O que o *Hack* da NASA tem a ver com seu *software*?

Cyber Security e Desenvolvimento Seguro

Mário Jorge L dos Santos

Objetivos

- Definir CyberSecurity, mostrar o impacto que essa área tem nas nossas vidas.
- Mostrar como o desenvolvimento de software está ligado a cibersegurança e apresentar o caminho para quem deseja aprender a desenvolver software mais seguro.

O que é Segurança da Informação?

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Glossário de segurança da informação - **PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021**

Atualizada em 28/02/2025.

Tríade CIA

Confidencialidade, Integridade e Disponibilidade

O que é **Cyber Security?**

Cibersegurança é a convergência entre pessoas, processos e tecnologia combinadas para proteger organizações, individuos e redes contra ataques digitais. **(tradução nossa)**

CISCO SYSTEMS(TM)

Conceitos importantes em Cyber Security:
=> Ameaça <=

Conjunto de fatores externos com o potencial de causar algum dano para um sistema ou organização; [Glossário de Segurança da Informação, GSI/PR](#).

Conceitos importantes em Cyber Security:

=> Ator de Ameaça <=

Um ator de ameaça é uma pessoa ou grupo que realiza um ação ou processo com intenção de causar dano usando computadores, dispositivos, sistemas ou redes. (CIS)(Tradução nossa).

Classificação dos
=> Atores de Ameaça <=

Os atores de ameaças são classificados em cinco grupos baseados nas suas motivações e afiliações:

- **Cybercriminosos ->** Ganho financeiro e ou de reputação;
- **Insiders ->** Ganho financeiro ou busca por vingança;
- **Estado-Nação ->** Espionagem, política, econômica ou militar;
- **Hacktivista ->** Hackers criminosos motivados por ideologia;
- **Organizações terroristas ->** Politica e ideologica, ganho financeiro, espionagem.

Fonte: (CIS)(Tradução nossa).

Conceitos importantes em Cyber Security:
=> Vulnerabilidade <=

Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores.

Consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha; **Glossário de Segurança da Informação, GSI/PR**.

Conceitos importantes em Cyber Security:
=> Vulnerabilidade <=

Uma fraqueza na lógica computacional (código) encontrada em componentes de software e hardware que, quando explorada, resulta em um impacto negativo para confidencialidade, integridade ou disponibilidade. (NIST). **Tradução nossa.**

=> Vulnerabilidade <=

CVE -> Sistema de numeração unificado para vulnerabilidades; (MITRE)

CVSS -> Classificação das vulnerabilidades; (FIRST)

KEV -> Catálogo de vulnerabilidades exploradas conhecidas. (CISA)

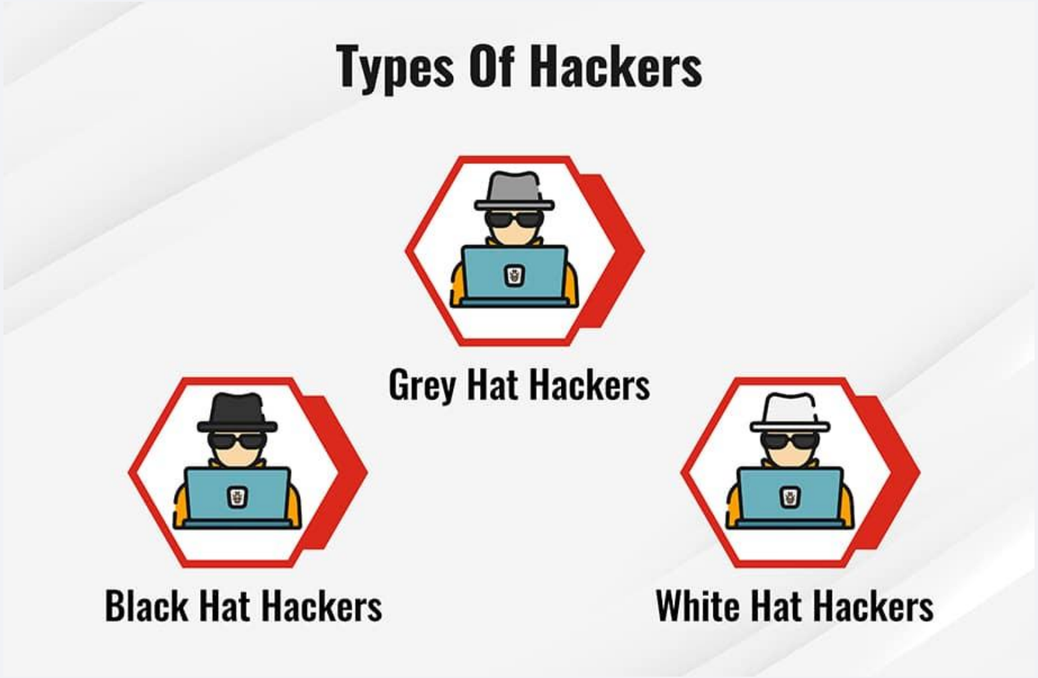
Conceitos importantes em Cyber Security:

=> Hacker <=

“Profissional de tecnologia da informação ou entusiasta que compromete (“hackeia”) a segurança de computadores.” (Britannica).

=> Tipos de Hacker <=

- Black Hat -> Criminoso;
- White Hat -> Hacker Ético/Profissional de CyberSec;
- Gray Hat -> Meio termo, não malicioso, mas nem sempre ético.

