
FORTINET
LINUXTIPS

$whoami

Henrique Falcão Moisés

Nerd e gamer nas horas vagas, trabalha como Arquiteto de Segurança para Ambientes de Nuvem há 2 anos na Fortinet.

Há mais de 7 anos atuando no mercado de Segurança da Informação, e em empresas de diferentes segmentos, do âmbito financeiro, telecomunicações, consultoria de segurança, e fabricantes de tecnologias para auxiliar na adoção de Segurança da Informação.

$whoami

Vanderson Santos

Gosto muito de animes e games nas horas vagas ajudo com mentoria e currículos, atualmente trabalho como Arquiteto de Segurança para Ambientes de Nuvem há 1 ano na Fortinet.

Atuando com Segurança da informação a 7 anos e com Tecnologia a 17 anos ao todo, atuando em empresas do setor de logistica, instituições financeiras, Telecomunicações e varejo, buscando sempre apoiar e implementar as melhores práticas de segurança da informação.


START

O que é Cibersegurança ou Segurança Cibernética?

É a prática de proteger computadores, redes, aplicações, sistemas essenciais e dados de possíveis ameaças digitais

Confiança do Cliente

Disponibilidade

Seguimento de Regulamentações

Controles do Dia-a-Dia

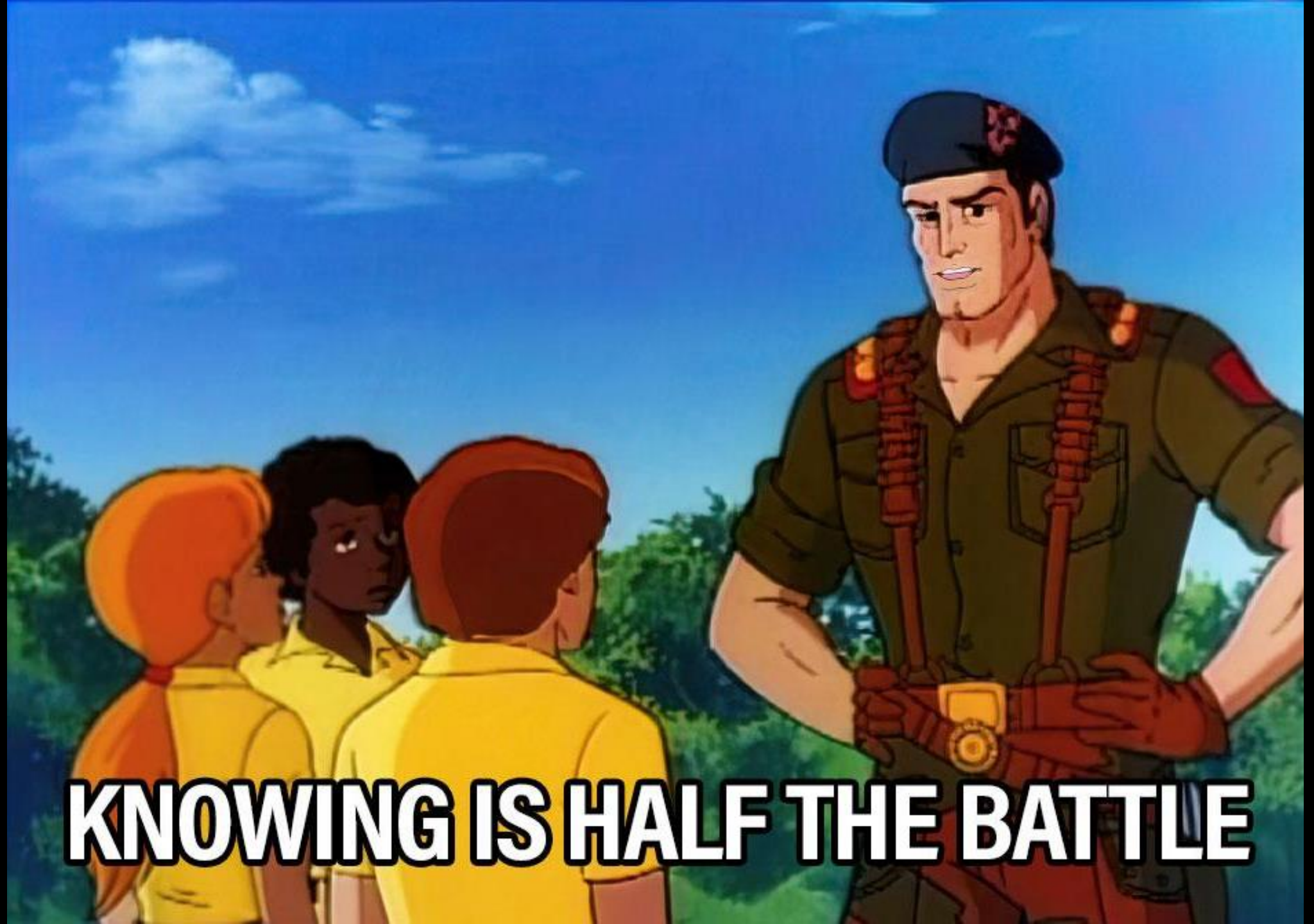
Duplo Fator de Autenticação

Trancar as Portas

Backup de Fotos

Lock-Picking

Então Chaveiros são Hackers???


KNOWING IS HALF THE BATTLE

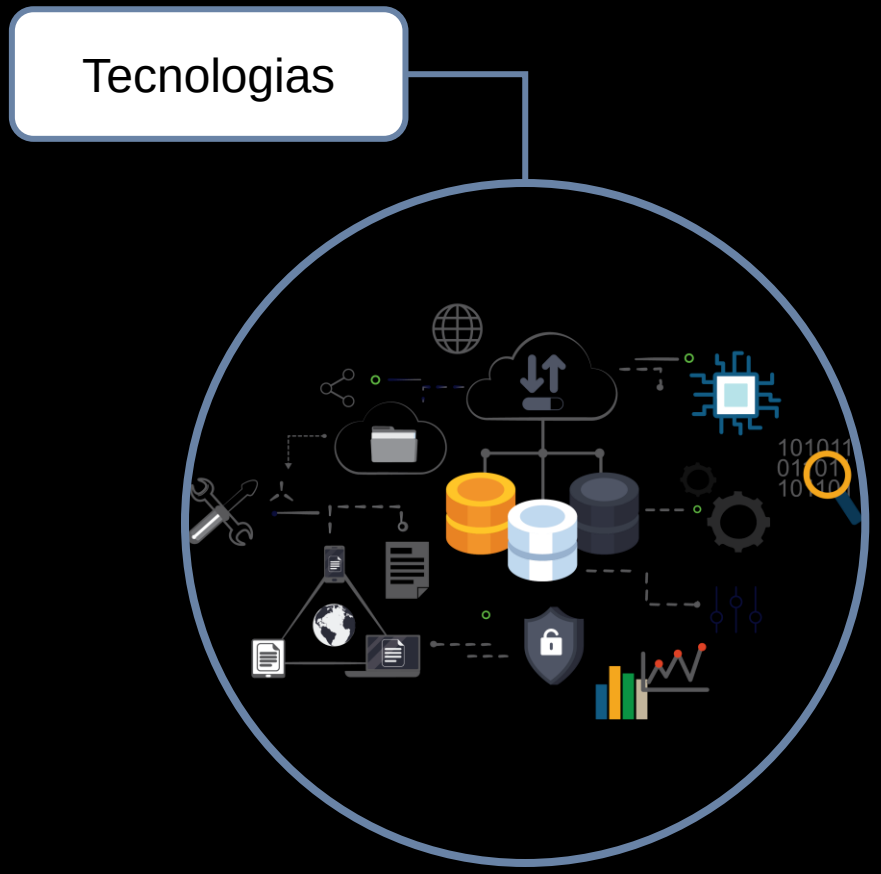
A Base da Cibersegurança

Pessoas

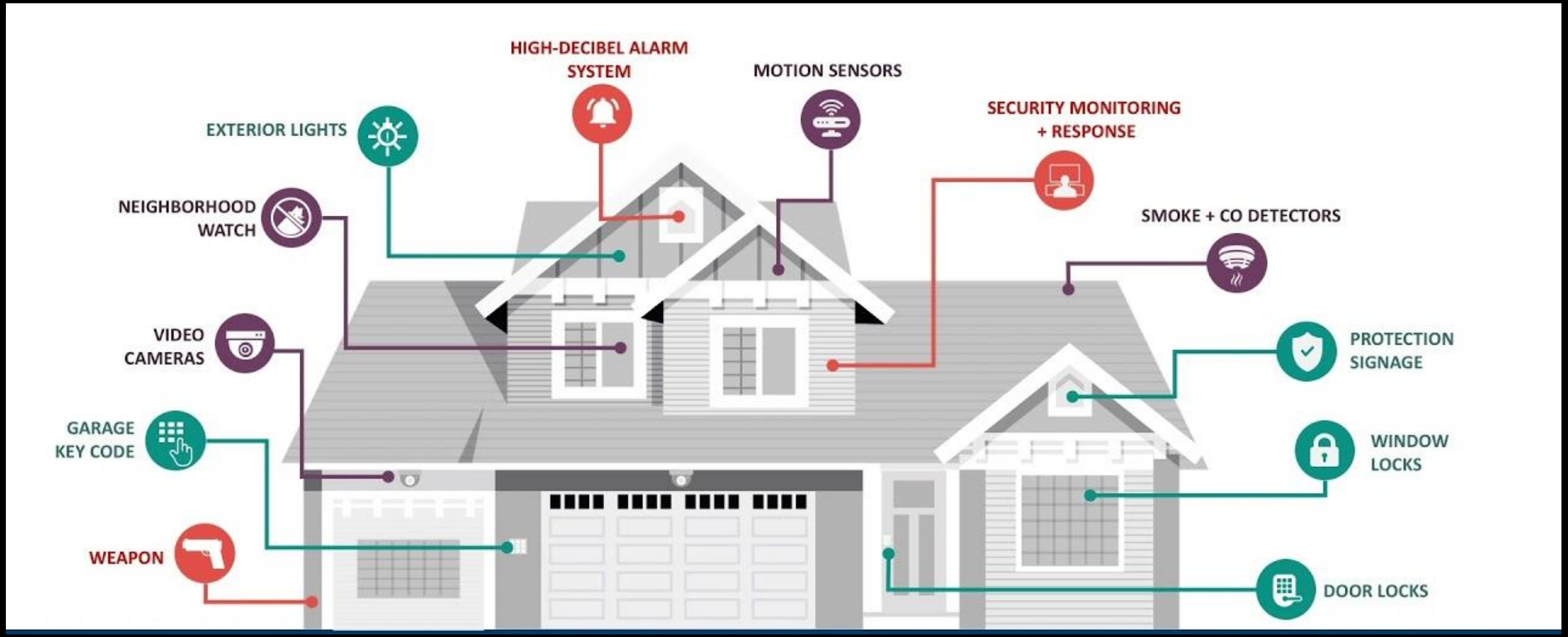
Tecnologias

Processos

Tecnologias no Cenário de Cibersegurança



Camadas de Proteção



Tecnologias Robustas são Necessárias

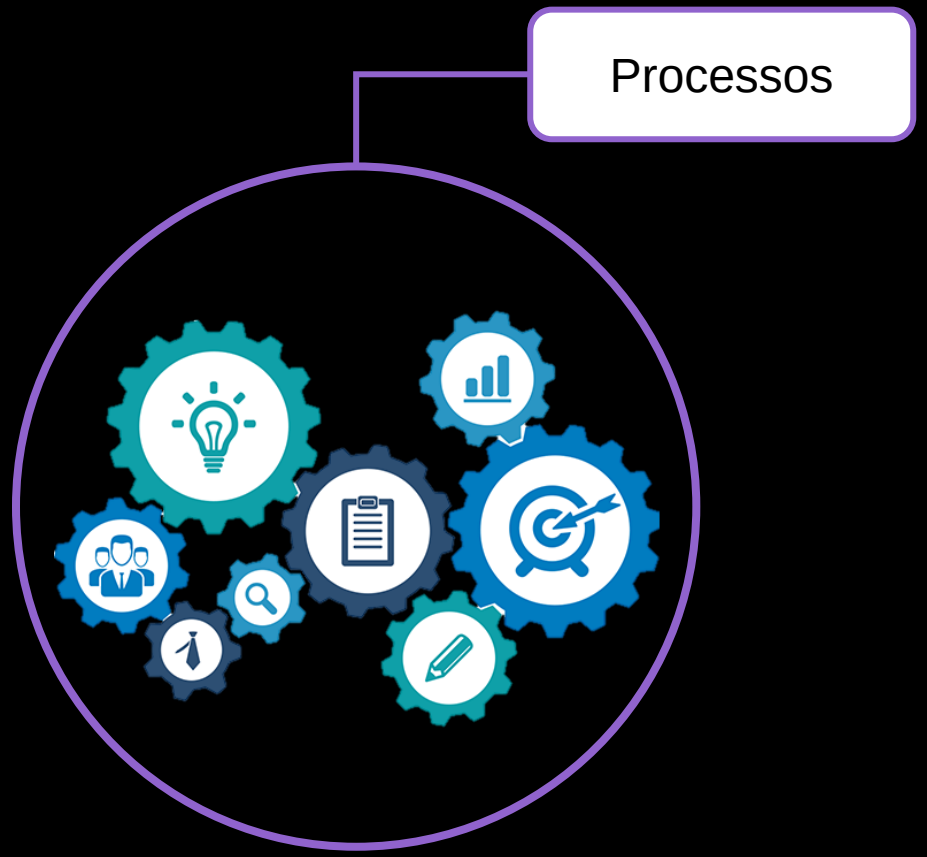
A Base da Cibersegurança

Pessoas

Tecnologias

Processos

Processos em Cibersegurança



Processos Precisam Estar Bem Implementados

A Base da Cibersegurança

Pessoas

Tecnologias

Processos

Pessoas Envolvidas com Cibersegurança

Pessoas

Usuários/Colaboradores Precisam Estar Atentos

Qualquer Descuido Pode Ser Fatal...

