Luís Stefan

OWASP Top 10 para Aplicações Desktop

Riscos comuns e Contramedidas para Mitigação

Agenda

- # WHOAMI
- Sobre a OWASP
- Introdução aos Top 10 da OWASP
- SDLC
- SSDLC
- Arquitetura Comum para Aplicações Desktop
- Detalhamento do OWASP Top 10 Desktop
- Mindmap para pesquisa de riscos em aplicações desktop
- Como Prevenir os Riscos do Top 10 Desktop Apps
- Bonus Content ☺
- Q&A

WHOAMI

Luis Stefan

CyberSecurity Researcher and Consultant

Ed:

Grad. Seg Informações

MBA em Cyber Security

Pós-Graduado em Segurança de Redes

Certs:

CISSP, CDL, ISFS, Pen+, Sec+, CEHP, MCP,

LPIC, KESA, ITIL, AWS

Sobre a OWASP

A OWASP (Open Web Application Security Project) é uma comunidade global dedicada a melhorar a segurança de software. Fundada em 2001, seu objetivo é educar e fornecer recursos para desenvolvedores, designers, gerentes de projetos e outros profissionais de tecnologia sobre as melhores práticas de segurança em aplicações web.

A OWASP mantém várias listas de "Top 10" vulnerabilidades mais críticas em aplicações web, além de guias, ferramentas e documentos que ajudam na identificação e mitigação de ameaças.

Suas iniciativas incluem conferências, projetos de código aberto e meios de prover conscientização sobre segurança cibernética na comunidade de tecnologia e desenvolvimento de software.

Introdução aos Top 10 da OWASP

O Top 10 de Segurança de Aplicativos Desktop da OWASP é um documento de conscientização para desenvolvedores, proprietários de produtos e engenheiros de segurança.

Ele representa um amplo consenso sobre os riscos de segurança mais críticos para aplicativos Desktop.

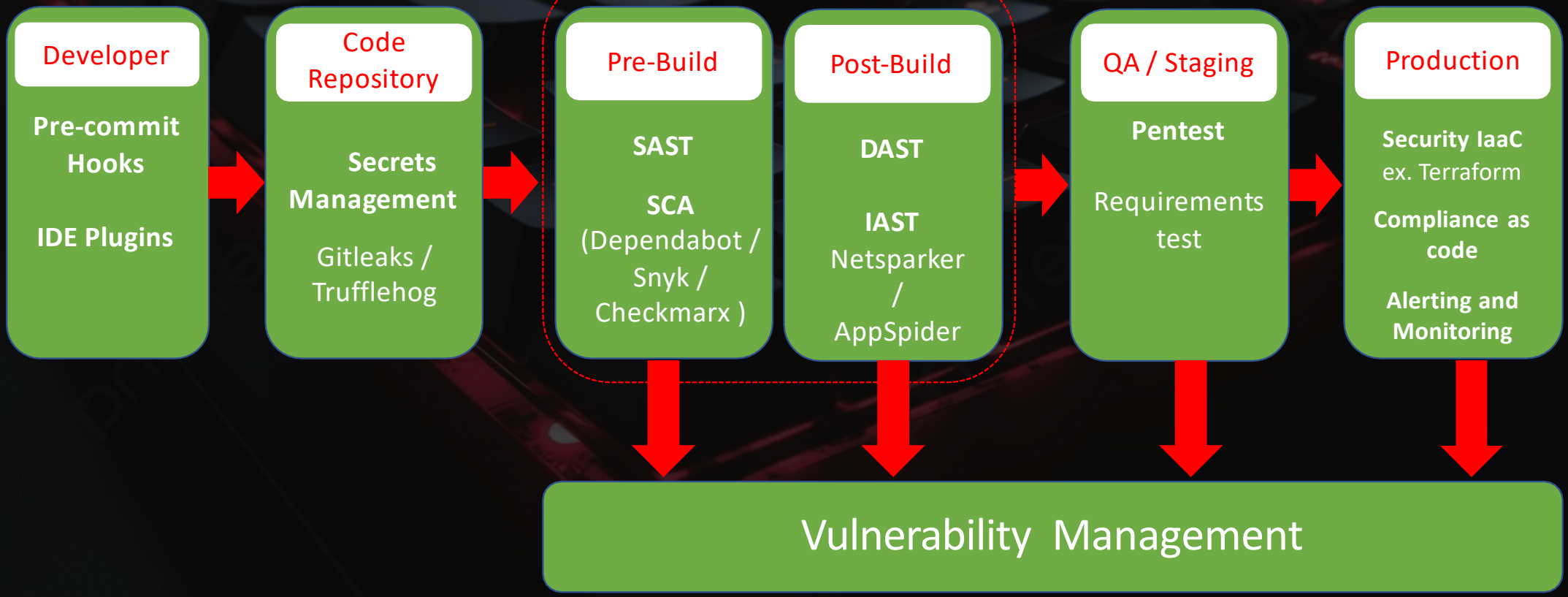
As empresas podem adotar este documento para efetuar o processo de identificar riscos em suas aplicações desktop e prover soluções para que esses riscos além de minimizados sejam rastreados e mitigados