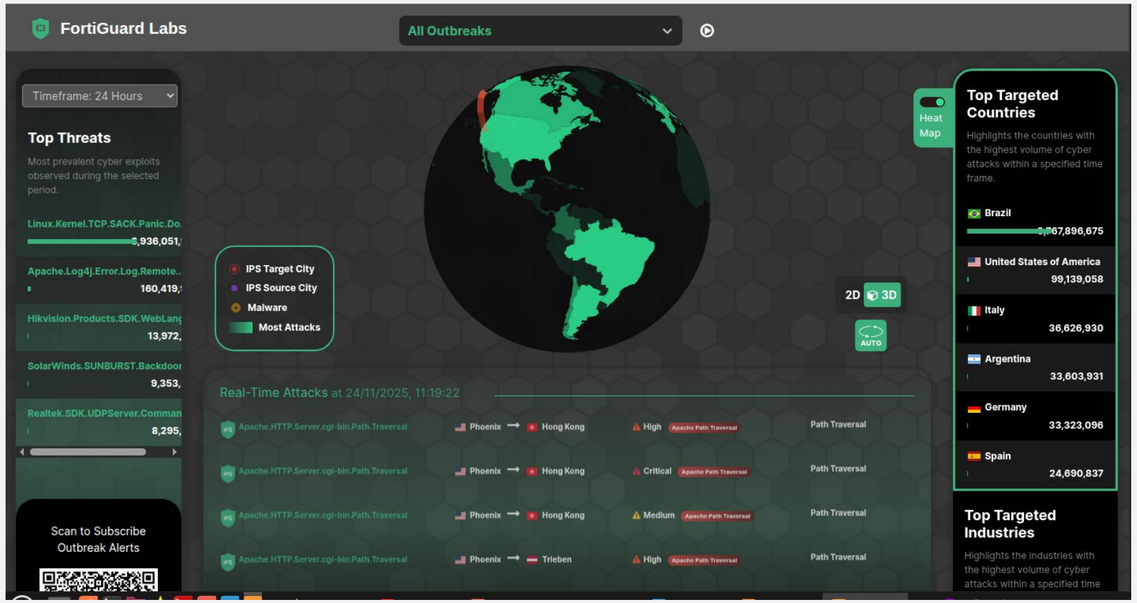


Ameaças Cibernéticas Comuns

- Malware (software malicioso)
- Phising
- Roubo de dados
- Ataques Man-in-the-Middle
- Ransonware
- Ataques DDoS (Negação de serviço)
- Fraudes
- Zero-day Exploits

Mapas de Ameaças Cibernéticas

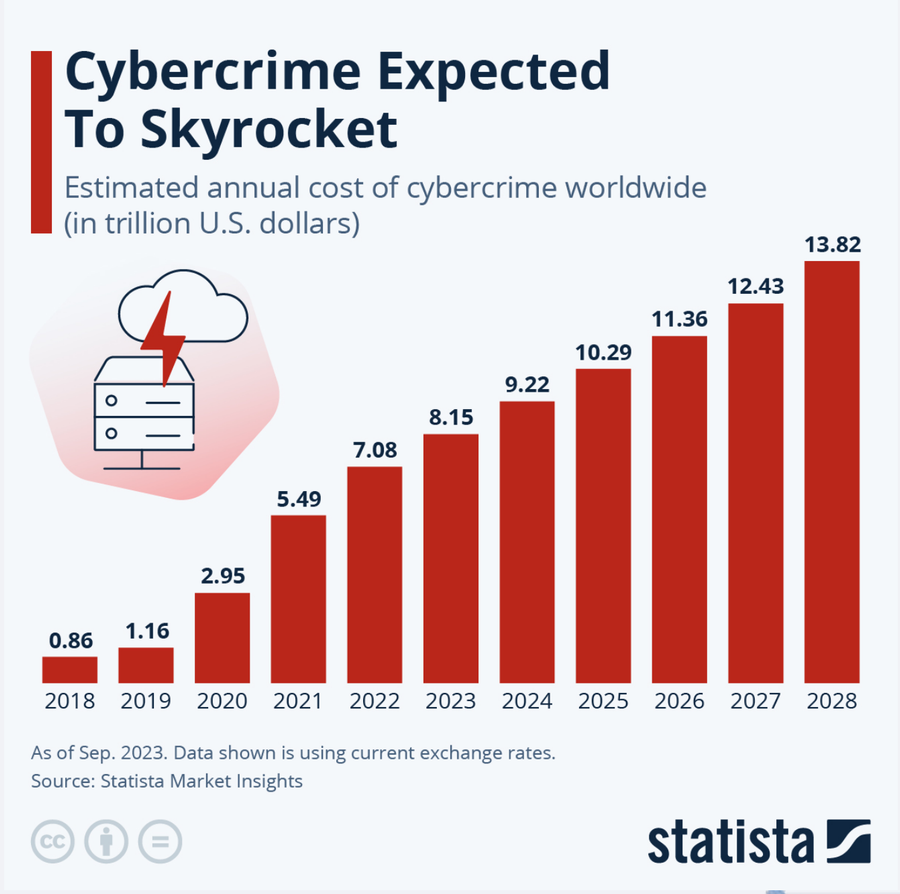
- Kaspersky
- Cisco Talos
- Fortinet
- Checkpoint
- Bitdefender
- Radware



Impacto de ataques cibernéticos

- Perdas Financeiras;
- Danos a reputação/imagem;
- Roubo de dados;
- Roubo de identidade/Estelionato;
- Interrupções em serviços;
- Danos em serviços de infraestrutura crítica.

Impacto de ataques cibernéticos / Cybercrime



Wannacry (2017)

O ataque de ransonware WannaCry foi um grande incidente de segurança que afetou organizações em todo o mundo. Em 12 de maio de 2017, o worm do ransomware WannaCry se espalhou para mais de 200 mil computadores em mais de 150 países. Vítimas ilustres incluem FedEx, Honda, Nissan e o Serviço Nacional de Saúde (NHS) do Reino Unido, que foi forçado a desviar algumas de suas ambulâncias para hospitais alternativos.

Terça-feira, 17/01/2017, às 18:45, por [redacted]

Ucrânia tem segundo apagão elétrico causado por ~~hackers~~

Empresas de segurança estão divulgando os primeiros detalhes sobre um ataque cibernético que teria causado um apagão e cortado parte do abastecimento de energia de Kiev, capital da Ucrânia, no dia 17 de dezembro.

Este é o segundo apagão elétrico causado por hackers. O primeiro ocorreu também na Ucrânia em 23 de dezembro de 2015. A ISSP, uma empresa de segurança ucraniana que conduz a investigação para a companhia de energia Ukrenergo, vê uma ligação entre este ataque e seu antecessor.

Violação da Pegasus Airlines da Turquia expõe 6,5 TB de dados

O bucket AWS S3 mal configurado que levou à violação agora foi protegido

Prajeet Nair (@prajeetspeaks) · 31 de maio de 2022

Uma violação de dados na empresa turca Pegasus Airlines colocou em risco mais de 6,5 TB de dados confidenciais de malas eletrônicas de voo, incluindo detalhes confidenciais do voo, código-fonte e dados da equipe, dizem pesquisadores de segurança cibernética da empresa de segurança Safety Detectives.

Grande vazamento de dados do Facebook revela 1,2 bilhão de registros de usuários, afirma hacker

Publicado: 21 de maio de 2025 · Última atualização: 22 de maio de 2025

Imagem de Cybernews.

Um enorme banco de dados de registros de usuários de 1,2 bilhão foi retirado do Facebook, de propriedade da Meta, por meio do abuso de uma das interfaces de programação de aplicativos (APIs) da plataforma de mídia social, alegam invasores. Enquanto isso, Meta não negou que a confusão tenha ocorrido.

Violação de dados do Yale New Haven Health afeta 5,5 milhões de pacientes

24 de abril de 2025 10:12 DA MANHÃ 0

O Yale New Haven Health (YNHHS) alerta que agentes de ameaças roubaram dados pessoais de 5,5 milhões de pacientes em um ataque cibernético no início deste mês.

O YNHHS é uma rede de saúde sem fins lucrativos em Connecticut, a maior do estado, que oferece atendimento abrangente em cinco hospitais e 360 locais ambulatoriais. Ela emprega 30.000 profissionais de saúde e tem uma receita anual de mais de US$ 5,6 bilhões.