A Base da Cibersegurança

Pessoas

Tecnologias

Processos

Todos os Pontos Precisam Estar Próximos...

Pessoas

- Entendimento básico
- Conscientização
- Treinamentos
- Visão de Riscos

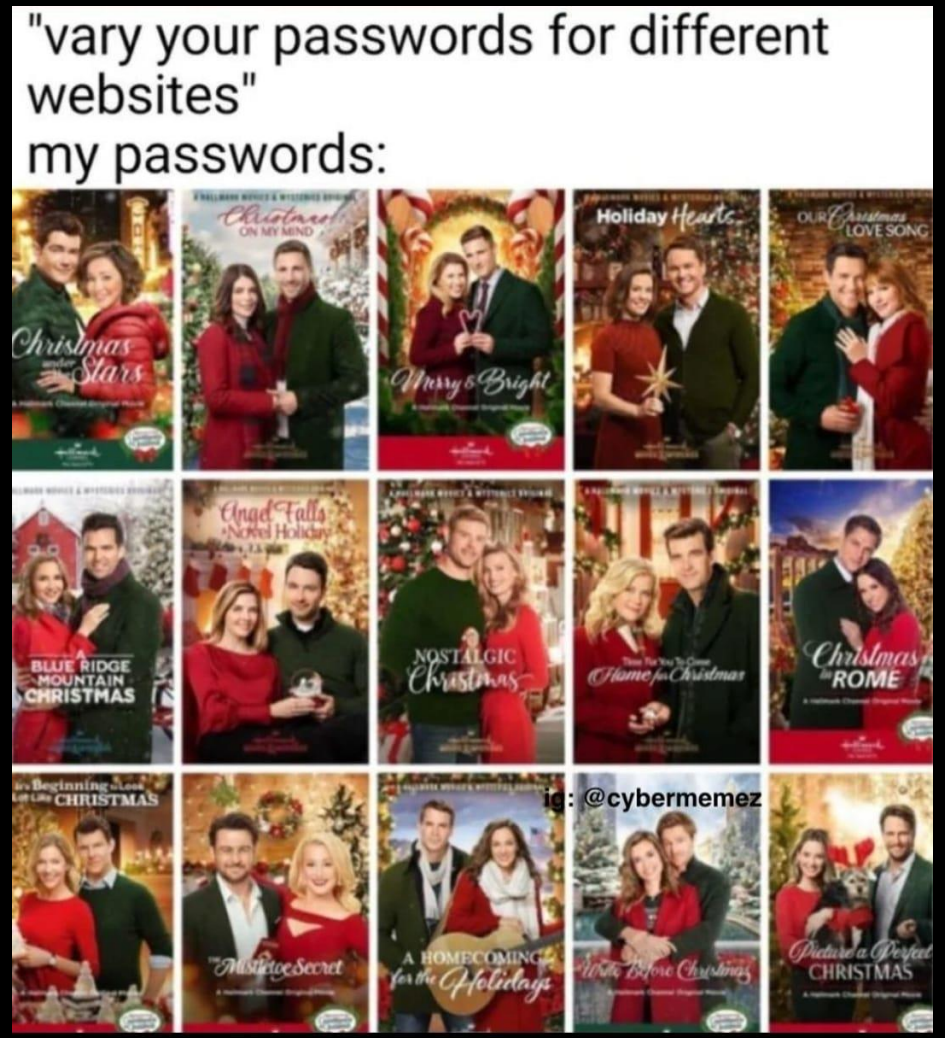
Tecnologias

- Ferramentas de Segurança como AV, FW, IPS, Sandbox...
- Updates de SW
- Testes de SW

Processos

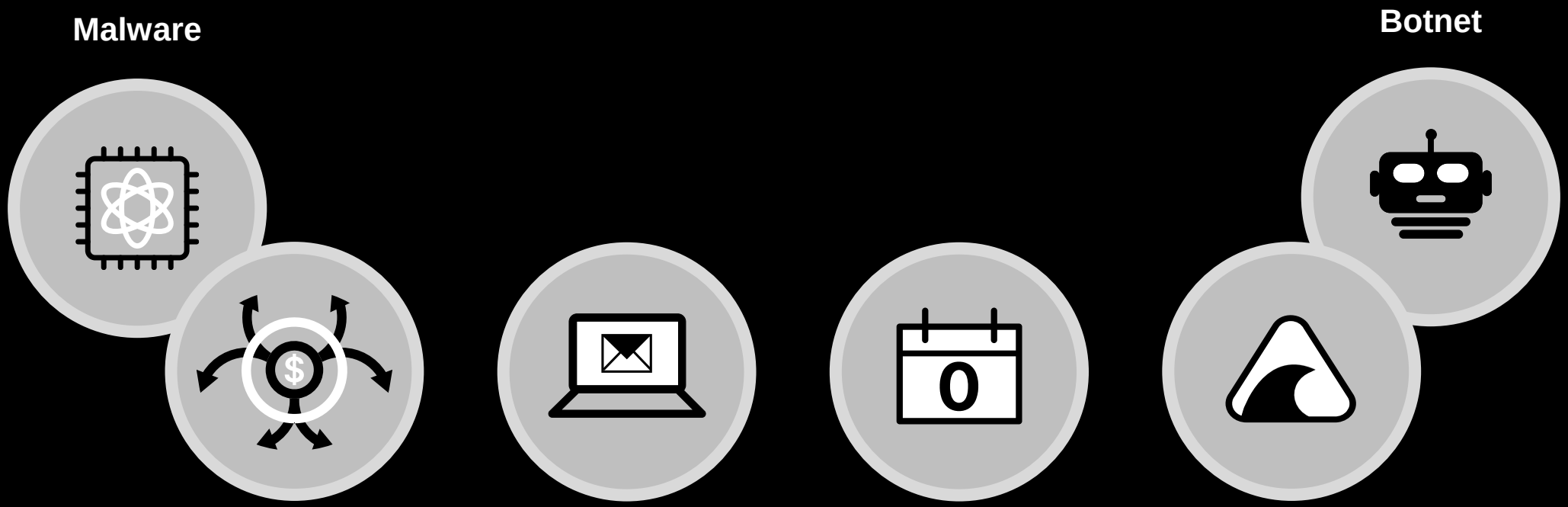
- Gestão de Sistemas
- Políticas
- Procedimentos
- Auditoria
- Governança

Cenário Pessoal Também Conta




Explorador
Hacktivista
Cyber Terrorista
Cyber Criminoso
Guerreiro Cyber

Cenário de ameaças



Cyber Kill Chain - Levantando as Possibilidades

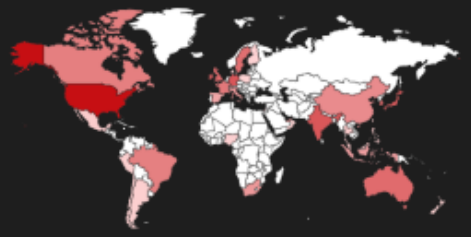
Reconhecimento

SHODAN | Explore | Downloads | Pric

TOTAL RESULTS

3,319,505

TOP COUNTRIES



United States	1,620,947
Germany	220,153
India	215,787
Japan	209,779
Ireland	190,483

More...

TOP PORTS

22	3,252,727
2222	34,279
122	7,757
7022	3,475
443	3,329

More...

Web Technologies

CDN

- Google Hosted Libraries

JavaScript Graphics

- particles.js

JavaScript Libraries

- OWL Carousel
- jQuery 3.2.1

UI Frameworks

- Bootstrap 3.3.7

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

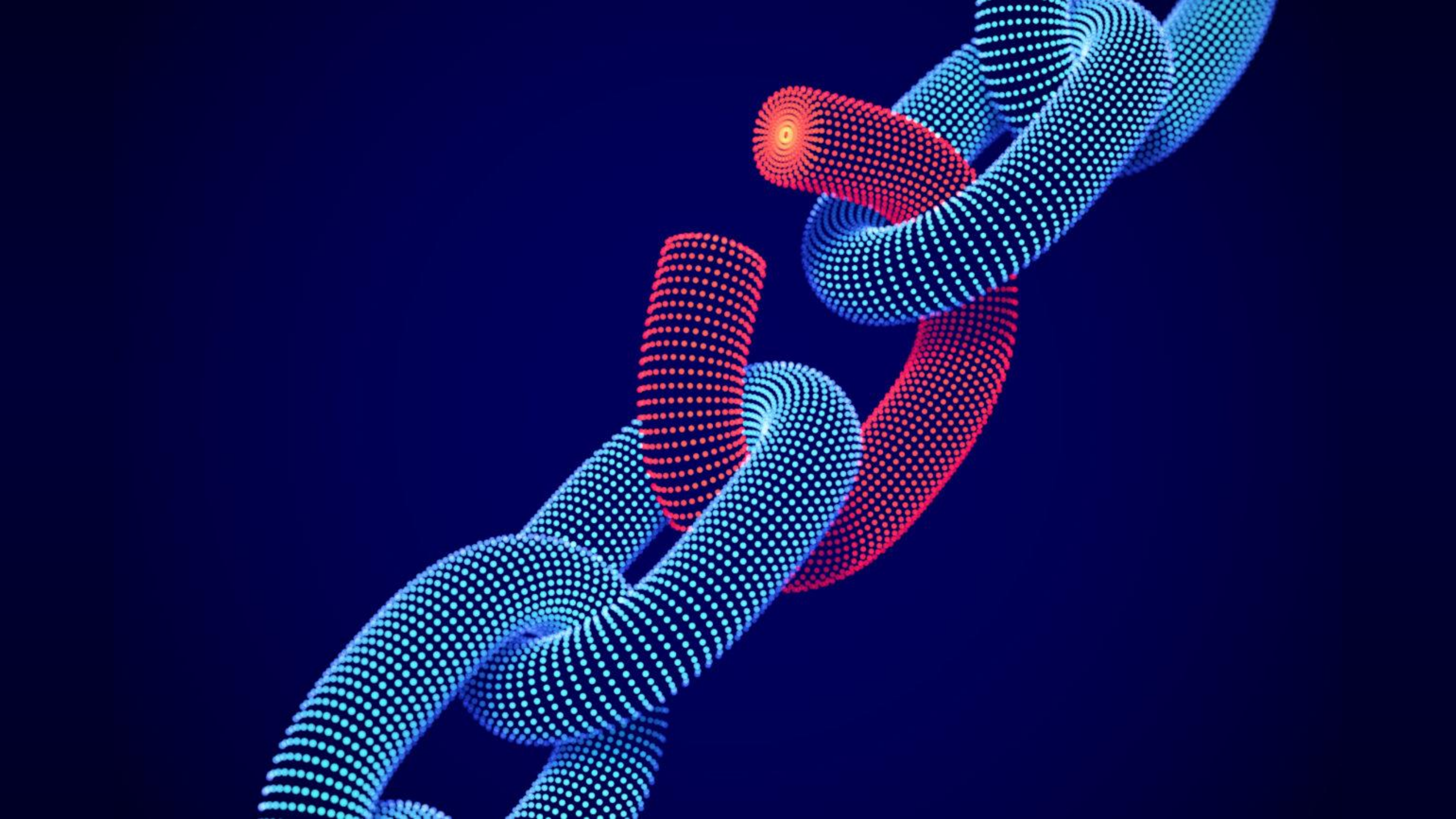
CVE-2023-45802	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
CVE-2023-31122	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2022-37436	Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later

```
        rsa-sha2-256
        ecdsa-sha2-nistp256
        ssh-ed25519

Encryption Algorithms:
        chacha20-poly1305@openssh.com
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-gcm@openssh.com
        aes256-gcm@openssh.com

MAC Algorithms:
        umac-64-etm@openssh.com
        umac-128-etm@openssh.com
        hmac-sha2-256-etm@openssh.com
        hmac-sha2-512-etm@openssh.com
        hmac-sha1-etm@openssh.com
        umac-64@openssh.com
        umac-128@openssh.com
        hmac-sha2-256
        hmac-sha2-512
        hmac-sha1

Compression Algorithms:
        none
        zlib@openssh.com
```

