TEMPEST talks

2022

TEMPEST talks 2022

Resiliência CyberEmocional

Preparando Times para resistir a um Incidente Cibernético

Anchises Moraes
@c6bank

TEMPEST talks 2022

Agenda

01 Importância da Resposta a Incidentes e Resiliência

02 Jornada rumo a Resiliência

03 Treinamentos e Conscientização

Importância da Resposta a Incidentes e Resiliência

TEMPEST talks 2022

Importância da Resposta a Incidentes e Resiliência

TEMPEST talks 2022

Cyber Resiliência

“The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”

(NIST)

Aquele que se empenha a resolver as dificuldades, resolve-as antes que elas surjam.

Sun Tzu

Cyber Resiliência

TEMPEST talks 2022

- **Minimizar o impacto de um incidente de segurança**
- **Rápida retomada das operações**

Aquele que se empenha a resolver as dificuldades, resolve-as antes que elas surjam.

Sun Tzu

O que importa não é o tamanho da c*g*d*, mas a velocidade da limpeza.

Sergio Dias

Demandas regulatórias e boas práticas

TEMPEST talks 2022

- **Lei Geral de Proteção de Dados Pessoais (LGPD**
  - Art. 48 - "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares."
- **Resolução 4.893/2021 do BACEN (antiga 4.658)**
  - Art. 6º - "As instituições referidas no art. 1º devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética."

