

Segurança da empresa ao software

Será que eu tranquei a porta?



Agenda

- Por onde começar
- Análise de ameaças e risco
- Segurança de pessoas
- Segurança de ativos



Quem somos



Daniel Paiva Fernandes

Formado em Direito pela FDSM (2004) e em Sistemas de Informação pela UNIFEI (2017) com graduação-sanduíche em Stockton University – EUA (2016), é aluno de Mestrado em Computação Aplicada (UNIFEI) e atualmente trabalha no Inatel Competence Center no projeto P&D de BSS da Ericsson, onde atua como Test Lead e Security Master.

[in/paivafernandes](https://www.linkedin.com/in/paivafernandes)


Frederico Augusto Laranjo Silva
Formado em Sistemas de Informação pela FAI (2013), Pós-graduado em Desenvolvimento de Aplicações para Dispositivos Móveis e Cloud Computing pelo Inatel (2018), atualmente trabalha no Inatel Competence Center no projeto P&D de BSS da Ericsson, onde atua como Product Owner e Team Leader.

[in/fredllaranjo](https://www.linkedin.com/in/fredllaranjo) 



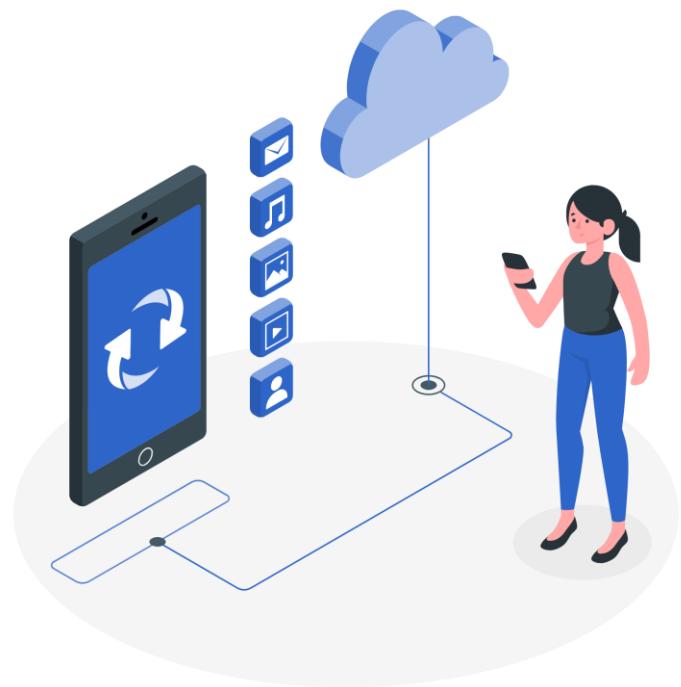
Uma breve introdução

Qual cenário nos encontramos



+ 300% crimes
cibernéticos
(FBI)

+ 630% ataques em
serviços cloud
(FinTech News)



Trabalho remoto =
falha de segurança
em 20% das
empresas
(MalwareBytes)

Qual cenário nos encontramos



Mercado de
US\$ 170,4 bi
até 2022
(Gartner)

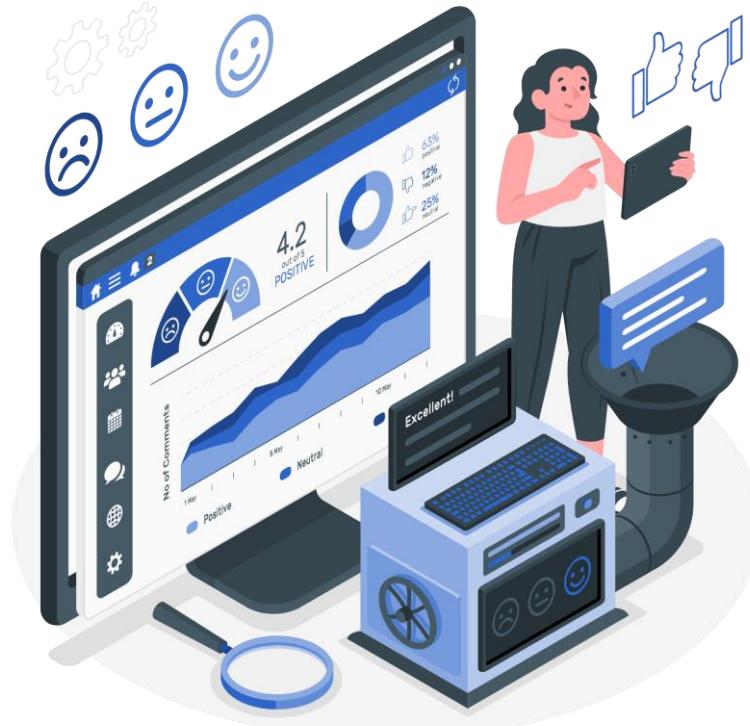
Custo médio de um
ataque US\$ 2,6 mi
(Accenture)



Ransomware: mais
de US\$ 20bi em 2021
com 1 ataque a cada
11 segundos

Sobre o retorno de investimento

A credibilidade de qualquer empresa está em jogo quando há violação de segurança



Uma empresa sem equipe preparada arca com US\$ 5,29 milhões em custos, contra US\$ 2 milhões quando as empresas estão preparadas (IBM)

LGPD e GDPR - Fique de olho



No primeiro ano a GDPR entrou em vigor, o valor total de multas foi de U\$63 milhões

LGPD: Empresas e órgãos públicos podem ser multados em até 2% do faturamento, com limite de R\$ 50 milhões (Senado)

...e você, deixou sua porta aberta?



01

Por onde começar?

Por onde começar?

Análise de ameaças e
risco

Segurança de ativos

Segurança de
pessoas

Qual estado a empresa se
encontra?

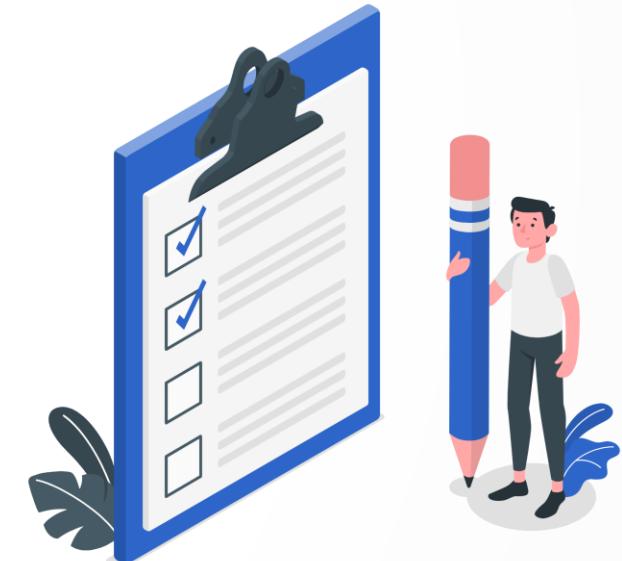
Estabelecimento de Governança e
Políticas de Segurança

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Qual estado a empresa se encontra?

Fazer um diagnóstico de sua empresa:

1. Qual é o tamanho da organização?
2. Quais os ativos que devem ser protegidos?
3. Quantos projetos existem?
4. Nossos projetos trabalham com informações que extrapolam o campo da segurança e também envolvem a gestão de dados privados?
5. Existe planos de expansão de projetos ou de ativos?
6. Quais são as políticas e estratégias existentes para garantir segurança e privacidade?



Qual estado a empresa se encontra?

Microsoft Security Assessment Tool (MSAT 4.0)

Perfil de risco da empresa (PRE): Medição dos riscos a que uma organização está exposta, com base no ambiente do negócio e no setor em que ela compete.

Índice de defesa em profundidade (IDP): Medida das defesas de segurança usadas por pessoas, processos e tecnologias para ajudar a atenuar os riscos identificados para uma empresa.