O uso dos Top 10 da OWASP é talvez o primeiro passo mais eficaz para mudar a cultura de desenvolvimento de software dentro de sua organização para uma que produza código mais seguro.

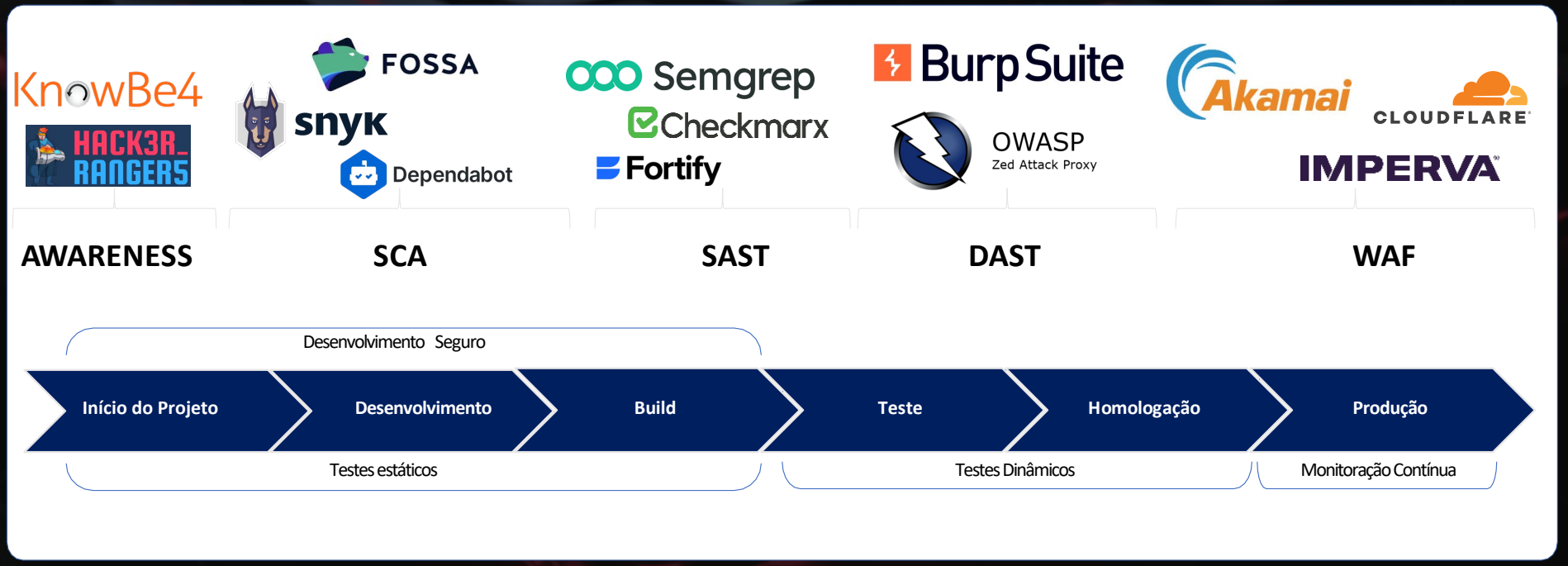
SDLC - Ciclo de vida do desenvolvimento de software