Ataque hacker em empresa que opera o sistema PIX desvia R$ 420 milhões; BC bloqueia R$ 350 milhões

Banco Central conseguiu bloquear R$ 350 milhões desviados. Sinqia, companhia que conecta bancos ao PIX, confirmou ter identificado o ataque e disse que ele ficou restrito ao ambiente do sistema.

[redacted] — Brasília

30/08/2025 17h42 · Atualizado há 2 meses

PF prende 21 pessoas responsáveis por ataque hacker que afetou Pix

Prisões foram em sete estados, na Espanha e na Argentina; ataque desviou R$ 813 milhões e parte foi transformada em cripto

[redacted] Brasília

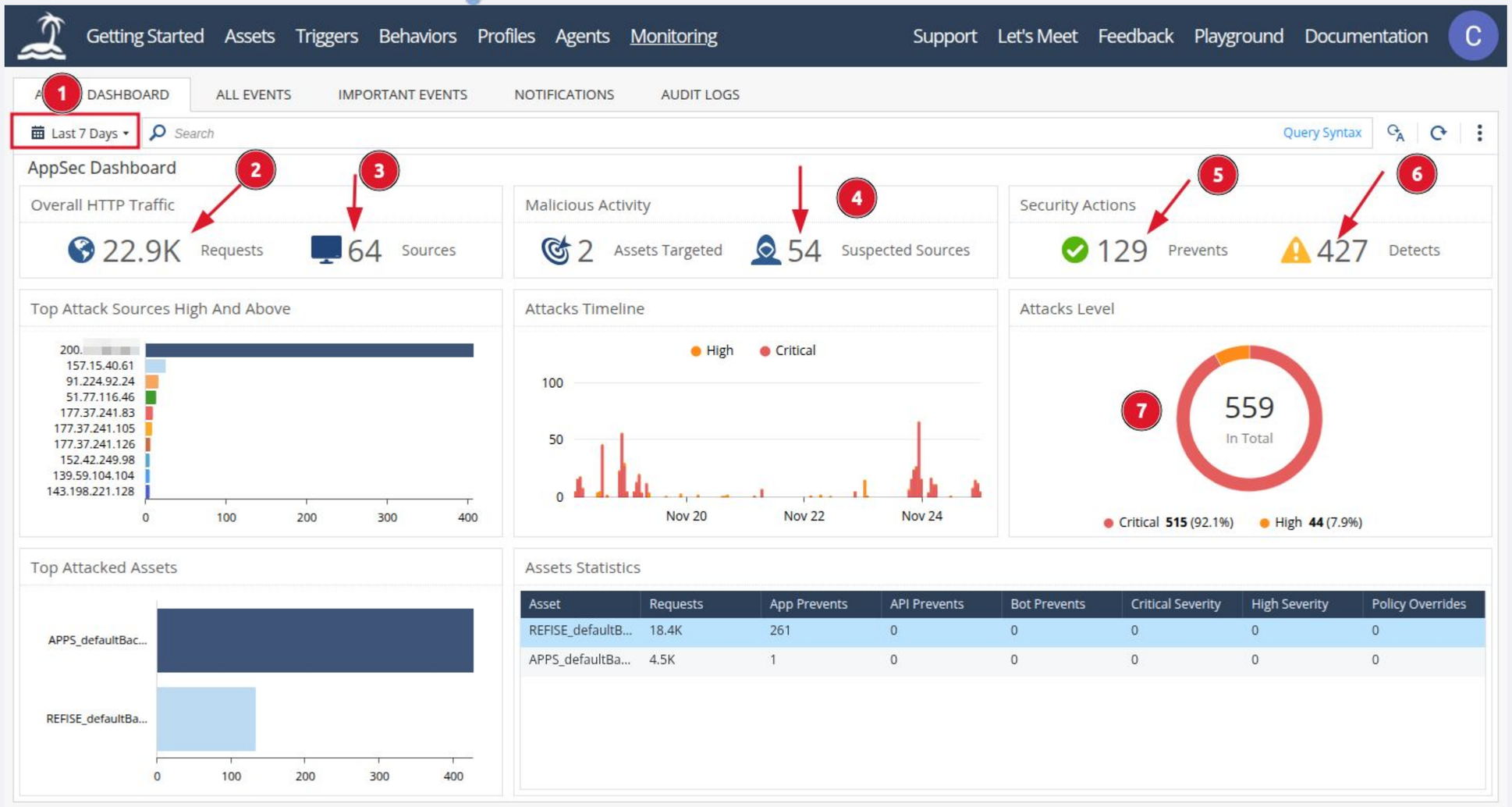
31/10/25 às 13:43 | Atualizado 31/10/25 às 13:43

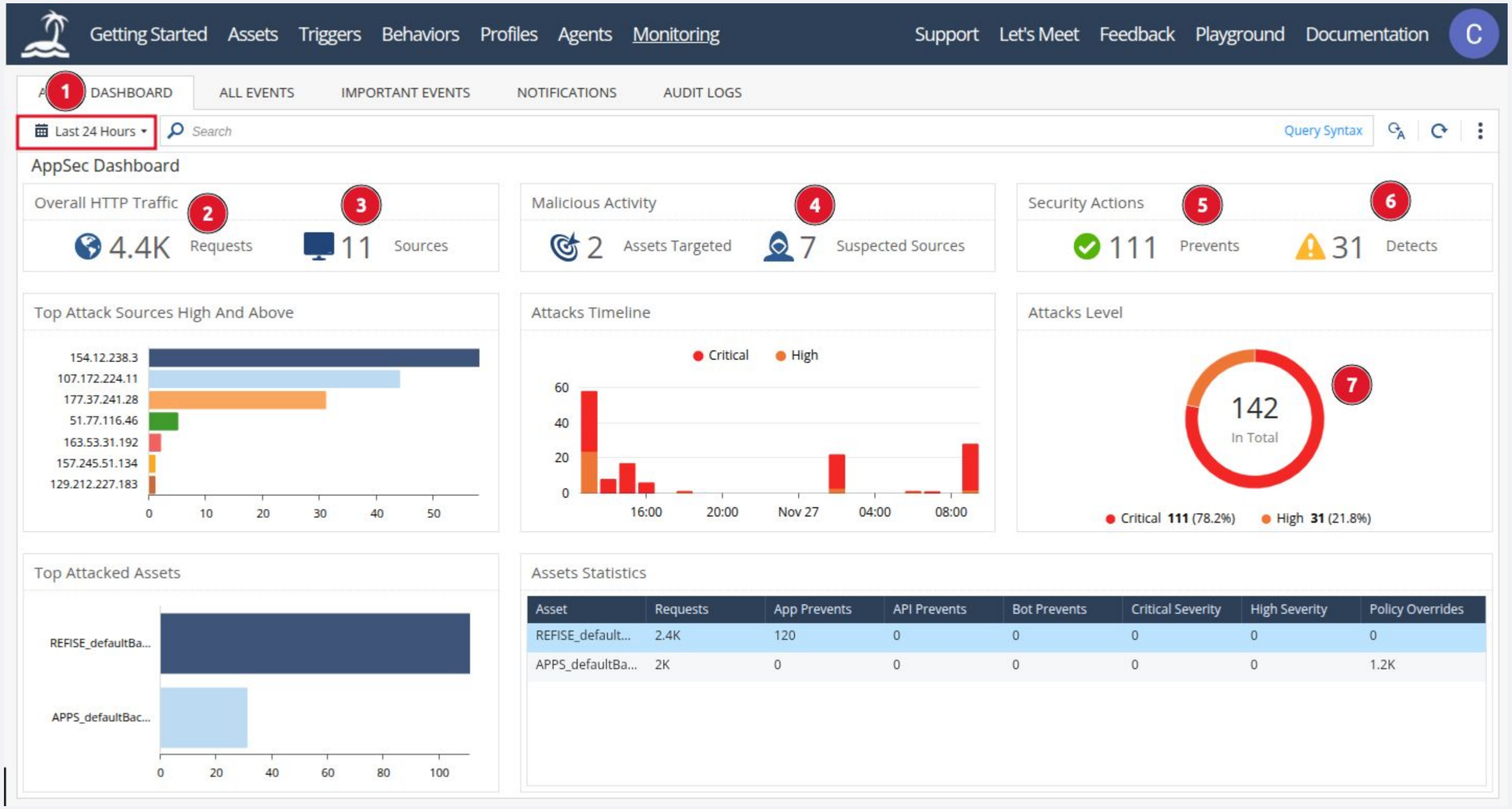
Hacking group claims to have cracked NASA drone