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Qual estado a empresa se encontra?

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar menu is titled "SAT > Avaliação modelo" and lists several categories: Infra-estrutura, Aplicativos, Operações, and Pessoal. Under "Infra-estrutura", there are sub-items: Defesa do perímetro, Autenticação, Gerenciamento e monitoramento, Implantação e uso, Projeto de aplicativos, and Armazenamento de dados e comunicações. The main content area is titled "Infra-estrutura" and contains the following text: "Esta seção se concentra no funcionamento correto da rede, quais os processos de negócios (internos ou externos) que deve suportar, como os hosts são instalados e implantados e como a rede será efetivamente gerenciada e mantida. Com o estabelecimento de um projeto sólido de infra-estrutura que seja compreendido e seguido, a organização pode identificar facilmente as áreas de risco e elaborar métodos para reduzir as ameaças. Você deve levar aproximadamente 10 minutos para preencher esta seção." At the bottom right of the content area is a "Avançar >" button. At the very bottom right of the entire window is a small box containing the text "Envie-nos seus comentários."

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Qual estado a empresa se encontra?

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar menu includes "SAT", "Avaliação modelo", and several sections with icons and status: "Infra-estrutura" (green checkmark), "Defesa do perímetro" (green checkmark), "Autenticação" (green checkmark), "Gerenciamento e monitoramento" (green checkmark); "Aplicativos" (yellow warning icon), "Implantação e uso" (yellow warning icon), "Projeto de aplicativos" (yellow warning icon), "Armazenamento de dados e comunicações" (yellow warning icon); "Operações" (yellow warning icon), "Ambiente" (yellow warning icon), "Política de segurança" (yellow warning icon), "Gerenciamento de patches e atualizações" (yellow warning icon), "Backup e restauração" (yellow warning icon); "Pessoal" (yellow warning icon), "Requisitos e avaliações" (yellow warning icon), "Resumo" (yellow warning icon). The main content area is titled "Aplicativos" and contains the following text: "Esta seção trata dos aplicativos do seu ambiente que são críticos para os negócios e os avalia do ponto de vista da segurança e da disponibilidade. Esta seção examinará as tecnologias usadas no ambiente para aumentar a defesa em profundidade. Você levará aproximadamente 10 minutos para preencher esta seção." It features a "Voltar" button (left) and an "Avançar >" button (right). At the bottom right, there is a link "Envie-nos seus comentários."

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Qual estado a empresa se encontra?

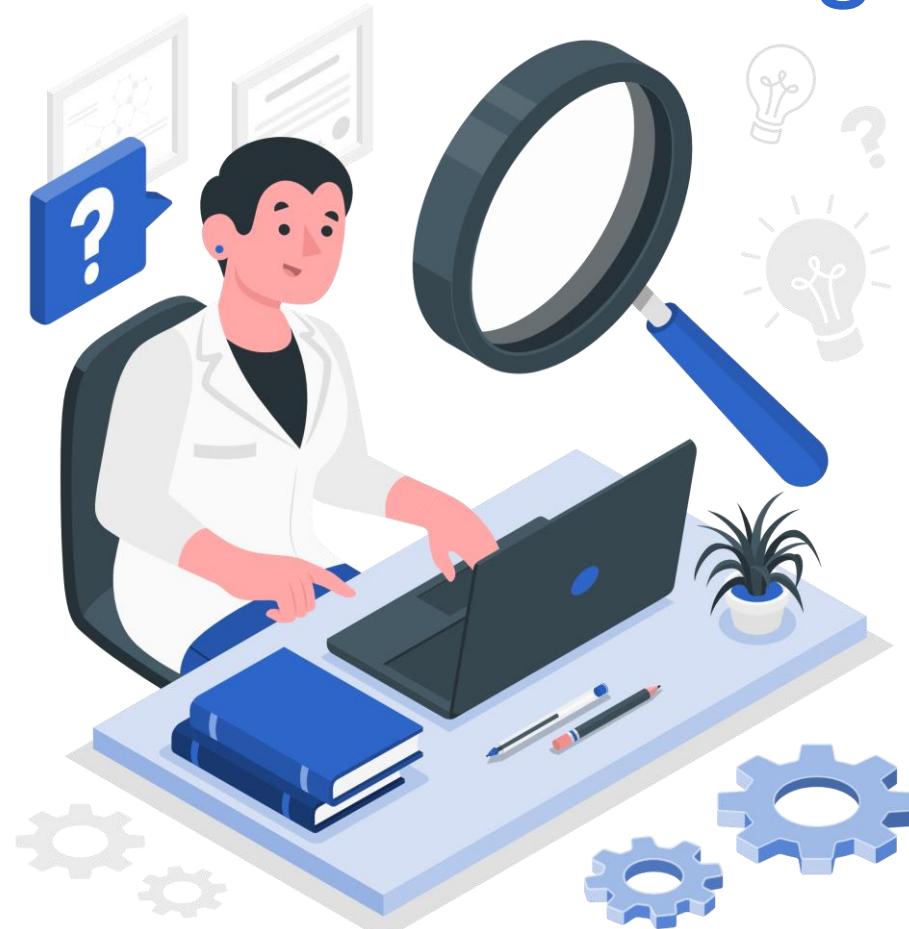
The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar menu is titled "Avaliação modelo" and lists three main categories: "Aplicativos" (with items "Implantação e uso", "Projeto de aplicativos", and "Armazenamento de dados e comunicações" marked with green checkmarks), "Operações" (with items "Ambiente", "Política de segurança", "Gerenciamento de patches e atualizações", and "Backup e restauração" marked with yellow warning signs), and "Pessoal" (with items "Requisitos e avaliações", "Política e procedimentos", and "Treinamento e conscientização" marked with yellow warning signs). The main content area is titled "Operações" and contains the following text: "Esta seção avalia as práticas, procedimentos e diretrizes operacionais que a organização segue para melhorar as estratégias de defesa em profundidade e incluir mais do que apenas tecnologias de defesa. Examina as áreas que controlam os builds (compilações) dos sistemas, a documentação de rede, backup e restauração no ambiente. Você deve levar aproximadamente 10 minutos para preencher esta seção." At the bottom right of the content area is a button labeled "Envie-nos seus comentários.". Navigation buttons "**< Voltar**" and "**Avançar >**" are located at the bottom of the screen.

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Qual estado a empresa se encontra?

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar lists sections: "Aplicativos" (checkmarks for Implantação e uso, Projeto de aplicativos, Armazenamento de dados e comunicações); "Operações" (checkmarks for Ambiente, Política de segurança, Gerenciamento de patches e atualizações, Backup e restauração); and "Pessoal" (yellow warning icons for Requisitos e avaliações, Política e procedimentos, Treinamento e conscientização). The main content area is titled "Pessoal" and contains the following text: "Esta seção examina os processos da empresa que controlam as políticas corporativas de segurança, os processos de RH e o treinamento e a conscientização de segurança dos funcionários. Também se concentra em lidar com a segurança na medida em que esta se relaciona com as operações do dia-a-dia. Esta seção ajuda a avaliar como são atenuados os riscos na área de pessoal. Você deve levar aproximadamente 10 minutos para preencher esta seção." At the bottom right of the content area is a button labeled "Envie-nos seus comentários.". Navigation buttons "< Voltar" and "Avançar >" are located at the bottom of the main content area.

Estabelecimento de Governança e Políticas de Segurança



Se tratando de incidentes, como a organização lida com incidentes no momento?

- analisar casos reais, incidentes registrados pela organização,
- estender o campo de observação para empresas no mesmo ramo de mercado.

