MISP na Petrobras: Seis Anos de Desafios e Inovações

5º *Workshop* MISP – CERT.br
31/07/2024

Alessandro Coutinho

alessandro.coutinho@petrobras.com.br

linkedin.com/in/alessandrocoutinho

Roosewelt Mota

roosewelt@petrobras.com.br

linkedin.com/in/roosewelt-mota-a0067933/

PETROBRAS

TLP:CLEAR

Agenda

Benefícios

- Visão Geral
- Principais Ganhos
- Integrações
- Estatísticas
- Utilização do Datalake

Desafios

- Recursos Humanos
- Técnicos
- Sustentação

Próximos passos

Benefícios

Benefícios

Visão Geral

1ª Recebe informações de provedor de soluções de Inteligência de Ameaças;

2ª Integração com processos internos;

3ª Compartilhamento de IoCs com parceiros.

Integrações :

O **MISP** está integrado com demais componentes da arquitetura de segurança cibernética da Petrobras, tais como:

TLP:CLEAR

Benefícios

Principais Ganhos

Principais ganhos:

- **Ampliação do conhecimento** sobre as ameaças cibernéticas.
- **Otimização da análise** dos times de resposta de incidentes.
- **Redução do tempo** médio de identificação das intrusões bem sucedidas.

Plataforma de Inteligência de Ameaças

25 Integrações MISP

Proteções Tecnológicas

TLP:CLEAR

Benefícios

Integrações

- Serviços contratados de Threat Intel
- Feeds pagos e gratuitos
- Parceiros

Plataformas de Inteligência de Ameaças

Proteções Tecnológicas

- SIEM
- SOAR
- Firewall
- Scan de Vulnerabilidades
- NVD (National Vulnerablility Database) - CVE
- IDS
- XDR
- Datalake
- Painéis técnicos e estratégicos
- Filtro de DNS

- Análise de feeds e outras notícias
- Tratamento de incidentes
- Análise de malware
- Pesquisa
- Apoio *threat hunting*

TLP:CLEAR

Benefícios

Estatísticas

2023/2024

Principais Desafios

Desafios

Recursos Humanos

PETROBRAS

Desafios

- Gestão de Pessoas
- Rotatividade na equipe
- Perfil DevSecOps

O que fizemos?

- Métodos ágeis para gestão das atividades;
- Gestão do conhecimento (Gravação de treinamentos, repositório de informações importantes e código fonte)
- Seleção de profissionais com conhecimento em Python, Linux, Shell Linux, Docker e Certificações (CompTIA Security+)

TLP:CLEAR

Desafios

Técnicos

Desafios

- Validação dos IoCs externos
- Enriquecimento de IoCs
- Integração com SOAR
  - Conhecimento avançado da API do MISP para integração com SOAR;
- Automatização na resposta
  - Bloqueio do hash do putty
  - Bloqueio da url de empresa do grupo
  - Bloqueio do github (classe de ip)
- Limitação das ferramentas de proteção
  - Firewall, 10mb por feed
  - Endpoint, 15 mil linhas
- Mudança de tecnologia

O que fizemos?

- API Virus Total, AbuseIPDB, Shodan e APIs das soluções de firewall e endpoint;
- APIs de parceiros de threat intelligence e Datalake;
- Definição de fontes confiáveis e validação via API com soluções de proteção de parceiros;
- Warning lists;
- Rotatividade da lista de IoCs;
- Criação de rotinas para verificar se a solução já tem conhecimento do IoC antes de entrar na lista;
- Revalidar e ajustar automatização ao mudar de tecnologia.
- Critério de segurança para contratação (licitação) de soluções;

Desafios

Técnicos

Desafios

- Limitação do banco de dados do MISP
- Administração do ambiente
  - SOs obsoletos ou não homologados
  - Patches
  - Atualizações frequentes
- Quebra de pacotes
- Lentidão no ambiente
- Queda do ambiente
- Indicadores gerenciais

O que fizemos?

