Gamificação do Processo Preparatório para Simulação de Incidente Cibernético no Ambiente de Automação Industrial: Lições Aprendidas e Resultados Obtidos

11º Fórum de CSIRTs – CERT.br
31/07 e 01/08/2023

PALESTRANTES:

Rodrigo Rosa

Leandro Marinho

Alessandro Coutinho

BR PETROBRAS

TLP:CLEAR

Quem sou eu?

15 Anos de PETROBRAS

PETROBRAS

TLP:CLEAR

SUMÁRIO

PÚBLICA

TLP:CLEAR

RECAP
Refinaria de Capuava

UTGCA
Unidade de Tratamento de Gás Monteiro Lobato

REDUC
Refinaria Duque de Caxias

P-66
Plataforma P-66

UTE-IBT
Usina Termelétrica Ibirité

Impactos Midiáticos

AgênciaBrasil

Hacker tenta envenenar água de cidade da Flórida

Objetivo era provocar envenenamento em massa

veintitres

Ministério Público belga investiga ciberataques à infraestrutura portuária do país

Todas as notícias sobre ataques cibernéticos e hackers

O GLOBO

ECONOMIA

Autoridades chinesas descobrem mutação do vírus que afetou sistemas no mundo

Ataque se espalhou nesta segunda-feira pela Ásia, que por causa do fuso horário não foi tão atingida na sexta-feira

MUNDO CONECTADO

Companhias petrolíferas da Europa estão sofrendo ciberataques

Ataques à terminais acontece em meio a crise entre Rússia e Ocidente

Este ataque hacker roubou mais de R$ 500 milhões de investidores

Um **ataque hacker** invadiu plataforma que funciona como "ponte de criptomoedas", tipo de rede em que investidores podem transferir variadas dívidas digitais entre distintas blockchains. Os criminosos roubaram US$ 100 milhões. A **rede Horizen** foi alvo do ataque.

Como ransomware REvil fez milhares de vítimas de uma só vez em novo ataque

Ransomware REvil contaminou milhares de clientes da empresa de TI Kaseya; pedido de resgate chega a US$ 70 milhões

Ransomware Nefilim mira vítimas com receitas acima de US$ 1 bilhão

Estudo da Trend Micro alerta para ataques cibernéticos com foco em organizações globais altamente rentáveis

Redação

PÚBLICA

TLP:CLEAR

PÚBLICA

TLP:CLEAR

Simulado de Incidente Cibernético

Testar (treinar): **Processo, Comunicação, Tecnologia, Tratamento e Resposta ao Incidente e Recuperação do Ambiente durante um ataque cibernético.**

Mensurar o retorno seguro do ambiente operacional.

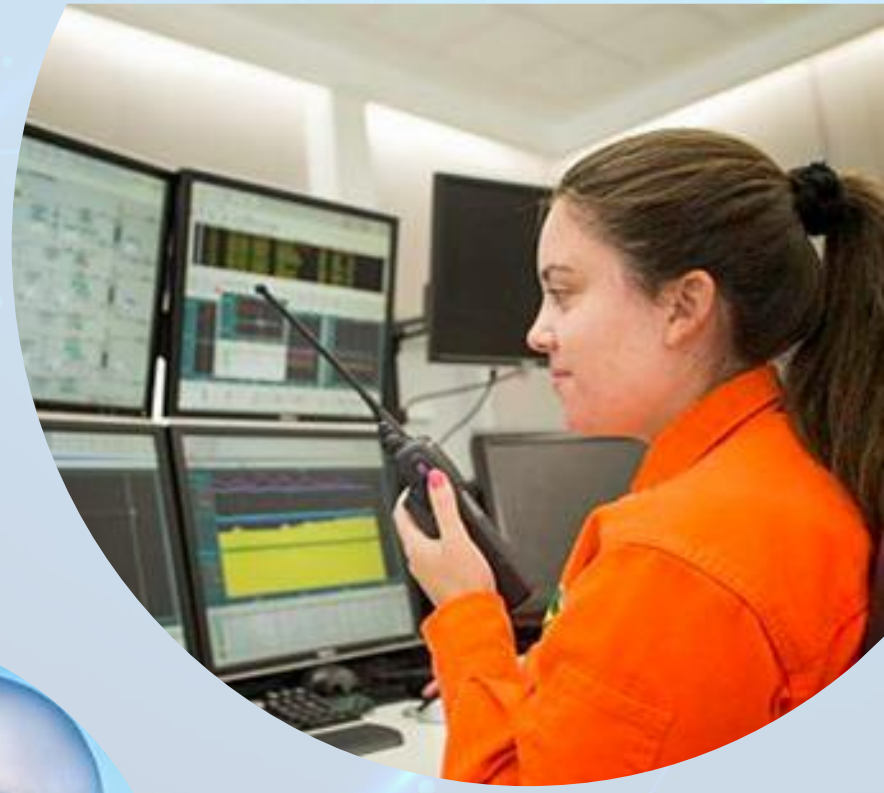
Oportunidade para discutir o
Dano em Potencial ao Processo de Negócios.

PÚBLICA

TLP:CLEAR

Desafios / Barreiras

- Não pode causar impacto operacional;
- Entender o processo de negócio e possíveis impactos;
- Aprofundar tecnicamente na operação. Entendimento além dos computadores;
- Conhecimento TI vs TA.



Um mundo novo...
Tecnologias atuais convivendo com o legado...
Muito aprendizado!