// 80 / TCP

Apache httpd 2.4.29

```
HTTP/1.1 200 OK
Date: Sat, 25 May 2024 23:51:09 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Fri, 11 Jun 2021 18:18:50 GMT
ETag: "232c3-5c4818a20f8fd"
Accept-Ranges: bytes
Content-Length: 144067
Vary: Accept-Encoding
Content-Type: text/html
```



CVEs = Common Vulnerabilities & Exposures

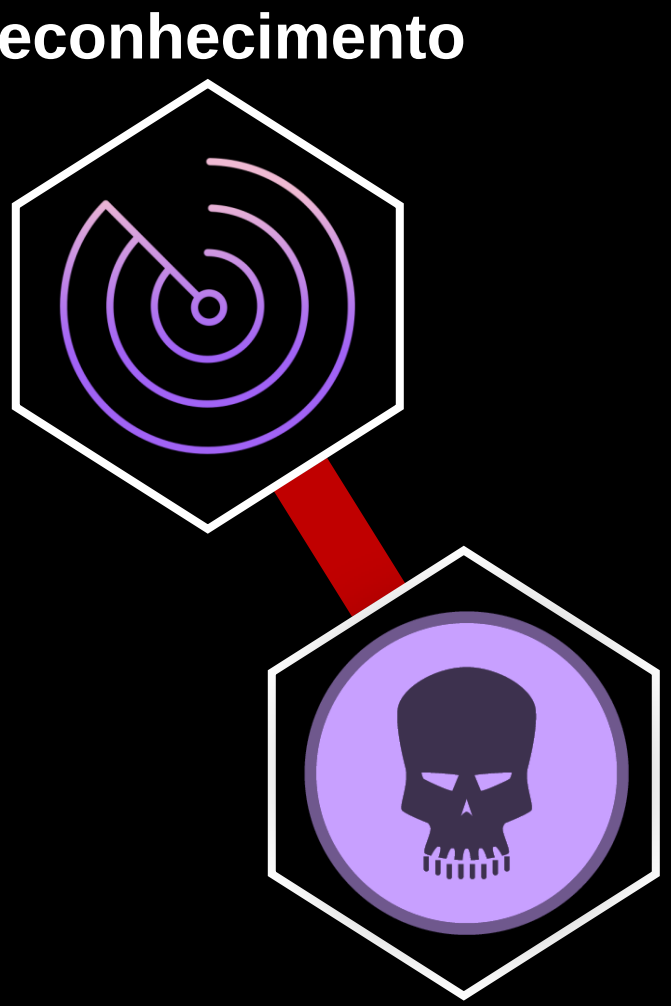
Fraquezas/Pontos Vulneráveis que podem ser explorados
(via Vetores de Ataques)


CVSS = Common Vulnerability Scoring System
Nível de Risco de Cada Vulnerabilidade

Cyber Kill Chain - Levantando as Possibilidades

Reconhecimento

Cyber Kill Chain - Preparando o Payload



The Digital S

HOME NII HC

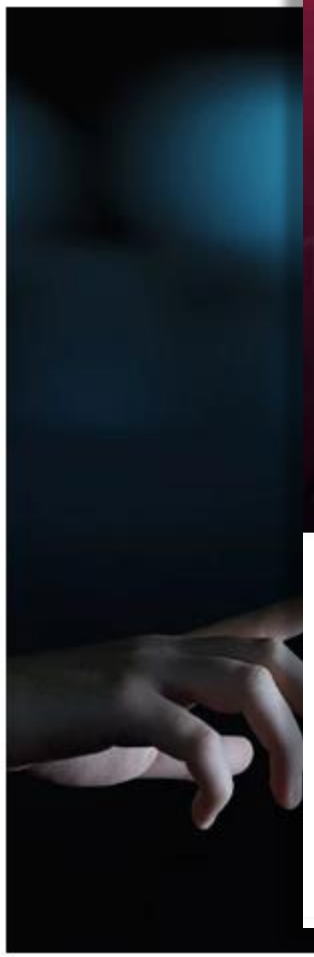
Malwar
Dark Sic

February 14, 20
Research, Security

Malware Development Part 1 - Chetan Nayak

Chatting
Polymor

Eran Shimony And



Infosecurity Magazine

Log In Sign Up

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

Infosecurity Magazine Home » News » Malware-as-a-Service Now the Top Threat to Organizations

NEWS 6 FEB 2024

Malware-as-a-Service Now the Top Threat to Organizations

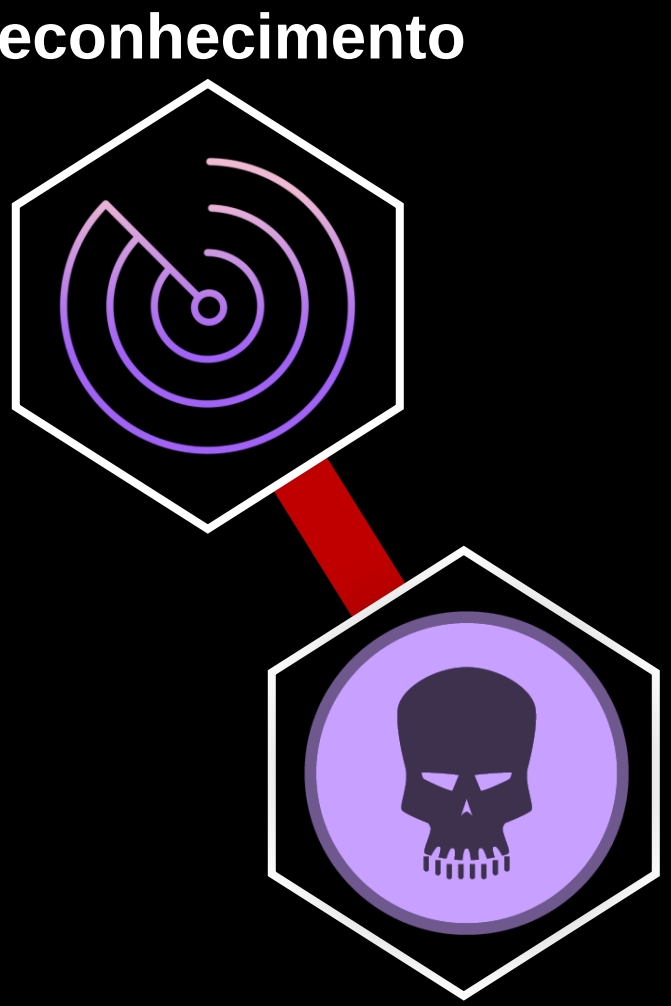
James Coker
Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

Malware-as-a-Service (MaaS) infections were the biggest threat to organizations in the second half of 2023, according to a new Darktrace report.

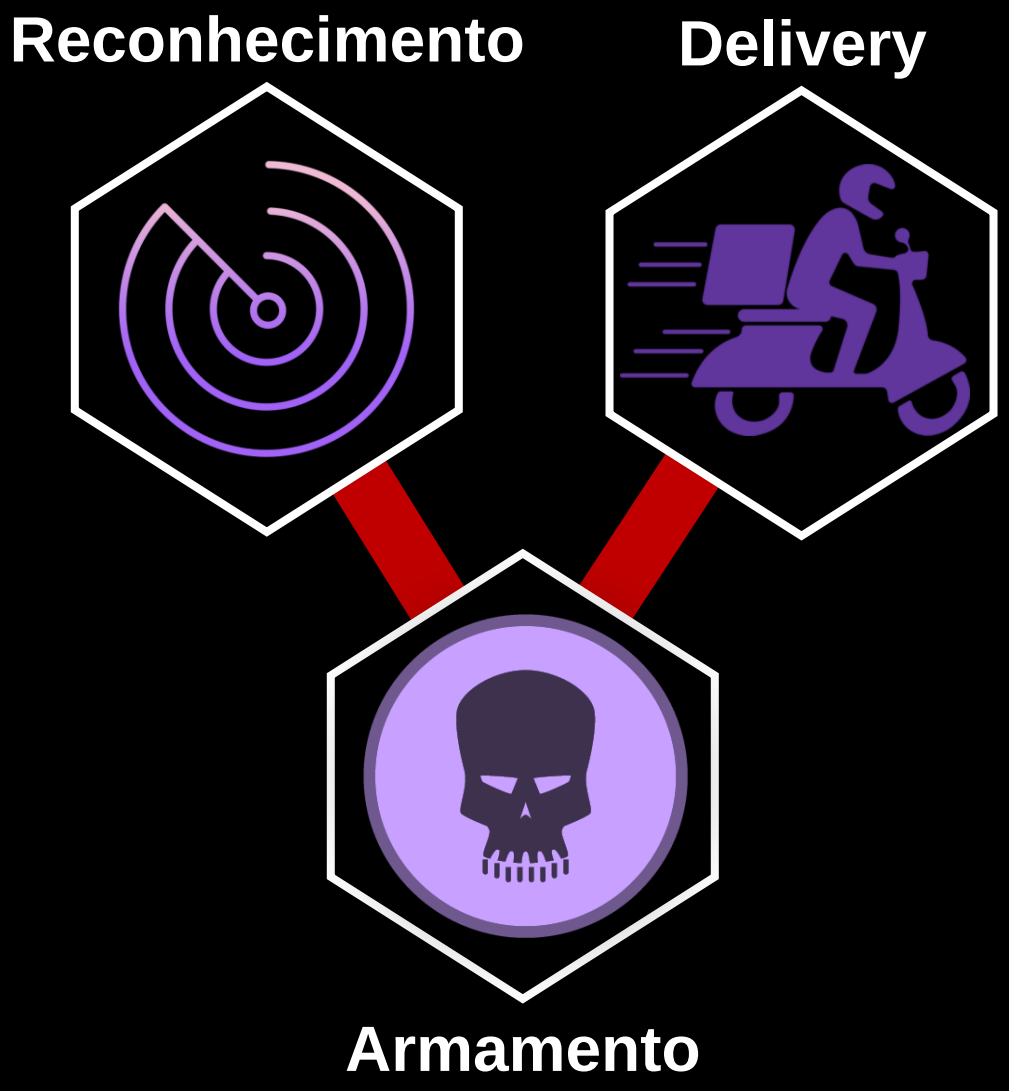
The *2023 End of Year Threat Report* highlighted the cross-functional adaption of many of the malware strains. This includes malware loaders like remote access