Um grupo de hackers disse que assumiu o controle de um drone da NASA e roubou dados de seu sistema, mas a agência espacial nega as alegações.

Em 31 de janeiro, o grupo de hackers AnonSec publicou cerca de 250 GB de dados e um "zine" de 300 páginas detalhando sua suposta exploração de sistemas da NASA por meses e sua tentativa de lançar um drone multimilionário Global Hawk no Oceano Pacífico.

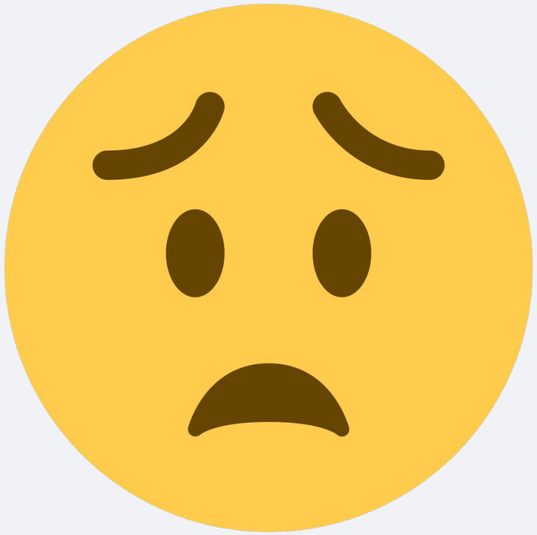
"Vários membros discordaram sobre isso porque, se funcionasse, seríamos rotulados de terroristas por possivelmente derrubar um drone americano de US$ 222,7 milhões", escreveram os hackers. "Mas continuamos mesmo assim."


Getting Started
Assets
Triggers
Behaviors
Profiles
Agents
Monitoring
Support
Let's Meet
Feedback
Playground
Documentation
C
DASHBOARD
ALL EVENTS
IMPORTANT EVENTS
NOTIFICATIONS
AUDIT LOGS
1
Last 7 Days
Search
Query Syntax
AppSec Dashboard
2
3
4
5
6
Overall HTTP Traffic
22.9K Requests
64 Sources
Malicious Activity
2 Assets Targeted
54 Suspected Sources
Security Actions
129 Prevents
427 Detects
Top Attack Sources High And Above
200.
157.15.40.61
91.224.92.24
51.77.116.46
177.37.241.83
177.37.241.105
177.37.241.126
152.42.249.98
139.59.104.104
143.198.221.128
0
100
200
300
400
Attacks Timeline
High
Critical
100
50
0
Nov 20
Nov 22
Nov 24
Attacks Level
7
559
In Total
Critical 515 (92.1%)
High 44 (7.9%)
Top Attacked Assets
APPS_defaultBac...
REFISE_defaultBa...
0
100
200
300
400
Assets Statistics
Asset
Requests
App Prevents
API Prevents
Bot Prevents
Critical Severity
High Severity
Policy Overrides
REFISE_defaultB...
18.4K
261
0
0
0
0
0
APPS_defaultBa...
4.5K
1
0
0
0
0
0

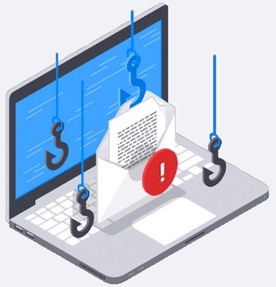

Getting Started
Assets
Triggers
Behaviors
Profiles
Agents
Monitoring
Support
Let's Meet
Feedback
Playground
Documentation
C
1
DASHBOARD
ALL EVENTS
IMPORTANT EVENTS
NOTIFICATIONS
AUDIT LOGS
Last 24 Hours
Search
Query Syntax
AppSec Dashboard
Overall HTTP Traffic
2
3
4.4K
Requests
11
Sources
Malicious Activity
4
2
Assets Targeted
7
Suspected Sources
Security Actions
5
6
111
Prevents
31
Detects
Top Attack Sources High And Above
154.12.238.3
107.172.224.11
177.37.241.28
51.77.116.46
163.53.31.192
157.245.51.134
129.212.227.183
0
10
20
30
40
50
Attacks Timeline
Critical
High
60
40
20
0
16:00
20:00
Nov 27
04:00
08:00
Attacks Level
7
142
In Total
Critical 111 (78.2%)
High 31 (21.8%)
Top Attacked Assets
REFISE_defaultBa...
APPS_defaultBac...
0
20
40
60
80
100
Assets Statistics
Asset
Requests
App Prevents
API Prevents
Bot Prevents
Critical Severity
High Severity
Policy Overrides
REFISE_default...
2.4K
120
0
0
0
0
0
APPS_defaultBa...
2K
0
0
0
0
0
1.2K