PÚBLICA

TLP:CLEAR

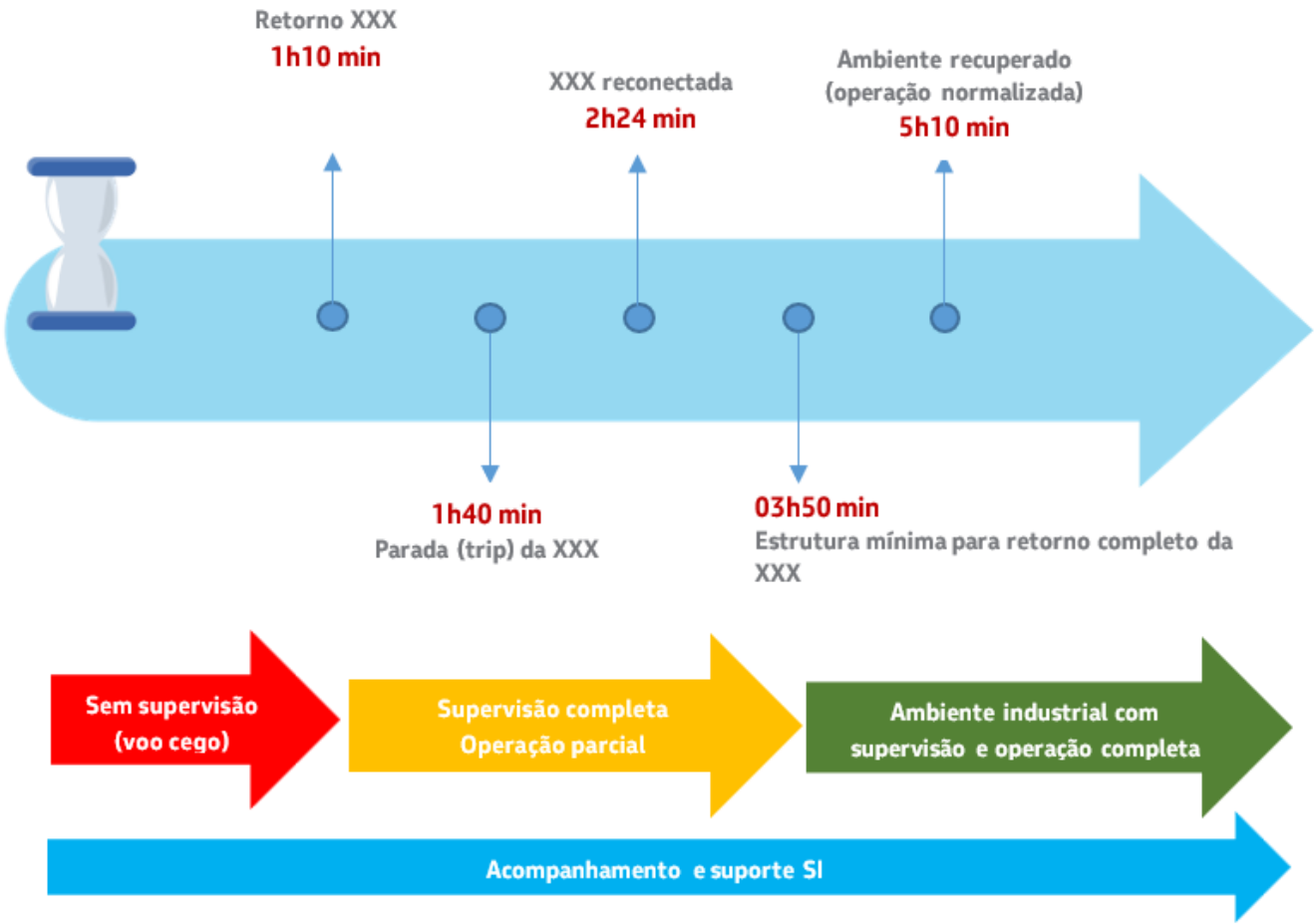
Estrutura & Planejamento

Cada simulação é **ÚNICA**

Orquestração

Para realizar uma simulação de incidente cibernético em uma planta industrial, várias áreas empresariais são envolvidas, tais como:

Exemplo (Fictício)
Cronologia & Linha do Tempo



TLP:CLEAR

Lições Aprendidas

- **Todos na mesma página;**
- Um incidente cibernético pode ir além do técnico:
  - Alinhamento gerencial;
  - SI deve fazer parte da estratégica de negócio para tratamento de crises internas e comunicação com o mundo exterior.
- **Playbook do CSIRT deve refletir a criticidade do negócio;**
- Ações mapeadas, aplicáveis ao contexto, não se discute, se executa;
- **Treinar equipes SI, TI e TA (linguajar diferente);**
- Ter VM reduz o tempo de recuperação do ambiente. Para equipamentos físicos, gerar imagem é uma excelente alternativa;
- **Backup segregado salva vidas.**

