


SEMAC 2025

Oportunidades e Desafios na **Cibersegurança**

Msc. Juliano Nóbrega

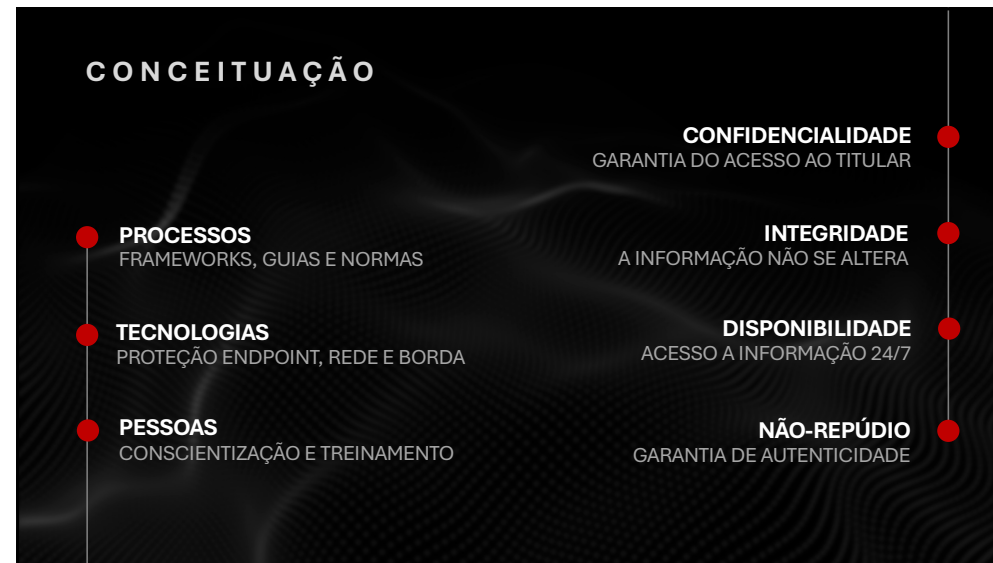
unesp 

1

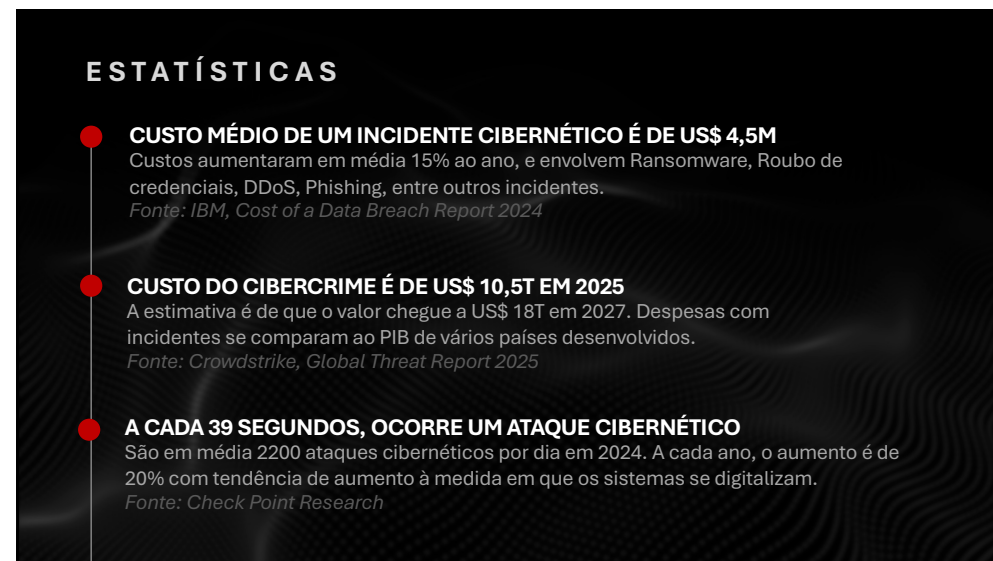
PROGRAMA

- **CONCEITUAÇÃO E ESTATÍSTICAS**
Dados importantes sobre o atual cenário global
- **CONTEXTO**
Informações sobre atuais demandas e
- **DESAFIOS**
Custos aumentaram em média 15% ao ano, e envolvem Ransomware, Roubo de
- **OPORTUNIDADES**
Custos aumentaram em média 15% ao ano, e envolvem Ransomware, Roubo de
- **CONCLUSÃO**
Custos aumentaram em média 15% ao ano, e envolvem Ransomware, Roubo de

