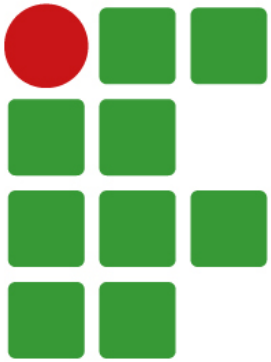


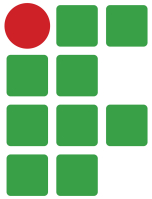
INSTITUTO FEDERAL
DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
São Paulo

ETIR / IFSP: NÚMEROS, AMEAÇAS, RISCOS E VULNERABILIDADES

Ado Cardoso da Silva

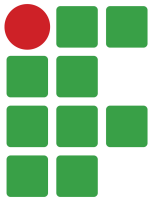
PRD / DTI / CAOTI / ETIR
IFSP

20/06/2023



Sumário

A ETIR EM NÚMEROS (2022/2 E 2023/1)
Quem Somos?!
Pentest (Testes de Segurança Cibernética)
Gerenciamento de Vulnerabilidades
Alertas de ameças, riscos e vulnerabilidades
Respostas a Incidentes
Ações de Educação e Conscientização
Ações de Inteligência sobre Ameaças Cibernéticas
AMEAÇAS E RISCOS (2022/2 E 2023/1)
Ameaças, Riscos e Vulnerabilidades
Exposição de Serviços Sensíveis
Exposição de Credenciais
PLANOS FUTUROS ETIR/IFSP
DÚVIDAS



QUEM SOMOS?! - 2022/2 - 2023/1

A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, um grupo de trabalho permanente, multidisciplinar, **de atuação primordialmente reativa e não exclusiva.**

A ETIR do IFSP é formada atualmente por 6 integrantes:

- **4 representantes da DTI** (Diretoria de Tecnologia da Informação) ou seus setores componentes, sendo um designado agente responsável:
  - **Rafael Manochio (Agente Responsável)**
  - Ado Cardoso da Silva
  - Gabriel Gracioso Remondini
  - William Lira Ferreira
- **2 representantes do CTIC** (Comitê de Tecnologia da Informação);
  - Dirlei Paulino Pinto
  - Matheus Cavecci

Nosso público alvo:

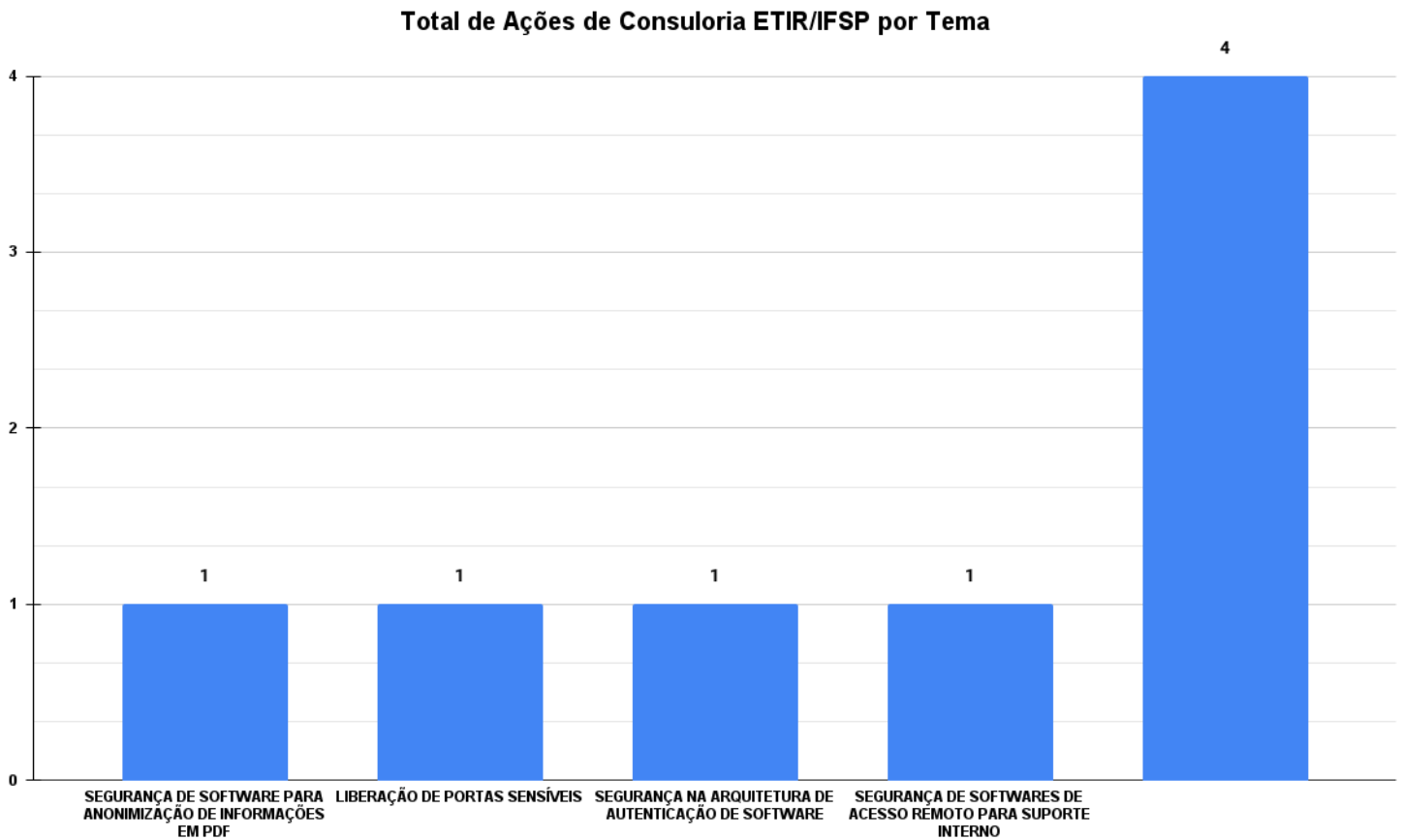
- A ETIR atenderá diretamente todas as unidades da Diretoria de Tecnologia da Informação, por convocação ou chamado registrado eletronicamente.
- A ETIR atenderá indiretamente e pontualmente aos demais setores da Reitoria do IFSP e as Coordenadorias de Tecnologia da Informação (CTIs) dos Campus do IFSP, atuando, inicialmente de forma consultiva, por convocação ou chamado registrado eletronicamente, sempre com prévia autorização da Chefia Imediata da Coordenadoria de Arquitetura e Operações de Tecnologia da Informação (CAOTI).

Nossa responsabilidade:

- Gestão centralizada para tratamento de incidentes de segurança em redes computacionais;
- Estabelecer um ponto central para comunicação de vulnerabilidades e registros de incidentes em redes computacionais;
- Realizar ações preventivas aos incidentes em redes computacionais;
- Propor melhorias contínuas nos processos, serviços, sistemas e infraestrutura em relação a segurança em Redes de Computadores.
- Analisar, Investigar e tratar incidentes de segurança em redes computacionais;
- Definir planos de contenção e estabelecer ações para promover a continuidade dos serviços e sistemas em caso de incidentes graves;
- Acompanhar de forma objetiva a evolução e o domínio dos aspectos da segurança em Redes de Computadores;

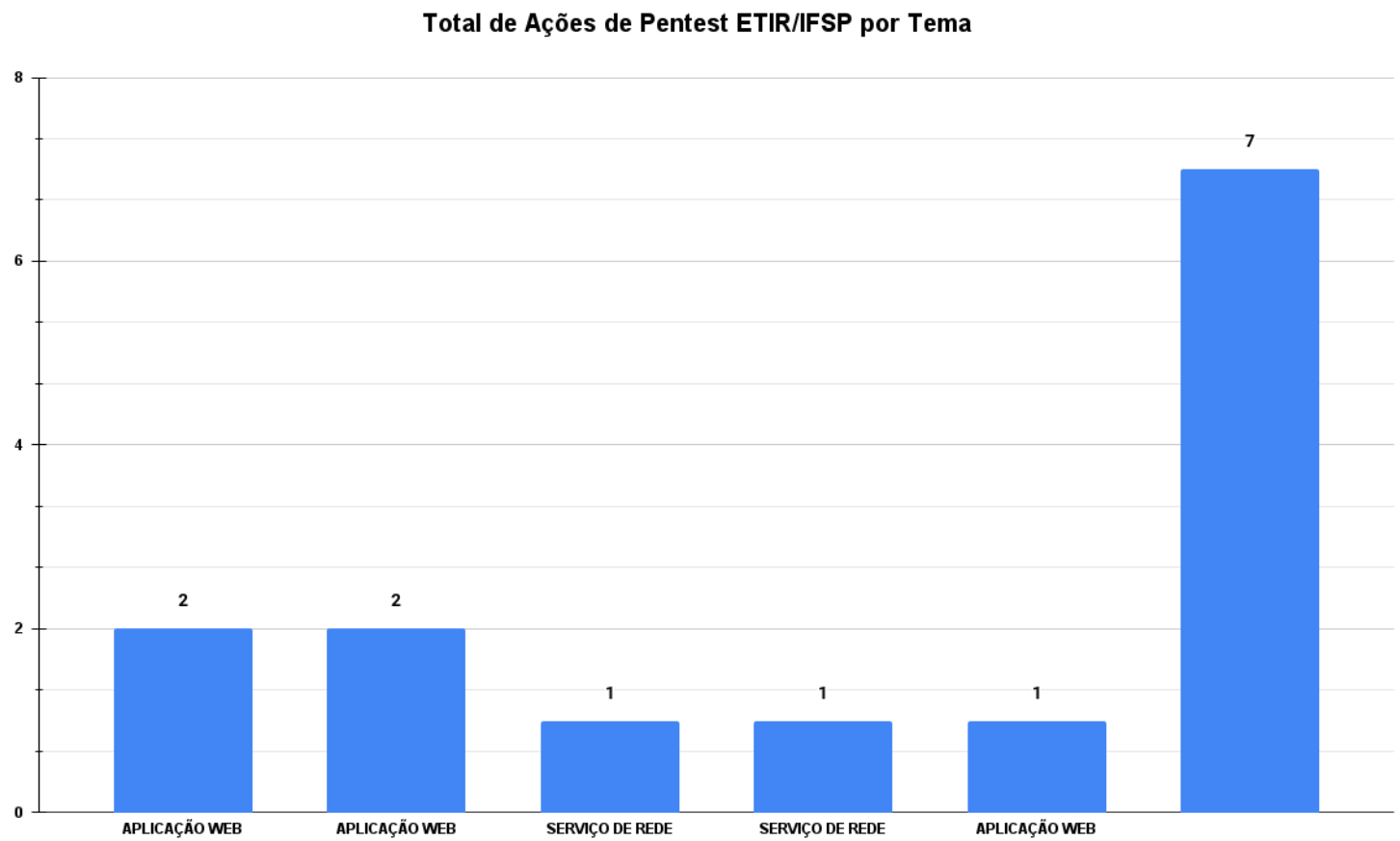
CONSULTORIAS - 2022/2 - 2023/1

- Apoio a necessidades institucionais em que seja necessário o esclarecimento de temas relacionados à segurança cibernética.