Disseminação para as verticais de negócio

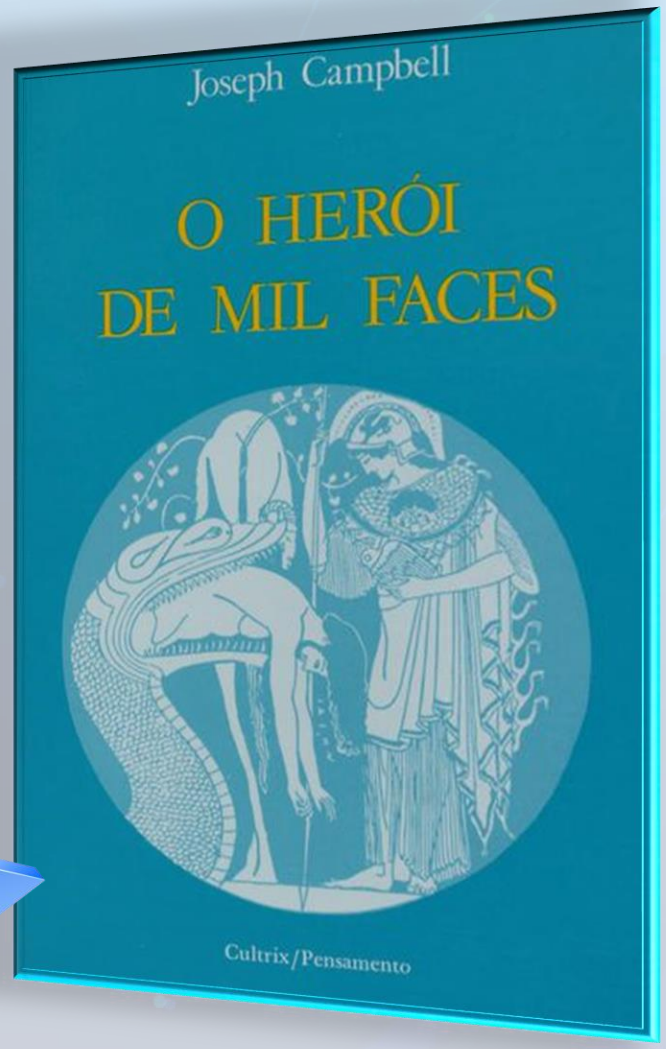
TLP:CLEAR

Jornada do Herói

As etapas tradicionais da jornada do herói, também conhecida como a Monomito, foram descritas pelo mitólogo **e escritor Joseph Campbell em seu livro "O Herói de Mil Faces" (1949).**

Essas etapas seguem uma **estrutura narrativa** comum encontrada em *mitos*, *contos de fadas*, *lendas* e *histórias épicas* ao redor do mundo.

Aqui estão as principais etapas da jornada do herói....



Jornada do Herói

A gamificação da simulação foi baseada no livro "O Herói de Mil Faces", de Joseph Campbell (1949)

1. **Mundo comum ordinário**
2. **A chamada da aventura**
3. **Recusa ao chamado:** Obstáculos à implementação da simulação
4. **Encontro com o mentor**
5. **Cruzamento do primeiro limiar**
6. **Testes, aliados e inimigos**
7. **Aproximação da caverna secreta**
8. **Provação suprema**
9. **Conquista da recompensa**
10. **Caminho de Volta:** Retorno com o Elixir

1. MUNDO COMUM (Ordinário)

1.MUNDO COMUM (Ordinário)

RECAP
Refinaria de Capuava

UTGCA
Unidade de Tratamento de Gás Monteiro Lobato

REDUC
Refinaria Duque de Caxias

P-66
Plataforma P-66

UTE-IBT
Usina Termelétrica Ibirité

2. CHAMADO À AVENTURA

Impactos Midiáticos

AgênciaBrasil

Hacker tenta envenenar água de cidade da Flórida

Objetivo era provocar envenenamento em massa

veintitres

Ministério Público belga investiga ciberataques à infraestrutura portuária do país

Todas as notícias sobre ataques cibernéticos e hackers

O GLOBO

ECONOMIA

Autoridades chinesas descobrem mutação do vírus que afetou sistemas no mundo

Ataque se espalhou nesta segunda-feira pela Ásia, que por causa do fuso horário não foi tão atingida na sexta-feira

MUNDO CONECTADO

Companhias petrolíferas da Europa estão sofrendo ciberataques

Ataques à terminais acontece em meio a crise entre Rússia e Ocidente

Este ataque hacker roubou mais de R$ 500 milhões de investidores

Um **ataque hacker** invadiu plataforma que funciona como "ponte de criptomoedas", tipo de rede em que investidores podem transferir variadas dívidas digitais entre distintas blockchains. Os criminosos roubaram US$ 100 milhões. A **rede Horizen** foi alvo do ataque.

Como ransomware REvil fez milhares de vítimas de uma só vez em novo ataque

Ransomware REvil contaminou milhares de clientes da empresa de TI Kaseya; pedido de resgate chega a US$ 70 milhões

Ransomware Nefilim mira vítimas com receitas acima de US$ 1 bilhão

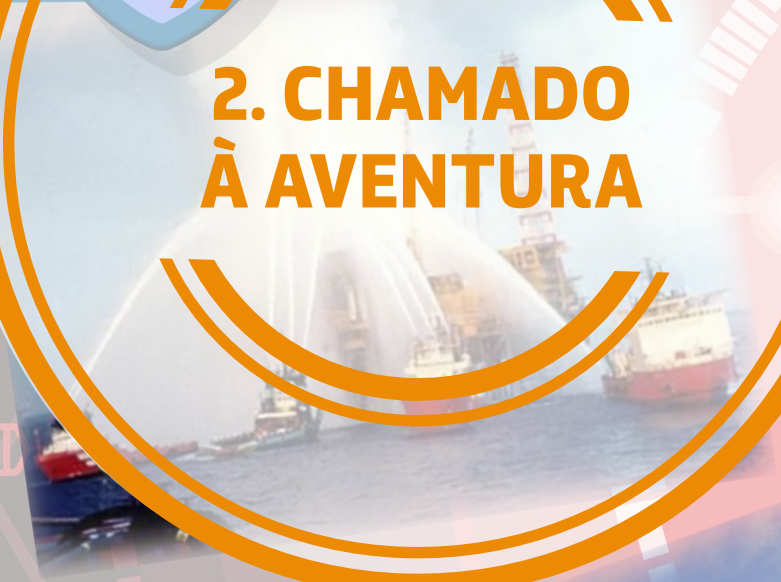
Estudo da Trend Micro alerta para ataques cibernéticos com foco em organizações globais altamente rentáveis

Redação

PÚBLICA

TLP:CLEAR

2. CHAMADO À AVENTURA



2. CHAMADO À AVENTURA

Simulado de Incidente Cibernético

Testar (treinar): **Processo, Comunicação, Tecnologia, Tratamento e Resposta ao Incidente e Recuperação do Ambiente durante um ataque cibernético.**

Mensurar o retorno seguro do ambiente operacional.