2



3



4

ESTATÍSTICAS

● ESTÃO CATALOGADOS 280 GRUPOS CIBERCRIMINOSOS

A plataforma Ransomware.live cataloga os principais grupos de cibercrime. Destacam-se os grupos qilin (Russia) e Akira (Russia) no modelo RaaS
Fonte: Ransomware.live

● EM 2024 FORAM CATALOGADAS ~40K VULNERABILIDADES

A plataforma CVE (Common Vulnerabilities and Exposures) é responsável pelo registro de vulnerabilidades encontradas em hardwares e softwares.
Fonte: Portal CVE (cve.org)

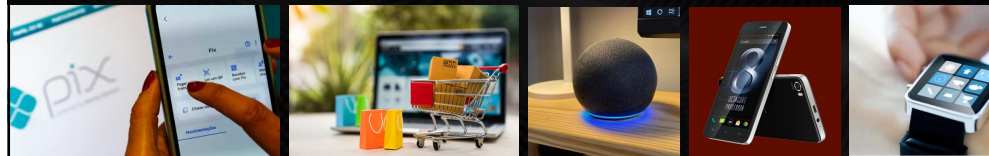
● EMPRESAS DE TECNOLOGIA PASSARAM A SER O ALVO (23%)

Seguidas por Consultoria (15%), manufatura (12%), serviços financeiros (10%), saúde (9%) e telecomunicação (7%), governo (6%), indústrias (4%) e acadêmico (3%).
Fonte: Crowdstrike, Global Threat Report 2025

5

CONTEXTO

AMPLIAÇÃO DA SUPERFÍCIE DE ATAQUE SEGUE A DIGITALIZAÇÃO DE SERVIÇOS



6

CONTEXTO

AMPLIAÇÃO DA SUPERFÍCIE DE ATAQUE

Conexões entre IoT, Mobiles, Hosts e Periféricos, assim como a migração massiva para ambientes cloud e home office não possuem camadas suficientes para garantir a confidencialidade, integridade e disponibilidade dos dados, aliado a falta de conscientização e investimento das empresas.

ESCASSEZ DE PROFISSIONAIS QUALIFICADOS

Estimativas apontam déficit global de 4 milhões de profissionais com competência para mitigar incidentes e implementar as medidas adequadas para empresas e projetos.

Fonte: ISC²

7

CONTEXTO

AUMENTO DA QUANTIDADE E QUALIDADE DOS ATAQUES

Ocorrências envolvem Ransomwares 3.0 (sequestro, extorsão e exploração de todo o ecossistema conectado) mais sofisticados para contornar defesas. Uso de Vishing e Phishing direcionados exploram melhor as vulnerabilidades humanas. (Exemplo do ataque de deepfake em Hong Kong, 2024)

ATAQUES NÃO POSSUEM BARREIRAS GEOGRÁFICAS

Qualquer serviço exposto na internet passa a ser um alvo de grupos criminosos em qualquer local do planeta. Plataformas como a Kaspersky Live apontam altos volumes de ataques com origem na Rússia, Ucrânia, EUA e China.

Fonte: <https://cybermap.kaspersky.com/pt>

8



9

INCIDENTES NO SISTEMA FINANCEIRO NACIONAL

- ATAQUE HACKER A BANCO CENTRAL DESVIA R\$ 1B**
 Vazamento de credenciais válidas permitiram o acesso ao ambiente de produção de Fintech responsável pela gestão de Pix (C&M Software) entre BC e outros bancos.
JULHO/2025
- ATAQUE HACKER A FINTECH SINQIA DESVIA R\$ 710M**
 Banco HSBC foi atacado por meio de vulnerabilidades na plataforma da Sinqia, Fintech responsável pela comunicação do Banco com o BC
AGOSTO/2025
- SISTEMA DE TED RECEBE ATAQUE COM PREJUÍZO DE R\$ 5M**
 Fintech envolvida (Monbank) sofreu ataque no ambiente de transferências via TED e PIX.
SETEMBRO/2025