Para o processo e ciclo de desenvolvimento de software é ideal que a segurança de informações esteja inserida nas etapas de desenvolvimento

SSDLC - Ciclo de vida do desenvolvimento seguro de software



SSDLC - Ciclo de vida do desenvolvimento seguro de software (exemplo)



ROI do programa de segurança de aplicações

- Redução de vulnerabilidades de segurança
- Desenvolvimento de software mais eficiente (e seguro ☺)
- Software de alta qualidade
- **Redução** de **tempo** na **entrega** do produto para o mercado
- **Redução** de **custos** e **elimina débitos** de tecnologia e suporte de sistemas legados
- **Agilidade** de negócios e **produtividade** da equipe

Principais 10 Riscos de Segurança de Aplicativos Desktop da OWASP (2021)

OWASP Top 10 de Aplicativos Desktop	Exemplos
DA1 - Injeções	SQLi, LDAPi, XMLi, RCE, Comandos de Sis.Op., etc.
DA2 - Autenticação Quebrada & Gerenciamento de Sessões	Autenticação de conta do SO/App, de sessões, autenticação para compartilhamentos de rede ou outros dispositivos periféricos
DA3 - Exposição de Dados Sensíveis	Dados na memória após o logout do aplicativo, logs com informações sensíveis, segredos em arquivos, etc.

Principais 10 Riscos de Segurança de Aplicativos Desktop da OWASP (2021)

OWASP Top 10 de Aplicativos Desktop	Exemplos
DA4 - Uso Incorreto de Criptografia	Uso de algoritmos desatualizados, uso incorreto de criptografia na verificação de integridade
DA5 - Autorização Incorreta	Falhas em permissões de arquivo/pasta, ausência do princípio do privilégio mínimo,

Principais 10 Riscos de Segurança de Aplicativos Desktop da OWASP (2021)