PENTEST (TESTES DE SEGURANÇA CIBERNÉTICA) - 2022/2 - 2023/1

- Metologia adaptada ao cenário do IFSP, com 4 fases macro, baseadas na OWASP e no PTES.
  - Pentest em aplicações e serviços, com ações manuais e automatizadas.

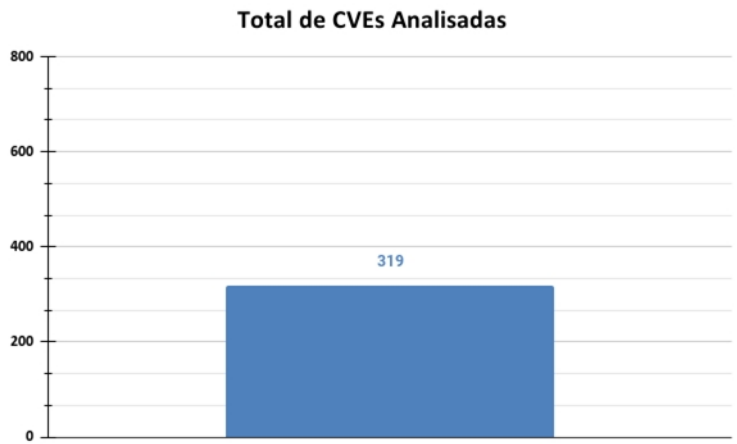


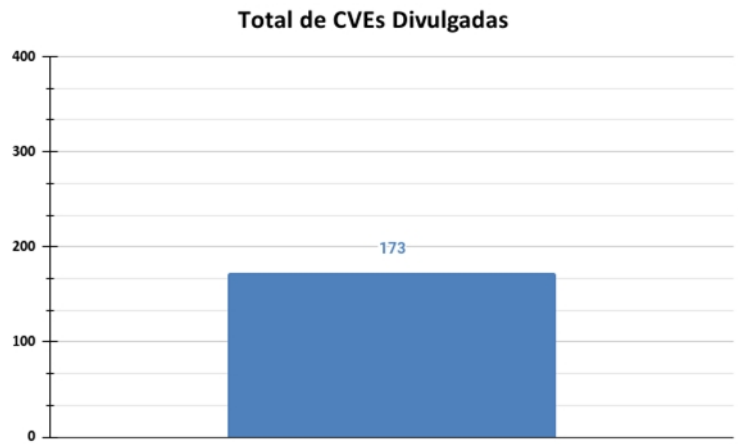
PROCESSO VOLTADO AO NEGÓCIO:

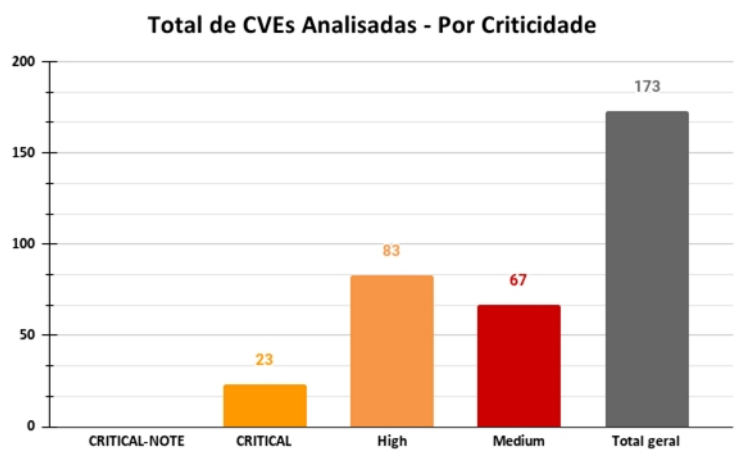
- Não são divulgadas todas as vulnerabilidades analisadas, evitando um excesso de informações e alardes internos sem necessidade.
- Recebemos a informaçoes das diversas fontes (alertas de fornecedores, testes de segurança, ações de inteligências, fontes de inteligência externas e internas, feeds, usuários, etc);
- **ATENÇÃO À COLABORAÇÃO (responsabilidade de todos, sem centralização);**
- Verificamos individualmente quais estão ligadas aos fornecedores e tecnologias de soluções que o IFSP possui;
- Verificamos qual o real impacto interno e a criticidade para a Instituição.
- Classificamos, catalogamos, priorizamos e divulgamos.

GERENCIAMENTO DE VULNERABILIDADES - 2022/2 - 2023/1

- Vulnerabilidades divulgadas por fornecedores de tecnologias e serviços comuns no ambiente do IFSP:
  - CVE - Common Vulnerabilities and Exposures - Toda vulnerabilidade identificada, confirmada e catalogada por um fornecedor, recebe um número rastreador, referência para explicá-la e contê-la.

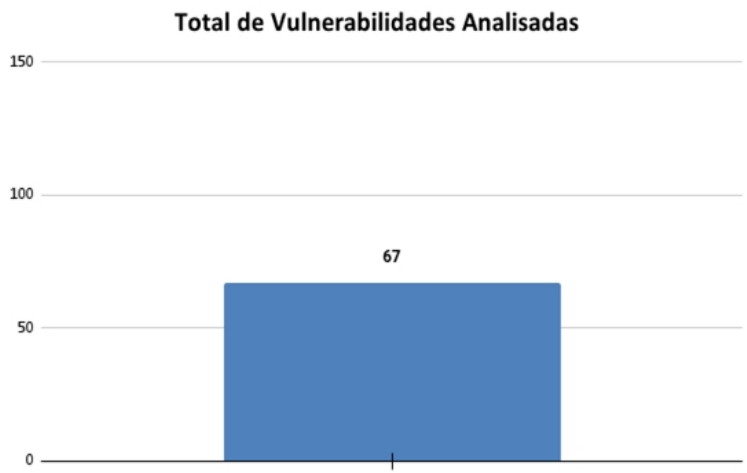


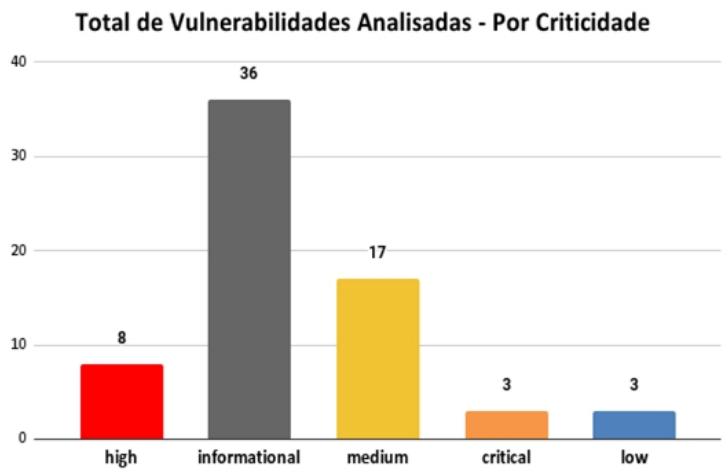




GERENCIAMENTO DE VULNERABILIDADES - 2022/2 - 2023/1

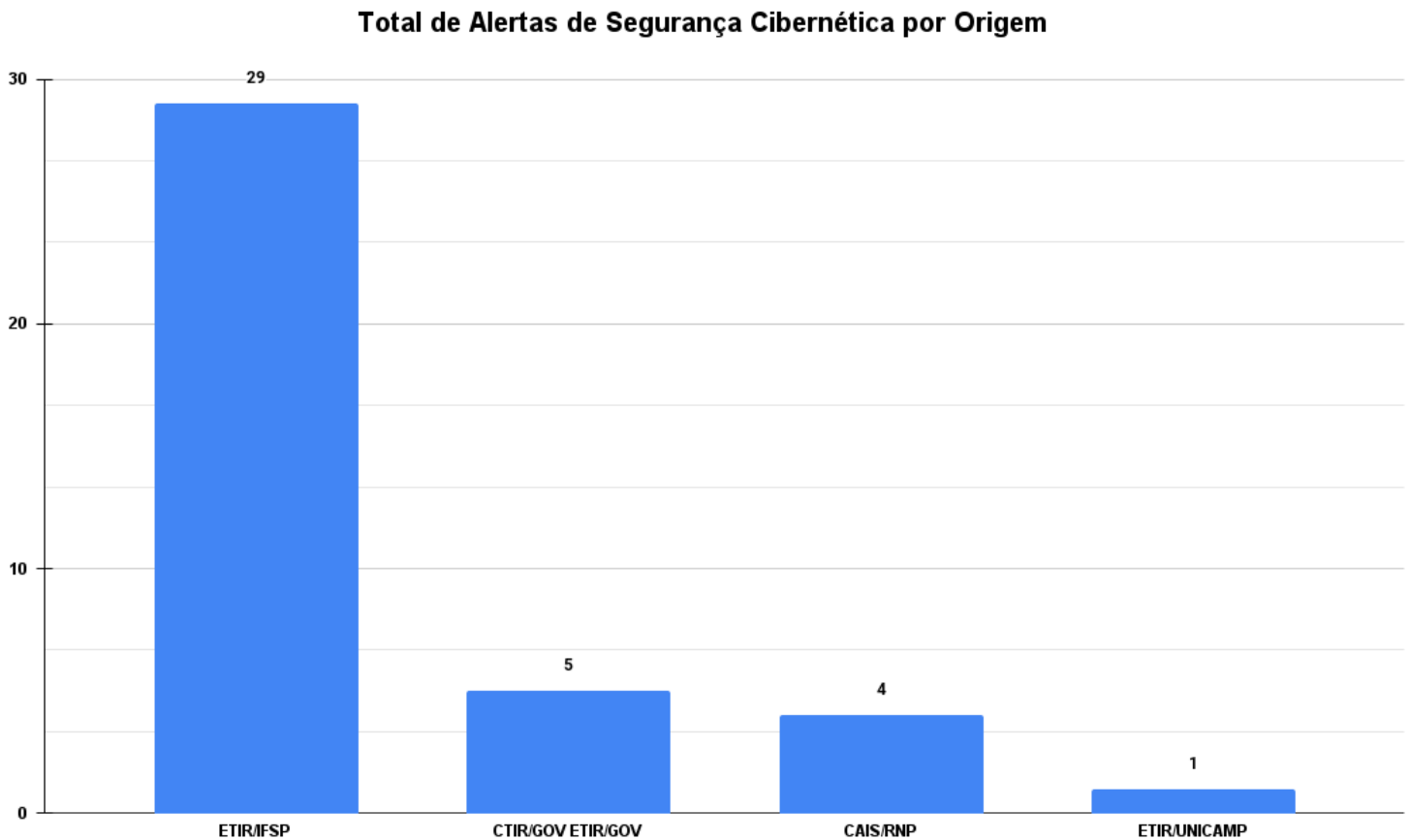
- Vulnerabilidades identificadas através de Pentest, Ações de inteligência sobre ameças e informadas por usuários:





