Antivirus Software

FIAP-CHALLENGE
PRIDE SECURITY

Integrantes:
Pedro Henrique,
Guilherme Borges,
Vitor Saavedra,
Jader Vogel.

PRIDE SECURITY FIAP

Apresentação

Solução de Segurança Avançada contra Ransomware Proteger dados é proteger o futuro da empresa.

O Problema

70% dos ataques cibernéticos envolvem ransomware. Empresas vítimas de ransomware perdem milhões por parada de operação e pagamento de resgate. Backup não é suficiente se o ataque não for detectado rapidamente

Progresso Atual

Ransomware

Estudamos como ransomwares funcionam, suas formas de propagação, o processo de criptografia de dados e como atacam redes corporativas.

Antivírus

1. *Monitoramento em tempo real: vigia ações suspeitas.*
2. *Honeyfiles: arquivos isca que avisam se forem tocados.*
3. *Sandbox dinâmico: executa arquivos suspeitos isoladamente.*
4. *Resposta imediata: mata processos e desconecta da rede.*

Como Evitar

- Detecta comportamento, não apenas ameaças conhecidas.
- Tempo de resposta automático.
- Arquitetura modular: adaptável a novos ransomwares.

Funcionalidades

1 – Detecção rápida de ameaças: Monitoramento contínuo do sistema

2 – Bloqueio do ataque antes da criptografia: Identifica um comportamento malicioso.

3 – Recuperação de arquivos modificados: Uso de backups temporários e isolados no sistema.

- Todo arquivo ou aplicativo suspeito é executado inicialmente dentro de uma **micro-VM**, garantindo que, se for malicioso, ele permaneça contido e sem impacto no sistema real. Durante essa execução, a **análise comportamental avançada** monitora em tempo real as ações do processo dentro da micro-VM e, caso detecte comportamentos anômalos, aciona imediatamente o bloqueio local e gera um alerta. Paralelamente, o **IDS/IPS** realiza o monitoramento externo: se o malware tentar se conectar à rede, a comunicação é interceptada, podendo ser bloqueada para evitar exfiltração de dados, além de registrar a tentativa para análise posterior. A integração entre as camadas fortalece a defesa: a análise comportamental fornece indicadores de comprometimento (IoCs), como hashes e padrões de comportamento, para que o IDS/IPS atualize as regras de rede; enquanto o IDS/IPS envia eventos de tráfego suspeito de volta à análise, reforçando os modelos de detecção. Por fim, o uso da microvirtualização assegura que, mesmo que alguma detecção falhe, o impacto da ameaça permaneça limitado.

Finalidade

Oferecer uma proteção leve mas muito eficiente para empresas.

Obrigado pela atenção.

FIAP-CHALLENGE
PRIDE SECURITY

PRIDE
SECURITY