10

CONTEXTO



Roubo ao BC (2025)
Prejuízo de R\$900M



Reunião fake em empresa de Hong Kong
Prejuízo de US\$ 25M

11

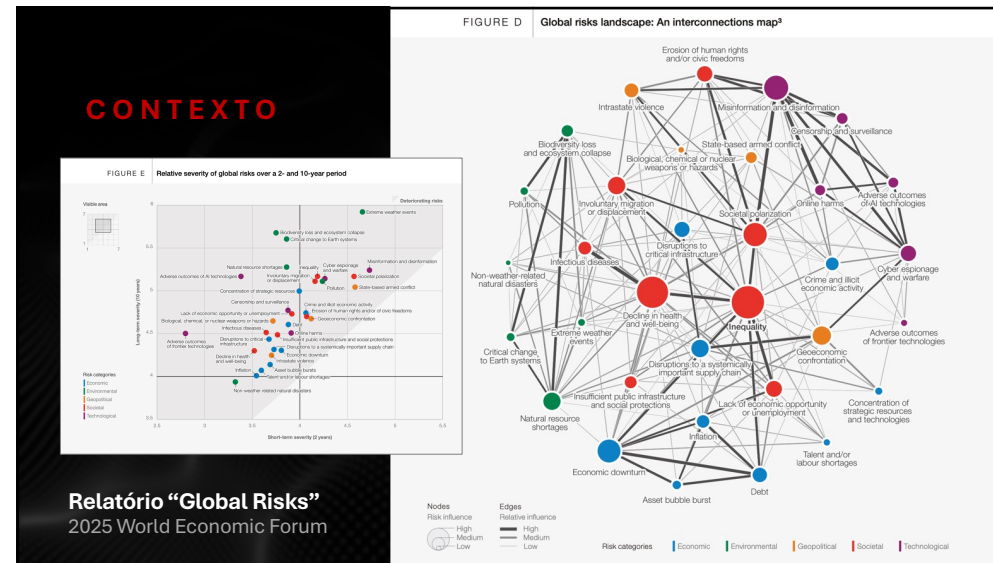
CONTEXTO

CIBERSEGURANÇA PASSA A SER ESTRATÉGICO

Estimativas apontam déficit global de 4 milhões de profissionais com competência para mitigar incidentes e implementar as medidas adequadas para empresas e projetos.

Fonte: Relatório do Fórum Econômico Mundial (WeForum 2025)

12



13



14

DESAFIOS

USO DA IA

A Inteligência Artificial está impulsionando os ataques cibernéticos por meio da geração de textos, imagens, vídeos e conteúdos utilizados em Engenharia Social direcionada. Uso de deepfake dificulta detecções das ameaças.

MONITORAMENTO INADEQUADO

A falta (ou dificuldade) de monitoramento é responsável pelo gap temporal entre detecção e evolução (movimento lateral) do atacante na rede. As ferramentas de SOC, NOC e Endpoint Protection estão em constante atualização e atuam em ambientes híbridos/multicloud.

15

DESAFIOS

ABUSO DE DNS

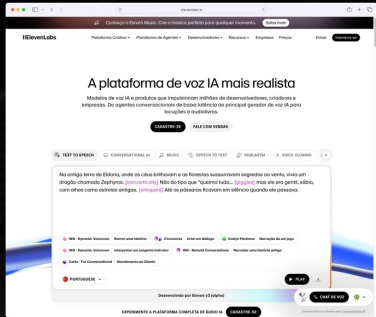
Explorar o próprio funcionamento da internet para gerar páginas e e-mails fraudulentos é o primeiro passo para um ataque cibernético. Classificar como malicioso um novo domínio é fundamental para mitigar ameaças.

GESTÃO DE IDENTIDADES

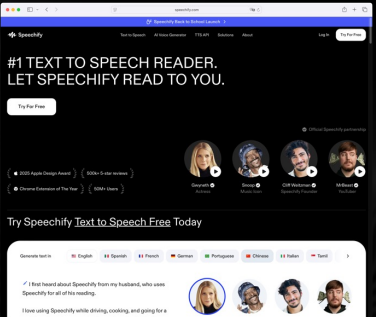
O roubo (ou vazamento) de credenciais é o vetor no. 1 em ataques cibernéticos (OWASP TOP10) . Implementar cultura Zero-Trust é a forma adequada para mitigação deste risco.