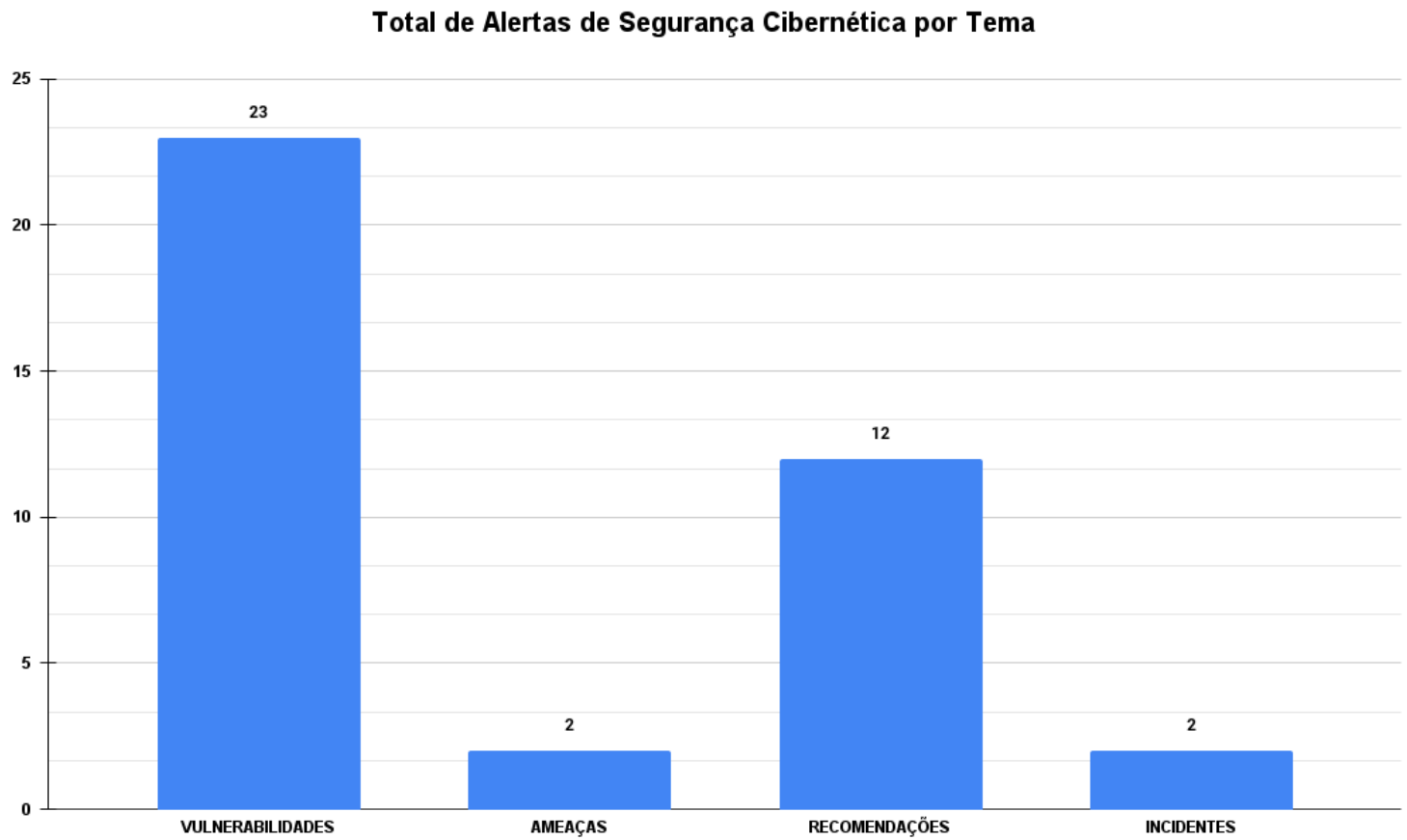
ALERTAS DE AMEAÇAS, RISCOS E VULNERABILIDADES - 2022/2 - 2023/1

- Divulgar alertas/comunicados, pesquisar sobre ameaças e soluções para contê-las, e informar às áreas responsáveis.
  - Parte do processo de Gerenciamento de Vulnerabilidades.
    - 39 Alertas / Comunicados



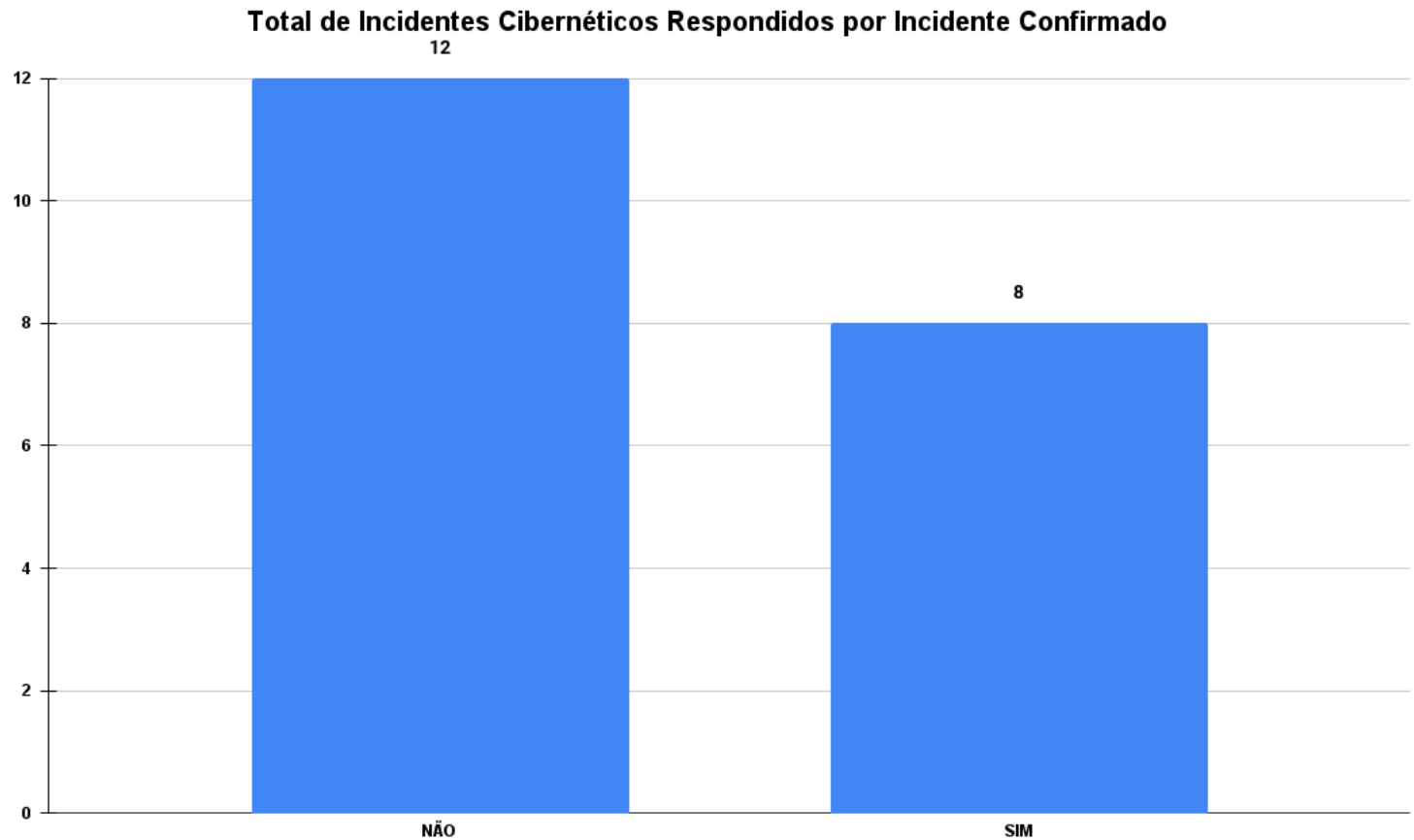
ALERTAS DE AMEAÇAS, RISCOS E VULNERABILIDADES - 2022/2 - 2023/1

- Divulgar alertas/comunicados, pesquisar sobre ameaças e soluções para contê-las, e informar às áreas responsáveis.
  - Parte do processo de Gerenciamento de Vulnerabilidades.
    - 39 Alertas / Comunicados



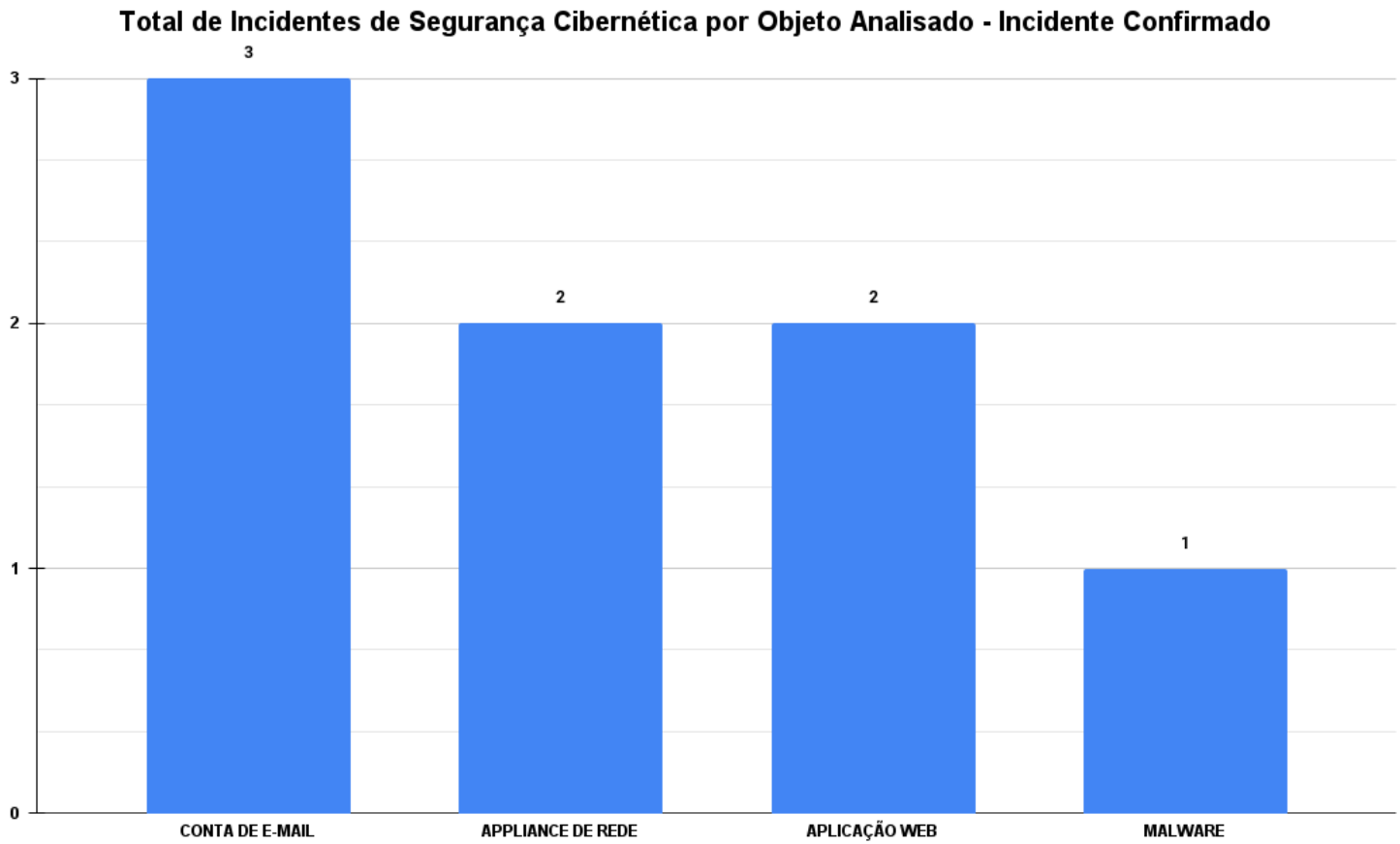
RESPOSTAS A INCIDENTES - 2022/2 - 2023/1