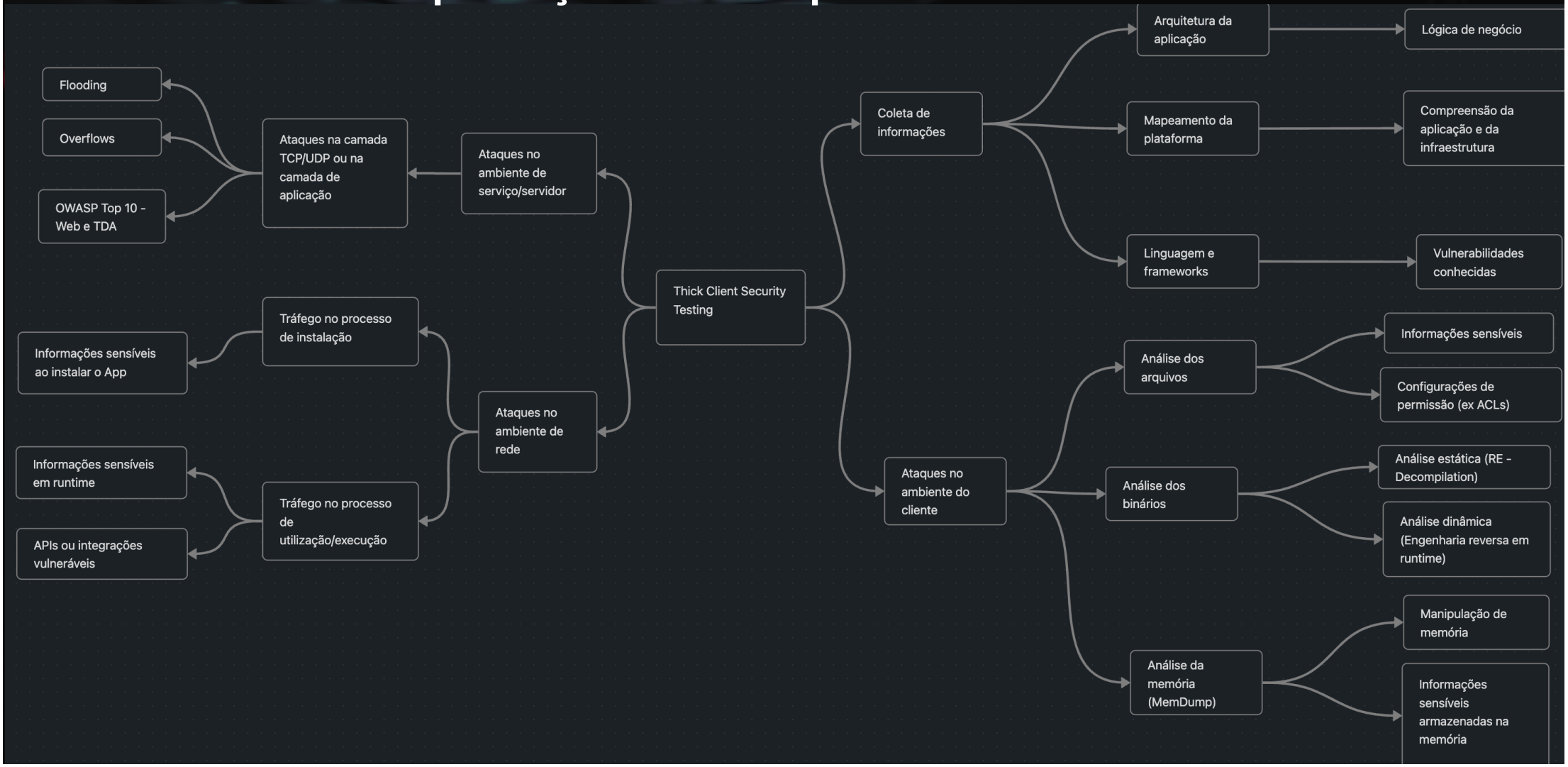
OWASP Top 10 de Aplicativos Desktop	Exemplos
DA6 - Configuração de Segurança Incorreta	Políticas de segurança mal configuradas no sistema, falta de verificação de tipo de arquivo no processamento, serviços de terceiros mal configurados, etc.
DA7 - Comunicação Insegura	Uso de cifras fracas ou tráfego de informações não criptografadas ou ainda usando protocolo sem criptografia (http, ftp, telnet, etc)

Principais 10 Riscos de Segurança de Aplicativos Desktop da OWASP (2021)

OWASP Top 10 de Aplicativos Desktop	Exemplos
DA8 - Baixa Qualidade de Código	Falta de assinatura e verificação de integridade no código, falha em ofuscação, injeção de DLLs, Race Condition, falta de proteção no binário (null pointers, mem corruption, buffer overflow), etc.
DA9 - Uso de Componentes com Vulnerabilidades Conhecidas	Uso de componentes de Softwares desatualizados ou vulneráveis
DA10 - Registro e Monitoramento Insuficientes	Registro inadequado de atividades ou falta de monitoração para detecção de incidentes

Arquiteturas comuns em aplicações desktop

Mindmap para pesquisa de riscos em aplicações desktop



Como Prevenir os Riscos do OWASP Top 10 Desktop Apps

DA1 - Injeções

Problemas como injeção de SQL, LDAP, XML, comando do SO, etc. ocorrem quando entrada não confiável é passada para o interpretador como parte de uma consulta/comando.

Um atacante pode enganar os interpretadores para executar comandos arbitrários para realizar operações indesejadas ou coletar dados não autorizados.

Como prevenir:

Implemente a validação de entrada de dados em todos os pontos onde dados não confiáveis possam ser inseridos em comandos ou consultas.

Realizar testes de segurança regulares, incluindo pentests para identificar e corrigir vulnerabilidades.

Educar desenvolvedores sobre as melhores práticas de segurança para evitar vulnerabilidades de injeção desde o início do desenvolvimento.

DA2 - Falha de Autenticação e Gestão de Sessões

Isso inclui problemas como implementação de autenticação insegura, bypass de autenticação, sessão imprópria, etc.

Um atacante pode explorar a implementação insegura para comprometer sessões de usuário, senhas e chaves ou assumir a identidade do usuário do aplicativo.