Oportunidade para discutir o
Dano em Potencial ao Processo de Negócios.

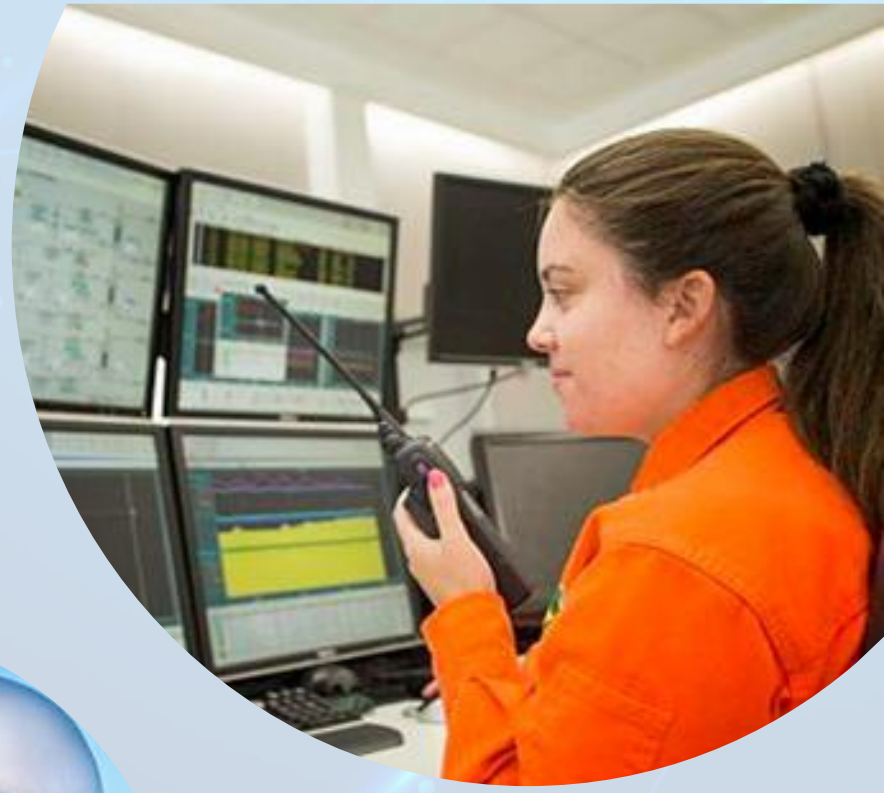
Desafios / Barreiras

3. RECUSA AO CHAMADO: Obstáculos à Implementação da Simulação

- Não pode causar impacto operacional;
- Entender o processo de negócio e possíveis impactos;
- Aprofundar tecnicamente na operação. Entendimento além dos computadores;
- Conhecimento TI vs TA.

4. ENCONTRO COM O MENTOR

Um mundo novo...
Tecnologias atuais
convivendo com o legado...
Muito aprendizado!