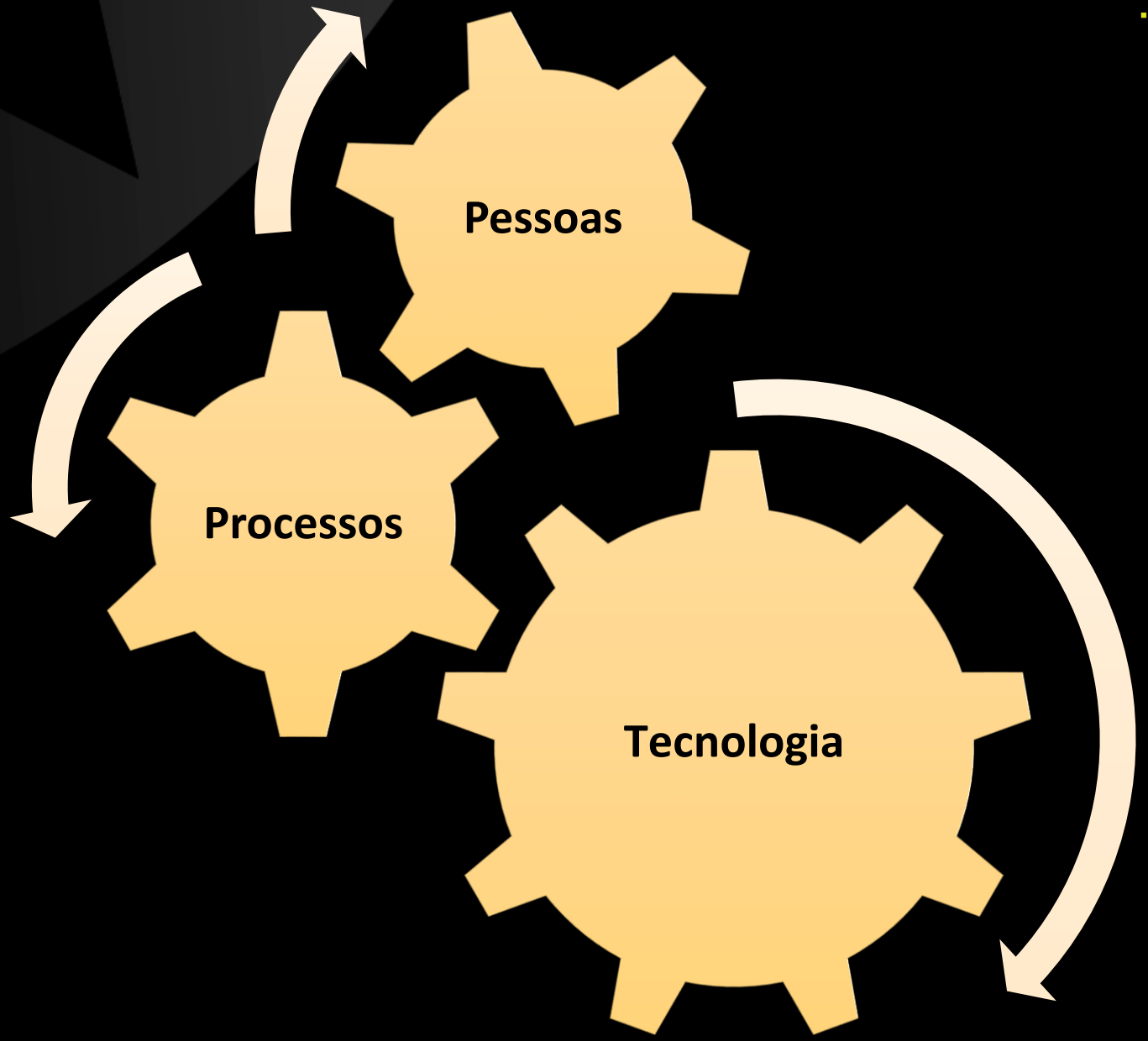
- **Cyber Resilience Act (EU)**

Jornada rumo a Resiliência

TEMPEST talks 2022

Desafio

TEMPEST talks 2022



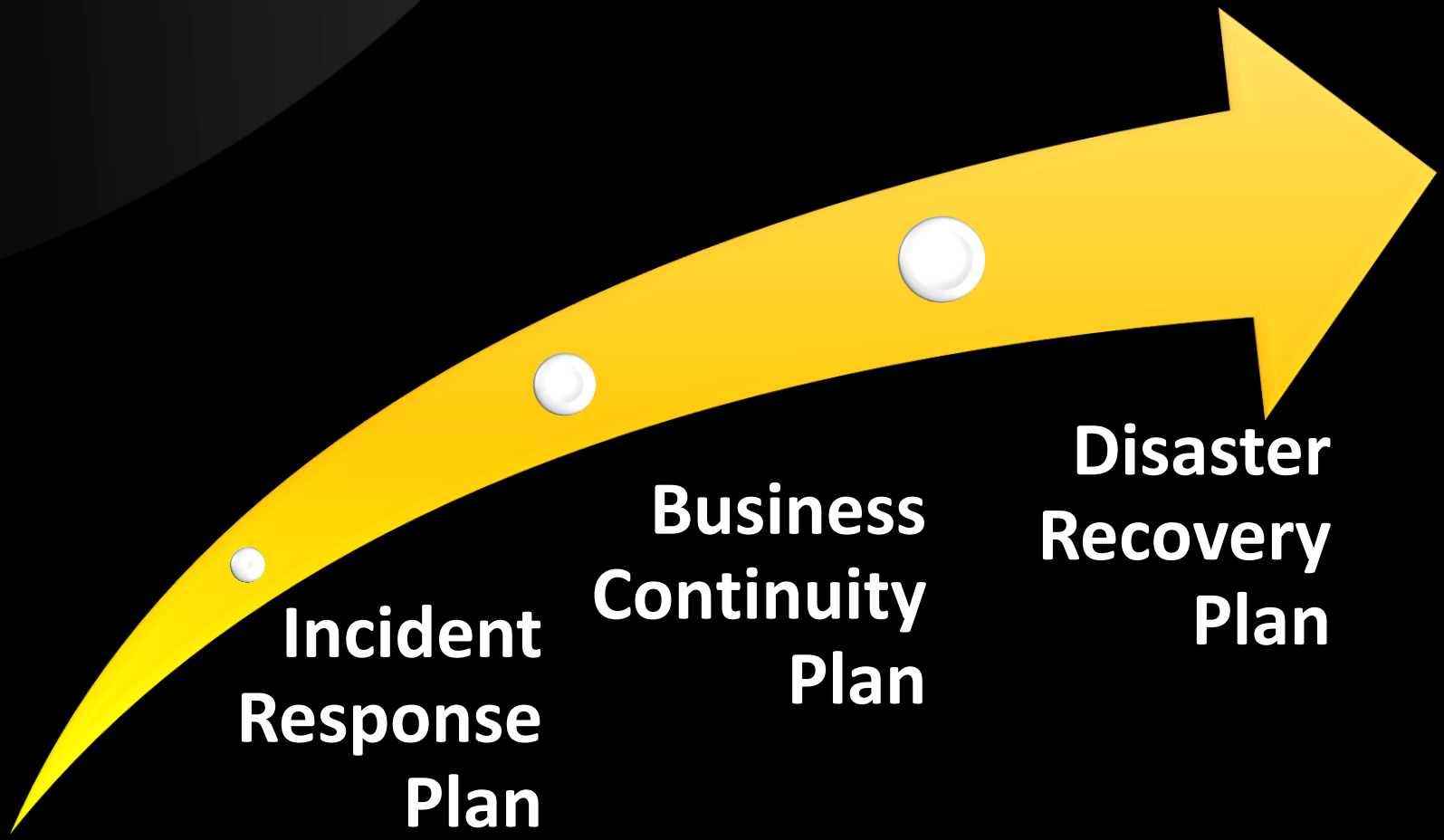
Desafio

TEMPEST talks 2022

E se a tecnologia falhar

Jornada rumo a Resiliência

TEMPEST talks 2022



Jornada rumo a Resiliência

TEMPEST talks 2022

- Revisão do Plano de Resposta a Incidentes
- Jornada com executivos
- Table Top Exercise

Revisão do Plano de Resposta a Incidentes

TEMPEST talks 2022

- **Revisar**
  - Boas práticas
  - Legislações
- **Divulgar**
- **Treinar**

C6 BANK Intranet - C6 Bank

Início Gente e Gestão Transparência Marca Roadmap 2021 C6 Service Desk ★ Seguindo

Enviar para Leitura Avançada

Norma de resposta a incidentes: saiba como tratamos casos envolvendo privacidade e segurança

Comunicacao

Publicada em 30/04/2021

Em janeiro de 2018, o Ministério Público constatou que um incidente de segurança **comprometeu dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras de clientes de um site de comércio eletrônico**. A empresa teve que pagar R$ 500 mil de indenização por danos morais após o vazamento de dados de quase dois milhões de clientes. Após o incidente, a marca se comprometeu a **adotar medidas adicionais de proteção de dados pessoais e a fazer campanhas de conscientização sobre "melhores práticas para privacidade".**

Essa é uma entre tantas histórias de vazamentos de dados e de incidentes desse tipo. Eles podem acontecer com qualquer pessoa e qualquer empresa, por isso, um trabalho de prevenção deve ser adotado para que, quando aconteça um erro que possa afetar a segurança de nossos clientes, dados ou sistemas, todos tenham a capacidade de identificá-lo com agilidade para diminuir os danos.

Saiba o que fazer caso você seja vítima de vazamento de dados.

Aqui no C6, diversos times estão envolvidos nessa empreitada a qual chamamos formalmente de **"resposta a incidentes"**. Esse processo de identificação e contenção a incidentes de segurança, além de ser uma necessidade de negócio, é também uma exigência regulatória, que está presente na LGPD (Lei Geral de Proteção de Dados Pessoais) e na Resolução 4.893 do Banco Central, entre outras. Para isso, temos diversas ferramentas tecnológicas de monitoramento, identificação e bloqueio caso seja identificado qualquer comportamento suspeito que possa indicar atividades potencialmente maliciosas.