Como prevenir:

Realizar auditorias regulares de segurança para identificar e corrigir potenciais vulnerabilidades de autenticação e gestão de sessões.

Manter-se atualizado com as melhores práticas de segurança e padrões de autenticação reconhecidos.

Educar desenvolvedores sobre os riscos de segurança associados à implementação inadequada de autenticação e gestão de sessões.

DA3 - Exposição de Dados Sensíveis

Exposição não intencional de informações sensíveis como PII, informações financeiras, informações de saúde ou chaves e segredos de aplicativos.

Isso pode incluir dados na memória após o logout do aplicativo, logs com informações sensíveis, segredos codificados em arquivos (dll, binários, arquivos de configuração), etc.

Como prevenir:

Realizar auditorias de segurança regulares para identificar e corrigir potenciais exposições de dados sensíveis.

Educar desenvolvedores e operadores sobre a importância da proteção de dados sensíveis e as melhores práticas para evitar exposições acidentais.

Implementar políticas de segurança que limitem o acesso a dados sensíveis apenas a pessoal autorizado e com necessidade de acesso.

DA4 - Uso Incorreto de Criptografia

Problemas como uso de algoritmos criptográficos fracos, chaves fracas ou segredos, funções criptográficas personalizadas e gerenciamento inseguro de chaves.

Um atacante pode explorar essas falhas para recuperar informações sensíveis ou atacar os usuários das diferentes instâncias do mesmo aplicativo.

Como prevenir:

Utilize algoritmos criptográficos comprovadamente seguros

Implemente um gerenciamento seguro de chaves.

Evite o uso de funções criptográficas personalizadas

DA5 - Falha de Autorização

Falhas de autorização incluem permissões de arquivo/pasta fracas por função de usuário, ausência do princípio do privilégio mínimo, funções de usuário incorretas, acesso não autorizado ao registro ou variáveis de ambiente, etc.

Usuários não privilegiados podem acessar essas funções sem autorização se souberem como chamar.

Como prevenir:

Atribua apenas os privilégios necessários para cada usuário ou credencial no sistema ou aplicação.

Configure corretamente as permissões de arquivos, pastas e registros.

Realize revisões periódicas dos papéis e permissões dos usuários e ACLs

DA6 - Configuração de Segurança Incorreta

As falhas incluem políticas de grupo, registro, regras de firewall mal configuradas, falta de verificação de tipo ou conteúdo do arquivo no processamento, serviços de terceiros ou integrações inseguras/mal configuradas (SQL, AD, etc.).

Como prevenir:

Utilize padrões de configuração segura e mantenha-os atualizados

Realize revisões regulares das configurações de segurança.

Forneça treinamento adequado e estabeleça procedimentos claros para configuração de segurança.

DA7 - Comunicação Insegura

Quando qualquer aplicativo precisa se comunicar com serviços remotos como servidores SQL, APIs da web, serviços em nuvem ou outros, a comunicação pode ser interceptada, manipulada ou falsificada.

Isso pode levar à exposição de dados sensíveis por interceptação de comunicações ou execução de comandos maliciosos.

Como prevenir:

Use TLS/DTLS com cifras fortes.

Implemente criptografia para todas as comunicações.

Substitua protocolos de comunicação em texto simples por alternativas seguras.

DA8 - Baixa Qualidade de Código

Problemas de qualidade de código incluem a falta de assinatura e verificação de código para integridade do arquivo, falta de ofuscação de código, pré-carregamento ou injeção de DLL, condições de corrida, falta de proteção binária (estouros, ponteiros nulos, corrupção de memória), etc.

Como prevenir:

Adote práticas seguras no desenvolvimento, incluindo assinatura de código e verificação de integridade.

Utilize técnicas de ofuscação para dificultar a engenharia reversa.

Utilize ferramentas para detectar e corrigir vazamentos de memória e buffer overflow.

DA9 - Uso de Componentes com Vulnerabilidades Conhecidas

O uso de softwares, serviços ou components obsoletos ou desatualizados de terceiros como bibliotecas ou funções, podem introduzir vulnerabilidades conhecidas em aplicativos Desktop.