- Incidente de Segurança Cibernética é um evento adverso, confirmado ou suspeito, relacionado à segurança dos sistemas ou das redes de computadores do IFSP.
  - 20 Respostas a incidentes cibernéticos



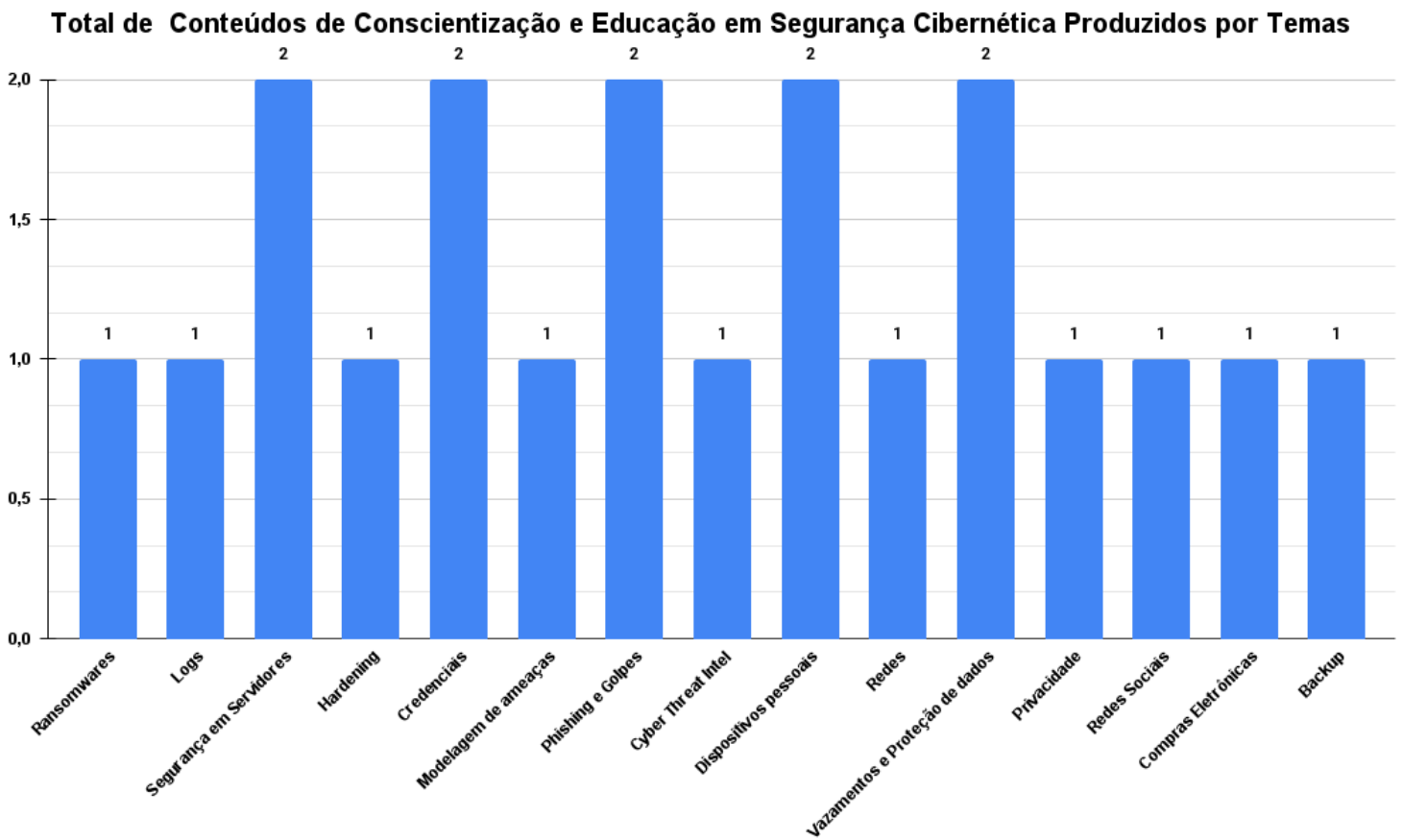
RESPOSTAS A INCIDENTES - 2022/2 - 2023/1

- Incidente de Segurança Cibernética é um evento adverso, confirmado ou suspeito, relacionado à segurança dos sistemas ou das redes de computadores do IFSP.
  - 8 Respostas a incidentes cibernéticos de segurança



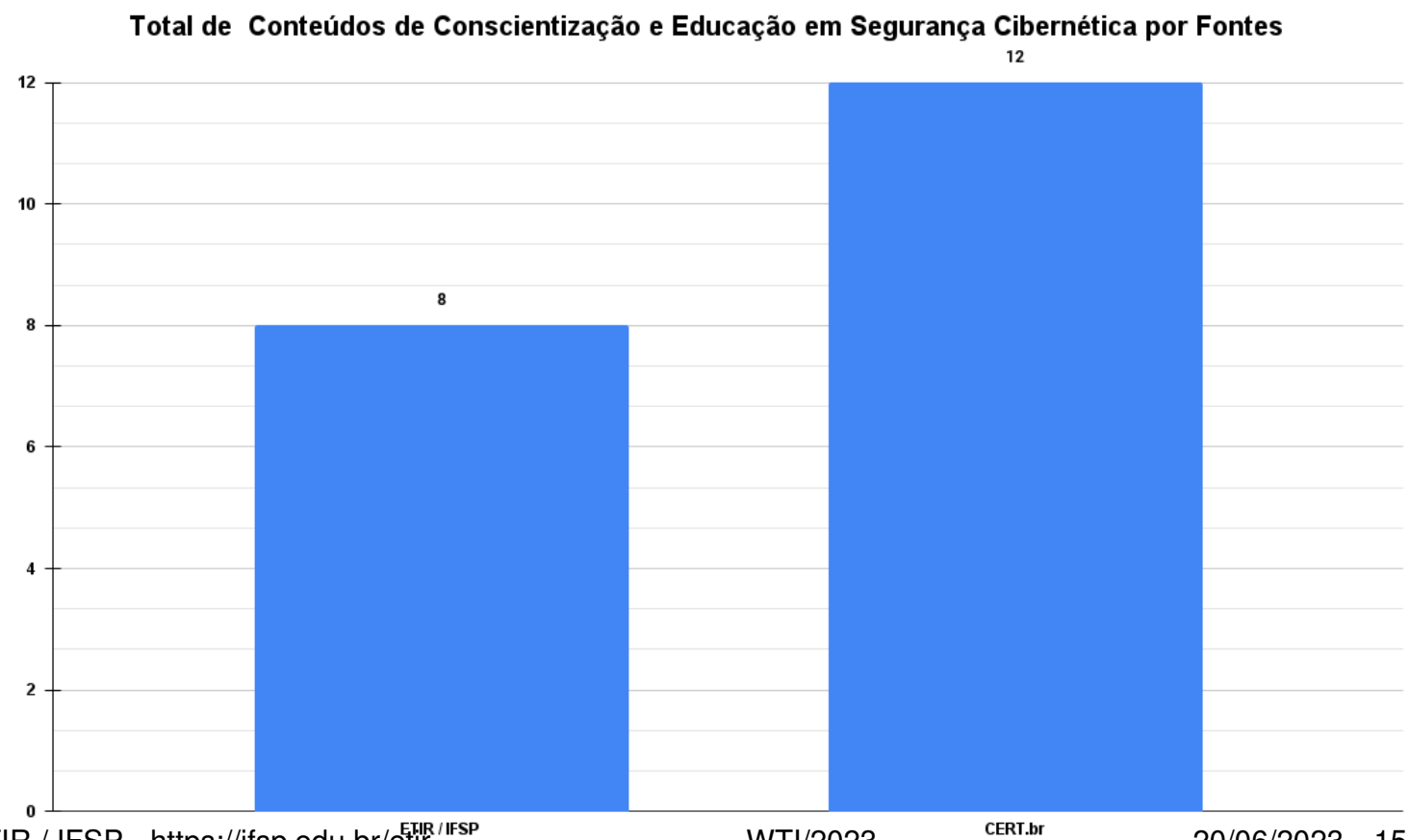
AÇÕES DE EDUCAÇÃO E CONSCIENTIZAÇÃO - 2022/2 - 2023/1

- Conscientização do público institucional, através de temas que se relacionem à segurança da informação e as rotinas administrativas e acadêmicas.
  - 20 Ações de Conscientização e Educação de Segurança Cibernética.



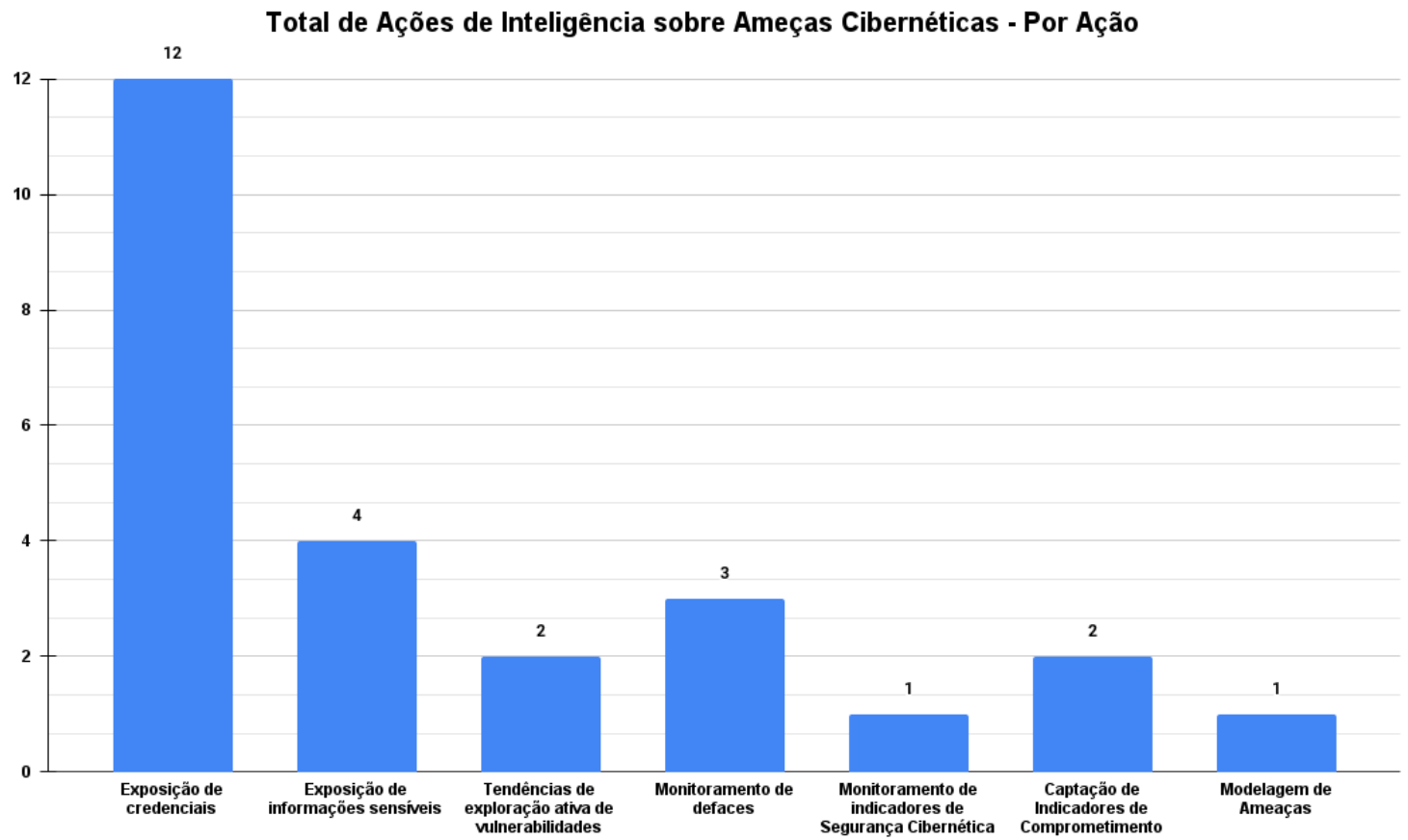
AÇÕES DE EDUCAÇÃO E CONSCIENTIZAÇÃO - 2022/2 - 2023/1