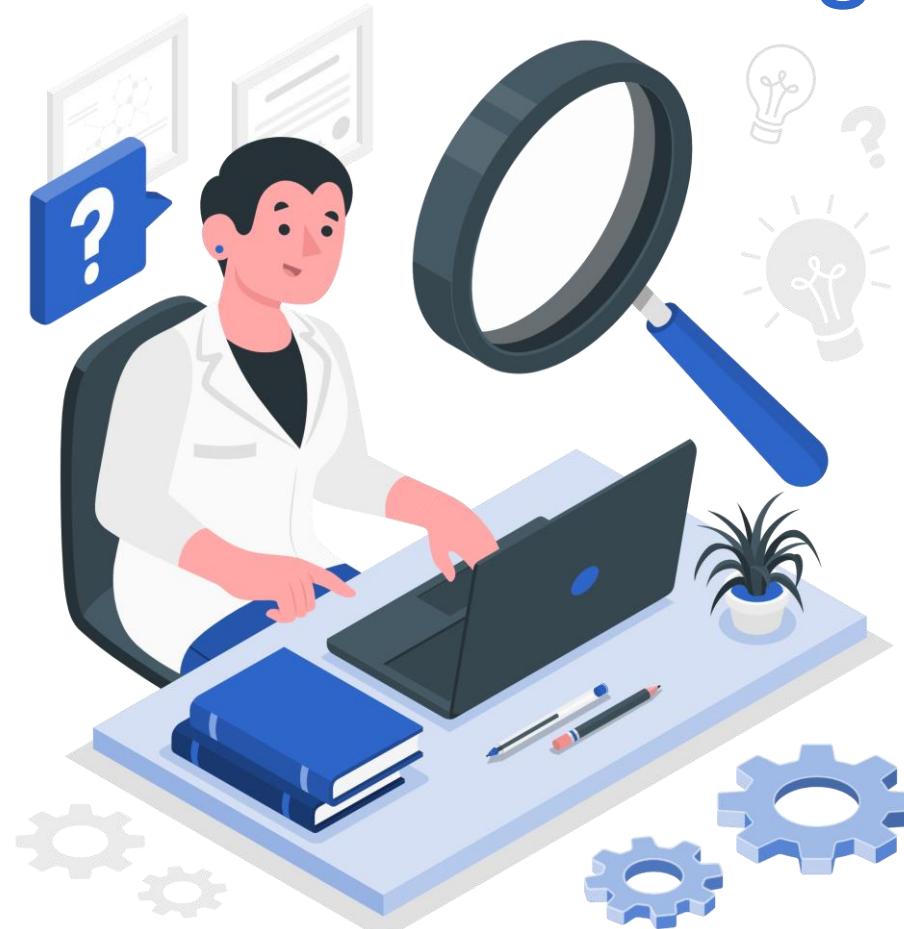
Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Estabelecimento de Governança e Políticas de Segurança



O seu plano de gestão seria capaz de mitigar os incidentes?

O que faltou para que o incidente recebesse o devido tratamento?

Por onde começar?

Análise de ameaças e risco

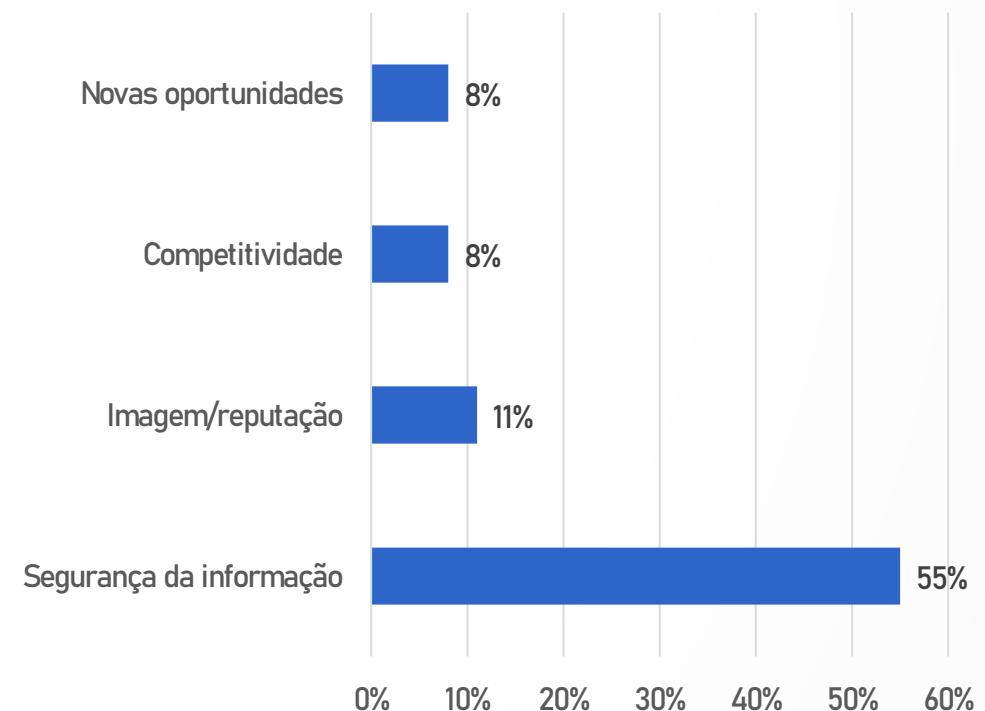
Segurança de pessoas

Segurança de ativos

Estabelecimento de Governança e Políticas de Segurança



Melhorias após adoção da ISO27001
(Help Net Security, 2016)



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Estabelecimento de Governança e Políticas de Segurança

Definição de requisitos de segurança

Exemplo, RFC3871 define requisitos de seguranças operacional para infraestrutura de redes de ISP IP networks (roteadores e switches):

2.2.4. Permitir a seleção de parâmetros criptográficos

Requisito.

O dispositivo DEVE permitir que o operador selecione parâmetros criptográficos. Isso deve incluir comprimentos-chave e algoritmos.

Justificativa.

A criptografia usando certos algoritmos e comprimentos-chave pode ser considerada "forte" em um ponto no tempo, mas "fraca" em outro.

O aumento constante do poder computacional reduz continuamente o tempo necessário para quebrar a criptografia de uma certa força.

Fraquezas podem ser descobertas em algoritmos. A capacidade de selecionar um algoritmo diferente é uma ferramenta útil para manter a segurança diante de tais descobertas.

Exemplos.

Des de 56 bits já foi considerado seguro. Em 1998 foi quebrado por uma máquina construída sob medida em menos de 3 dias. A capacidade de selecionar algoritmos e comprimentos-chave daria ao operador opções (diferentes algoritmos, chaves mais longas) em face de tais desenvolvimentos.

Avisos.

Nenhum

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Estabelecimento de Governança e Políticas de Segurança

OWASP Proactive Controls – C1:

Quatro etapas para implementar requisites de segurança:

- Descoberta e Seleção
- Investigação e documentação
- Implementação
- Teste

Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

02

Análise de ameaças e risco

Definição de ativos e classificação de segurança

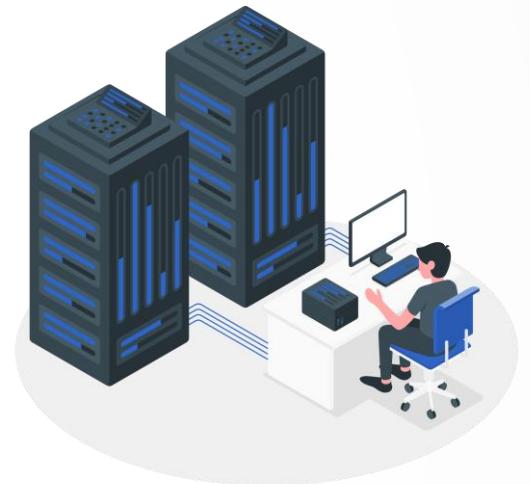
Data flow diagram

Classificação de ameaças com STRIDE

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Definição de ativos e classificação de segurança

Os ativos da empresa são tudo aquilo que pode estar sujeito a ameaças cuja perda da confidencialidade, integridade ou disponibilidade podem implicar em prejuízo.