- Integração e exportação de dados para uma infraestrutura de Datalake
- Atualização tecnologia (Storage All Flash - SSD)
- Adoção de containers. Criação das próprias imagens (**não utilização de imagens prontas)**
- Listas exclusivas do MISP no endpoint e firewall para mapear a efetividade dos IoCs cadastrados

Desafios

Sustentação

PETROBRAS

Desafios

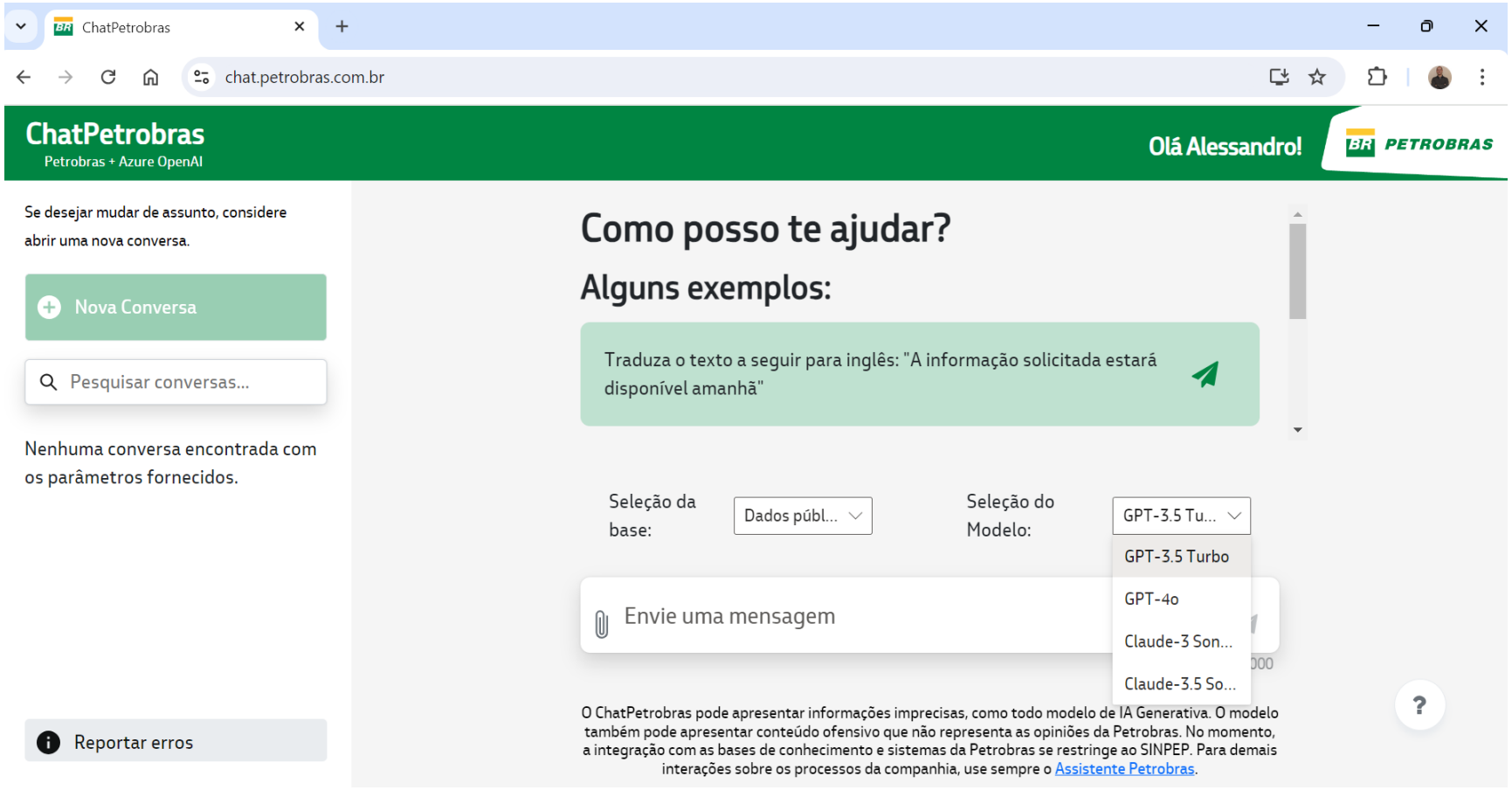
- Perda de sincronismo com o parceiro
- Modificação de regras de firewall
- Ajuste regras no WAF
- Políticas anti-ddos

O que fizemos?

- Monitoração da comunicação com o parceiro
- Inclusão de atividades no baseline
- Revalidar políticas de WAF
- Revisão contínua de políticas Anti-DDOS

TLP:CLEAR

Inovações



- Criação de scripts PyMisp
- Integrações com API com soluções parceiros

TLP:CLEAR

Próximos Passos

- Utilização do Cortex (TheHive Project)
- Expansão do uso de IA

Cortex

https://github.com/TheHive-Project/Cortex

TLP:CLEAR

Muito Obrigado!

Alessandro Coutinho

alessandro.coutinho@petrobras.com.br

linkedin.com/in/alessandrocoutinho

Roosewelt Mota

roosewelt@petrobras.com.br

linkedin.com/in/roosewelt-mota-a0067933/

PETROBRAS

TLP:CLEAR