- Conscientização do público institucional, através de temas que se relacionem à segurança da informação e as rotinas administrativas e acadêmicas.
  - Parceria com a Comunicação do IFSP.
  - 20 Ações de Conscientização e Educação de Segurança Cibernética.



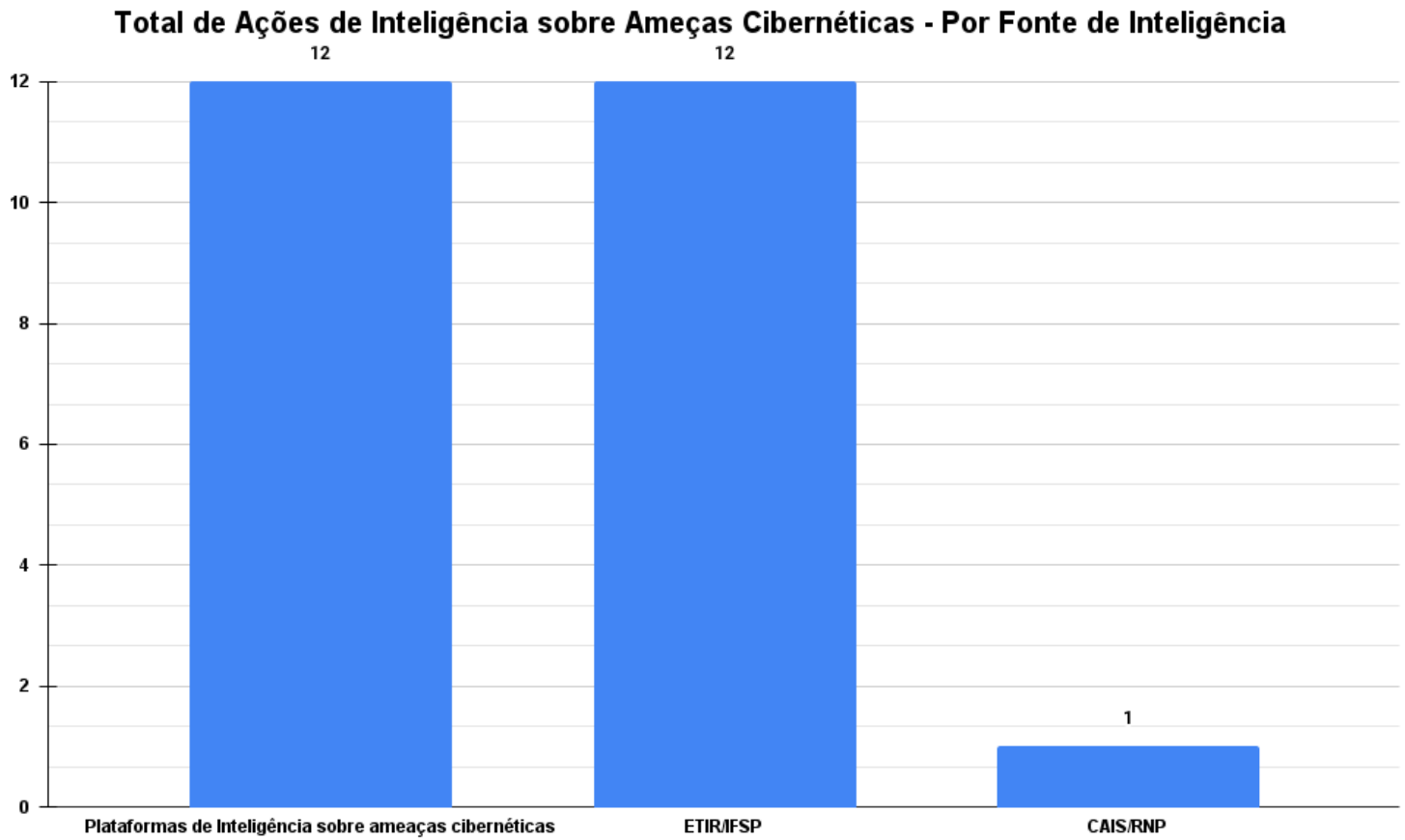
AÇÕES DE INTELIGÊNCIA SOBRE AMEAÇAS CIBERNÉTICAS - 2022/2 - 2023/1

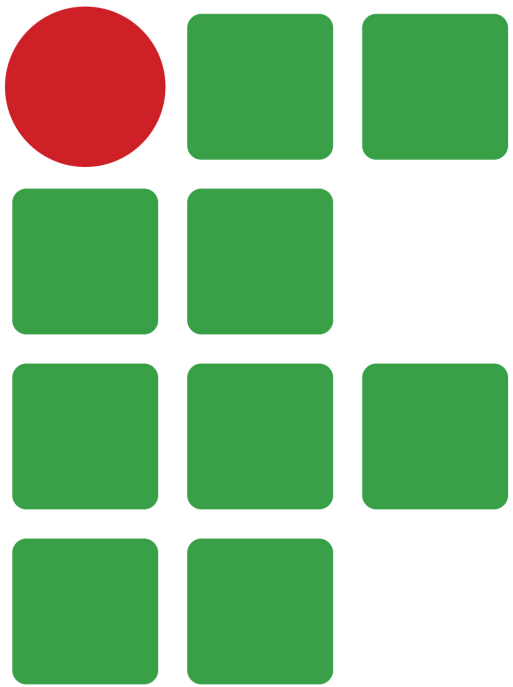
- Processos manuais ou automatizados buscando por ameaças ao ambiente interno e externo, antecipando incidentes de segurança em redes de computadores.
  - 25 Ações de Inteligência Cibernética sobre Ameaças. (Cyber Threat Intel - CTI)

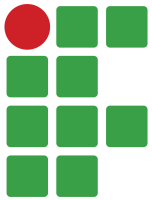


AÇÕES DE INTELIGÊNCIA SOBRE AMEAÇAS CIBERNÉTICAS - 2022/2 - 2023/1

- Processos manuais ou automatizados buscando por ameaças ao ambiente interno e externo, antecipando incidentes de segurança em redes de computadores.
  - 25 Ações de Inteligência Cibernética sobre Ameaças. (Cyber Threat Intel - CTI)







AMEAÇAS, RISCOS e VULNERABILIDADES

AMEAÇAS

- EXTERNAS e/ou INTERNAS.
- MAPEADAS, mas geralmente FORA DO CONTROLE.
- **Ex:** Atacantes (externos/internos), 0-days, novas vulnerabilidades, novas técnicas, etc.

RISCOS

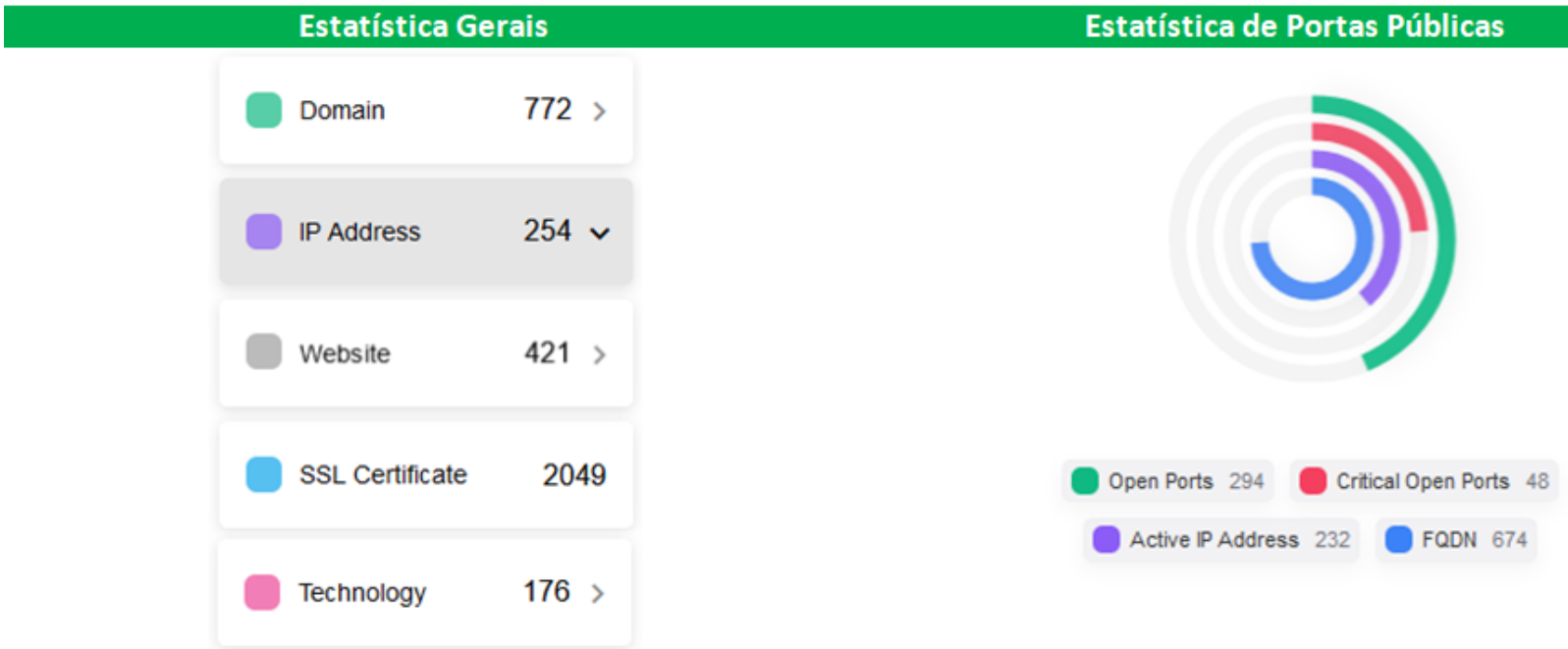
- EXTERNOS e/ou INTERNOS.
- MINIMIZADOS/MITIGADOS, geralmente CONTROLÁVEIS.
- **Se podemos controlá-los, por que nos sujeitamos?**
- **Ex:** Exposições **serviços/portas/informações sensíveis** (acessos a informações ou ambientes críticos, direta ou indiretamente. **Ex: ssh, telnet, rdp, ftp, ldap, rpc, netbios, smb, interfaces admin, databases, manuais técnicos, etc);**
- Teoria do feriado prolongado. Risco mas não vulnerabilidade?!