Cybersecurity Career Guidance – Part 1 –

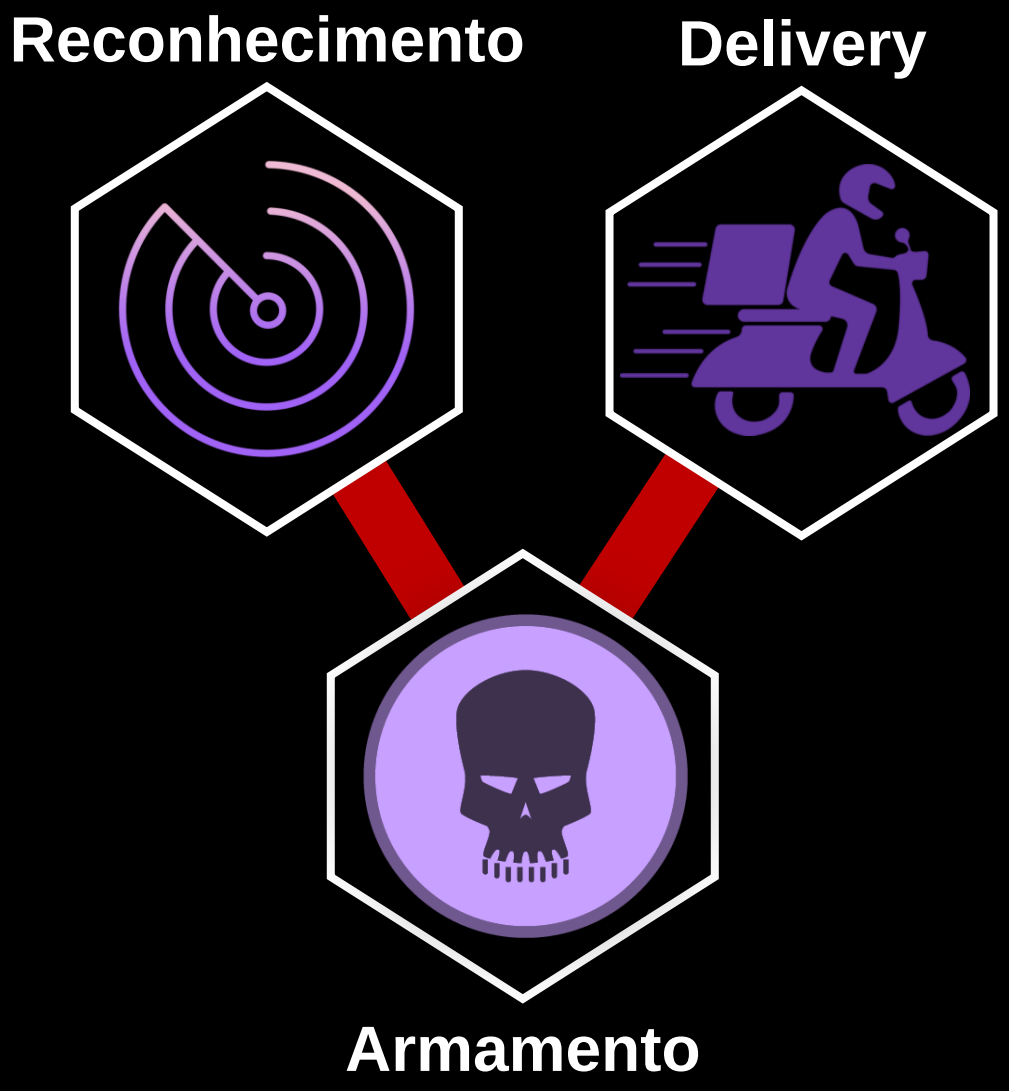
Cyber Kill Chain - Preparando o Payload



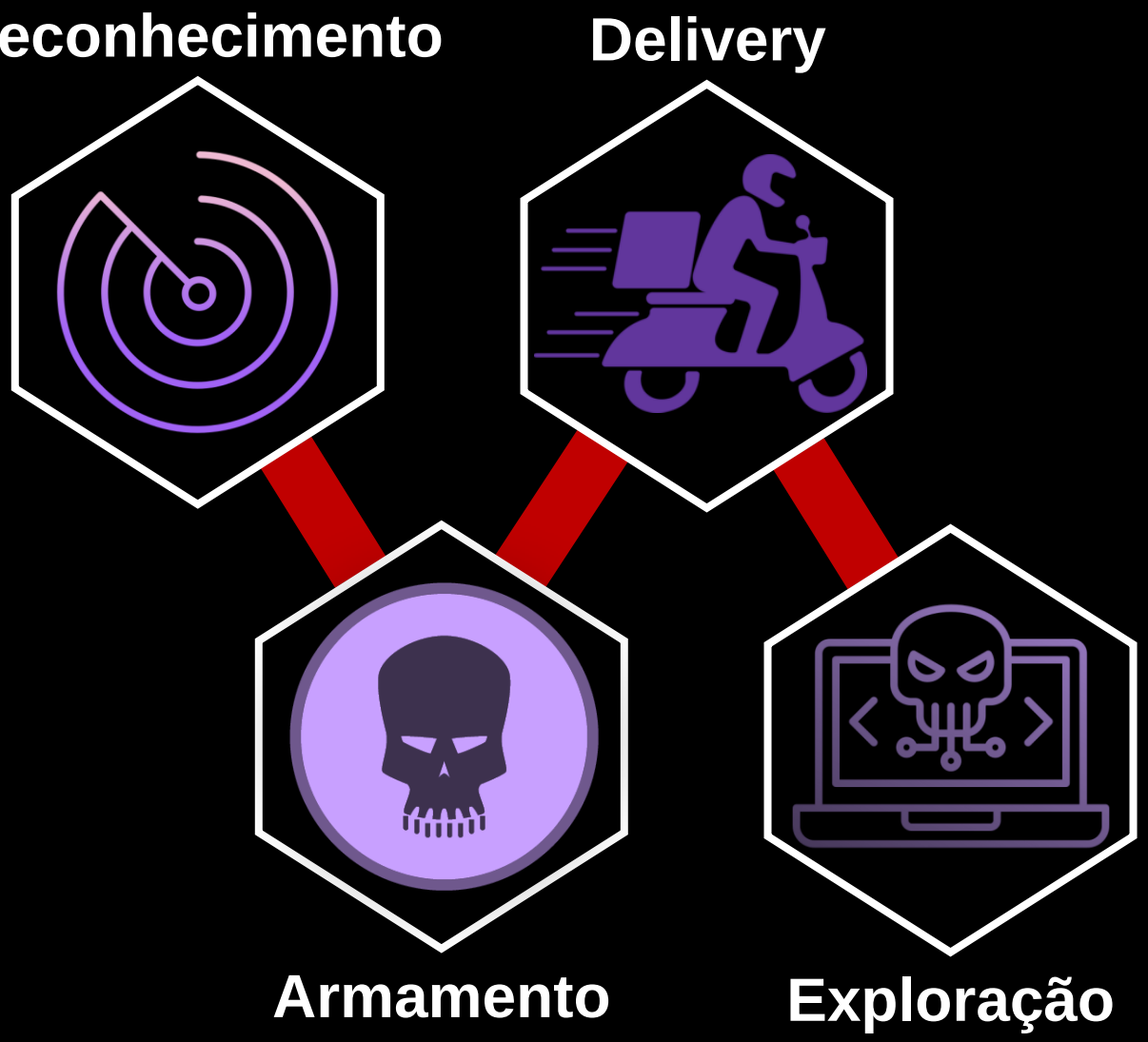
Cyber Kill Chain - Distribuindo o Payload



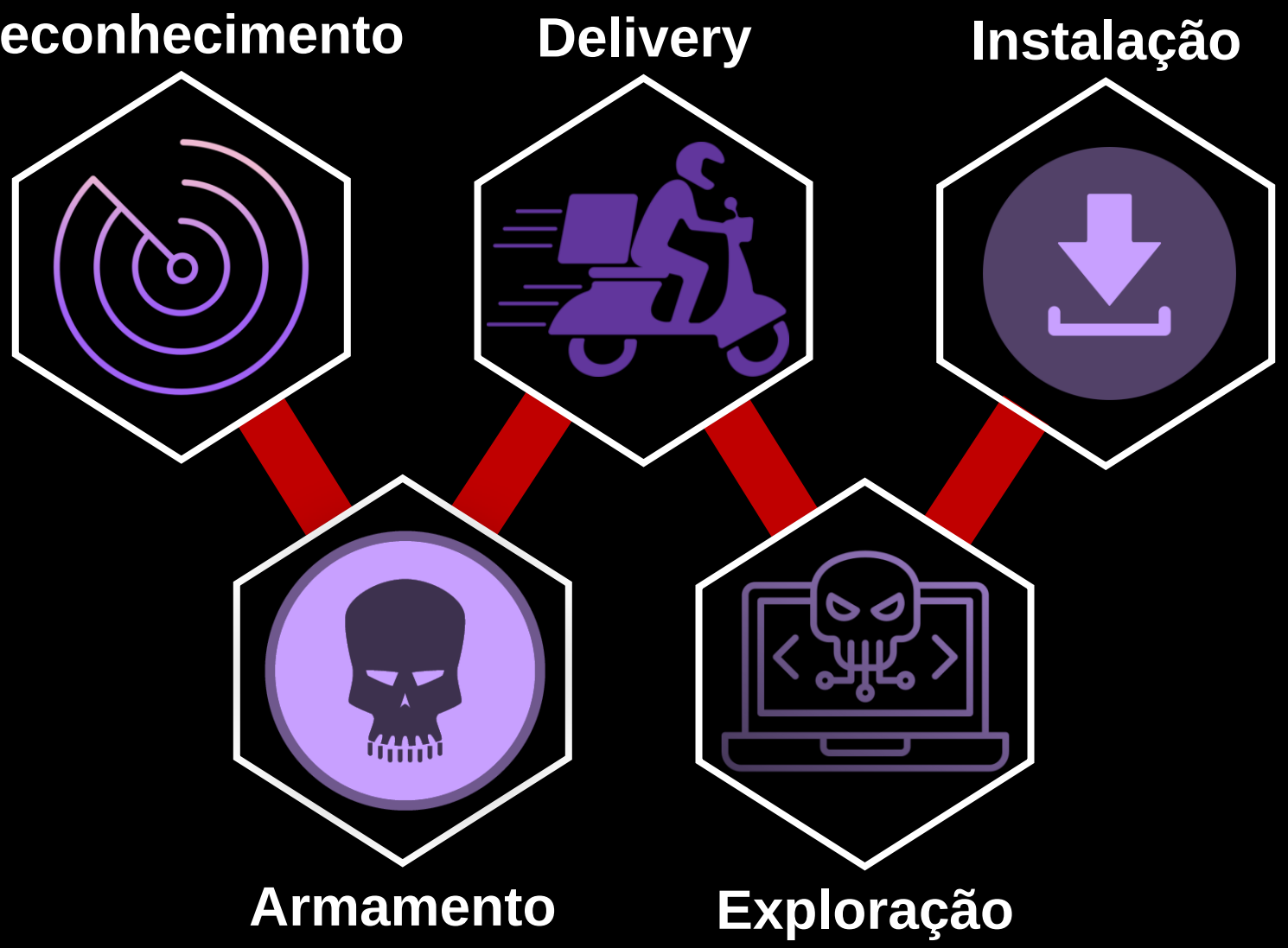
Cyber Kill Chain - Distribuindo o Payload



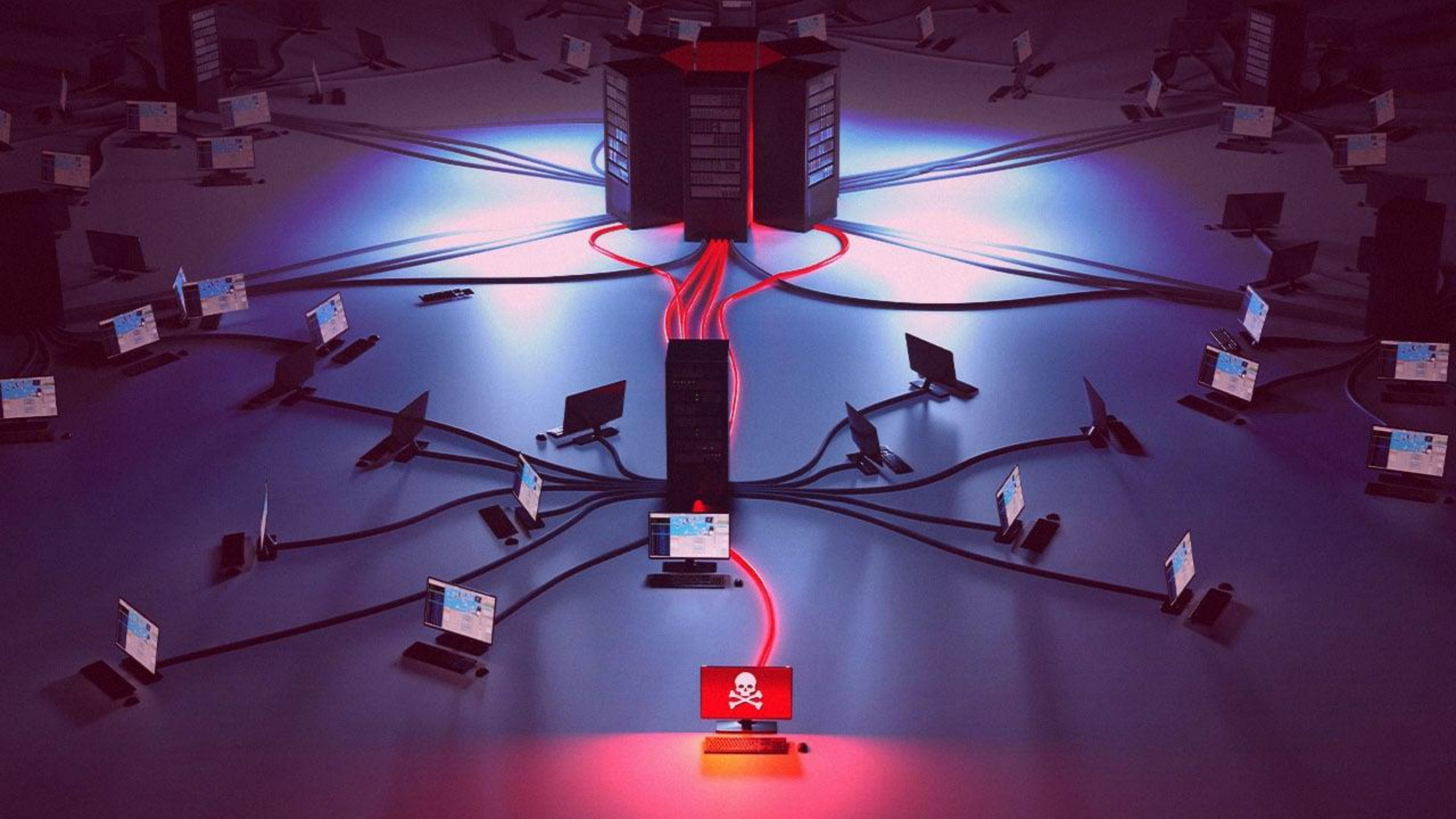
Cyber Kill Chain - Explorando a Vulnerabilidade