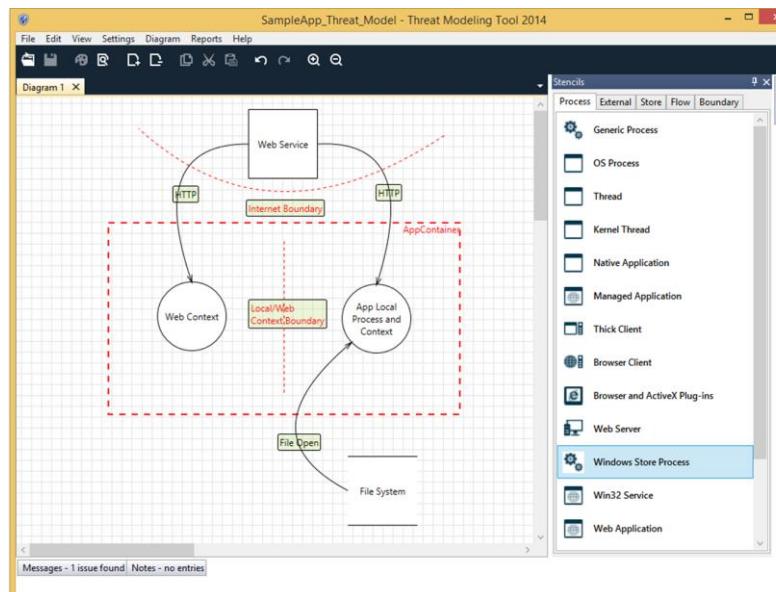
Dispositivos físicos: Roteadores, servidores, câmeras, equipamentos

Software: Sistemas operacionais, firewall, máquinas virtuais

Serviços de rede: VPN, protocolos wireless, redes ópticas

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

- O data flow diagram (DFD) deve:
- Complementar a compreensão da instituição sobre o fluxo de informações
- Identificar conjuntos de dados e subconjuntos compartilhados entre sistemas
- Identificar aplicativos compartilhando dados
- Destacar a classificação dos dados que estão sendo transmitidos



Data flow diagram

Tem por objetivo capturar os principais componentes de um Sistema de Informações, como os dados se movem dentro do sistema, pontos de interação do usuário e os limites de confiança.

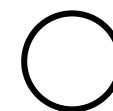
Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Data flow diagram



Processo: atividades que podem modificar ou redirecionar a entrada recebida para suas saídas adequadas



Data store: dados armazenados de forma temporária ou permanente.



Entidade externa: pode ser um processo, armazenamento de dados ou até mesmo um sistema completo fora do seu controle direto.



Fluxo de dados: A movimentação de dados entre a fonte de dados e o destino.



Limites de confiança: são usados para descrever o fluxo de dados à medida que cruza diferentes níveis de zona de confiança.

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Classificação de ameaças com STRIDE

Spoofing: ou falsificação, consiste em passar por alguém.

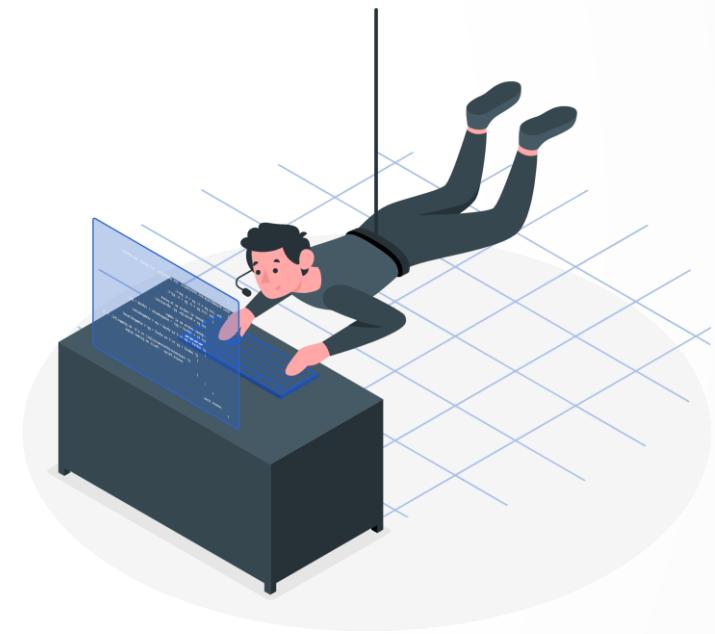
Tampering: ou adulteração de dados sem autorização.

Repudiation: evitar ser responsabilizado por uma ação.

Information disclosure: acessar dados sem permissão.

Denial of service: sobrecarregar o sistema para torná-lo indisponível.

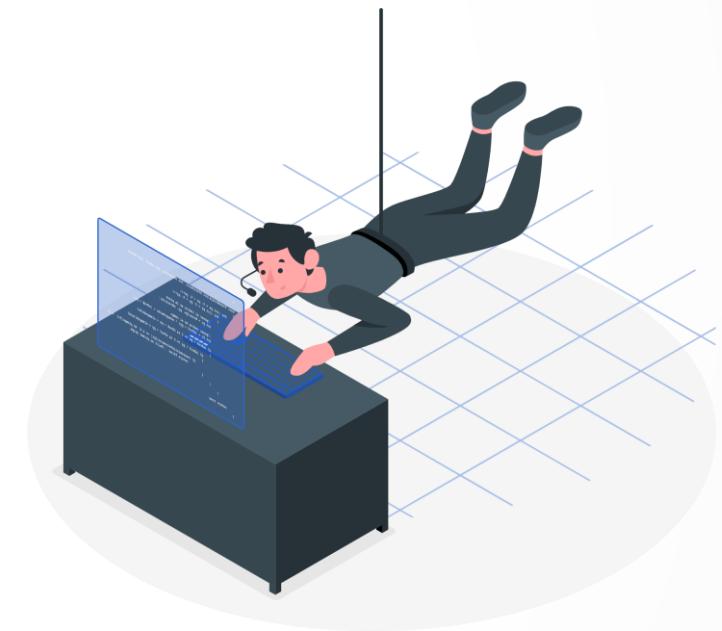
Elevation of privilege: conseguir mais privilégios do que o devido no sistema.



Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Classificação de ameaças com STRIDE

Ameaça	CS	DFD
Spoofing	Autenticação	Processo, entidade externa
Tampering	Integridade	Processo, data store e fluxo de dados
Repudiation	Não-repúdio	Processo, entidade externa e data store
Information disclosure	Confidencialidade	Processo, data store e fluxo de dados
Denial of service	Disponibilidade	Processo, data store e fluxo de dados
Elevation of privilege	Autorização	Processo



Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Evento	Ação	Plano
Não cumprir obrigações de conformidade	EVITAR	Implementar processo formal de monitoramento de conformidade
Falha na coleta de recebíveis em tempo hábil	REDUZIR	Implementar o rastreamento de recebíveis e o processo de acompanhamento de devedores
Ataque de ransomware	TRANSFERIR	Acionar o Seguro de cyber risk
Ocorrência de um desastre natural	ACEITAR	Recuperar ativos não afetados pelo desastre

Identificação e avaliação de riscos e planos de mitigação

Evitar

Reducir

Compartilhar ou Transferir

Aceitar

03

Segurança de pessoas

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Segurança de pessoas

Treinamento

Conscientização e avaliação

Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Segurança de pessoas



Toyota, 2019: Prejuízo de **US\$ 37 mi**

Condado de Cabarrus, EUA, 2018: Prejuízo de **US\$ 1,7 mi**

Pesquisa LastPass (2017):
59% compreendem importância de senhas seguras
91% entendem os riscos do reuso de senhas
41% usavam senhas fáceis de lembrar
61% usavam senhas iguais ou semelhantes