16

DESAFIOS



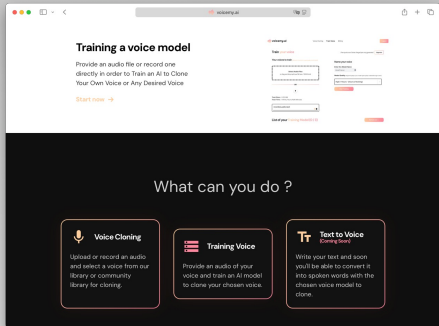
Clonador de Voz
elevenlabs.io



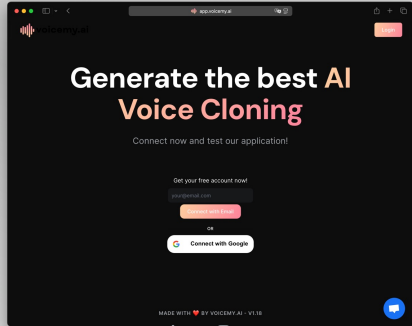
Clonador de Voz
speechify.com

17

DESAFIOS

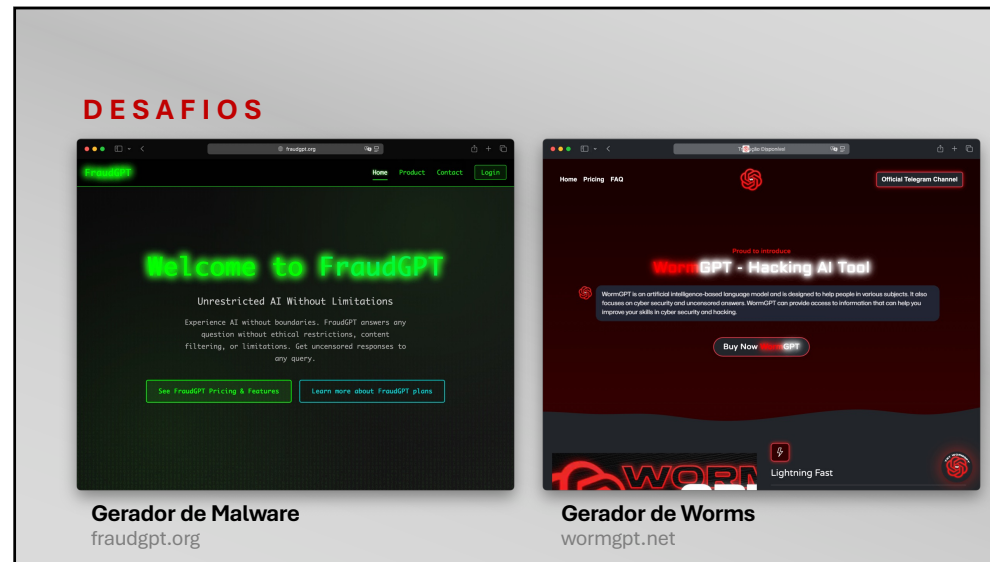


Clonador de Voz
voicemy.ai

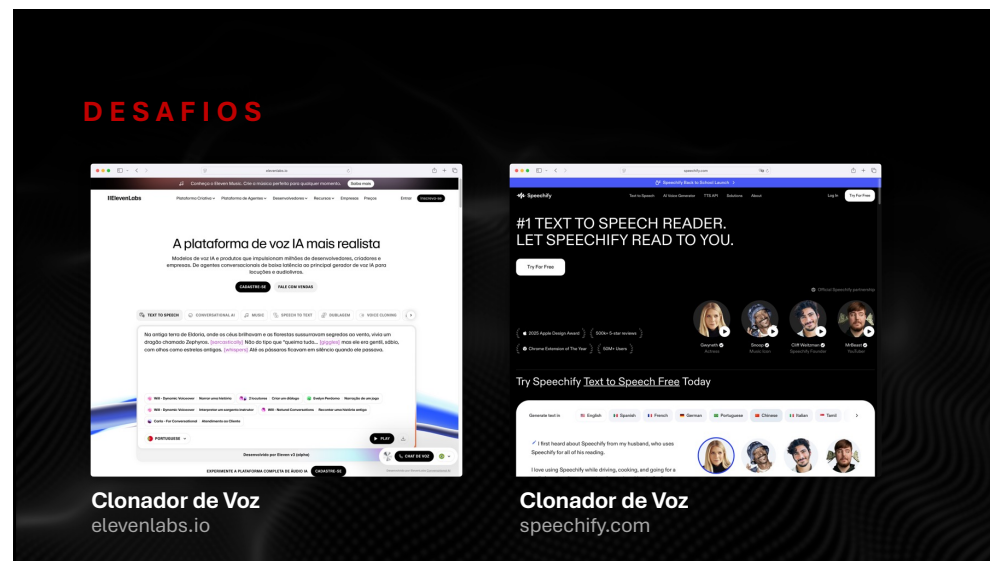


Clonador de Voz
app.voicemy.ai

18



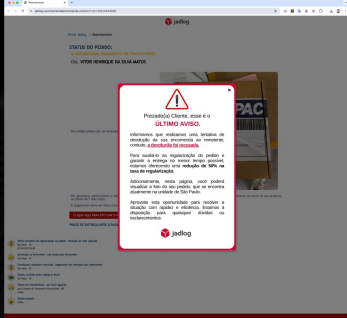
19



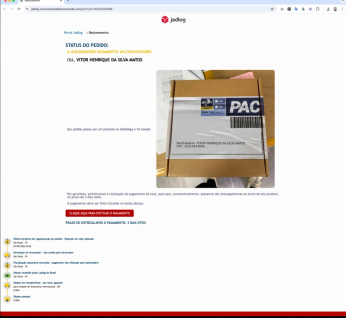
20

DESAFIOS

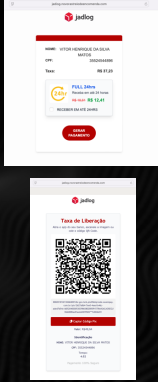
jadiog.novorastreiodeencomenda.com



Vazamento JadLog (SET/2025)




JadLog: Golpe da entrega PAC




21

DESAFIOS



Geopolítica
Presidente da Ucrânia se rendendo

A deepfake video of Volodymyr Zelenskyy surrendering to Russia.
(Source - The Daily Show with Trevor Noah)



Geopolítica
Influência em eleições presidenciais nos EUA

FAKE BIDEN ROBOCALL TELLS NH DEMOCRATS NOT TO VOTE ON TUESDAY
FAKE AUDIO
[ROBOCALL] We'll need your help in electing Democrats up and down the ticket. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again.

Deepfakes like the Biden robocall are a threat — even to those who don't fall for it.
(Source - MSNBC)

22

TENDÊNCIAS



23

TENDÊNCIAS

ATAQUES FILELESS

Ataques sofisticados sem uso de arquivos são ameaças que operam na memória do sistema, executando ações maliciosas, e são difíceis de serem detectadas por ferramentas de proteção de *endpoints*.

PERSONIFICAÇÃO VIA IA

Ataques de phishing altamente sofisticados, simulando vídeo, voz e imagens de pessoas. Usuários passam a ficar “acomodados” no processo de digitalização dos processos e tecnologias.

24

TENDÊNCIAS

USO DE CRIPTOGRAFIA PÓS-QUÂNTICA

De acordo com o NIST, existe a tendência de que computadores quânticos explorem criptografias RSA (Rivest-Shamir-Adleman) e ECC (Elliptic Curve Cryptography), e dê espaço a modelos PQC (Post Quantum Cryptography). O governo dos EUA já emitiu um memorando obrigando o uso dessa tecnologia.