Phishing e Senhas

O ser humano como vetor de ataque



Phishing e Senhas

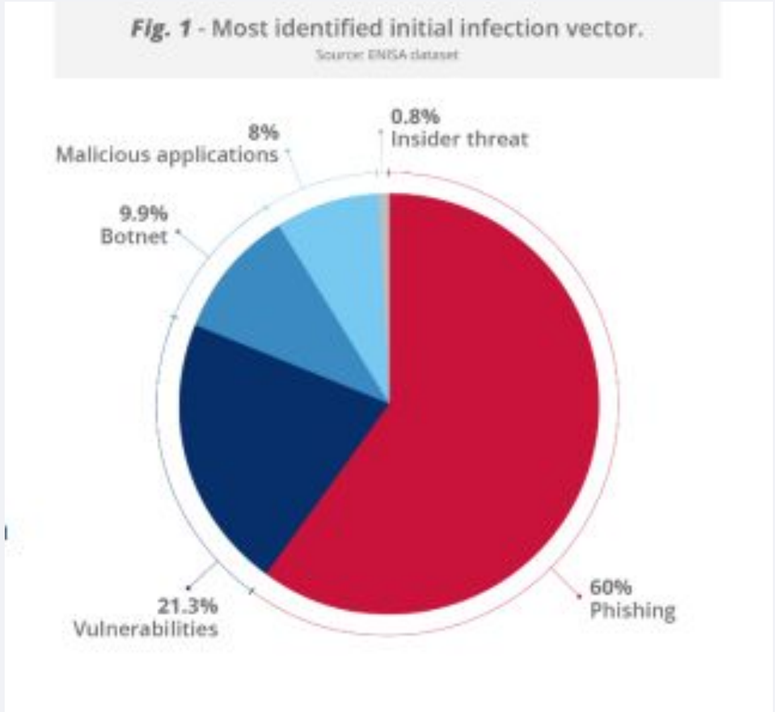


- Phishing ainda é o vetor de ataque dominante (60%);
- 80% das campanhas de engenharia social usaram IA;

Dados retirados do ENISA Threat Landscape Report 2025.

Disponível em:

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025



Phishing e Senhas
Boas Práticas

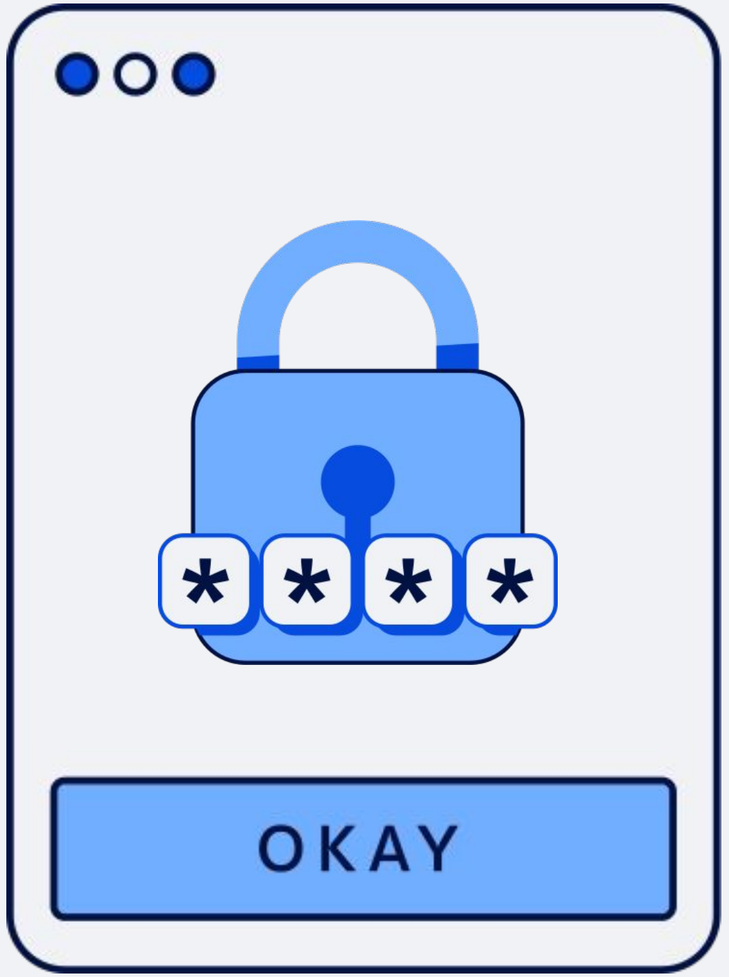
Phishing:

- Clicar em Links suspeitos, cai fora dessa!
  - Ponha o ponteiro do mouse sobre o link e veja o destino do link na parte inferior do navegador;
  - Se o link for encurtado, copie o link, cole na barra de navegação e acrescente o caractere “+” na frente do link para verificar o destino;
  - Desconfie e verifique!

Phishing e Senhas
Boas Práticas

Senhas:

- Use senhas longas e contendo caracteres especiais;
- Compartilhar senhas pode lhe trazer sérios problemas;
- Usar a mesma senha em diferentes sites/serviços ajuda o criminoso;
- Use um gerenciador de senhas;
- Use um segundo fator de autenticação!



