisa em modelagem de ameaças em organizações não-hierárquicas. As principais considerações incluem:

- **Adaptação às Estruturas Horizontais**: A diversidade de abordagens oferece insights sobre como diferentes métodos podem ser adaptados para ambientes organizacionais distribuídos e colaborativos. Por exemplo, o **Security Cards** promove uma colaboração criativa, alinhando-se bem com estruturas horizontais que valorizam a participação distribuída.
- **Equilíbrio entre Consistência e Abrangência**: A comparação mostra que métodos como **STRIDE** e **Persona Non Grata** oferecem maior consistência e menor incidência de falsos positivos, enquanto **Security Cards** proporciona uma identificação mais abrangente de ameaças. Esse equilíbrio é crucial para desenvolver um protocolo que valorize a horizontalidade, garantindo tanto a confiabilidade quanto a abrangência na identificação de riscos.
- **Facilitação da Colaboração e Inclusão de Diversas Perspectivas**: Métodos que incentivam a colaboração, como o **Security Cards**, podem ser particularmente benéficos para organizações não-hierárquicas, onde a contribuição de múltiplos stakeholders é essencial. Isso reforça a confiança distribuída e a governança horizontal, pilares fundamentais para a segurança organizacional em ambientes descentralizados.
- **Flexibilidade e Adaptabilidade**: A variabilidade observada no **Security Cards** sugere que, embora este método possa ser mais suscetível a inconsistências, ele também oferece uma maior flexibilidade para adaptar a modelagem de ameaças às especificidades de cada organização. Isso é alinhado com a necessidade de protocolos que possam se ajustar dinamicamente às mudanças e à evolução das ameaças em estruturas horizontais.
- **Identificação de Vetores de Ataque Prioritários**: A abordagem do **Persona Non Grata** para focar em ameaças prioritárias com alta confiança pode ser integrada com outras metodologias para garantir que as ameaças mais críticas sejam identificadas de forma consistente, complementando a abrangência oferecida por métodos mais criativos.