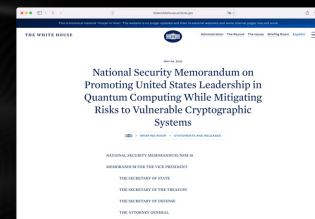
<https://bidenwhitehouse.archives.gov>

25

DESAFIOS

DIA A DIA DO SOC

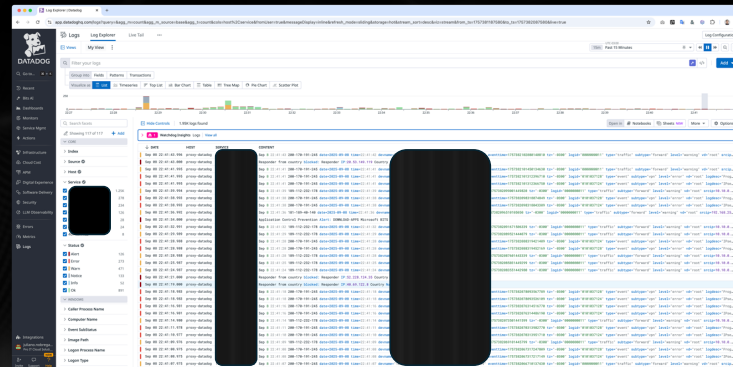
O SOC (Security Operations Center) faz o monitoramento, detecção, análise e resposta a incidentes cibernéticos 24/7. Adoção da ferramenta SIEM (Security Information and Event Management) para gerenciamento de Logs da infraestrutura do cliente.



<https://bidenwhitehouse.archives.gov>

26

DESAFIOS - SOC



Ingestão de Logs pelo SIEM

27

OPORTUNIDADES



28

OPORTUNIDADES

CERTIFICAÇÕES

São fundamentais em um processo seletivo. Exames como Security+ ou Cysa+ (ComptIA) são os iniciais na carreira. Outras certificações de fabricantes como CrowdStrike, Fortinet, Cisco, entre outras também é desejável.

ATUAÇÃO

Atuação como Red Team (Exploração, PenTest, BugBounty) ou Blue Team (SOC, Conscientização, Reports e Defesa) são os grupos de segurança que trabalham em conjunto. Analistas e engenheiros de cibersegurança também são valorizados.

29

OPORTUNIDADES

VAGAS

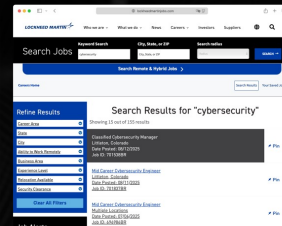
Oportunidades em empresas brasileiras e estrangeiras são possíveis por meio de Home-Office ou de forma presencial em grandes centros (capitais).

PERFIL

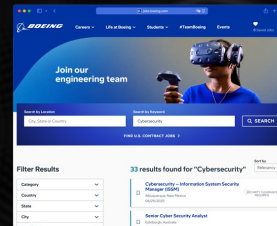
Profissionais com perfil investigativo, inglês avançado, domínio das ferramentas de segurança, programação, matemática e redes tem grande potencial para vagas.

30

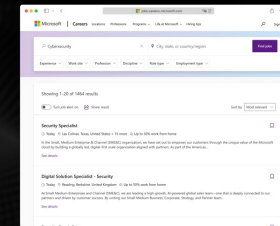
OPENING JOBS



LOCKHEED MARTIN (EUA)
155 Open Jobs
US\$ 130k – 220k/year



BOEING (EUA)
33 Open Jobs
US\$ 115k – 150k/year



MICROSOFT (EUA)
1464 Open Jobs
US\$ 40 – 80/hour

31

CONCLUSÃO

DESAFIOS

A cibersegurança está repleta de desafios que envolvem técnicas para mitigação de incidentes e proteção de infraestruturas de todos os perfis e tamanhos.

FORTE REDE DE CONHECIMENTO


Plataformas de conhecimento (TryHackMe, Let's Defend, Hack The Box), assim como inúmeras bases de conhecimento e guias (NIST CSF, CIS 18 Controls, Mitre Att&CK, CVE, CWE, aliada aos grandes relatórios anuais das empresas de segurança (Cloudflare, Palo Alto, CrowdStrike, Microsoft, etc.) entre outras garantem muito conteúdo de alto nível para interessados em atuar na área.

32

Q & A

QUESTIONS & ANSWERS

CONTATO
Juliano.nobrega@proitcs.com.br



The QR code is a standard black and white matrix code. In the bottom right corner, there is a small logo for 'TQRCG' with the text 'TQRCG' next to it.

33