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Treinamento

- Survey para coleta e dados
- Modelagem de programas de treinamentos e focados em papéis
- Ensinar sobre os principais vetores de ameaça:
 - Identificar Phishing*
 - Engenharia social*
 - Criação de senhas válidas (utilização de gerenciadores e autenticação multifatores)*
 - Cuidados na rede wi-fi doméstica*
 - Utilização adequada do equipamento da empresa*
 - Responsividade a eventos*



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Treinamento

Cursos gratuitos:

[Information Security: Context and Introduction | Coursera](#)

[Cybersecurity for Everyone | Coursera](#)

[NSE Institute: Library \(fortinet.com\)](#)

Aprendizado gratuito na Udemy



Segurança da informação para iniciantes na prática

Emerson Patron, Marcus Oliveira

4.6 ★★★★★ (107)

42 horas no total • 11 aulas • Iniciante

Gratuito



Cyber Security Course for Beginners - Level 01

FourTrails Technologies

4.1 ★★★★★ (11.383)

1 hora 46 min • 13 aulas • Iniciante

Gratuito



Security Awareness Campaigns (Lite)

Michael Goedeker

4.2 ★★★★★ (5.345)

31 minutos no total • 8 aulas • Iniciante

Gratuito



Build Your Own Cyber Lab at Home

Kyle Stoen

4.4 ★★★★★ (2.023)

1,3 horas no total • 22 aulas • Técnico avançado

Gratuito



Cybersecurity Awareness Training

Erie Schwartzman

4.5 ★★★★★ (2.348)

38 minutos no total • 12 aulas • Técnico avançado

Gratuito

Por onde começar?

Análise de ameaças e risco

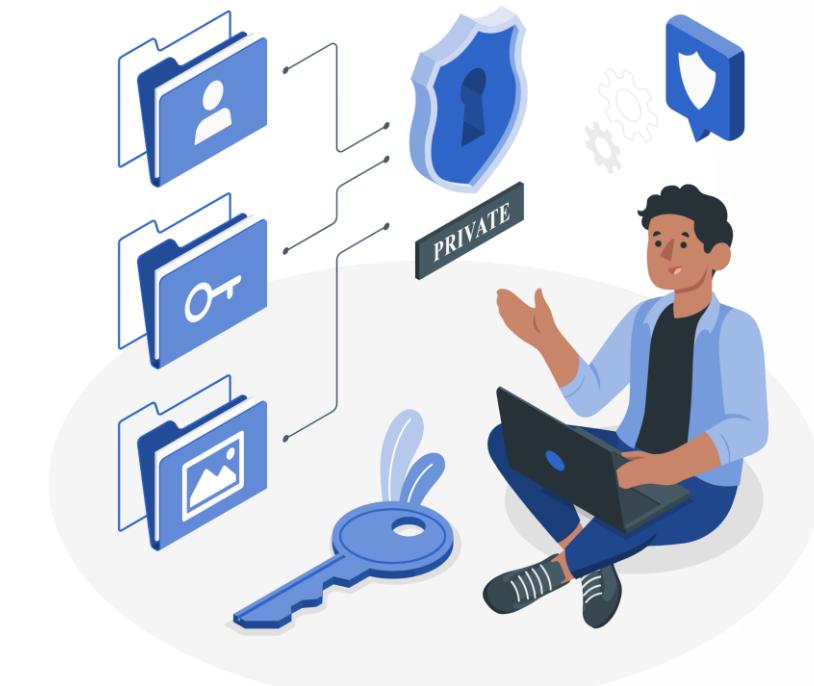
Segurança de pessoas

Segurança de ativos

Conscientização e avaliação

Mecanismos de incentivo e/ou recompensa:

- sistema de pontuação por desempenho nos treinamentos
- scoreboard
- programas de recompensa ou vouchers para concessão de descontos
- seleção de “embaixadores da segurança”



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Conscientização e avaliação

Com os resultados, será possível definir novas políticas para reforçar o engajamento

Definição de um processo cílico de melhoria contínua.



04

Segurança de ativos

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Hardening
Infraestrutura
Segurança em Cloud
Segurança no ambiente de desenvolvimento

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Hardening

Também conhecido por **blindagem de sistemas** trata-se de técnicas para prover mais segurança em servidores e serviços, sejam esses externos (web) ou internos como bancos de dados, arquivos e outros ativos acessíveis através da rede.

Sair do "*default*"

[Pesquisa SonicWall\(29 jul 2021\)](#):

304,7 milhões, foi o número de ataques no 1º semestre de 2021 ultrapassando todo o ano passado

Brasil foi **5º** o país mais atacado com 9.1 milhões, computando o aumento de:

917% Governo
615% Educação
594% Saúde
264% Varejo



Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Hardening

Segurança física

Sistemas Operacionais

Aplicações

Ferramentas de segurança

Redes e serviços

Auditoria e monitoramento de sistemas

Controle de acesso

Encriptação de dados

Correções e atualizações

Backup do sistema

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Hardening

CIS® – Center for Internet Security, Inc.

CIS-CAT

CIS Hardened Images

The screenshot displays the CIS Center for Internet Security website. It features two main sections: 'Secure Your Organization' and 'Secure Specific Platforms'.
Secure Your Organization:

- CIS Controls®**: Prioritized & simplified best practices
- CIS RAM**: Information security risk assessment method
- CIS Controls Community**: Help develop and maintain the Controls
- CIS CSAT**: Assess & measure Controls implementation

Secure Specific Platforms:

- CIS Benchmarks™**: 100+ vendor-neutral configuration guides
- CIS-CAT®**: Assess system conformance to CIS Benchmarks
- CIS Benchmarks Community**: Develop & update secure configuration guides
- CIS Hardened Images®**: Virtual images hardened to CIS Benchmarks

Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Hardening

Itens no plano de segurança de informação:

- Particionamento de discos
- Serviços desnecessários e inseguros
- Política de força e renovação de senhas
- Usuários inválidos
- Desconexão de usuários não autorizados
- GRUB (senha criptografada)

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Hardening

- Políticas de rede / utilização
- Gerenciamento de privilégios (root/admin)
- Segurança no Terminal (logout)
- SSH
- Portas abertas
- Permissões de execução

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Hardening

Hardening - Artigo Revista Infra Magazine 1

<https://www.devmedia.com.br/hardening-artigo-revista-infra-magazine-1/20818>

Security Hardening Standards: Why do you need one?

<https://www.packetlabs.net/security-hardening-standards/>

The Center for Internet Security, Inc. (CIS®)

<https://www.cisecurity.org/about-us/>



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Infraestrutura

Cada camada a ser protegida é importante.

Identificação do valor do bem protegido e dos impactos diretos e indiretos no acesso indevido.

- Assim como casas tem portões, portas e ainda assim guardamos o que temos de valor dentro de cofres.

Pesquisa CSO/ESG(2020):

378 desenvolvedores e profissionais de segurança,
uso:

56% API Security Vulnerability (ASV)

40% IaCode - Configuração

40% Static application security testing (SAST)

29% IDE, Microserviços



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Infraestrutura

A grande disponibilidade de ferramentas facilita o uso, mas antes um levantamento das vulnerabilidades e riscos precisa ser feito para identificar onde são necessárias.

Prevenção, combate e auditoria.

Oportunidade para prestadores de serviço

Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Infraestrutura

Onde atuar:

- Backup
- Inventário
- Antivírus
- Monitoramento
- Firewall
- Navegação
- Patch
- Wireless
- AD (Active Directory)
- E-mail e SPAM
- Padronização SO
- Rede

Por onde começar?