Como prevenir:

Utilize ferramentas para gerenciar e manter dependências atualizadas.

Monitore regularmente vulnerabilidades em componentes utilizados e aplique patches ou atualizações rapidamente.

Realize avaliações de segurança periódicas para identificar e corrigir componentes vulneráveis.

DA10 - Registro e Monitoramento Insuficientes

A falta de registro ou registro inadequado de atividades de usuários, eventos do sistema ou falhas de segurança pode dificultar a detecção de abusos ou violações de segurança.

Um sistema de registro e monitoramento eficaz é crucial para identificar e responder a incidentes de segurança em tempo hábil.

Como prevenir:

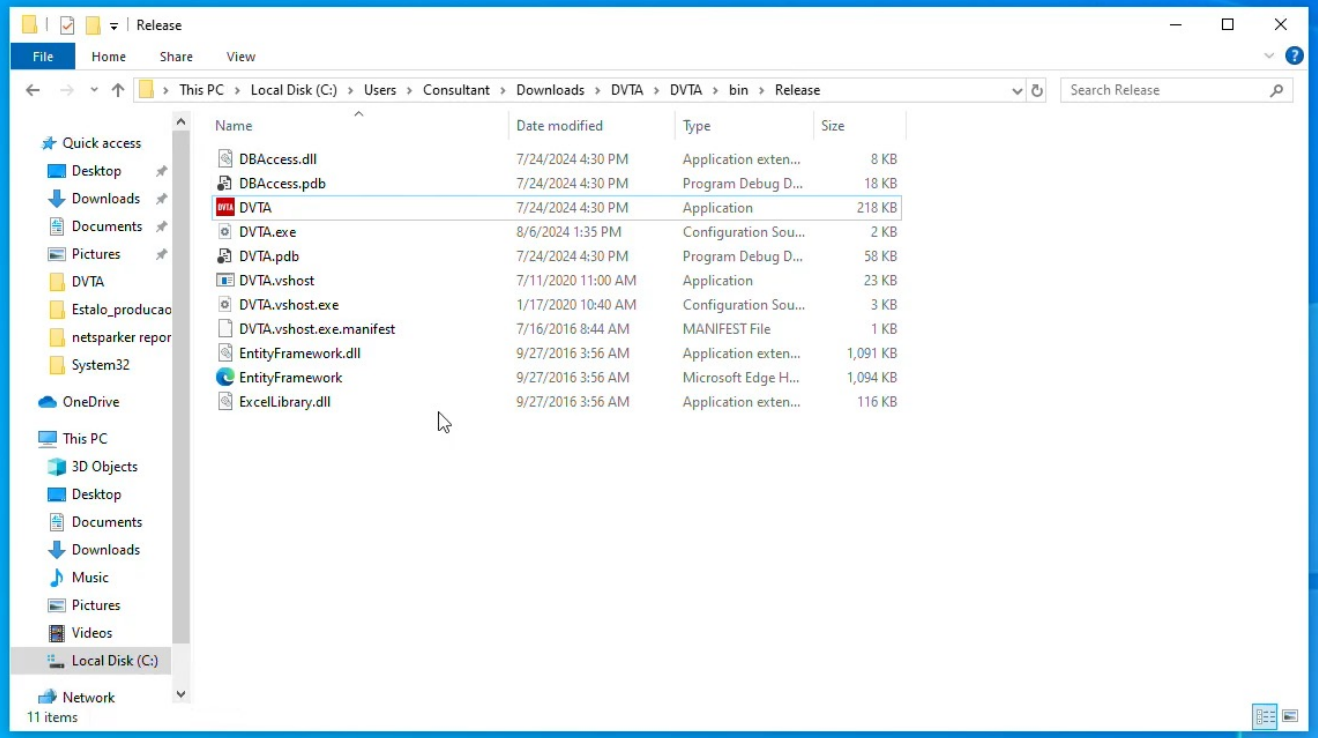
Use ferramentas de monitoramento para detectar atividades suspeitas.

Proteja logs contra manipulações e mantenha integridade dos dados.

Registrar tentativas com falha, acesso negado, falhas de validação de entrada ou qualquer falha nas verificações da política de segurança.