PÚBLICA

TLP:CLEAR

Estrutura & Planejamento

5. CRUZAMENTO DO PRIMEIRO LIMIAR

Cada simulação é **ÚNICA**

6. TESTES, ALIADOS E INIMIGOS

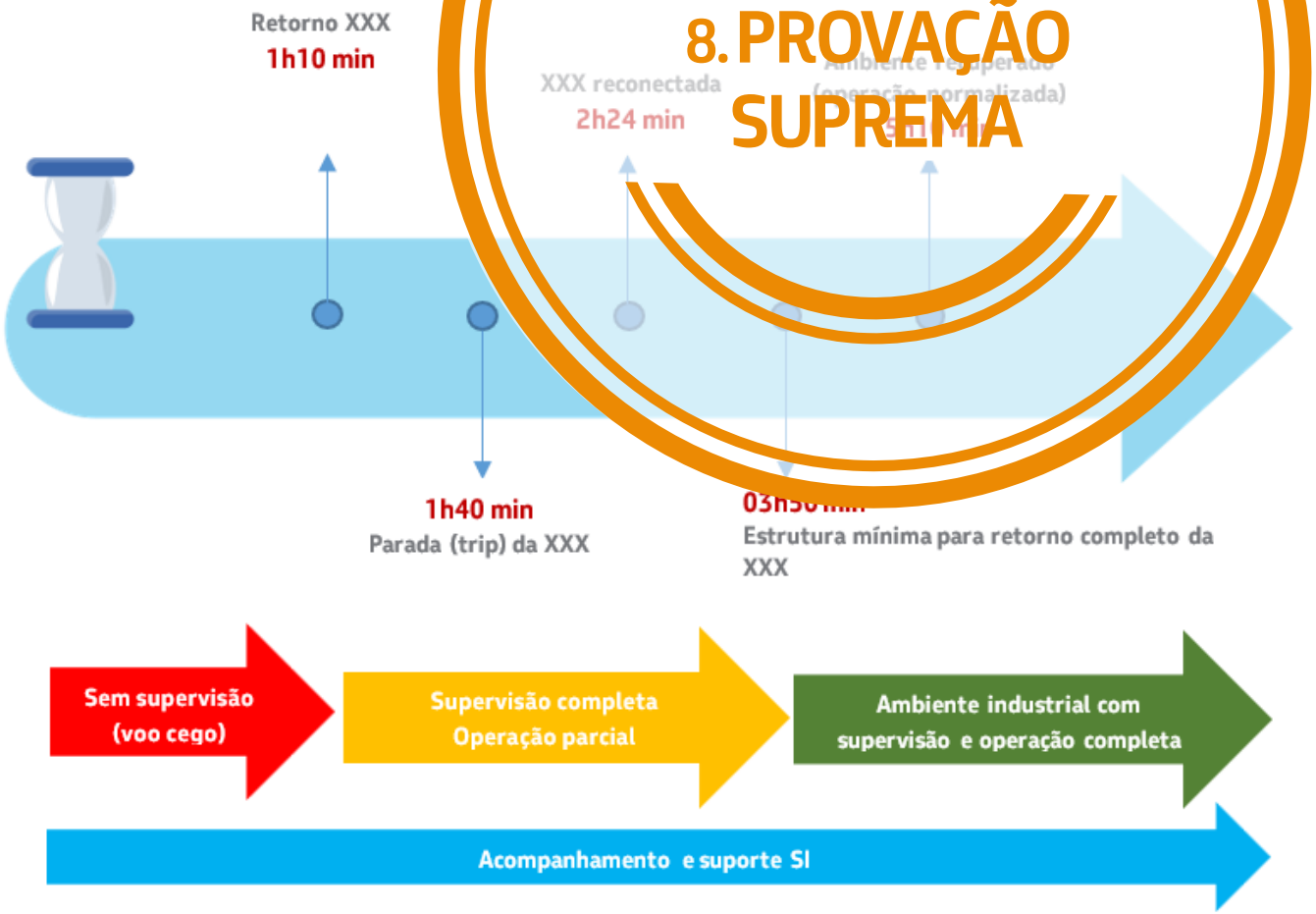
Orquestração

Para realizar uma simulação de incidente cibernético em uma planta industrial, várias áreas empresariais são envolvidas, tais como:

Exemplo (Fictício)
Cronologia & Linha do Tempo

7. APROXIMAÇÃO DA CAVERNA SECRETA

8. PROVAÇÃO SUPREMA



Lições Aprendidas

9. CONQUISTA DA RECOMPENSA

- Todos na mesma página.
- Um incidente cibernético pode ir além do técnico:
  - Alinhamento com nível gerencial;
  - SI deve fazer parte da estratégica de negócio para tratamento de crises internas e comunicação com o mundo exterior.
- *Playbook* do CSIRT deve refletir a criticidade do negócio.
- Ações mapeadas, aplicáveis ao contexto, não se discute, se executa.
- O básico não se discute, deve estar mapeado, assim reduz o tempo de recuperação do ambiente.
- Treinar equipes SI, TI e TA (linguajar diferentes).
- Ter VM reduz o tempo de recuperação do ambiente. Para equipamento físicos, gerar imagem é uma excelente alternativa.
- Backup segregado salva vidas.

10. CAMINHO DE VOLTA: Retorno com o Elixir

Disseminação para as verticais de negócio

TLP:CLEAR

Mas ainda tínhamos um grande problema:

As pessoas tinham muita dificuldade para lembrar dos padrões, quem procurar e o que a outra gerência faz...

...e a Gamificação é uma forma lúdica de aprendizagem. Então...

TLP:CLEAR

Os padrões documentais corporativos são complexos e muito extensos, o que provoca aos colaboradores, entendimentos diferentes sobre qual tomada de decisão é a mais correta a ser executada para enfrentar um incidente cibernético em uma planta industrial.

E assim decidimos GAMIFICAR AINDA MAIS as ações!

Materiais de apoio da Simulação

- Diretriz de Segurança XXXX
- Prover Inteligência e Resposta a Incidentes Cibernéticos
- Guia de Elaboração de XXXX
- Gestão de Segurança Cibernética dos XXXX
- Apoio à Resposta de Incidente Cibernético XXX
- Guia de Elaboração de XXXX

Criamos a narrativa
Storytelling

Definimos as **fases;**
Desenhamos o **tabuleiro,**
os **personagens**...

E assim começa a jornada do herói!
Na verdade, as **analogias**.

START

Um fato estranho acontece na planta industrial ...