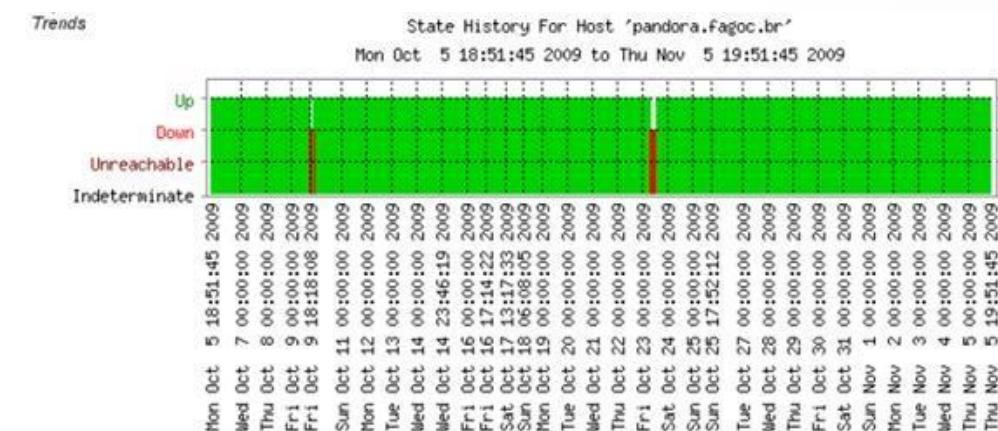
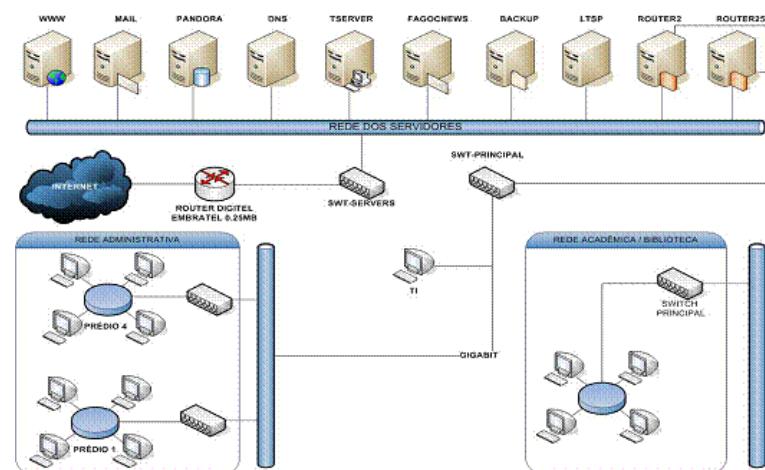
Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Infraestrutura

Nagios



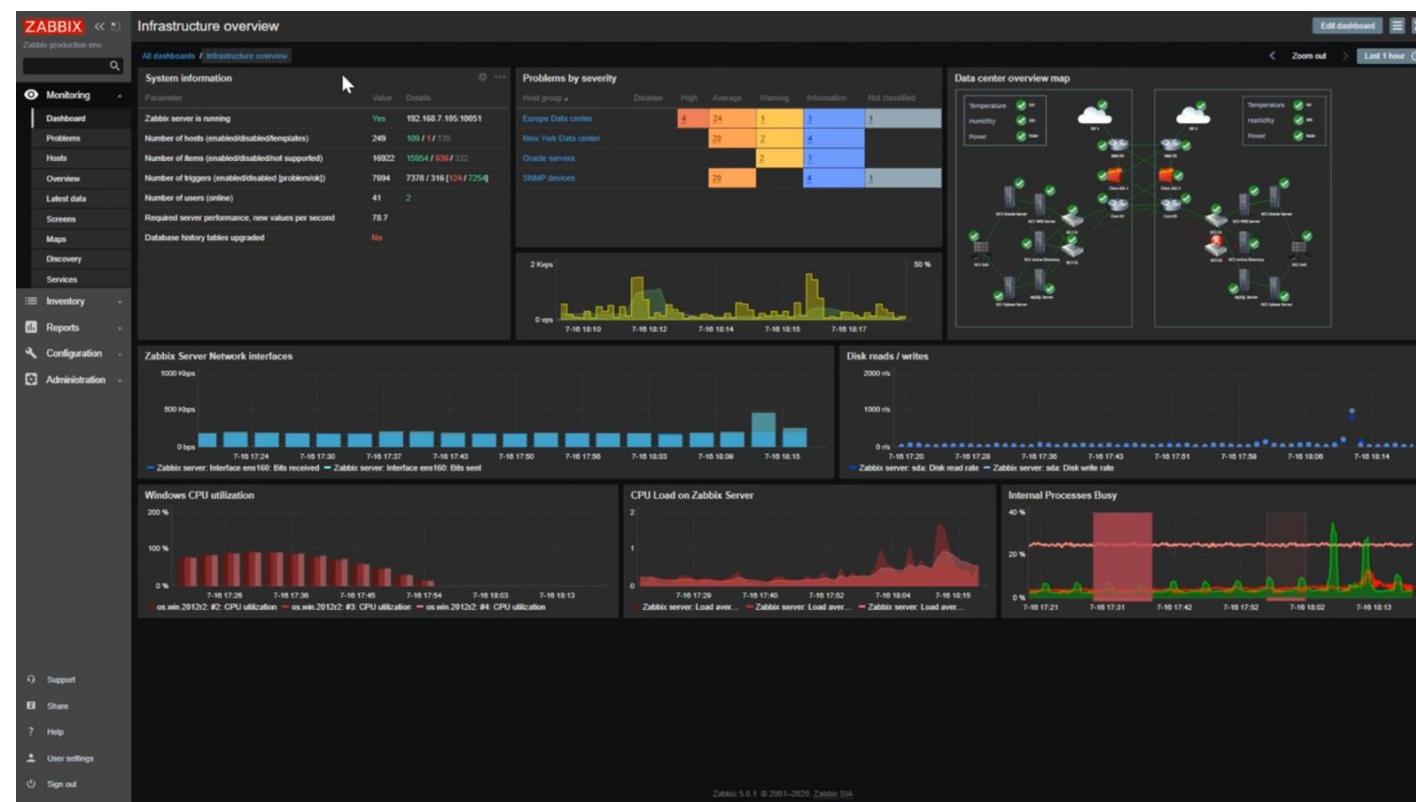
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
HTTP	98.270% (98.270%)	0.000% (0.000%)	0.000% (0.000%)	1.730% (1.730%)	0.000%
MySQL	95.389% (95.389%)	0.000% (0.000%)	0.000% (0.000%)	4.611% (4.611%)	0.000%
PING	95.609% (95.609%)	0.503% (0.503%)	0.000% (0.000%)	3.889% (3.889%)	0.000%
Average	96.423% (96.423%)	0.168% (0.168%)	0.000% (0.000%)	3.410% (3.410%)	0.000%

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Infraestrutura

Zabbix (Open Source)



Por onde começar?