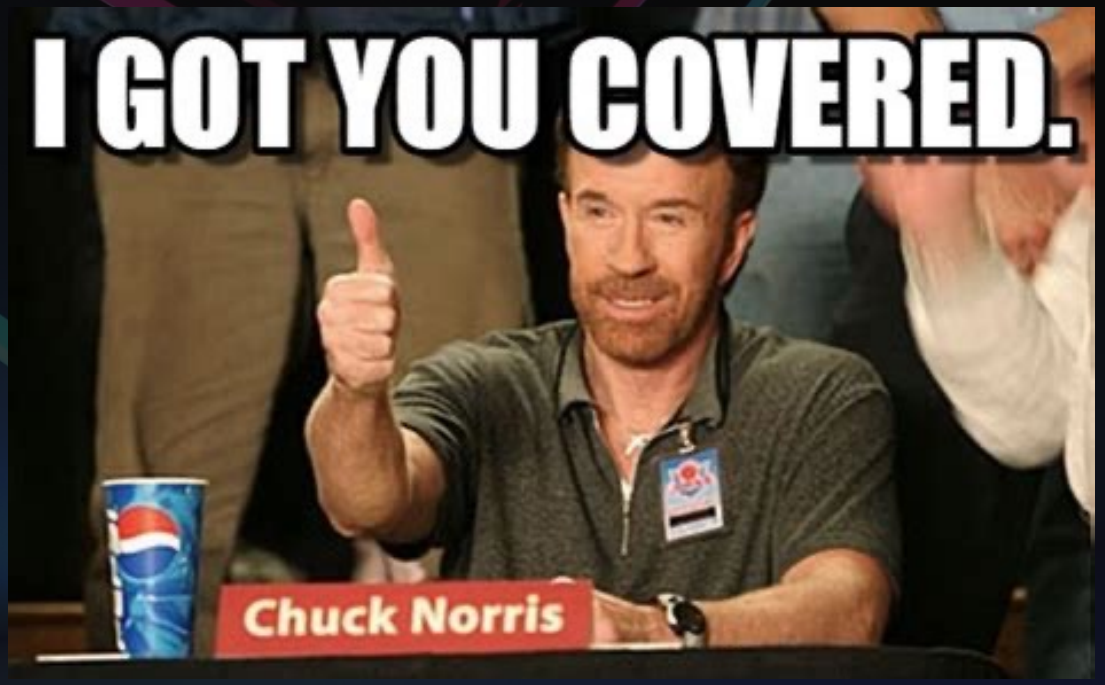
Preferencialmente que os logs sejam formatados para que outras ferramentas possam consumi-los também.

Integre com SIEMs e outros dashboards, ferramentas de monitoramento e alerta.


Release
File
Home
Share
View
This PC › Local Disk (C:) › Users › Consultant › Downloads › DVTA › DVTA › bin › Release
Search Release
Quick access
Desktop
Downloads
Documents
Pictures
DVTA
Estalo_producao
netsparker repor
System32
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
11 items
Name
Date modified
Type
Size
DBAccess.dll 7/24/2024 4:30 PM Application exten... 8 KB
DBAccess.pdb 7/24/2024 4:30 PM Program Debug D... 18 KB
DVTA 7/24/2024 4:30 PM Application 218 KB
DVTA.exe 8/6/2024 1:35 PM Configuration Sou... 2 KB
DVTA.pdb 7/24/2024 4:30 PM Program Debug D... 58 KB
DVTA.vshost 7/11/2020 11:00 AM Application 23 KB
DVTA.vshost.exe 1/17/2020 10:40 AM Configuration Sou... 3 KB
DVTA.vshost.exe.manifest 7/16/2016 8:44 AM MANIFEST File 1 KB
EntityFramework.dll 9/27/2016 3:56 AM Application exten... 1,091 KB
EntityFramework 9/27/2016 3:56 AM Microsoft Edge H... 1,094 KB
ExcelLibrary.dll 9/27/2016 3:56 AM Application exten... 116 KB

Q&A

Contact me @LinkedIn



https://www.linkedin.com/in/luis-s-bb7452aa