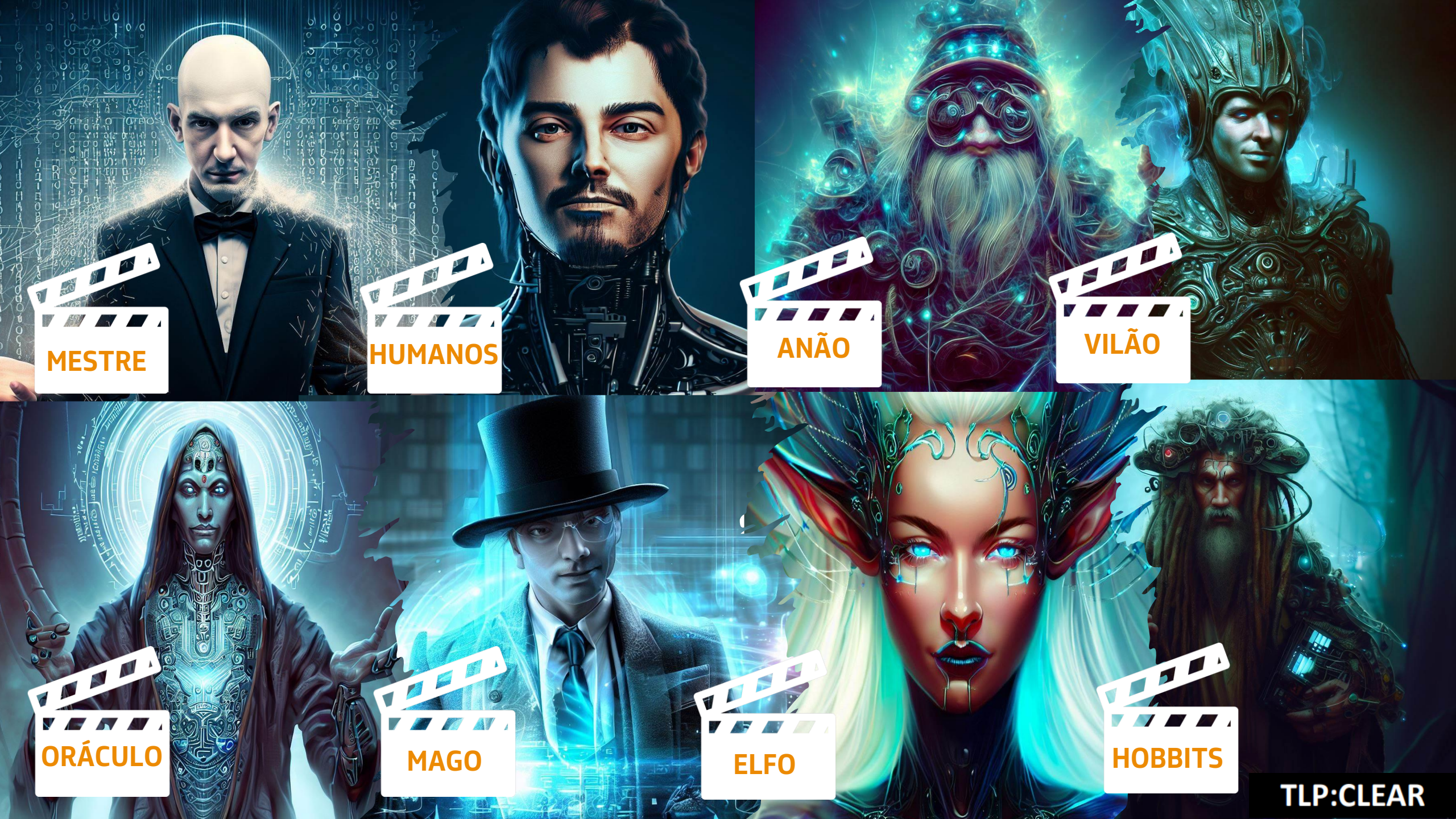
TLP:CLEAR

Personagens

Na Gamificação, eles foram classificados em função da sua **CULTURA e RAÇA**, destacando cada característica particular, que refletem suas funções reais no simulado e na organização:

- PODERES
- ATRIBUTOS
- HABILIDADES
- RESPONSABILIDADES

TLP:CLEAR

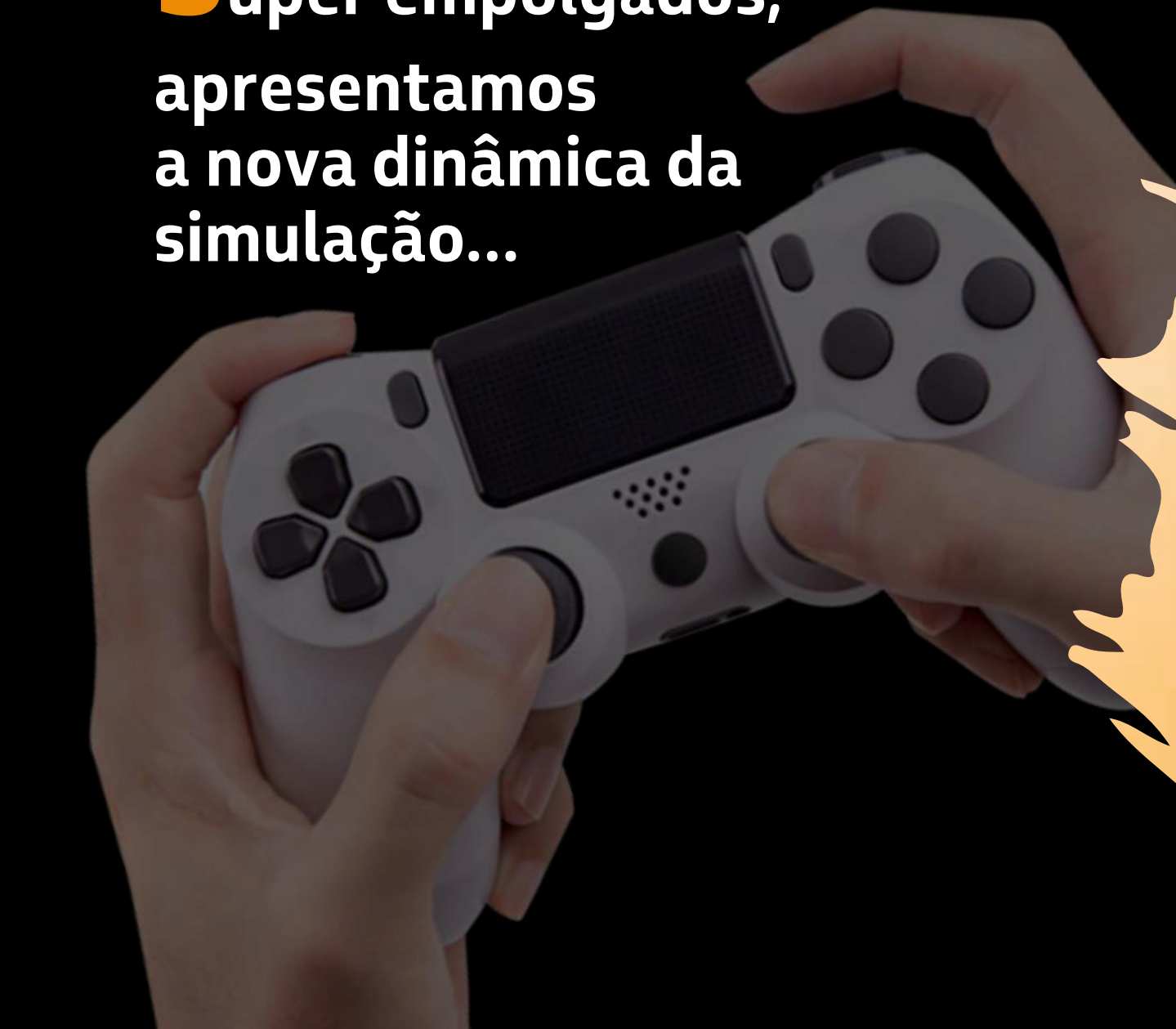

MESTRE
HUMANOS
ANÃO
VILÃO
ORÁCULO
MAGO
ELFO
HOBBITS
TLP:CLEAR

Personagens

Os personagens começam a ser construídos com base na metodologia de jogo “RPG”.