VULNERABILIDADE = RISCO + EXPOSTO A AMEÇAS

- ETIR ALERTA SOBRE AMEAÇAS! ANALISE SEUS RISCOS.
- Vulnerabilidade não é só CVE. É uma SITUAÇÃO/ESTADO.

EXPOSIÇÃO DE SERVIÇOS SENSÍVEIS

- **Resumo de como nos veem de fora. (vulgo ameaças)**

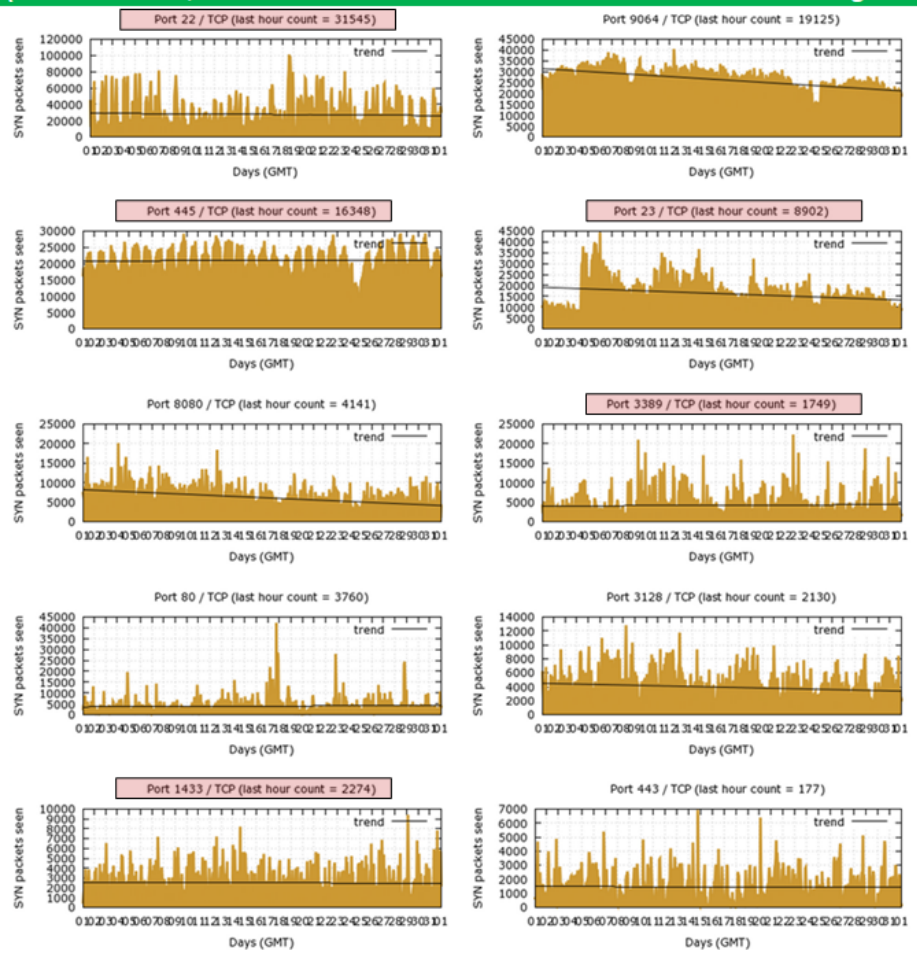


- **EXPOSIÇÃO(RISCO) + AMEAÇAS = VULNERABILIDADE**

EXPOSIÇÃO DE SERVIÇOS SENSÍVEIS

- **Inteligência Cibernética e Prevenção, na prática:**
  - **Dados do mês de Janeiro de 2015**

Portas exploradas – honeyTARG – CERT.br – https://honeytarg.cert.br/honeypots/
Sensores espalhados por várias Universidades e empresas brasileiras
(dos 49 sensores, 16 estão no estado de SP = Nossa realidade educacional e regional)



EXPOSIÇÃO DE SERVIÇOS SENSÍVEIS

Inteligência Cibernética e Prevenção, na prática:

- **Dados do mês de junho de 2023**

Destination TCP Ports -- 2023-06-12 UTC

#	Key	Port	Name	Total		Max	Avg
01		23	TELNET	2.45 GB	92.11 %	49.72 KB/s	28.32 KB/s
02		22	SSH (Secure Shell)	41.92 MB	1.58 %	836.87 B/s	485.15 B/s
03		445	Microsoft-DS Active Directory	31.32 MB	1.18 %	473.72 B/s	362.49 B/s
04		3389	RDP (Microsoft Terminal Server)	19.25 MB	0.72 %	1.99 KB/s	222.85 B/s
05		80	HTTP (Hypertext Transfer Protocol)	8.59 MB	0.32 %	477.80 B/s	99.47 B/s
06		443	HTTPS (Hypertext Transfer Protocol over TLS/SSL)	5.38 MB	0.20 %	649.66 B/s	62.24 B/s
07		8080	HTTP Proxy	2.56 MB	0.10 %	173.14 B/s	29.63 B/s
08		1433	Microsoft SQL Server	2.14 MB	0.08 %	50.33 B/s	24.73 B/s
09		3306	MySQL	1.45 MB	0.05 %	76.78 B/s	16.75 B/s
10		21	FTP (File Transfer Protocol - control)	1.35 MB	0.05 %	314.77 B/s	15.62 B/s

Destination TCP Ports -- 2023-06-13 UTC

#	Key	Port	Name	Total		Max	Avg
01		23	TELNET	3.10 GB	93.72 %	55.07 KB/s	35.83 KB/s
02		445	Microsoft-DS Active Directory	35.98 MB	1.09 %	728.46 B/s	416.46 B/s
03		22	SSH (Secure Shell)	30.74 MB	0.93 %	1.65 KB/s	355.80 B/s
04		443	HTTPS (Hypertext Transfer Protocol over TLS/SSL)	10.17 MB	0.31 %	1.49 KB/s	117.75 B/s
05		80	HTTP (Hypertext Transfer Protocol)	9.78 MB	0.30 %	460.50 B/s	113.14 B/s
06		3389	RDP (Microsoft Terminal Server)	7.75 MB	0.23 %	227.74 B/s	89.69 B/s
07		8080	HTTP Proxy	3.59 MB	0.11 %	381.68 B/s	41.52 B/s
08		1433	Microsoft SQL Server	1.84 MB	0.06 %	70.84 B/s	21.29 B/s
09		3306	MySQL	1.51 MB	0.05 %	77.90 B/s	17.42 B/s
10		21	FTP (File Transfer Protocol - control)	1.31 MB	0.04 %	190.45 B/s	15.13 B/s

Destination TCP Ports -- 2023-06-14 UTC

#	Key	Port	Name	Total		Max	Avg
01		23	TELNET	2.87 GB	91.30 %	69.30 KB/s	33.21 KB/s
02		445	Microsoft-DS Active Directory	41.85 MB	1.33 %	652.67 B/s	484.40 B/s
03		22	SSH (Secure Shell)	17.79 MB	0.57 %	550.12 B/s	205.88 B/s
04		80	HTTP (Hypertext Transfer Protocol)	9.71 MB	0.31 %	860.94 B/s	112.43 B/s
05		3389	RDP (Microsoft Terminal Server)	7.31 MB	0.23 %	283.99 B/s	84.62 B/s
06		443	HTTPS (Hypertext Transfer Protocol over TLS/SSL)	6.99 MB	0.22 %	495.67 B/s	80.86 B/s
07		8080	HTTP Proxy	3.32 MB	0.11 %	149.46 B/s	38.38 B/s
08		1433	Microsoft SQL Server	1.93 MB	0.06 %	57.38 B/s	22.38 B/s
09		139	NETBIOS Session Service	1.67 MB	0.05 %	164.55 B/s	19.28 B/s
10		3306	MySQL	1.54 MB	0.05 %	83.15 B/s	17.82 B/s

Destination TCP Ports -- 2023-06-15 UTC

#	Key	Port	Name	Total		Max	Avg
01		23	TELNET	2.76 GB	86.50 %	53.56 KB/s	31.93 KB/s
02		443	HTTPS (Hypertext Transfer Protocol over TLS/SSL)	158.38 MB	4.97 %	5.22 KB/s	1.83 KB/s
03		445	Microsoft-DS Active Directory	32.42 MB	1.02 %	872.43 B/s	375.29 B/s
04		22	SSH (Secure Shell)	29.82 MB	0.93 %	699.76 B/s	345.15 B/s
05		139	NETBIOS Session Service	9.41 MB	0.30 %	835.49 B/s	108.96 B/s
06		80	HTTP (Hypertext Transfer Protocol)	9.33 MB	0.29 %	383.38 B/s	107.98 B/s
07		3389	RDP (Microsoft Terminal Server)	5.72 MB	0.18 %	283.75 B/s	66.26 B/s
08		8080	HTTP Proxy	3.46 MB	0.11 %	171.90 B/s	40.05 B/s
09		1433	Microsoft SQL Server	1.94 MB	0.06 %	94.61 B/s	22.49 B/s
10		21	FTP (File Transfer Protocol - control)	1.80 MB	0.06 %	506.58 B/s	20.79 B/s

EXPOSIÇÃO DE SERVIÇOS SENSÍVEIS

- **Inteligência Cibernética e Prevenção, na prática:**
  - **Portas críticas reforçadas pela ETIR/IFSP**
    - **Não taxativas. Mais importante do que uma lista de portas, é o que discutimos até aqui...**
    - **A teoria do FDS e do Poder de Reação**

SERVIÇO	PORTA
TELNET	23
SSH	22
Microsoft AD, SAMBA, RPC	445 / 139 / 135 / 137 / 138
RDP (Área de Trabalho Remota do Windows)	3389
BD SQL Server	1433
BD MySql / MariaDB	3306
POSTGRESQL	5432
FTP	21
LDAP	636 / 389
WEBMIN	10000
PROXMOX	8006
ACESSOS A GERENCIAMENTOS REMOTOS	80/443
VNC	5900

- ***O objetivo da ETIR/IFSP, no aspecto de serviços, não é reprimir, mas analisar, alertar e buscar soluções SEGURAS conjuntas.***