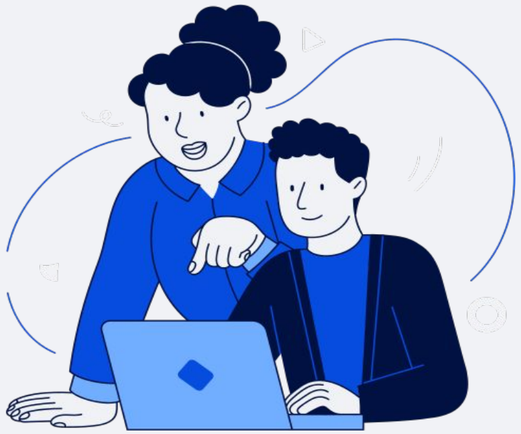
Carreiras em CyberSec

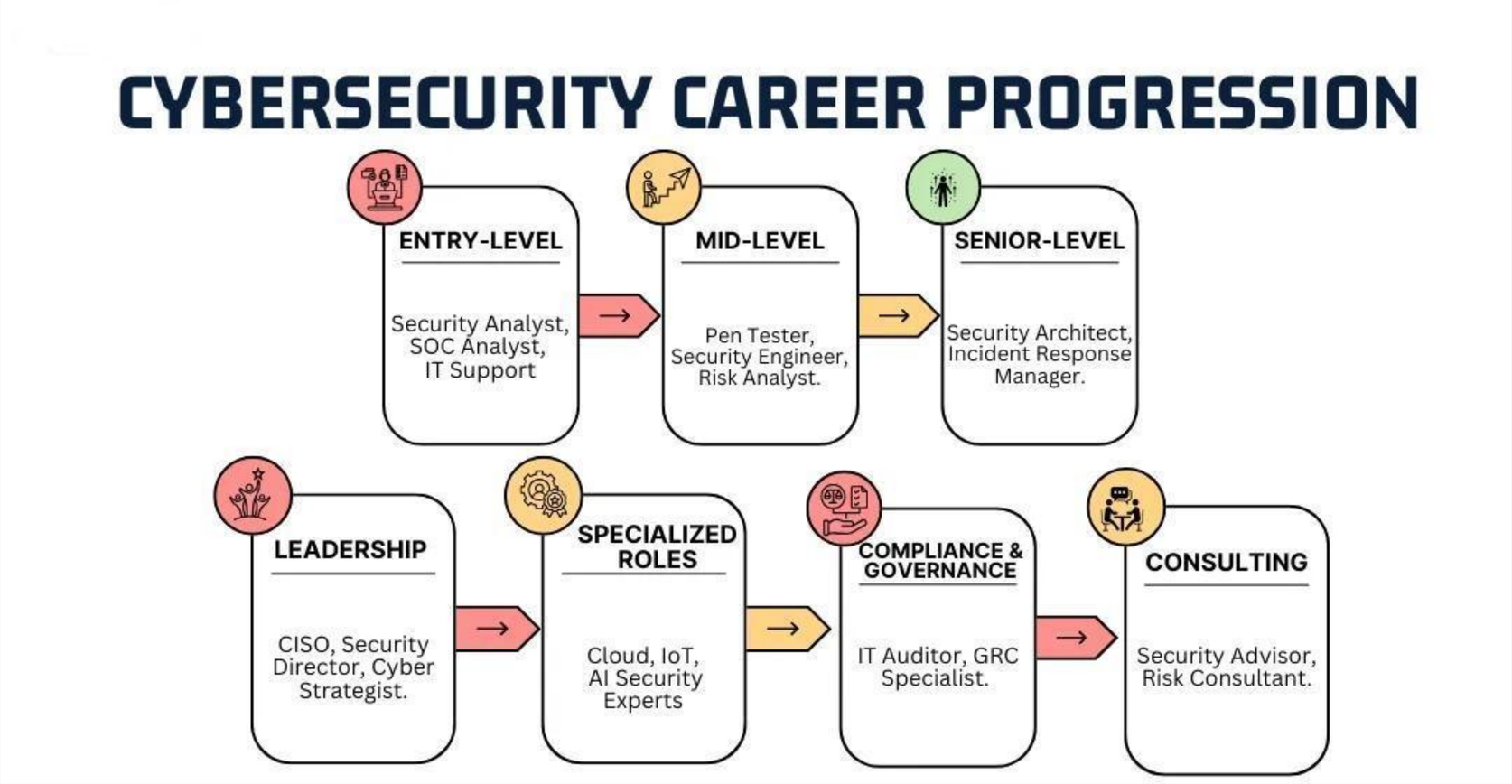
- **Segurança Defensiva**
  - **Impedir que intrusões ocorram;**
  - **Detectar intrusões quando elas ocorrem e responder adequadamente.**
- **Segurança Ofensiva**
  - **Simulações de ataques;**
  - **Identificações de vulnerabilidades;**
  - **Correção e fortalecimento;**
  - **Melhoria contínua.**

Carreiras em CyberSec

- **Governança, Risco e Conformidade (GRC)**
  - **Alinhamento da segurança com os objetivos do negócio;**
  - **Gestão de Riscos Cibernéticos;**
  - **Garantir a conformidade com a legislação e os órgãos reguladores.**