Nós temos **duas normas** que formalizam todo o processo para identificar e resolver um incidente de segurança, a MN-088 - Resposta a eventos & incidente de segurança da informação, que inclui diretrizes sobre a gestão do processo de resposta a incidentes, e a nova norma MN-122 - Plano de Resposta a Incidentes Cibernéticos, que aborda detalhes mais operacionais do nosso plano de resposta a incidentes.

Compartilhamento com pares na indústria

TEMPEST talks 2022

- Eventos
- Grupos e Comunidades
- Conversas com executivos de outras empresas

Treinamentos e Conscientização

Treinamentos

TEMPEST talks 2022

Treinamentos em Resposta a Incidentes

- Ex: CERT.br

“War Games” & “Cyber Range”

“Table Top Exercises”

Treinamentos

TEMPEST talks 2022

- **Treinamentos em Resposta a Incidentes**
  - Ex: CERT.br
- **“War Games” & “Cyber Range”**

Time de segurança

- **“Table Top Exercises”**

Toda Organização

War Games & Cyber Range

TEMPEST talks 2022

- **Interno**
- **Participação em competições de CTF**
- **War Games setoriais e nacionals**
  - Exercício Guardião Cibernético
    450 participantes, +120 organizações
  - Locked Shields Exercise (OTAN)
    2.000 participantes, 33 países

Treinamento “table top”

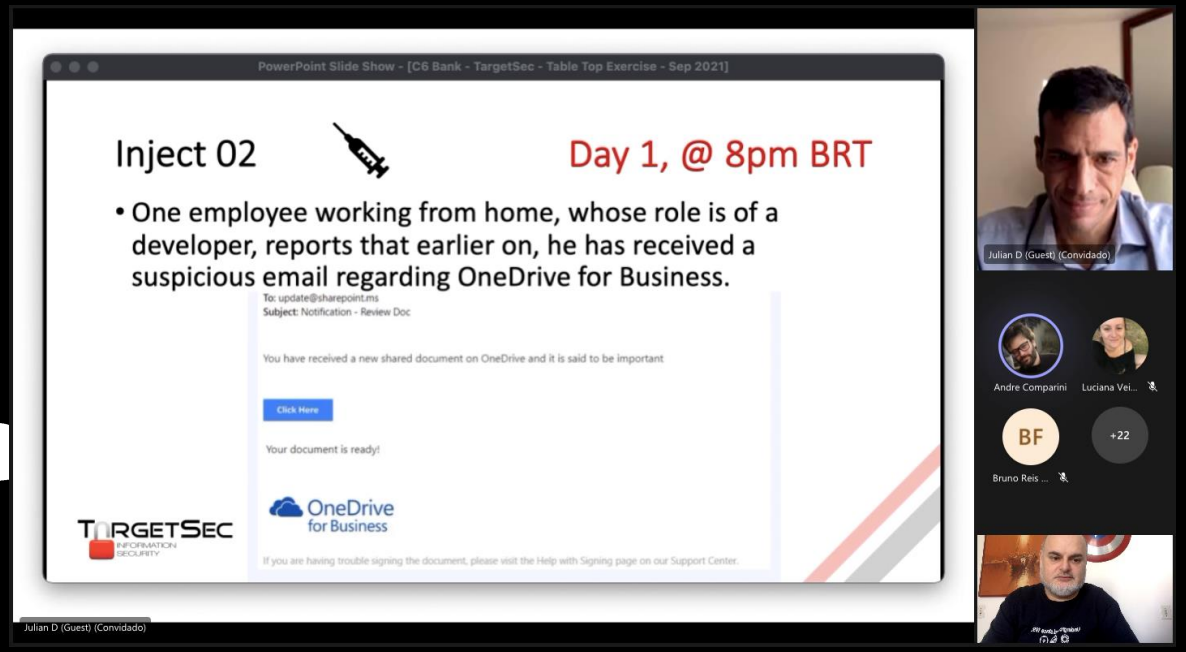
TEMPEST talks 2022

- “Table Top Exercise” (TTX), ou “Firedrill exercise”
- Simulação de Resposta a Incidentes
- Exercitar um cenário simulado de ciber ataque a organização