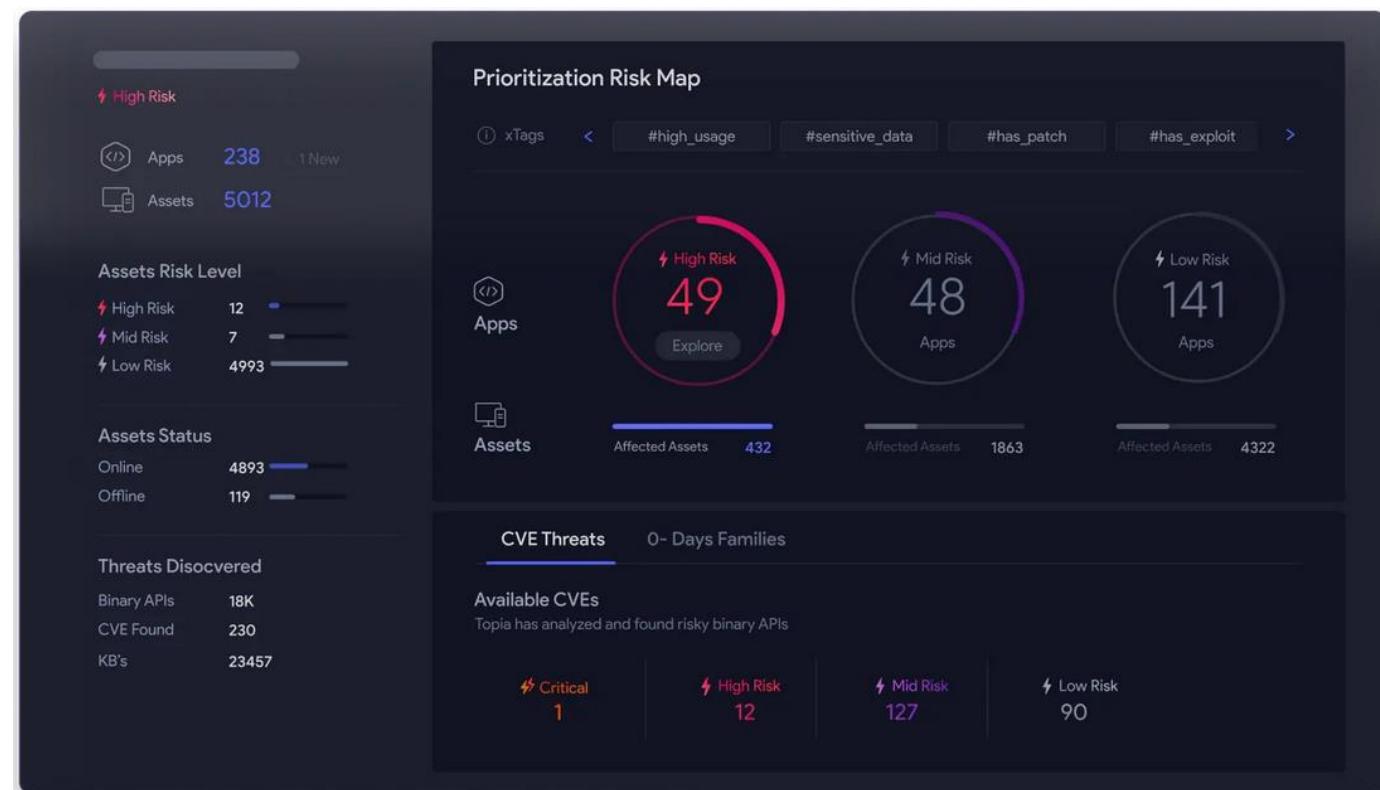
Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Infraestrutura

Vicarius



Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Infraestrutura

NESSUS

The screenshot displays the Nessus web interface. On the left, a sidebar includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). The main content area is divided into several categories:

- DISCOVERY:** Host Discovery (A simple way to discover live hosts and open ports).
- VULNERABILITIES:**
 - Basic Network Scan (A full system scan suitable for any host).
 - Advanced Scan (Configure a scan without using any recommendations).
 - Advanced Dynamic Scan (Configure a dynamic plugin scan without recommendations).
 - Malware Scan (Scan for malware on Windows and Unix systems).
 - Mobile Device Scan (Assess mobile devices via Microsoft Exchange or an MDM).
 - Web Application Tests (Scan for published and unknown web vulnerabilities).
 - Credentialed Patch Audit (Authenticate to hosts and download missing updates).
- COMPLIANCE:**
 - Audit Cloud Infrastructure (Audit the configuration of third-party cloud services).
 - Internal PCI Network Scan (Perform an internal PCI DSS (11.2.1) vulnerability scan).
 - MDM Config Audit (Audit the configuration of mobile device managers).
 - Offline Config Audit (Audit the configuration of network devices).
 - PCI Quarterly External Scan (Approved for quarterly external scanning as required by PCI).
 - Policy Compliance Auditing (Audit system configurations against a known baseline).
 - SCAP and OVAL Auditing (Audit systems using SCAP and OVAL definitions).

At the bottom left, there is a "Tenable News" section with the headline "Focus on the Fundamentals: 6 Steps to Defend Again..." and a "Read More" link.

Por onde começar?

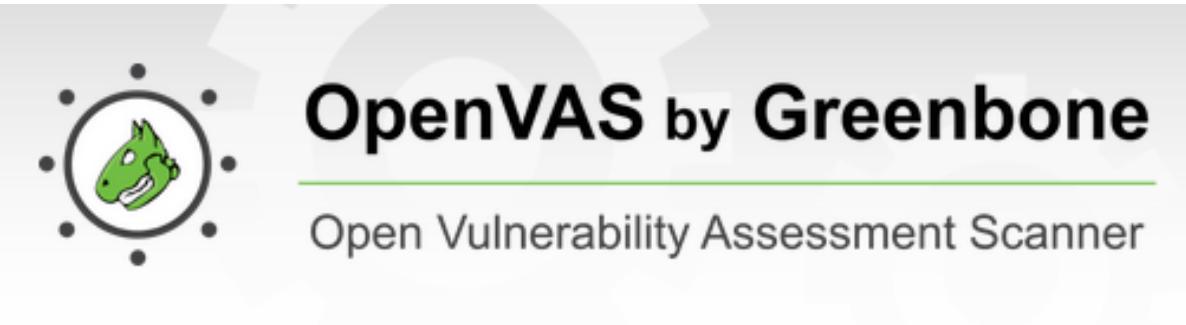
Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Infraestrutura

OpenVAS



Por onde começar?

Análise de ameaças e
risco

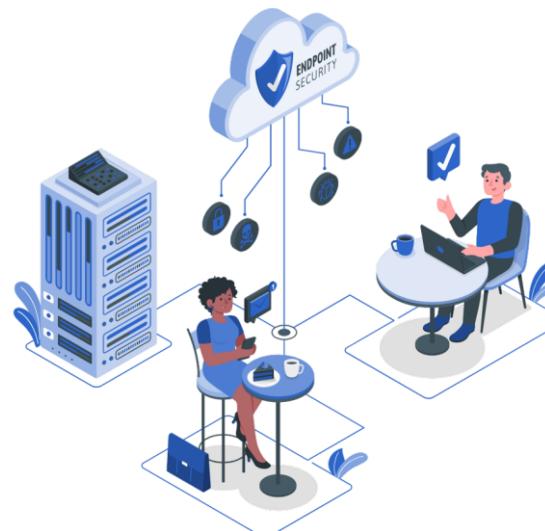
Segurança de
pessoas

Segurança de ativos

Segurança em Cloud

Maior exposição e suscetibilidade a ataques.

- Assegure que os dados e sistemas estejam seguros
- Acompanhe o estado dos dados e das configurações de segurança
- Monitoramento constante de parâmetros (notificação)



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Segurança em Cloud

- Recursos hospedados
- Perímetros
- Ameaças sofisticadas

Pesquisa CSO/ESG(2020):

41% possuíam chaves hardcoded utilizadas no provisionamento de recursos

89% possuíam recursos com controle de acesso e identidade altamente permissivos

Quase **todos** possuíam falhas nas configurações de roteamento

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Segurança em Cloud

Responsabilidade

- Conformidade (GDPR / LGPD)
- Softwares confiáveis
- Ciclos de vida
- Portabilidade
- Monitoramento
- Pessoal qualificado

Por onde começar?