EXPOSIÇÃO DE SERVIÇOS SENSÍVEIS

Prevenção

- CONSCIÊCIA;
- CONHECIMENTO;
- BOAS PRÁTICAS (PÁGINA ETIR);
- ATUALIZAÇÕES PERIÓDICAS;
- ATENÇÃO A VUNERABILIDADES DA TECNOLOGIA;

Reação

- CENÁRIOS DIVERSOS. VALE UMA CONSULTA À ETIR.
  - Possuímos alguns playbooks e runbooks (ações e atividades) para reações a alguns incidentes.
- MAS NO GERAL:
  - Isolamento do host;
  - Altere as credenciais técnicas que o host utilizava, se forem utilizadas em outros hosts;
  - Atenção com as credenciais de usuários que o host armazenava;
  - Atenção com o conteúdo que o host possuia e pode ter sido roubado;
  - Acessos deste a outros host;

- **Um incidente pode levar ao próximo tópico!**

EXPOSIÇÃO DE CREDENCIAIS

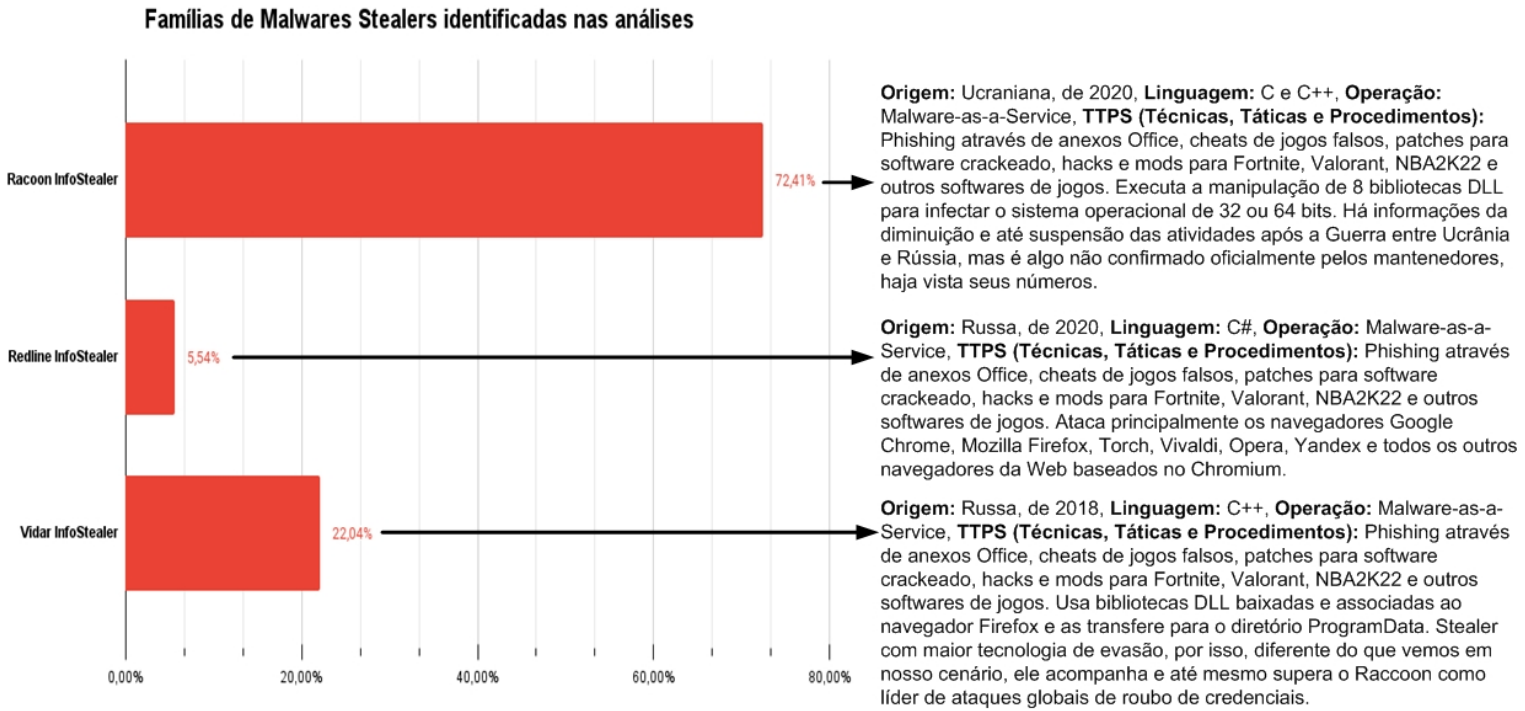
Principais motivos identificados:

- Utilização de senhas fáceis e já conhecidas;
- Ação de malwares (vírus) em seus dispositivos;
- Interações com phishing (mensagens falsas com links maliciosos, através de e-mails, aplicativos de mensagem, etc);
- Uso dessas credenciais em sites de terceiros, cujas bases de dados foram indevidamente clonadas por criminosos;

EXPOSIÇÃO DE CREDENCIAIS

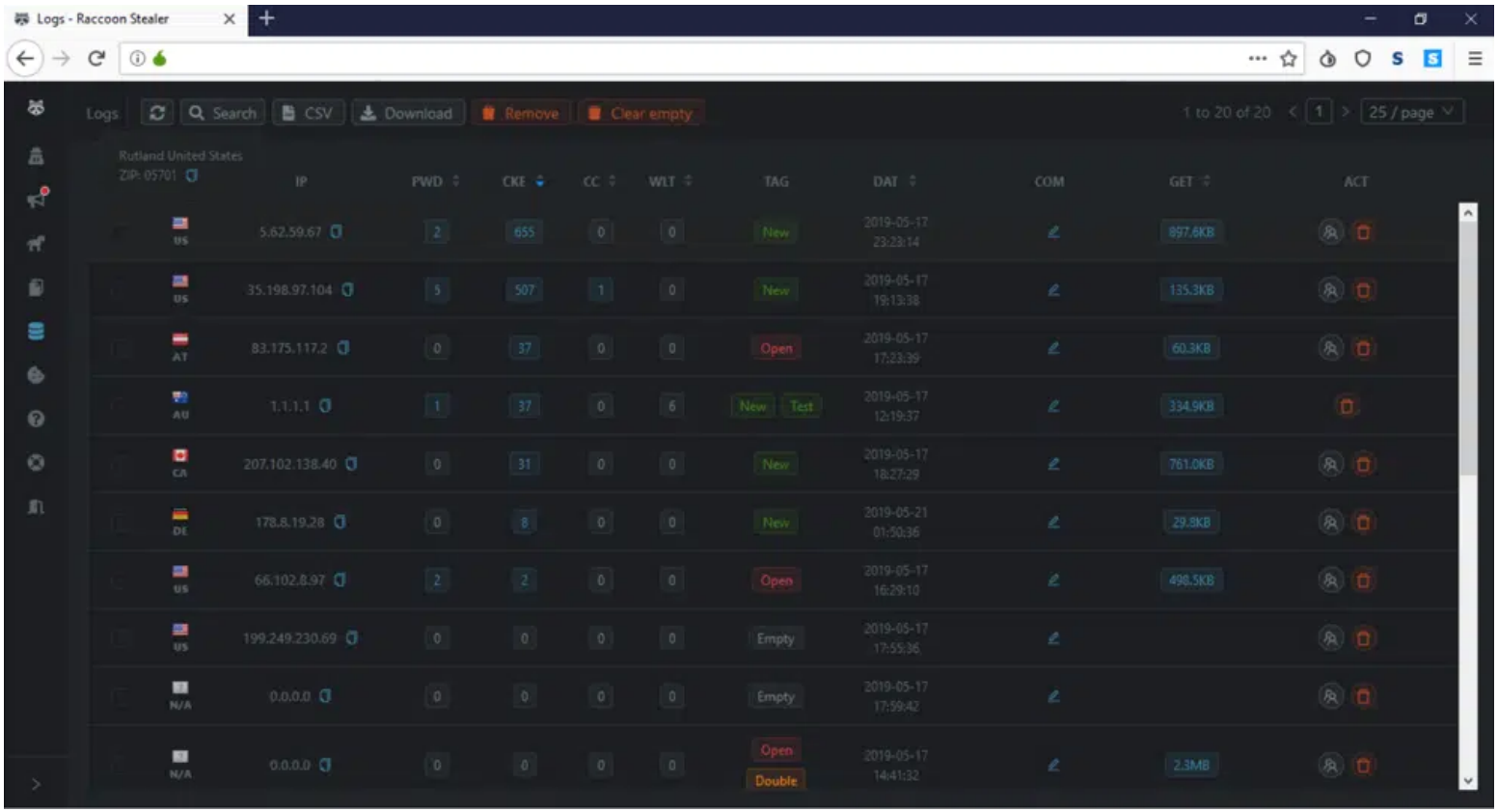
Os maiores vilões! MALWARES STEALERS

- O estudo da ETIR/IFSP.
- O que são Stealers?
  - Famílias identificadas nas análises
- Mercados de acessos iniciais (LapsusS e Operadores de Ransomwares)



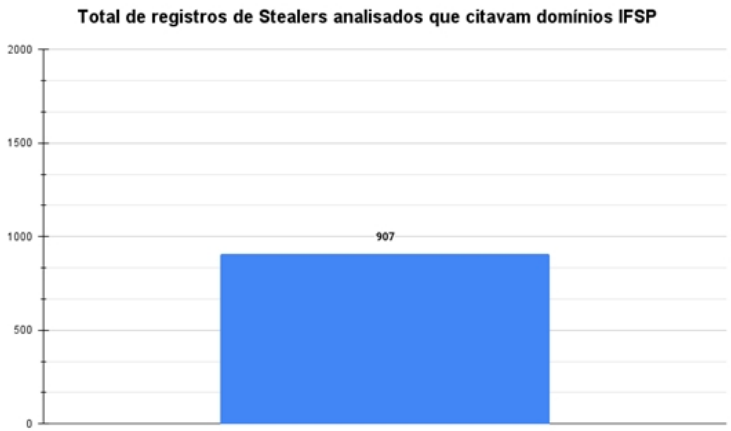
EXPOSIÇÃO DE CREDENCIAIS

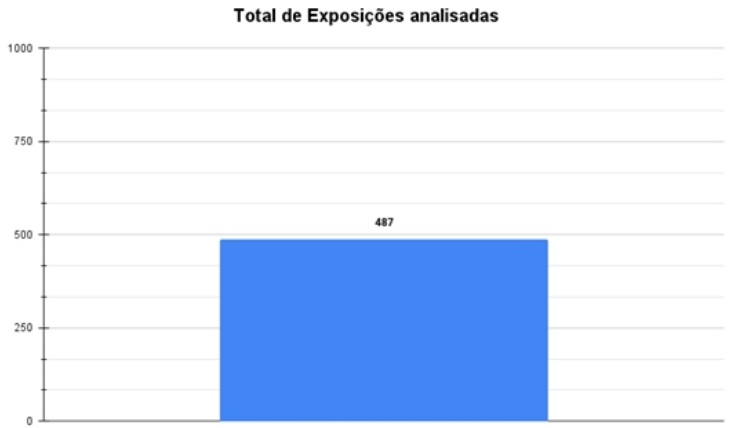
- Captura de tela da DashBoard de Comando e Controle do Raccoon.