TLP:CLEAR

Super empolgados,
apresentamos
a nova dinâmica da
simulação...



TLP:CLEAR


Não gosto de jogos!
E esses monstros? Esses personagens estranhos.
Já não basta os padrões, agora teremos que aprender outras coisas?
Eu nem sei o que é RPG!
RAÇAS é um termo preconceituoso.
Como será em um incidente real?
O pessoal de Operações não compreenderá essas analogias..
Trabalhamos em uma empresa séria, não estamos aqui para jogar!
Após a reunião, levaram o assunto ao gerente.
TLP:CLEAR

Reflexão: Ressureição

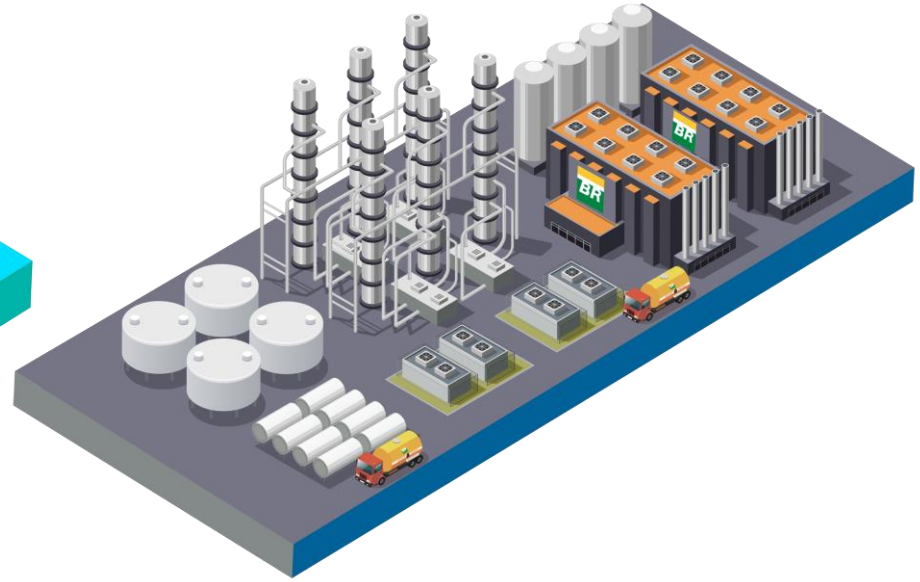
TLP:CLEAR

Gamificação é ferramenta lúdica para aprendizagem (exemplo fictício)

Planta Industrial

TABULEIRO
(ideia inicial)

PAINEL
(Atual)



Gerências

- Gerencia A
- Gerencia B
- Gerencia C
- Gerencia D
- Gerencia E
- Gerencia F
- Gerencia G
- Gerencia H
- Célula da Simulação

PÚBLICA

TLP:CLEAR

Gerência X
Resp: XXX
CSIRT

FERRAMENTAS
Ferramentas de monitoração e investigação

HABILIDADES
Monitoração, tratamento e resposta a incidentes cibernéticos

RESPONSABILIDADES
Monitoração, tratamento e resposta a incidentes cibernéticos

ATIVIDADES DELEGADAS
N/A

TLP:CLEAR

Gerência Y
Resp: XXX

FERRAMENTAS

HABILIDADES

RESPONSABILIDADES

ATIVIDADES DELEGADAS

TLP:CLEAR

Célula de Simulação
Resp: Y

FERRAMENTAS
Documentos

HABILIDADES
Criar evidencias

RESPONSABILIDADES
Dinâmica da simulação (simular equipes externas)

ATIVIDADES DELEGADAS

Célula de Simulação

Fabricante de Antivírus Anuncia a Disponibilidade da Vacina contra o Malware Nekker

Rio de Janeiro, 26/06/2023 - A empresa líder em segurança cibernética, juntamente com sua equipe de especialistas em ameaças, está orgulhosa em anunciar o desenvolvimento de uma nova vacina altamente eficaz contra o malware Nekker. A vacina já está disponível para os usuários em seu site oficial.

O malware Nekker tem sido uma fonte crescente de preocupação para indivíduos e empresas em todo o mundo. Com suas táticas avançadas de infiltração e criptografia de dados, o Nekker tem causado prejuízos significativos e interrupções operacionais. No entanto, a empresa de antivírus investiu tempo e recursos consideráveis para desenvolver uma solução eficaz para proteger os usuários contra essa ameaça.

A vacina contra o malware Nekker foi projetada para neutralizar e impedir a infecção por esse ransomware destrutivo. Com um mecanismo de detecção e remoção avançado, a vacina é capaz de identificar os indicadores de comprometimento (IoCs) associados ao Nekker e bloquear seu acesso aos sistemas infectados.

"A segurança cibernética é uma prioridade máxima para nós, e estamos comprometidos em proteger nossos usuários contra as ameaças emergentes", disse o porta-voz da empresa. "A disponibilidade da vacina contra o malware Nekker é um marco significativo em nossa missão contínua de fornecer proteção de primeira classe contra ataques cibernéticos. Encorajamos todos os usuários a visitarem nosso site e garantirem que estão protegidos contra essa ameaça."