Análise de ameaças e
risco

Segurança de
pessoas

Segurança de ativos

Segurança em Cloud

Infraestrutura, plataforma, software como serviço

- Autenticação
- Backup e restauração
- Ferramentas (AWS)

- Por onde começar?
- Análise de ameaças e risco
- Segurança de pessoas
- Segurança de ativos

Segurança no ambiente de desenvolvimento

Nenhuma falha conhecida deve ser levada pra produção

[37 \(Famous\) Software Failures](#)

[Top software failures in recent history](#)



Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Segurança no ambiente de desenvolvimento

Boas práticas:

- Gerenciamento de código fonte
- Realização de testes
- Correção de bugs
- Integração contínua
- Documentação
- Padrões de código seguro

[Pesquisa CSO/ESG\(2020\)](#):
378 desenvolvedores e profissionais de segurança
45% distribuem código com vulnerabilidades devido a deadline
60% admitem terem sofrido de itens no OWASP Top-10

Segurança no ambiente de desenvolvimento

As ameaças dentro de casa:

- 3PP (Third Party Product)
- FOSS (Free Open-Source Software)
- Docker images

Proteções:

- Análise de versões específicas
- Repositório de versões estáveis / checksum
- Testes de Integração

[Pesquisa CSO/ESG\(2020\)](#):

430% aumento anual de ataques a projetos open-source

79 outros 3PPs são usados em média por cada 3PP disponibilizados via npm de em média **39** diferentes mantenedores

5 principais pacotes são usados por 134mil+ outros pacotes

50% do código é composto de open-source, mas apenas **48%** das empresas investiram em medidas

Por onde começar?

Análise de ameaças e risco

Segurança de pessoas

Segurança de ativos

Segurança no ambiente de desenvolvimento

OWASP – Open Web Application Security Project

- Top 10 (<https://www.owasptopten.org/>)
- Guias de teste (Mobile)
- Comunidade



OWASP® Foundation

Membros

93.516

Grupos

232

Países

72

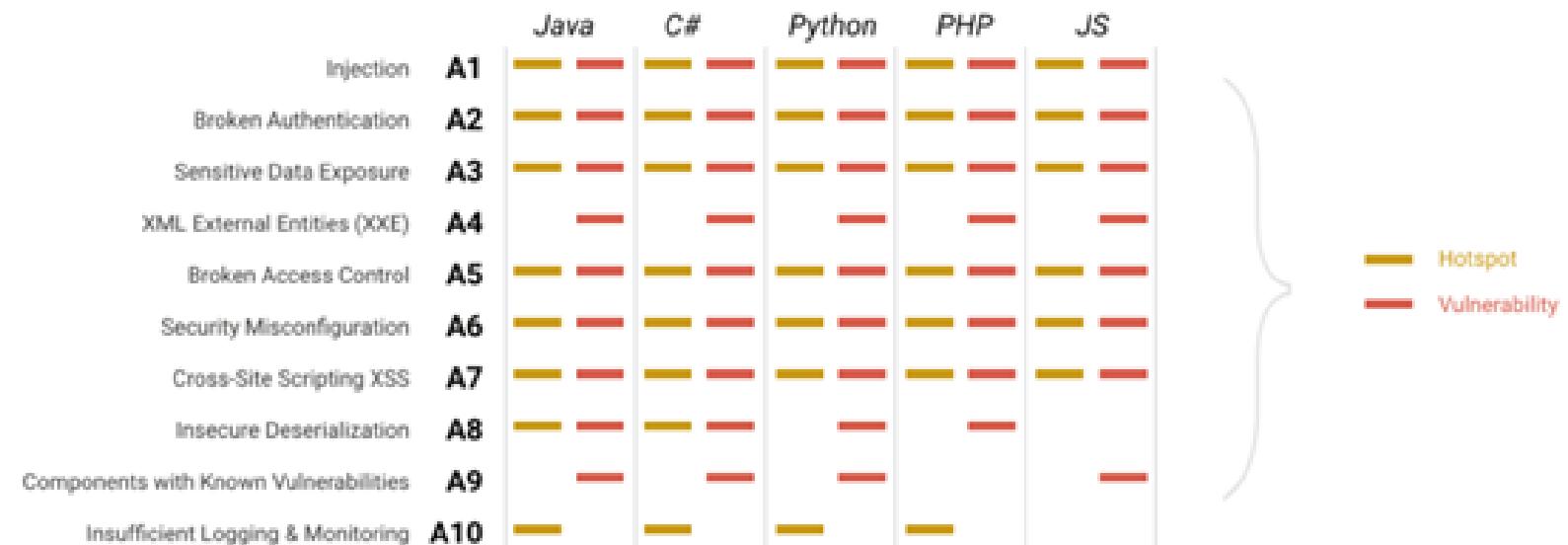
South America

- OWASP Asuncion, Paraguay
- OWASP Belem
- OWASP Belo Horizonte
- OWASP Bogota
- OWASP Bolivia
- OWASP Brasilia
- OWASP Cartagena
- OWASP Chile
- OWASP Cusco
- OWASP Fortaleza
- OWASP Guayaquil
- OWASP Lima
- OWASP Medellin
- OWASP Monterrey
- OWASP Natal
- OWASP Patagonia
- OWASP Porto Alegre
- OWASP Queretaro City
- OWASP Quito
- OWASP Recife
- OWASP Rio De Janeiro
- OWASP Santa Rita do Sapucai
- OWASP Sao Paulo
- OWASP Uruguay
- OWASP Vina Del Mar
- OWASP Vitoria

Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

Segurança no ambiente de desenvolvimento

- Integração Contínua/Distribuição Contínua (CI/CD)
- Static Application Security Testing (SAST) – SonarQube [SonarQube](#)



Por onde começar?
Análise de ameaças e risco
Segurança de pessoas
Segurança de ativos

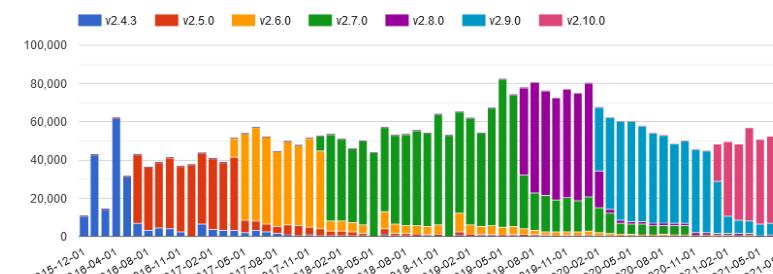
Segurança no ambiente de desenvolvimento

OWASP ZAP

Aplicações e websites vulneráveis

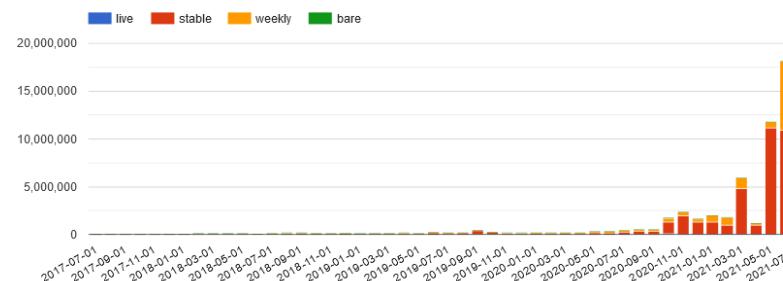
Direct Downloads

Direct downloads since v2.4.3. It is worth noting that downloads have reduced since the Docker images have become more popular.



Docker Pulls

Docker pulls since the ZAP Docker images were published.



Centro de Segurança Cibernética do Inatel:

<https://inatel.br/cxsc/>



Maiores informações, referências, links:



https://danielpfernandes.github.io/tdc_transformations_sec_inatel/

Todas as imagens foram desenvolvidas por Freepik, disponíveis em <https://storyset.com>

Obrigado!

Todas as imagens foram desenvolvidas por Freepik, disponíveis em <https://storyset.com>