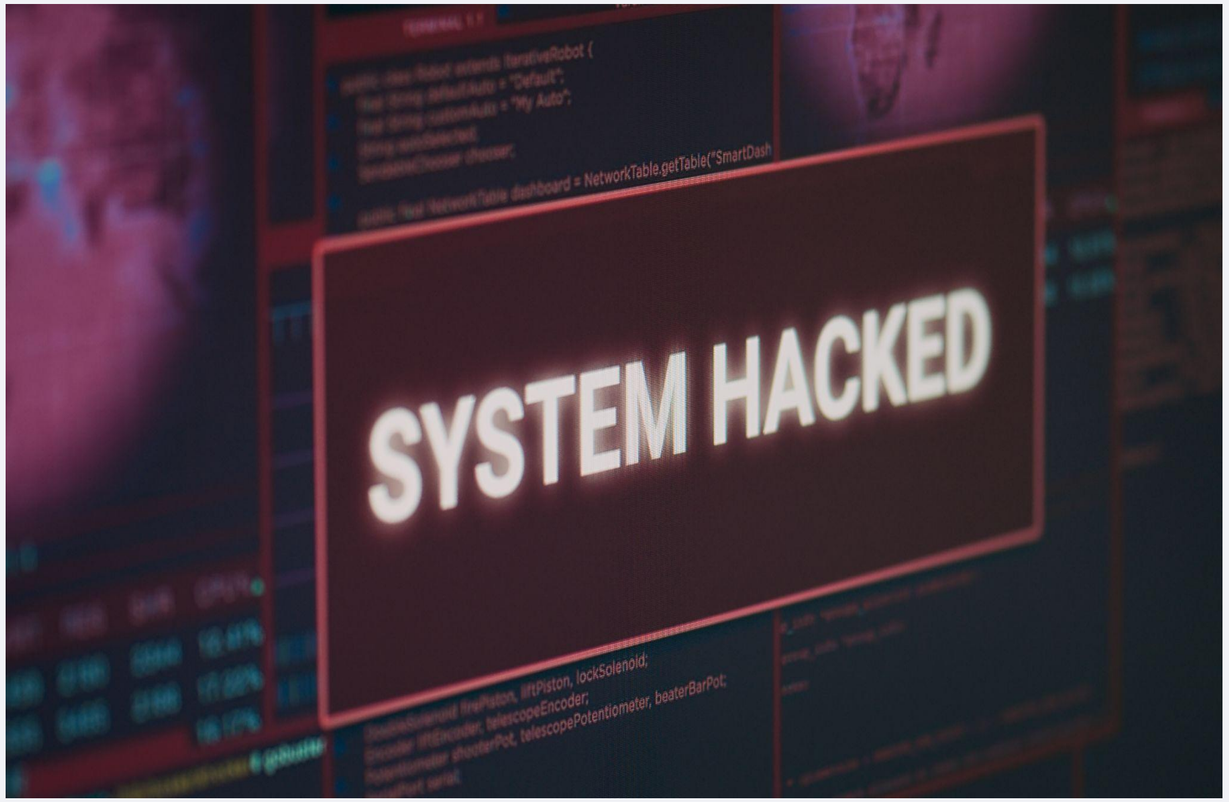
Carreiras em CyberSec

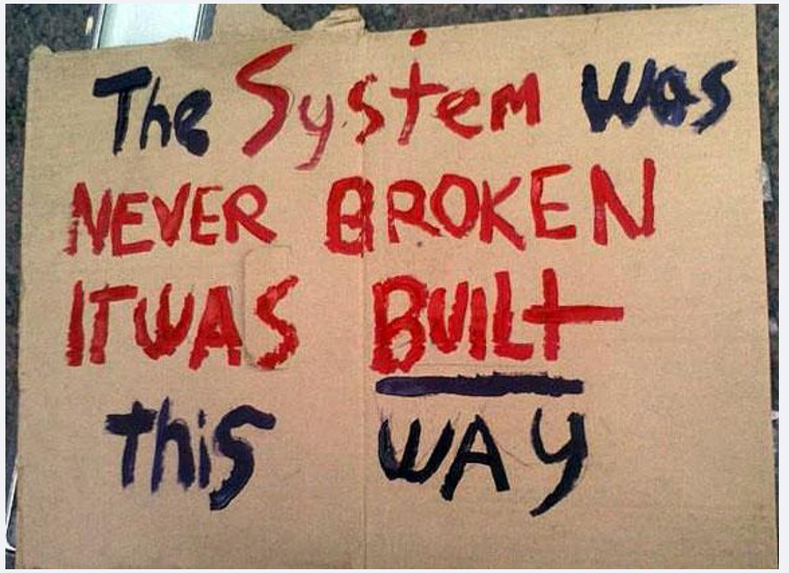




Vulnerabilidades em Software

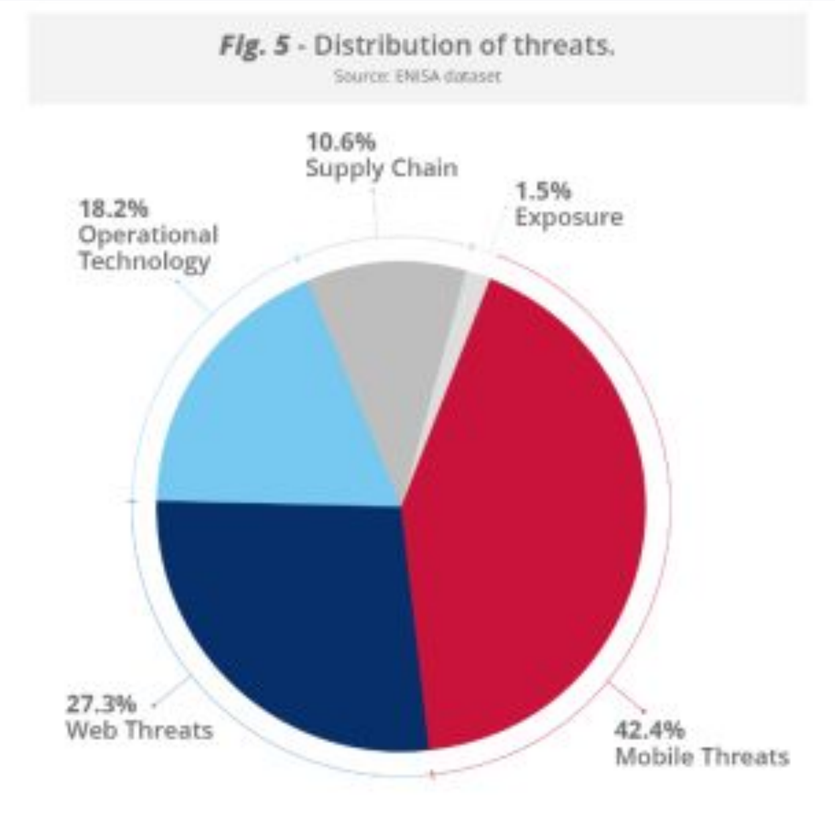
Sistemas como vetor de ataque

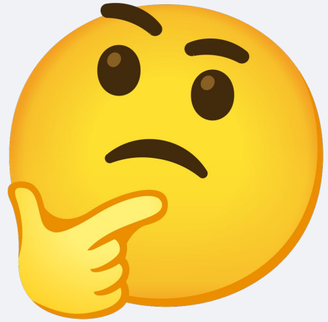




Vulnerabilidades em Software

Sistemas como vetor de ataque





O que os desenvolvedores de software podem fazer a respeito?

Como tornar os softwares mais seguros?

- Segurança desde a concepção

  Consiste em criar produtos, serviços e sistemas usando práticas seguras desde os estágios iniciais até a implantação final. (Checkpoint).

Como tornar os softwares mais seguros?

- Secure by design - Princípios:

1. **Modelagem de ameças**

   Identificar ameaças cibernéticas no início do desenvolvimento, permitindo que os desenvolvedores corrijam os problemas de forma proativa.

2. **Shifting left security**

   A integração da segurança no início do SDLC. Garante que a segurança seja um aspecto fundamental do desenvolvimento de software. Dois modelos que formalizam essa prática são o Secure SDLC e o DevSecOps.

Como tornar os softwares mais seguros?

- Secure by design - Princípios:

3. **Proteção de dados**

   Proteger os dados durante todo o ciclo de vida e impedir o acesso não autorizado, criptografar dados em repouso e em trânsito e implementar controles de acesso rígidos para restringir as permissões.

4. **Segurança como código (SaC)**

   O SaC envolve a automação de verificações e testes de segurança no processo de desenvolvimento. Dessa forma, as possíveis vulnerabilidades no código são identificadas antecipadamente e corrigidas antes da implantação em produção.

Como tornar os softwares mais seguros?

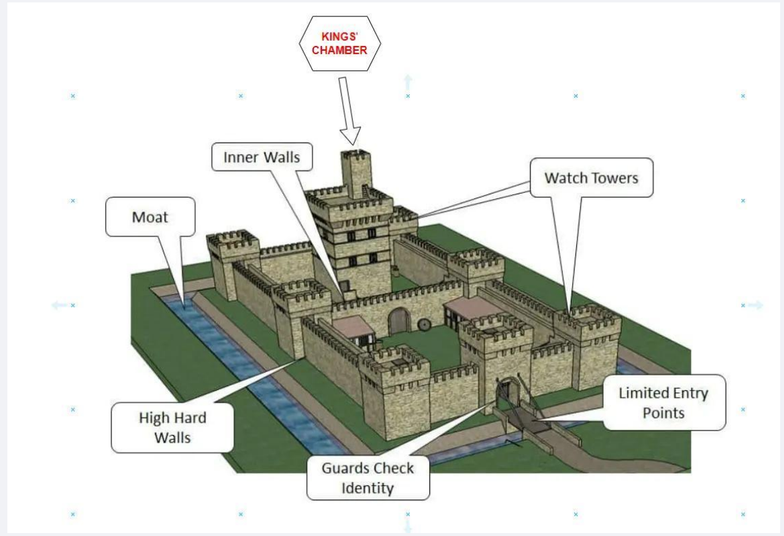
- Secure by design - Princípios:

5. Práticas de codificação segura

Os fundamentos da codificação segura incluem validação de entrada, codificação de saída, tratamento de erros, gerenciamento de exceções e uso de criptografia para proteger as comunicações.