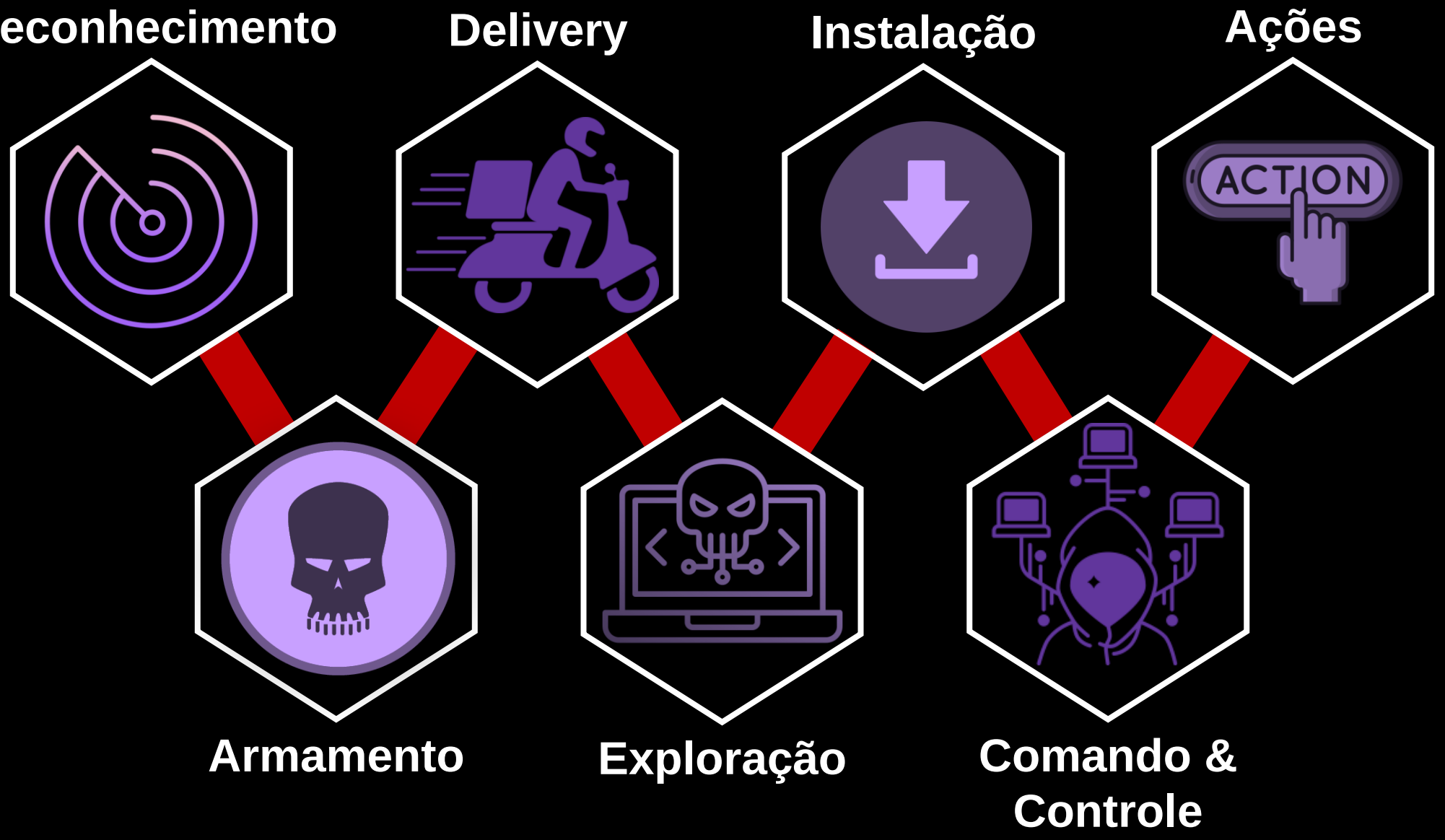
Cyber Kill Chain - Instalando o Malware



Cyber Kill Chain - Estabelecendo Comunicação



Cyber Kill Chain - Tomando as Ações



THE ART N

Art market | Museums & heritage | Exhibitions | Books | Podcasts

ewspaper and complete our reader survey today.

Hackers claim responsi
Christie's cyberattack a
release client data

The group RansomHub say they are behind
auction house's website earlier this month

Farm bu
concern

Collaboration
cybersecurity

By Diana

Reading Time: 3

"In ag and agri-food
impact of an attack
in Cybersecurity an

Cybersecurity i
collaborative su

Thousands of rugby fans' data leaked in breach

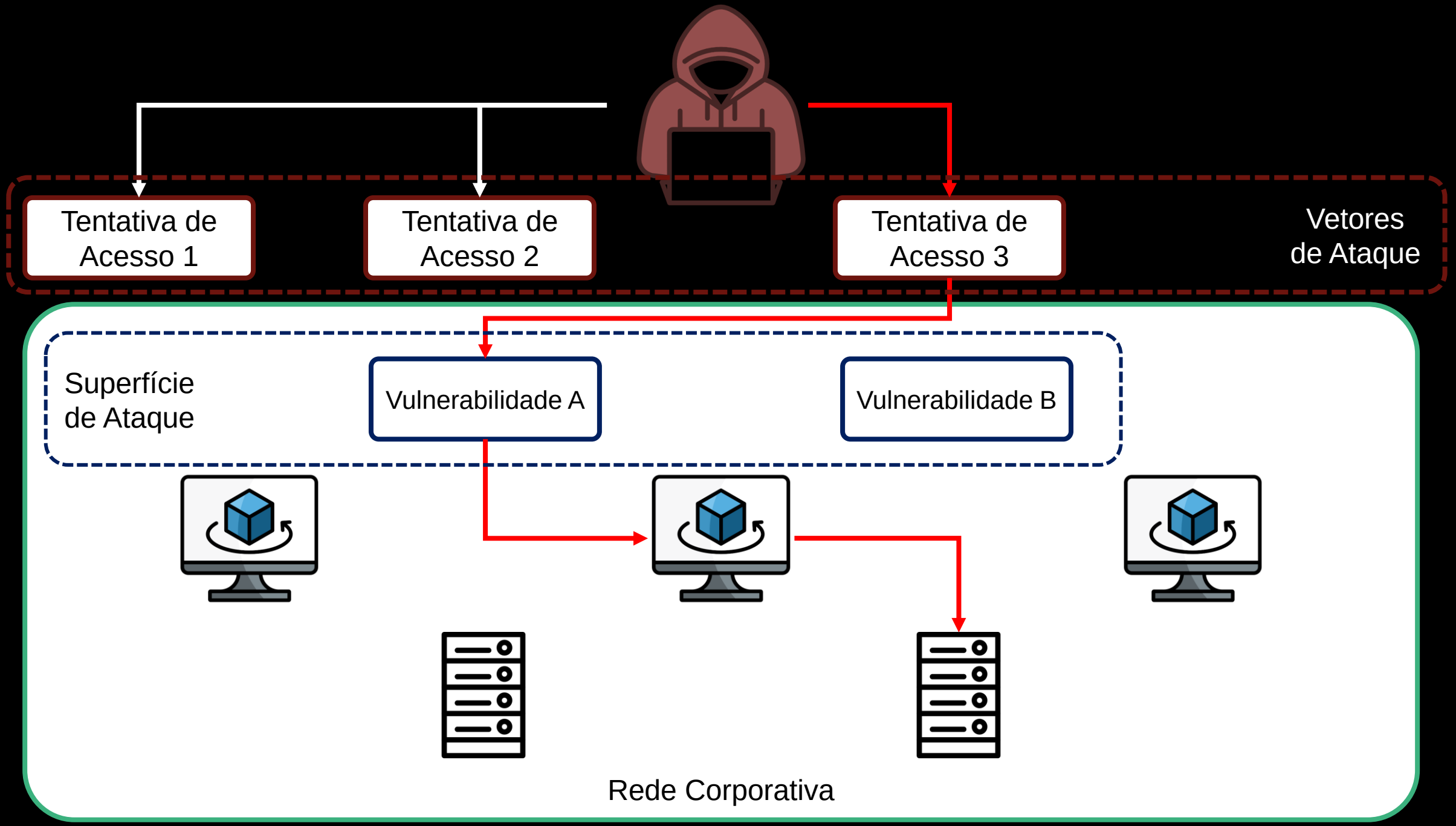
4 days ago

Share

James McCarthy, BBC News

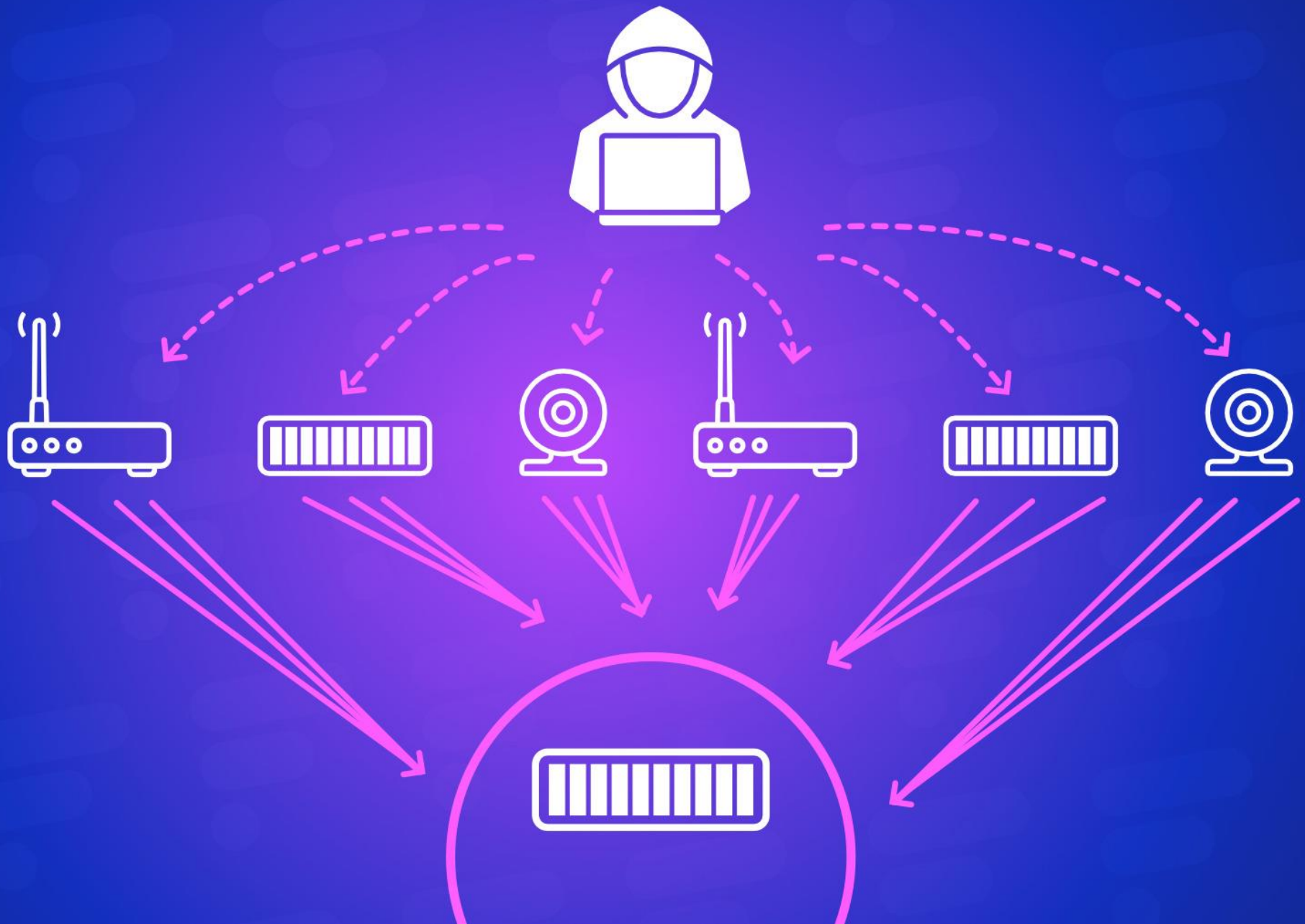
Details of about almost 70,000 members have been leaked

Data belonging to tens of thousands of Welsh Rugby Union supporters' club members has been exposed in a cybersecurity breach.