Treinamento “table top”

TEMPEST talks 2022

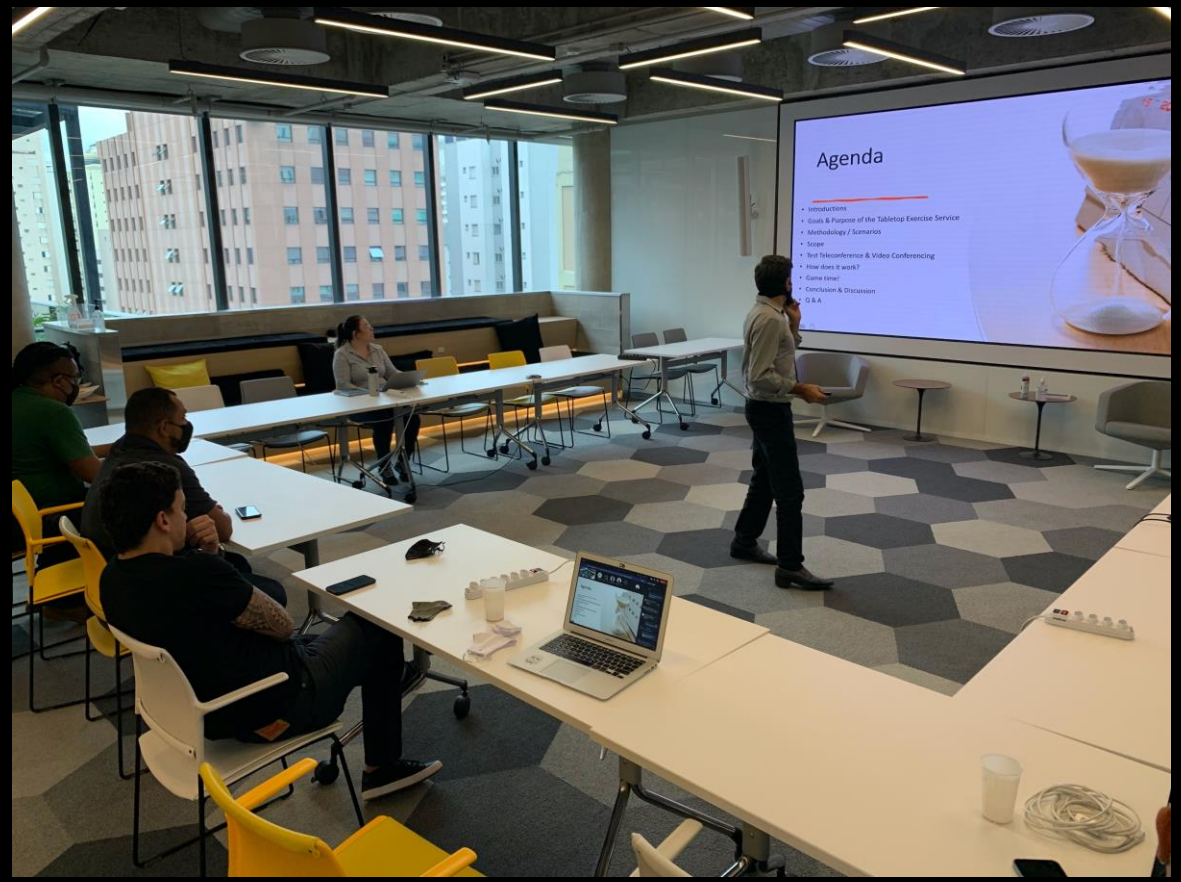
- **Estilo “role play game” (RPG)**
  - Exercícios e discussões guiadas
  - Passo-a-passo
- **Cenário hipotético de ciber ataq**



Treinamento “table top”

TEMPEST talks 2022

- **Exemplo:**
  - Cenário de Ataque de ransomware
  - Quais sistemas podem ser afetados?
  - É possível recuperar a operação?
  - Pagar ou não pagar o resgate?