6. Defesa em profundidade

Também conhecida como segurança em camadas, a prática de implementar sistemas e procedimentos defensivos sobrepostos aprimora a postura geral de segurança, reduzindo a probabilidade de comprometimento.



Como tornar os softwares mais seguros?

- Secure by design - Princípios:

7. **Configuração segura**

   As organizações reduzem ainda mais os riscos adotando configurações seguras padronizadas, aplicando políticas rígidas de controle de acesso e implementando um plano de gerenciamento de *patches* para regular as atualizações oportunas.

8. **Privilégio mínimo**

   O princípio do privilégio mínimo (PoLP) exige que os usuários e aplicativos recebam apenas as permissões mínimas necessárias para realizar suas tarefas. A adesão a essa prática reduz a superfície de ataque e minimiza possíveis danos em caso de comprometimento.

Como tornar os softwares mais seguros?

- Secure by default

Significa que os *softwares* são resilientes contra técnicas de exploração predominantes, sem custo adicional. O software deve iniciar em um estado seguro sem exigir uma configuração extensa do usuário, garantindo que as configurações padrão sejam sempre a opção mais segura. (OWASP Developer Guide).

Como tornar os softwares mais seguros?

Open Worldwide Application Security Project (OWASP)

É uma fundação sem fins lucrativos que trabalha para melhorar a segurança de software.

- **Recursos importantes:**

  - OWASP Developer Guide
  - OWASP Top Ten

Como tornar os softwares mais seguros?

OWASP Top Ten

- É uma lista que identifica as ameaças mais importantes para aplicações web e busca ranqueá-las em importância e severidade.

- Última lista foi publicada em 2021

- Deve ser usado como ponto de partida

Como tornar os softwares mais seguros?

OWASP Top Ten 2021

A01:2021 Broken Access Control

A02:2021 Cryptographic Failures

A03:2021 Injection

A04:2021 Insecure Design

A05:2021 Security Misconfiguration

A06:2021 Vulnerable and Outdated Components

A07:2021 Identification and Authentication Failures

A08:2021 Software and Data Integrity Failures

A09:2021 Security Logging and Monitoring Failures

A10:2021 Server-Side Request Forgery

Como tornar os softwares mais seguros?

OWASP Top Ten 2025

A01 Broken Access Control

A02 Security Misconfiguration

A03 Software Supply Chain Failures

A04 Cryptographic Failures

A05 Injection

A06 Insecure Design

A07 Authentication Failures

A08 Software or Data Integrity Failures

A09 Logging and Alerting Failures

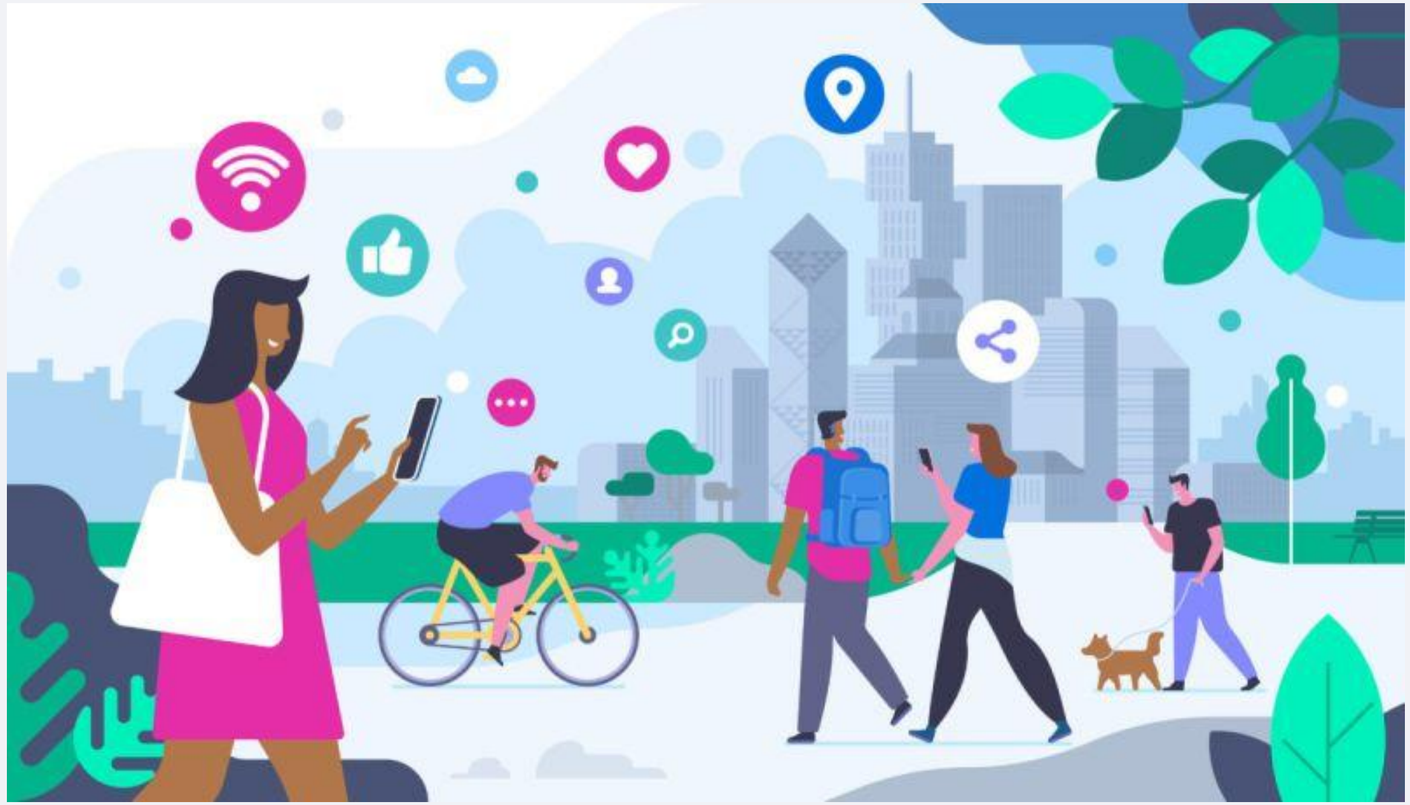
A10 Mishandling of Exceptional Conditions

Como tornar os softwares mais seguros?

Outro OWASP Top Ten

- API Security Top 10
- Citizen Development Top 10
- Data Security Top 10
- Mobile Top 10
- Serverless Top 10
- Top 10 CI/CD Security Risks
- Top 10 for Large Language Model Applications
- Top 10 Privacy Risks
- Top 10 Proactive Controls
- Top 10 Web Application Security Risks

Todos nós podemos contribuir para um mundo digital mais seguro!



Obrigado!

linkedin.com/in/mariojsantos

github.com/mariojsantos