Tentativa de Acesso 1
Tentativa de Acesso 2
Tentativa de Acesso 3
Vetores de Ataque
Superfície de Ataque
Vulnerabilidade A
Vulnerabilidade B
Rede Corporativa

Entendendo Tipos de Ataques & Técnicas Utilizadas

Ataques de Indisponibilidade/Negação de Serviço



Ataques de Indisponibilidade/Negação de Serviço

Ataques de Enganação

Ataques de Enganação

Engenharia Social

Phishing (e suas variações)

Phishing (e suas variações)


RANSOMWARE

Roubo do que é Mais Valioso

Seattle Public
Are Down Foll

Physical books, CDs, and DVDs can

By **Matt Novak** Published 2 hours ago

File photo of the Seattle Public Library in Seattle, Washir

The Seattle Public Library
several systems, including
a new report from the Wor

Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment

The transaction, visible on Bitcoin's blockchain, suggests the victim of one of the worst ransomware attacks in years may have paid a very large ransom.

Ransomware: 97% das organizações pediram ajuda às autoridades

28 de Maio, 2024 por Miguel Videira Rodrigues

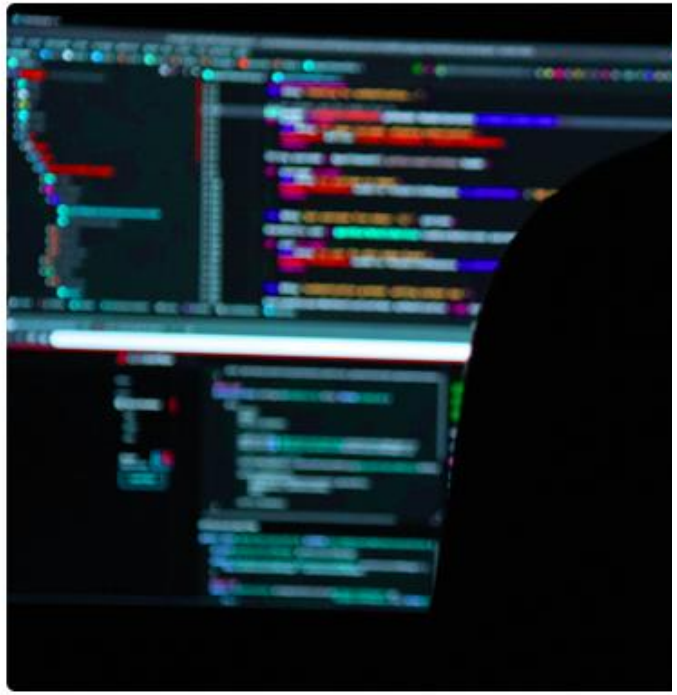
OUVIR O POST

Ransomware-as-a-service já é uma Realidade

New 'MichaelKors' Ransom

ESXi Systems

May 15, 2023 Ravie Lakshmanan



A new ransomware-as-service (RaaS) operation call
encrypting malware to target Linux and VMware ESX

Ransomware-as-a-service tops evolving global cyber risks

Also on the rise: Triple extortion schemes in which cyber criminals exploit multiple ransoms from a single target.

By Jose Seara | April 21, 2023 at 08:30 AM

As the insurance and risk management industry continues to make strides in understanding and mitigating cyber threats, the coverage opportunities are enormous. (Photo: WhataWin/Adobe Stock)

Instant Insights
Cybersecurity Insights

BEST PRACTICES

Stranger danger: Keys to avoiding scams & cyber missteps

Read More ›

MARKET INSIGHTS

Rising cyberattacks in Japan show how U.S., Europe are also vulnerable

Read More ›

NEWS

How cyber risks can reshape business interruption coverage


THE
BEEKEEPER


CRYPTOJACKING
CRYPTOJACKING
CRYPTOJACKING
CRYPTOJACKING
CRYPTOJACKING
CRYPTOJACKING
CRYPTOJACKING
CRYPTOJACKING

New cry| Kinsing crypto mining campaign targets 75 cloud-vulnerab native applications

News
Oct 07, 2022 • 3 mins

Cryptocurrency | Cyberattacks

While currently the campa used to deploy spyware o

News Analysis
May 08, 2024 • 6 mins

Application Security | Cryptocurrency | Malware

Five years after being discovered, the Kinsing cryptojacking operation remains very active against organizations, employing daily probes for vulnerable applications using an ever-growing list of exploits.

Exfiltração de Dados

News Features Expert analysis

Zeljka Zorz, Editor-in-Chief, Help Net Securit
April 10, 2024

New covert Share exfiltration techn

Varonis Threat Labs researchers have use can use for covert data and file ex server.

"These techniques can bypass the det traditional tools, such as cloud access SIEMs, by hiding downloads as less su noted.

SECURI

NEWS COLUMNS MANA

CYBERSECURITY | SECURIT

There was a 2023

By Security Staff

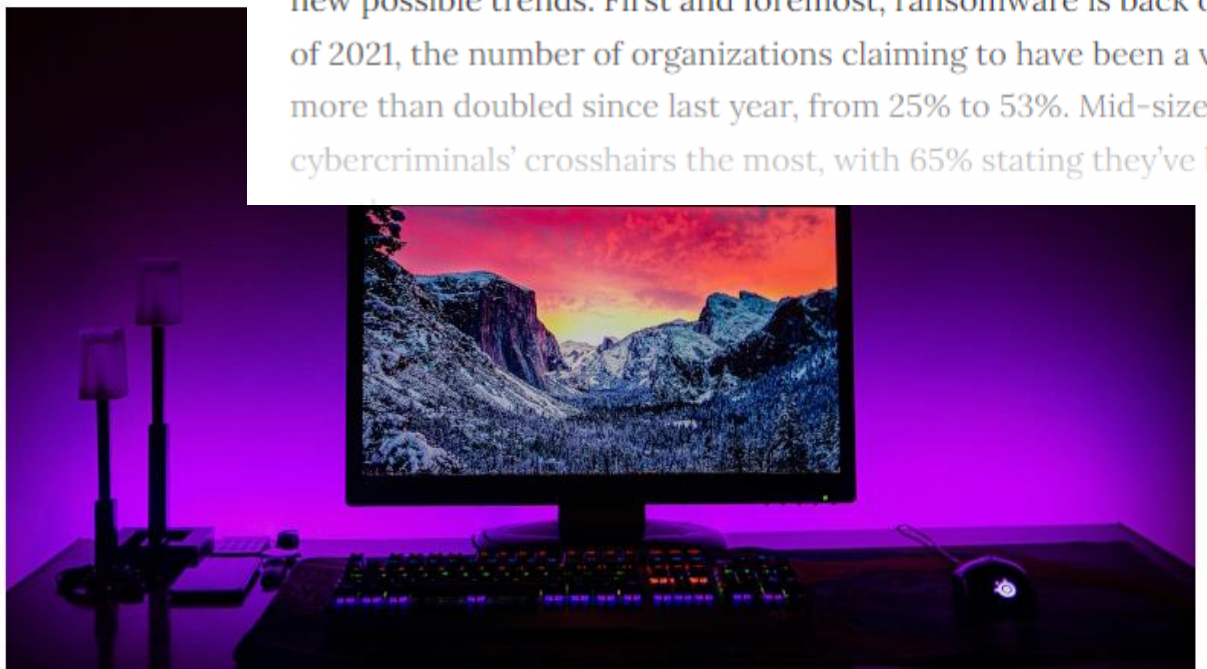
CYBERSECURITY | SECURITY NEWSWIRE | CYBERSECURITY NEWS

Research shows cybercriminals' motivation shifts to data exfiltration

By Security Staff

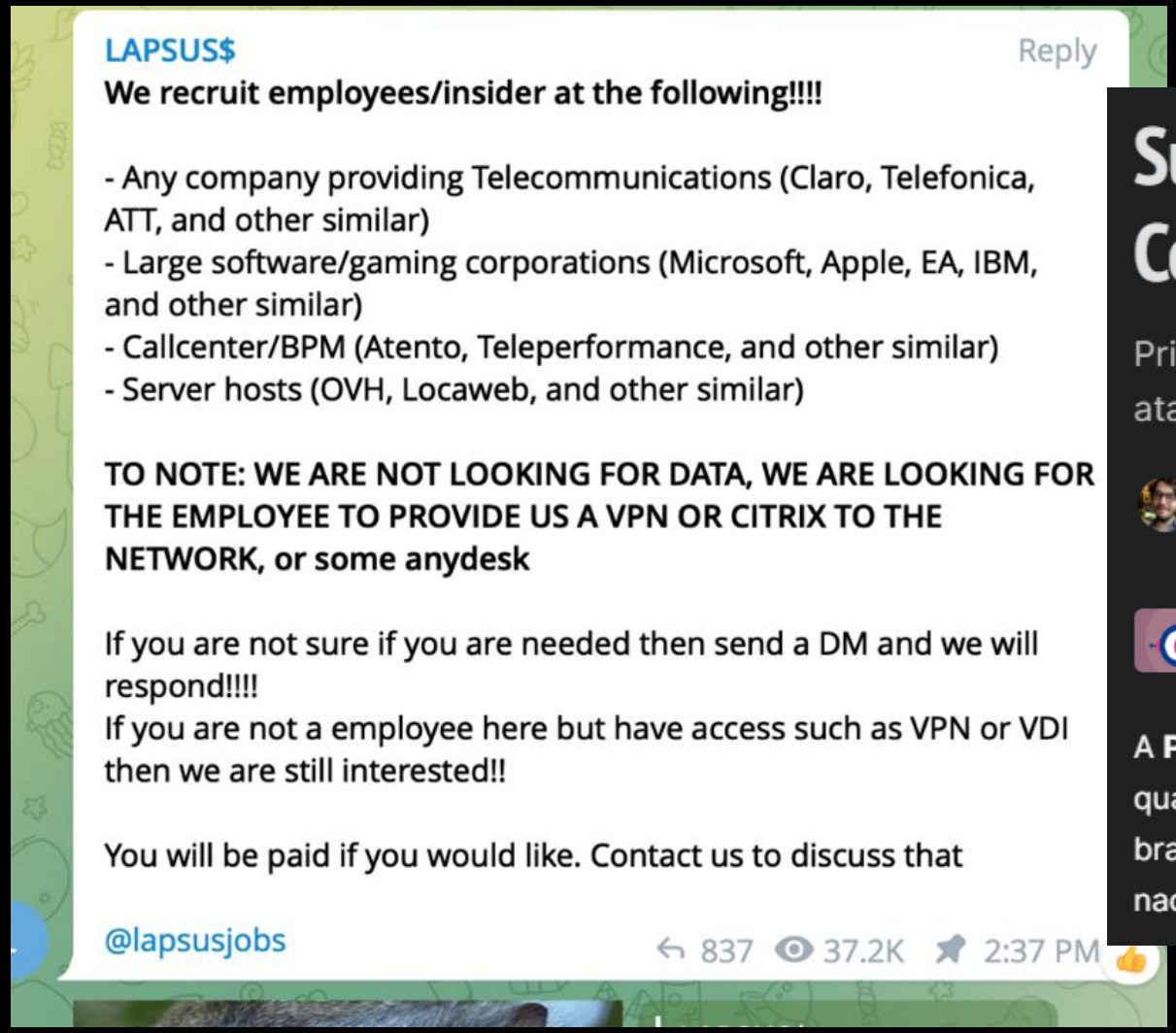
Delinea recently published its annual "State of Ransomware" report which shows that ransomware attacks are increasing again and reveals a change in strategy among cybercriminals. The familiar tactics of crippling a company and holding it hostage have been replaced by new strategies that use stealth to exfiltrate private and sensitive data. Cybercriminals then frequently threaten to sell it to the highest bidder on the darknet or leverage it to reap a handsome cyber insurance payment.

The report analyzed data from a Censuswide survey of more than 300 U.S. IT and Security decision-makers to identify significant changes compared to data from the previous year's report and uncover new possible trends. First and foremost, ransomware is back on the rise. Although not back at the levels of 2021, the number of organizations claiming to have been a victim of ransomware in the past 12 months more than doubled since last year, from 25% to 53%. Mid-sized companies appeared to be in cybercriminals' crosshairs the most, with 65% stating they've been a ransomware victim over the past 12




INSIDER

Ameaças Internas (Insider Threats)



LAPSUS$ Reply

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs 837 37.2K 2:37 PM

Suspeito de participar do Lapsus$, invasor do ConecteSUS, é preso no Brasil

Prisão foi realizada pela Polícia Federal na Bahia; Lapsus$ está por trás de ataques ao Ministério da Saúde, Microsoft, Uber e outras empresas

Por Bruno Gall De Blasi
20/10/2022 às 11:10

A **Polícia Federal** realizou mais um desdobramento da Operação Dark Cloud. Nesta quarta-feira (19), o órgão do **Ministério da Justiça e Segurança Pública** prendeu um brasileiro suspeito de participar do **Lapsus$**. O grupo hacker ficou conhecido nacionalmente por atacar o Ministério da Saúde e impedir o acesso ao ConecteSUS.