Treinamento “table top”

TEMPEST talks 2022

- Permite Testar o plano de resposta a incidentes
- Como reagir frente um problema crítico de segurança? Quem chamar? Quais os times envolvidos?
- Permite a participação de pessoas não técnicas (outras áreas, executivos)

Benefícios do TTX

TEMPEST talks 2022

Four Types of TTX/Fire Drills

Target	Objectives
Board of Directors TTX	Awareness, Crisis Management, Education
C-Suite TTX	Crisis Management, Business Continuity
Organization Fire Drill	Test Response Planning and Contingencies
Technical Team Fire Drill	Test Technical Responses (detect and respond)

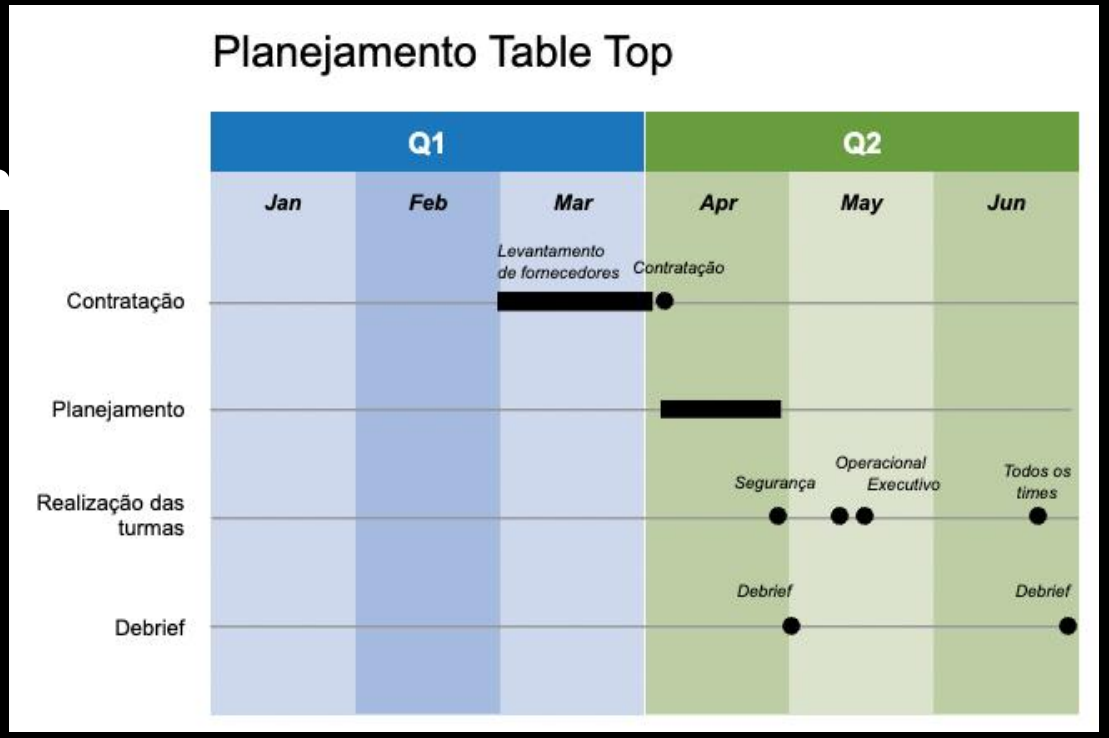
Fonte: CAMS MIT

TTX no C6 Bank

TEMPEST talks 2022

4 turmas planejadas (2021):

- **Turma 1 – Time de Ciber segurança**
- **Turma 2 – Times Operacionais**
- **Turma 3 – Executivos**
- **Turma 4 – Todos os Times (encerramento)**



“RFP”

TEMPEST talks 2022

A simulação deve ser realizada em um cenário fictício, através de exercícios e discussões guiadas através de recursos audiovisuais.