A empresa de antivírus também alerta os usuários sobre as melhores práticas de segurança cibernética, como evitar clicar em links suspeitos, manter seus sistemas operacionais e softwares atualizados, fazer backup regularmente de seus dados e estar atento a atividades online suspeitas.

A vacina contra o malware Nekker está disponível para download imediato no site oficial da empresa. A empresa continuará aprimorando suas soluções de segurança para enfrentar as ameaças emergentes e garantir a proteção contínua de seus usuários.

Equipamentos do Fabricante XPTO atingidos por ataque de ransomware Nekker

A **XPTO**, fornecedora líder de tecnologia para operação e monitoração de turbo gerador para ambiente de automação industrial, sofreu um **ataque de ransomware** provocado pelo grupo de cyber criminosos Nekker no dia 26 de junho de 2023, que afetou diretamente alguns dos seus equipamentos, segundo a própria empresa informou em comunicado enviado ao portal de notícias **BleepingComputer.**

Com sede em Zurique, na Suíça, a XPTO emprega aproximadamente 105 mil funcionários e obteve US$ 29,4 bilhões em receita em 2022. Como parte de seus serviços, a empresa desenvolve **equipamentos e sistemas de controle industrial (ICS) e sistemas SCADA para fornecedores de manufatura, energia, óleo e gás,** trabalhando com uma ampla gama de clientes.

O ataque cibernético, que afetou os equipamentos voltados ao controle de turbinas e centenas de dispositivos relacionados, teria supostamente interrompido as operações da empresa, atrasando projetos, impactando as fábricas e atingindo clientes que possuem os modelos dos equipamentos afetados. Em resposta ao ataque, a XPTO encerrou as conexões VPN com seus clientes para evitar a propagação do ransomware para outras redes, e está trabalhando em uma solução de contorno para resolver a vulnerabilidade que permitiu que o ransomware continue afetando seus equipamentos.

"Para resolver a situação, a XPTO tomou, e continua a tomar, medidas para correção da vulnerabilidade explorada pelo ranswomware. Tais medidas de contenção resultaram em algumas interrupções em suas vendas até que a empresa tenha a solução definitiva. A grande maioria de seus sistemas e fábricas estão funcionando e a XPTO continua atendendo seus clientes de maneira segura. A XPTO continua a trabalhar

Recuperação e TTPs

No ataque à XPTO, o Nekker conseguiu entrar nos sistemas da empresa usando técnicas de weblink maliciosas, como envenenamento por SEO e atualizações falsas do navegador para instalar o malware trojan Qakbot – uma tática que o grupo de ameaças costuma usar com frequência. A XPTO disse que o malware era um ransomware operado por humanos, exigindo a intervenção de uma pessoa para enviá-lo aos sistemas de destino. Rumores apontam que a XPTO pagou um resgate após o ataque.

O grupo Nekker surgiu em abril de 2022 e inicialmente tinha como alvo países de língua inglesa tais como: Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia. Para ter sucesso no ataque o malware precisa de privilégios de administrador, depois de executar o ransomware como administrador, ele remove os backups locais, desativa a recuperação e o reparo do Windows e inicializa o PC no modo de segurança.

Antes de inicializar o dispositivo infectado no modo de segurança, ele altera o papel de parede da área de trabalho e faz alterações em chaves de registro. O ransomware continua a criptografar os arquivos enquanto o dispositivo está no modo de segurança, anexando todos os arquivos criptografados com a extensão .Nekker. A nota de resgate é encontrada em todas as pastas que o ransomware afetou.

Como outras operações de ransomware voltadas para empresas, o Nekker emprega um esquema de extorsão dupla que envolve a exfiltração de dados confidenciais antes da criptografia para ameaçar as vítimas com a divulgação pública dos dados roubados.

A quadrilha realiza a fase de extorsão de seus ataques em seu site Tor, Nekker News, que contém uma lista de todas as vítimas que não pagaram o resgate.

A relação abaixo contém os principais IoCs (indicadores de comprometimento) encontrados até o momento:

200.192.40.60

200.192.40.61

200.192.40.62

200.192.40.63

PÚBLICA

TLP:CLEAR

Alguns dos Resultados

- Entendimento do processo e abertura de canal de comunicação
- Engajamento das equipes e gerencias
- Retenção e disseminação do conhecimento
- Foco nas ações, com base nos padrões

Vivenciar um incidente cibernético sem comprometer o ambiente

Muito obrigado!

E o herói volta para casa

Rodrigo Rosa
Gerente - SI / DC
rodrigo.rosa@petrobras.com.br
linkedin.com/in/rodrigo-rosa82

Leandro Marinho
Gerente Setorial - SI/DC/ANT
lmarinho@petrobras.com.br
linkedin.com/in/leandro-marinho-120037168

Alessandro Coutinho
Profissional Sênior - SI/DC/ANT
alessandro.coutinho@petrobras.com.br
linkedin.com/in/alessandrocoutinho

Agradecimentos

cert.br

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

MINISTÉRIO DA
DEFESA

TBG

NTT

indra
minsait

dec@tron

Gartner

TechBiz
FORENSE DIGITAL

GUARDIÃO CIBERNÉTICO 4.0

e profissionais e gerências Petrobras...

Referências

FIRST Annual Conference Edinburgh, Scotland, 2019
https://www.first.org
https://www.first.org/resources

Exercise in a Box
https://www.ncsc.gov.uk

ELECTIONS CYBER TABLETOP EXERCISE PACKAGE
https://www.cisa.gov

Kaspersky Interactive Protection Simulation
https://media.kaspersky.com

Rising Ransomware Threat To Operational Technology Assets
https://www.cisa.gov

#StopRansomware Guide
https://www.cisa.gov

Ransomware Guide
https://www.cisa.gov

Public Power Cyber Incident Response Playbook
https://www.publicpower.org