TOP 10

- 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 (SSRF)

Top 10 CI/CD Security Risks

CICD-SEC-1 Insufficient Flow Control Mechanisms

CICD-SEC-2 Inadequate Identity and Access Management

CICD-SEC-3 Dependency Chain Abuse

CICD-SEC-4 Poisoned Pipeline Execution (PPE)

CICD-SEC-5 Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-6 Insufficient Credential Hygiene

CICD-SEC-7 Insecure System Configuration

CICD-SEC-8 Ungoverned Usage of 3rd Party Services

CICD-SEC-9 Improper Artifact Integrity Validation

CICD-SEC-10 Insufficient Logging and Visibility

Cloud-Native Application Security Top 10

CNAS-1
Insecure cloud, container or orchestration configuration

CNAS-2
Injection flaws (app layer, cloud events, cloud services)

CNAS-3
Improper authentication & authorization

CNAS-4
CI/CD pipeline & software supply chain flaws

CNAS-5
Insecure secrets storage

CNAS-6
Over-permissive or insecure network policies

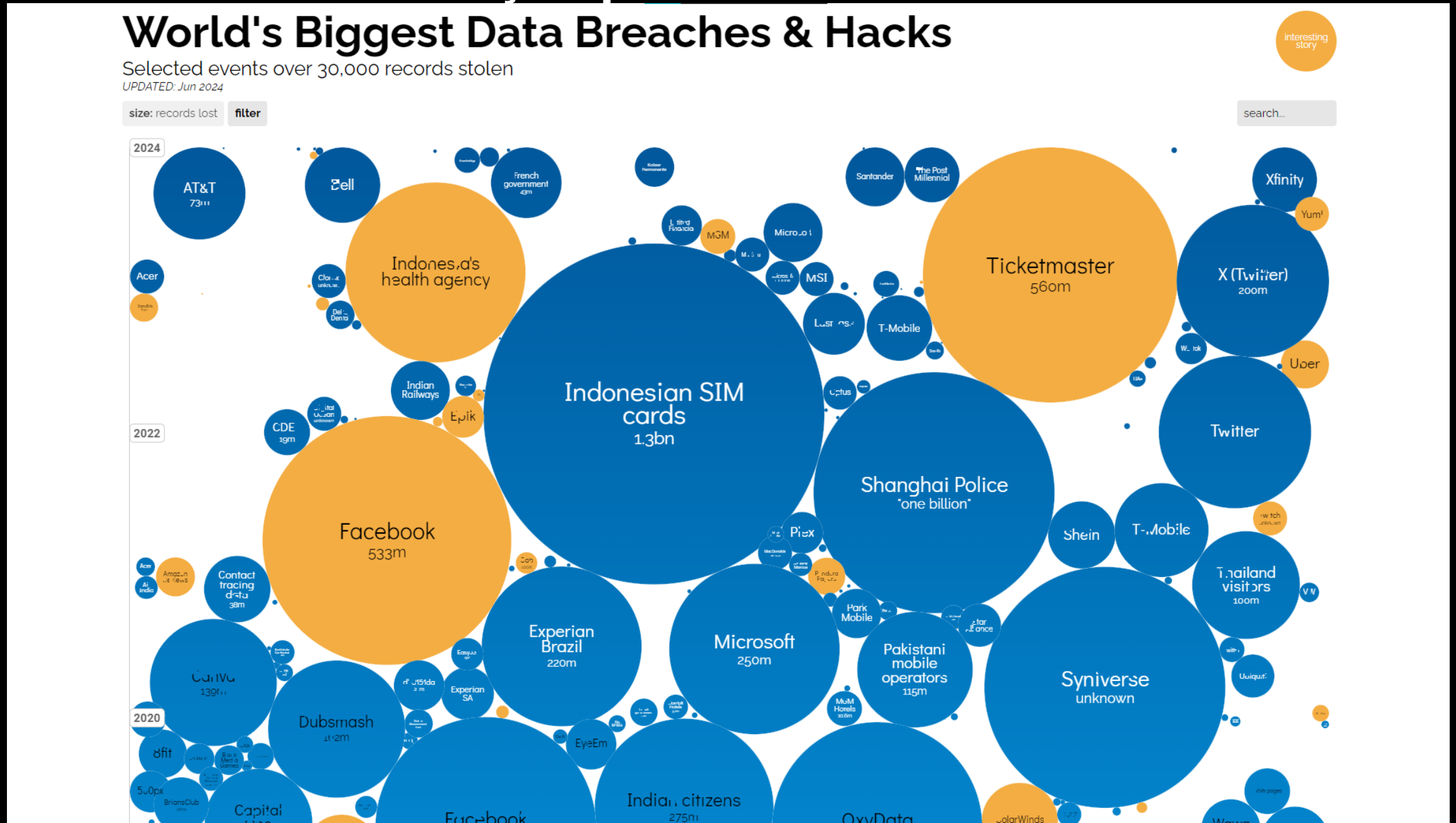
CNAS-7
Using components with known vulnerabilities

CNAS-8
Improper assets management

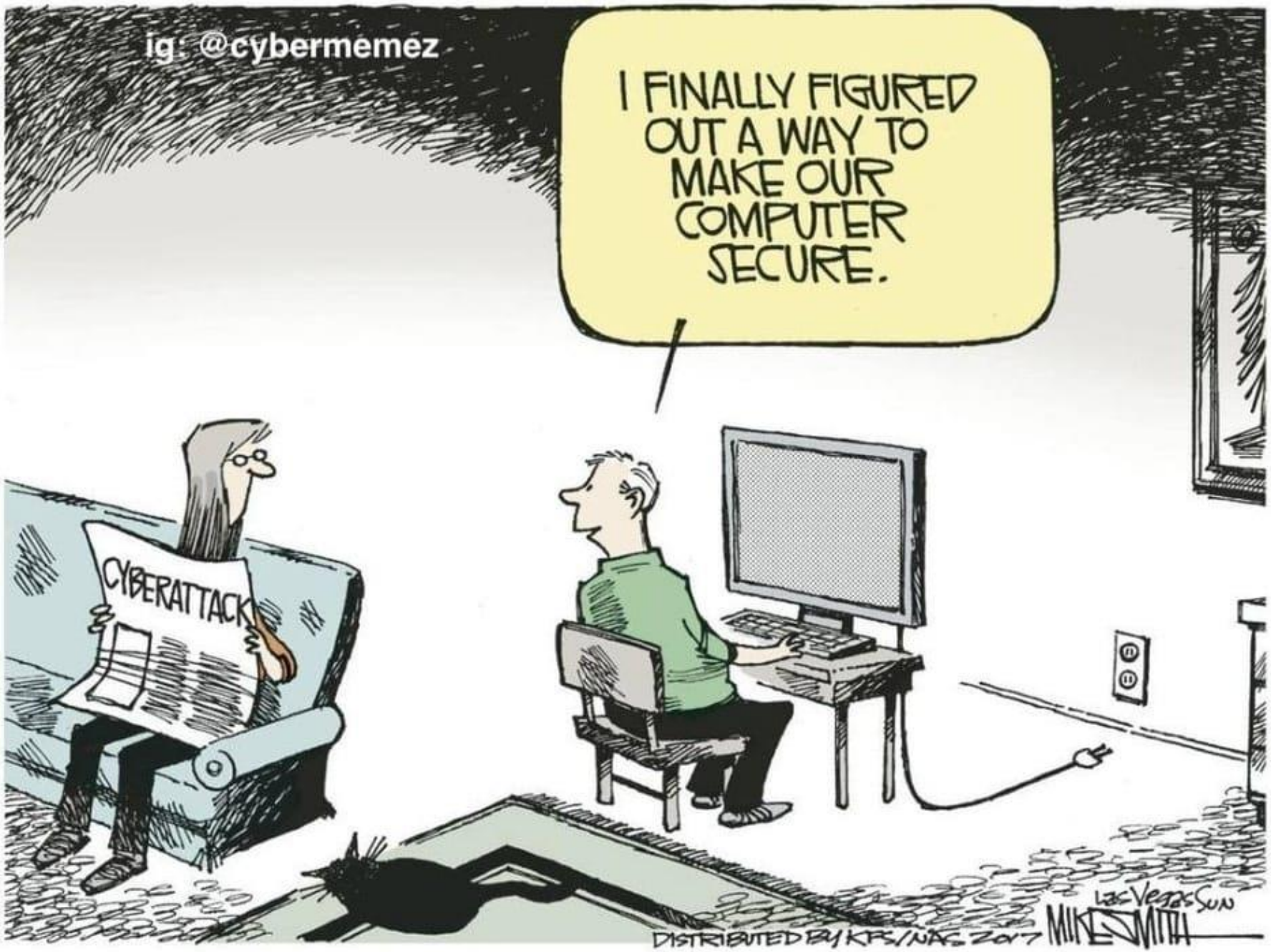
CNAS-9
Inadequate 'compute' resource quota limits

CNAS-10
Ineffective logging & monitoring (e.g. runtime activity)

Ameaças por Todos os Lados



E Como Trazer Segurança Para Tudo Isso?


ig: @cybermemez
I FINALLY FIGURED OUT A WAY TO MAKE OUR COMPUTER SECURE.
CYBERATTACK
DISTRIBUTED BY KFS/NAS 2017
LAS VEGAS SUN
MIKE SMITH