Duração: 2 a 3h

Os exercícios simulados devem contemplar os passos necessários para resposta a incidentes, incluindo:

1. Descritivo do exercício e expectativas
2. Descritivo do cenário de incidente
3. Detecção do incidente
4. Acionamento de crise e continuidade;
5. Acionamento do DPO
6. Reporte a clientes, imprensa e autoridades (ex BACEN, ANPD)
7. Acompanhamento macro do Processo para identificação, classificação, contenção, resposta e finalização do incidente cibernético
8. Validar:
    a. registro do incidente
    b. análise de causa (causa raiz)
    c. analise de impacto
    d. tratativa do incidente
    e. Relatório e report do incidente
9. Avaliação de resultados: pontos positivos, negativos e melhorias

Turmas:

Este projeto prevê a execução do exercício simulado (tabletop) em 4 turmas, que devem ser realizadas no formato ONLINE:

1. time de Segurança
2. time de continuidade de negócios e DPO
3. Executivos
4. Exercício com todos os envolvidos

Convite “Urgente: Os dados vazaram” ;)

TEMPEST talks 2022

Fomos procurados por um jornalista que nos informou que uma base de dados do C6 Bank está disponível na Internet, e o portal deles vai soltar a notícia em 30 minutos.

CALMA, ISSO NÃO É VERDADE! É SÓ UMA SIMULAÇÃO!

Mas, o que você faria numa situação dessas? Quem você vai chamar? Que times devem ser envolvidos? Que informações você precisa?

Para entender isso, nós vamos realizar um exercício simulado de **resposta a incidentes de segurança**. Os exercícios e discussões guiadas vão nos ajudar a entender como reagir na eventual ocorrência de um problema crítico de segurança, quais os times envolvidos e com quem você poderá contar imediatamente.

Reserve a sua agenda para esse exercício simulado! Esperamos você!

Pré-work

- Conhecer as normas MN-088 Resposta a eventos & incidentes de Segurança da Informação e MN-122 - Plano de Resposta a Incidentes
- Ver na Intranet: Norma de resposta a incidentes: saiba como tratamos casos envolvendo privacidade e segurança
- Exemplo da importância de testes e treinamento: filme "K-19: The Widowmaker (2002)"
    - trailer: https://www.youtube.com/watch?v=lZIFPBPxHzY

Feedbacks recebidos

TEMPEST talks 2022

“Ótima iniciativa. Tema super relevante para os times técnicos, e também para todos os funcionários do C6. Todos tem atuação numa situação dessas, e claro que alguns participarão mais ativamente e outros nem tanto. Mas todos devem conhecer o plano e saber qual o seu papel.”

“O treinamento foi excelente. Algumas situações propostas já estavam em nosso radar, mas outras não e foi possível levantar muitas possíveis melhorias em nossa resposta a incidentes.”

Referências

NIST SP 800-160 Vol. 2 Rev. 1 - Developing Cyber-Resilient Systems

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

Building Cyber-Resilient Organizations with Fire Drills and Tabletop Exercises

https://cams.mit.edu/wp-content/uploads/CAMS_Firedrills_and_Tabletop_Exercises.pdf

10 Benefits of Running Cybersecurity Exercises (DarkReading)

https://www.darkreading.com/operations/10-benefits-of-running-cybersecurity-exercises

Referências

TEMPEST talks 2022

Cyber Resilience Act (EU)

https://digital-strategy.ec.europa.eu/en/library/cyber-resilienc

Scottish government offers cyber resilience training to hundreds of organisations

https://www.csoonline.com/article/3669254/scottish-government-offers-cyber-resilience-training-to-hundreds-of-organisations.html

Locked Shields

https://ccdcoe.org/exercises/locked-shields/

#ficaadica

TEMPEST talks 2022

Backdoors & Breaches, an Incident Response Card Game

https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

Dúvidas?

TEMPEST talks 2022

Na paz, preparar-se para a guerra; Na guerra, preparer-se para a paz.

Sun Tzu

TEMPEST talks 2022

Obrigado


TEMPEST talks
2022