EXPOSIÇÃO DE CREDENCIAIS

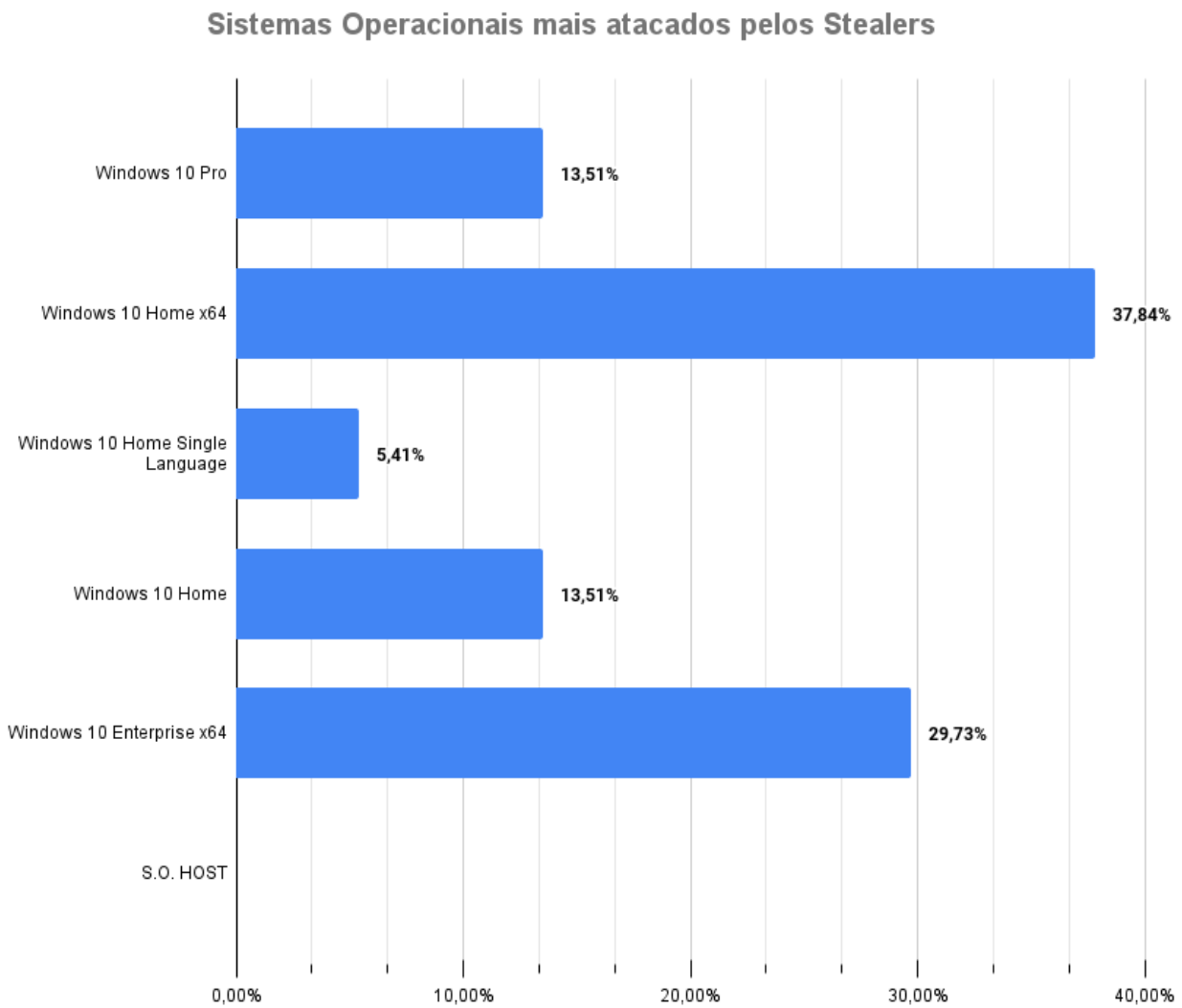
- Total de registros analisados pelas plataformas de inteligência: Logs de Stealer, Indícios e identificação de credenciais





EXPOSIÇÃO DE CREDENCIAIS

- Sistemas Operacionais Afetados:



EXPOSIÇÃO DE CREDENCIAIS

PREVENÇÃO INSTITUCIONAL E GERAL:

- Conscientização contra **PHISHING** e uso de **SOFTWARES/JOGOS PIRATAS** e **CRACKS**.(Stealers extrapolam limites institucionais);

Prevenção Institucional:

- **Revisão periódica de acessos e permissões**;
  - **Privilegiados** (T.I. e não T.I.);
  - **Sites/Portais** (Revisão de publicadores e administradores);
  - **Acessos à VPN local** (usuários e suas permissões);
  - **Acesso ao LDAP local** (usuários e suas permissões);
  - **Acesso aos Sistemas locais;**
    - Quem pode acessar?
    - Até quando pode acessar?
- **Padronização da infraestrutura local;**
  - Sugerida pela CAOTI do IFSP.
    - ETIR analisou dados de incidentes reportados pelos CAIS/RNP e os identificados em suas ações, constatou que nos ambientes padronizados o número de incidentes é extremamente menor.
  - Incidentes envolvendo a RNP como provedor, são mínimos.
  - NGFW inteligente para impedir o contato com o controle.

EXPOSIÇÃO DE CREDENCIAIS

REAÇÃO INSTITUCIONAL - INTERNA:

- **Protocolo de credenciais comprometidas em geral:**
  - Cenário - Detecções automatizadas Google
    - Vazamentos;
    - Spam;
  - Cenário - Detecções por Ações Threat Intel ETIR;
  - Cenário - Detecções pelos usuários;
  - Demais cenários
    - Qualquer suspeita deve ser registrada com um chamado no suporte, para acionamento do protocolo de credenciais comprometidas.
    - Acessos locais devem ser imediatamente suspensos e tomadas as providências para verificação das credenciais dos usuários afetados.
- **QUEM AQUI JA ATIVOU O MFA do Google?**
  - https://myaccount.google.com/intro/security-checkup

REAÇÃO INSTITUCIONAL - INTERNA:

- **Protocolo de credenciais comprometidas em geral:**
  - Troca dessa senha em todos os serviços que ela é utilizada, prioritariamente nos institucionais;
  - Ativação imediata do segundo fator de autenticação;
  - Verificação das configurações de encaminhamento de mensagens;
  - Aplicativos que podem usar as informações da sua conta;
  - Dispositivos conectados ou tiveram acesso à sua conta;
  - Check-up da segurança da conta de e-mail através da ferramenta online de check-up do Google: https://myaccount.google.com/intro/security-checkup
  - Verificações finais:
    - Versão mais recente do seu navegador.
    - Aplicativos e extensões desnecessárias ao seu navegador.
    - Credenciais no navegador. Para isso utilize aplicativos cofres de senhas.
    - Credenciais institucionais para fins particulares ou vice-versa.
    - Software antivírus instalado e atualizado em seus dispositivos, realizando varreduras frequentes.
- **QUEM AQUI JA ATIVOU O MFA do Google?**

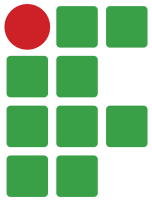
PLANOS FUTUROS ETIR/IFSP

Neste PRIMEIRO ANO de ETIR/IFSP:

- Inicialmente foram trabalhos estruturantes:
  - Criados os processos, procedimentos e metodologias para nortear os serviços Proativos e Reativos oferecidos pela ETIR/IFSP;
  - Trabalhos mais organizacionais paralelos aos técnicos;
    - Um dos motivos que, por enquanto, não houve o acionamento de emergência do membros.

Os próximos passos que estão em nosso ROADMAP:

- Amadurecimento dos processos criados para os serviços Reativos e Proativos;
- Automatização de tarefas ligadas ao portifólio de serviços;
- Prospecção e implementação de ferramentas para apoio;
- Atenção a ameças internas;
- Formas de autenticação seguras para credenciais privilegiadas;
- Busca por capacitações relacionadas ao portifólio de serviços, para a equipe;



AGRADECIMENTOS E MEU MUITO OBRIGADO PELA OPORTUNIDADE

A CADA UM DE VOCÊS AQUI!

- SEM A RESPONSABILIDADE COMPARTILHADA COM CADA UM AQUI, NÃO EXISTIRIA SEGURANÇA CIBERNÉTICA INSTITUCIONAL!

A TODO TIME DA PRO-PRD

- Na pessoa do Pró-Reitor Bruno Luz

A TODO O TIME DA DTI

- Na pessoa do Diretor Leonardo Menzani

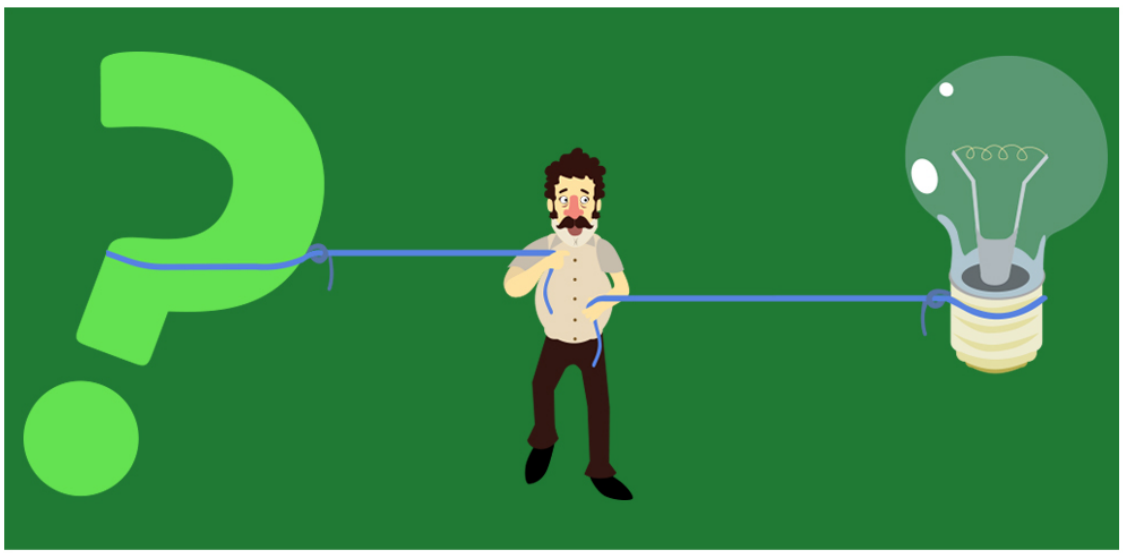
A TODO TIME DA CAOTI

- Na pessoa do Rafael Manochio

Sem a luta e o comprometimento de cada membro das equipes, os trabalhos da ETIR não seriam possíveis! Se ela existe e atua, esta conquista é de cada um(a)!

PERGUNTAS?

- **https://ifsp.edu.br/etir**



- *Fonte: https://opportunitymaker.com.br*