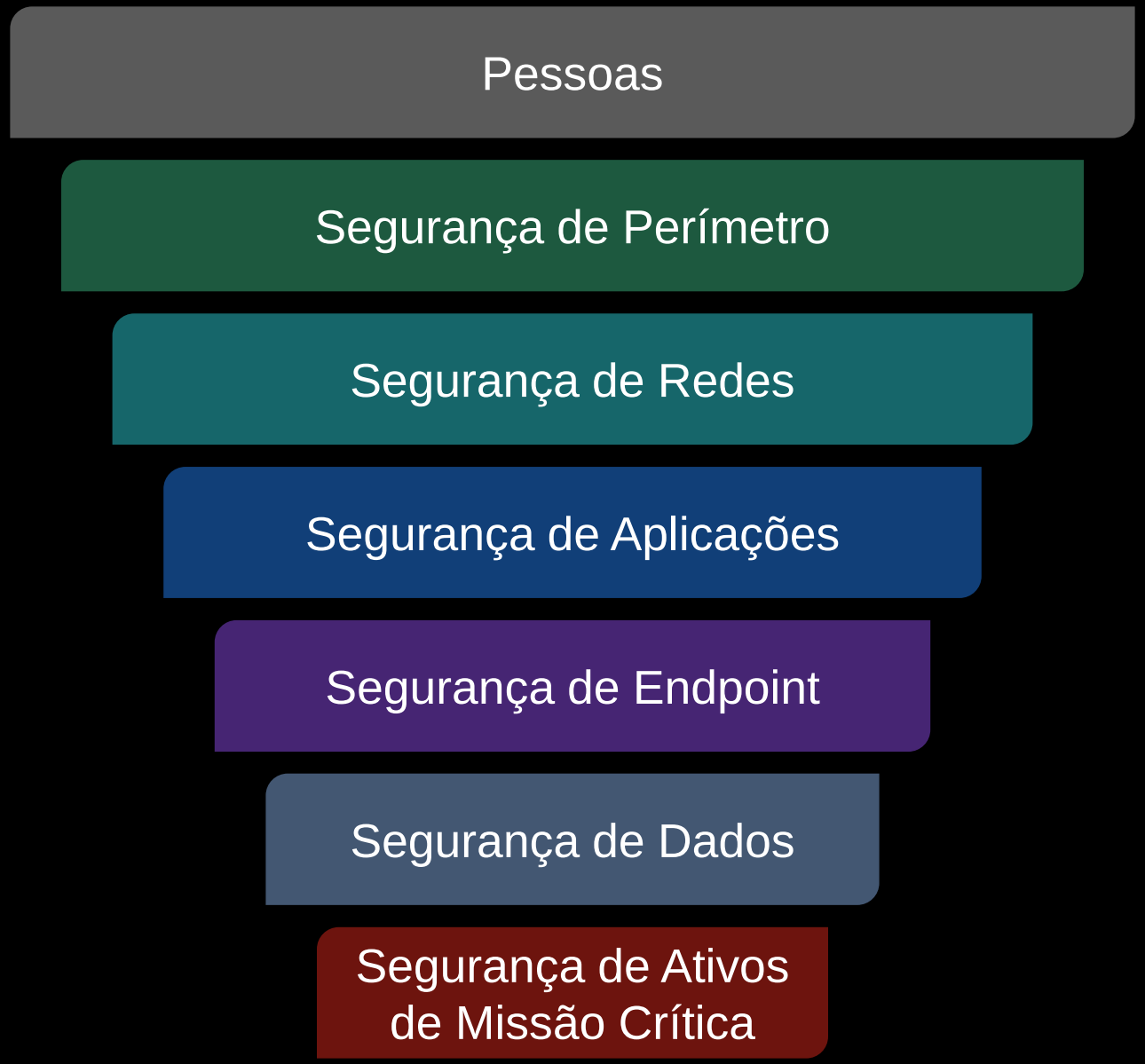
RED TEAM

VS

BLUE TEAM

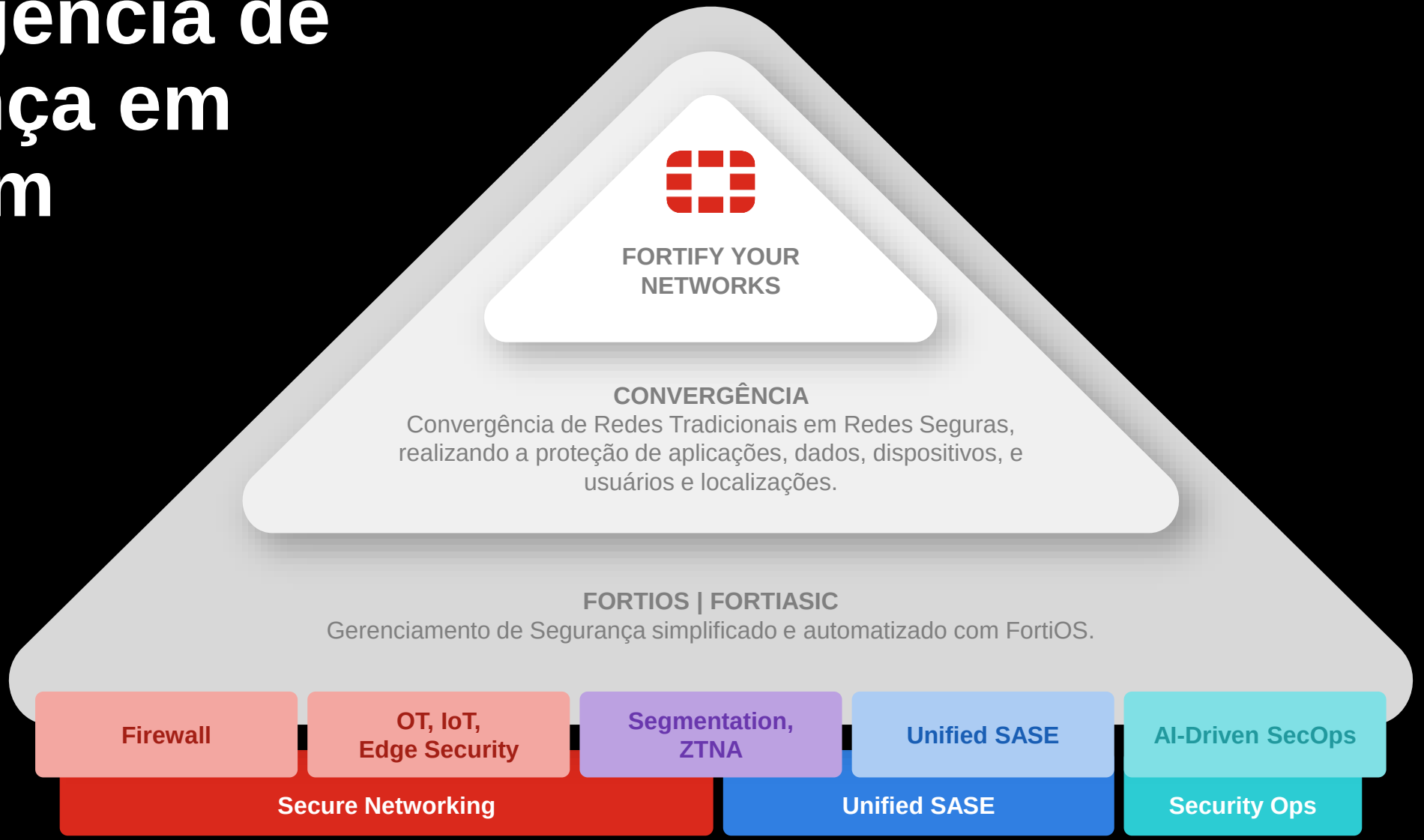
PURPLE TEAM

Cibersegurança Pensada & Feita em Camadas




FORTINET

Convergência de Segurança em Plataform



Nuvem de Inteligência Contra Ameaças

VISIBILIDADE

Telemetry
Network
Web
Sandbox
Email
Endpoint

Enforcement Partnerships

OSINT

Trusted Partnerships

CERTs

Zero-Day

CTA feeds

INOVAÇÃO

AI / Machine Learning

Fortinet Distribution Network

FortiGuard Labs

Detection and protection in milliseconds

Federated Machine Learning

INTELIGÊNCIA CONTRA AMEAÇAS

FORTIGUARD AI-POWERED SECURITY

- IPS
- Application Control
- Web Filtering
- Anti-Virus
- Anti-Spam
- Endpoint Vulnerability
- Indicators of Compromise (IoCs)

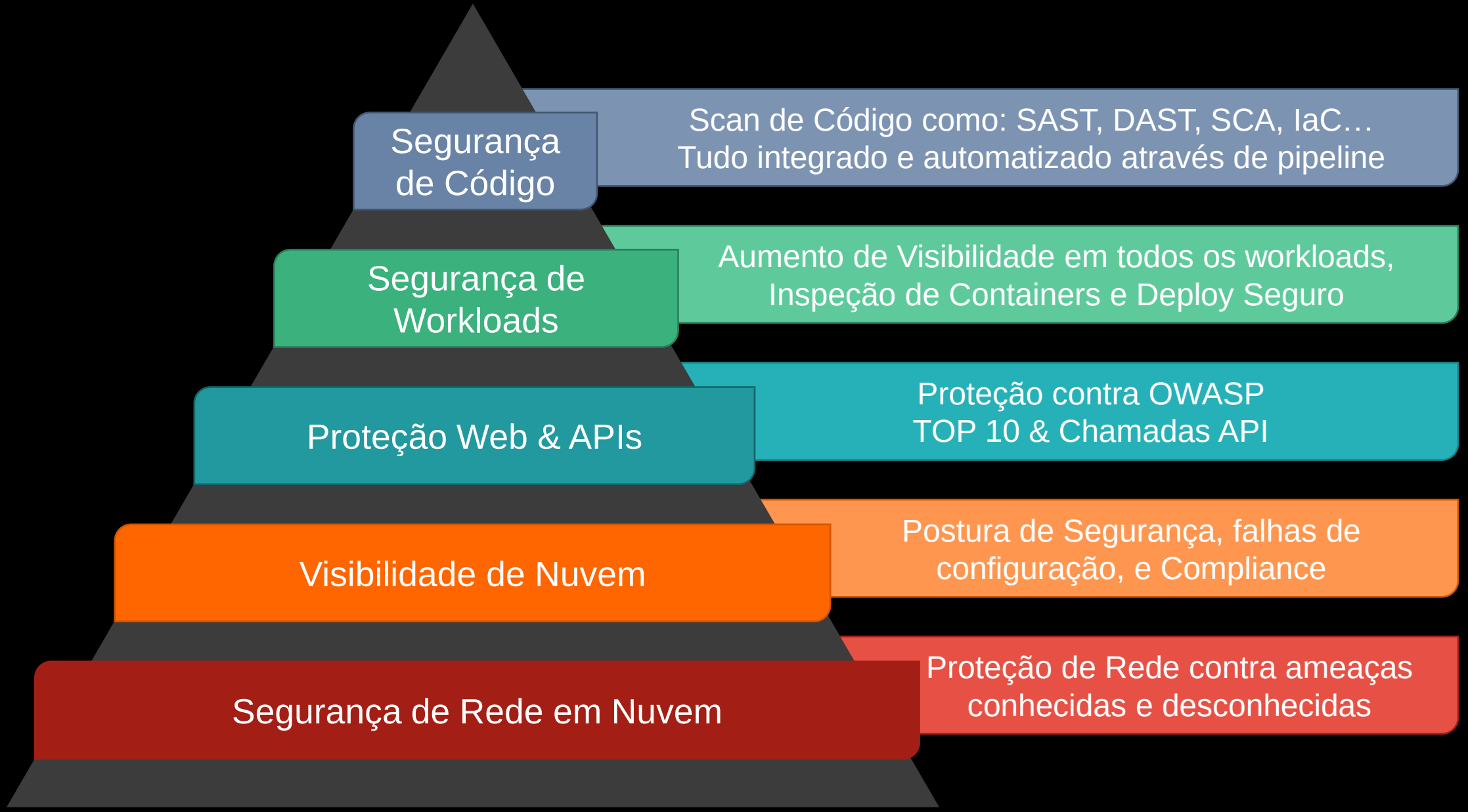
PROACTIVE RESEARCH

- Adversary Playbooks
- Security Blogs
- Threat Intel Briefs
- Threat Signals
- Virtual Patches

THREAT INTELLIGENCE SERVICES

- Penetration Testing
- Phishing Service
- Incident Response
- Detailed Threat Analysis
- Architecture Evaluation
- Cybersecurity Workshops

5 Principais Domínios para Proteção de Nuvem



Log in

Choose an authentication method

Public

Customers and public users please use this authentication method for access.

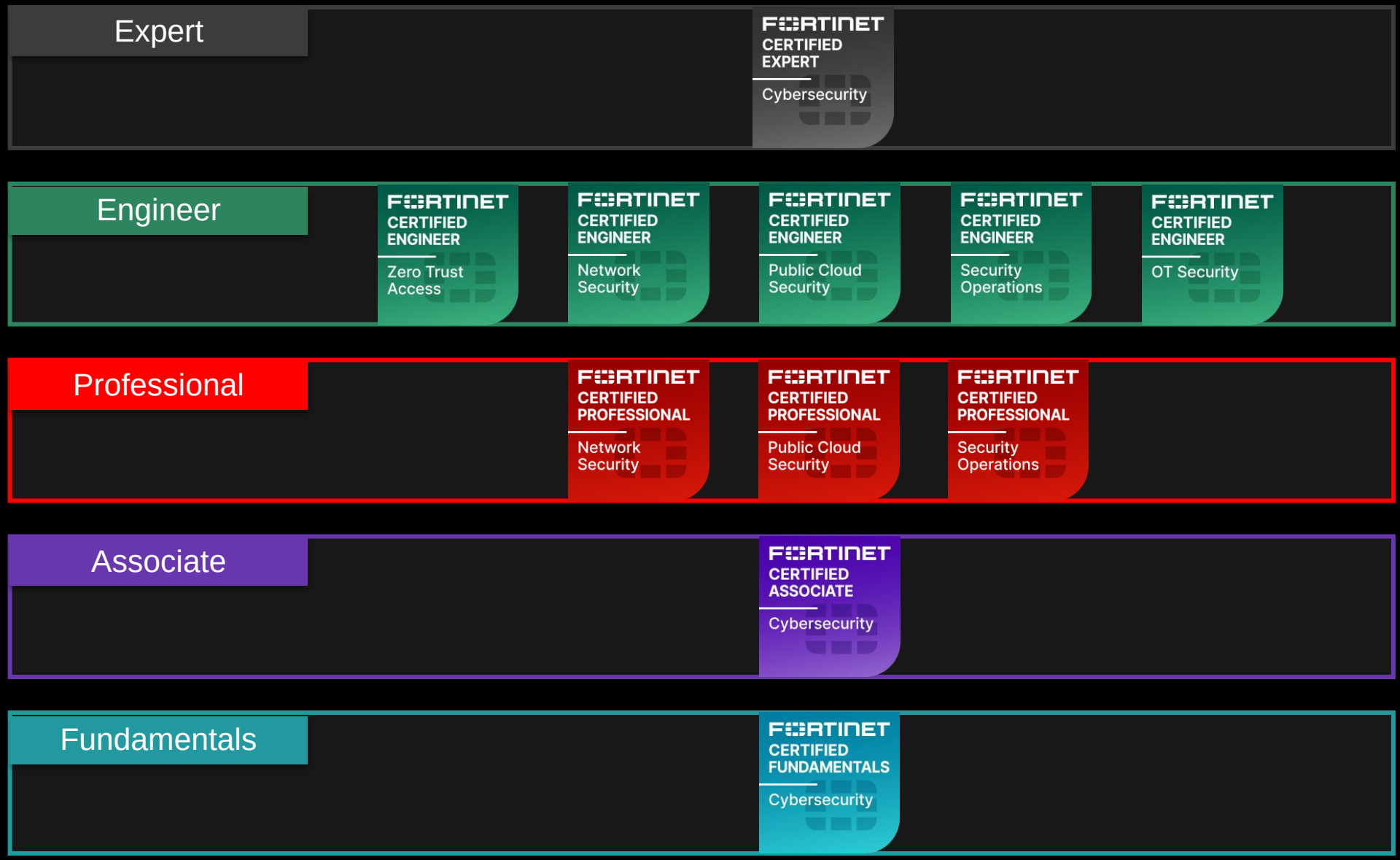
Partner

Partner portal SSO for all Distributors, Advocate, Select, Advanced, Expert and Global level partners.

Employee

Active directory credentials required. FortiToken used for secondary authentication.

Certificações NSE




FORTINET