Inter Forensics
CONFERÊNCIA INTERNACIONAL DE CIÊNCIAS FORENSES 2023

28 a 31 de Agosto/2023
BRASÍLIA / BRASIL

RANSOMWARE: ESTRATÉGIAS DE PREVENÇÃO, INVESTIGAÇÃO E RECUPERAÇÃO

MARCELO CAIADO, M.Sc.

CISSP, GCFA, GCIH, GSLC, CCO, CCPA, CHFI, CTIA, CCFC, CRC

REALIZAÇÃO: Fundação Justiça pela Ciência; Escola Nacional de Perícias; APCF Associação Nacional dos Peritos Criminais Federais

APOIO INSTITUCIONAL: Polícia Federal; Comitê Internacional da Cruz Vermelha

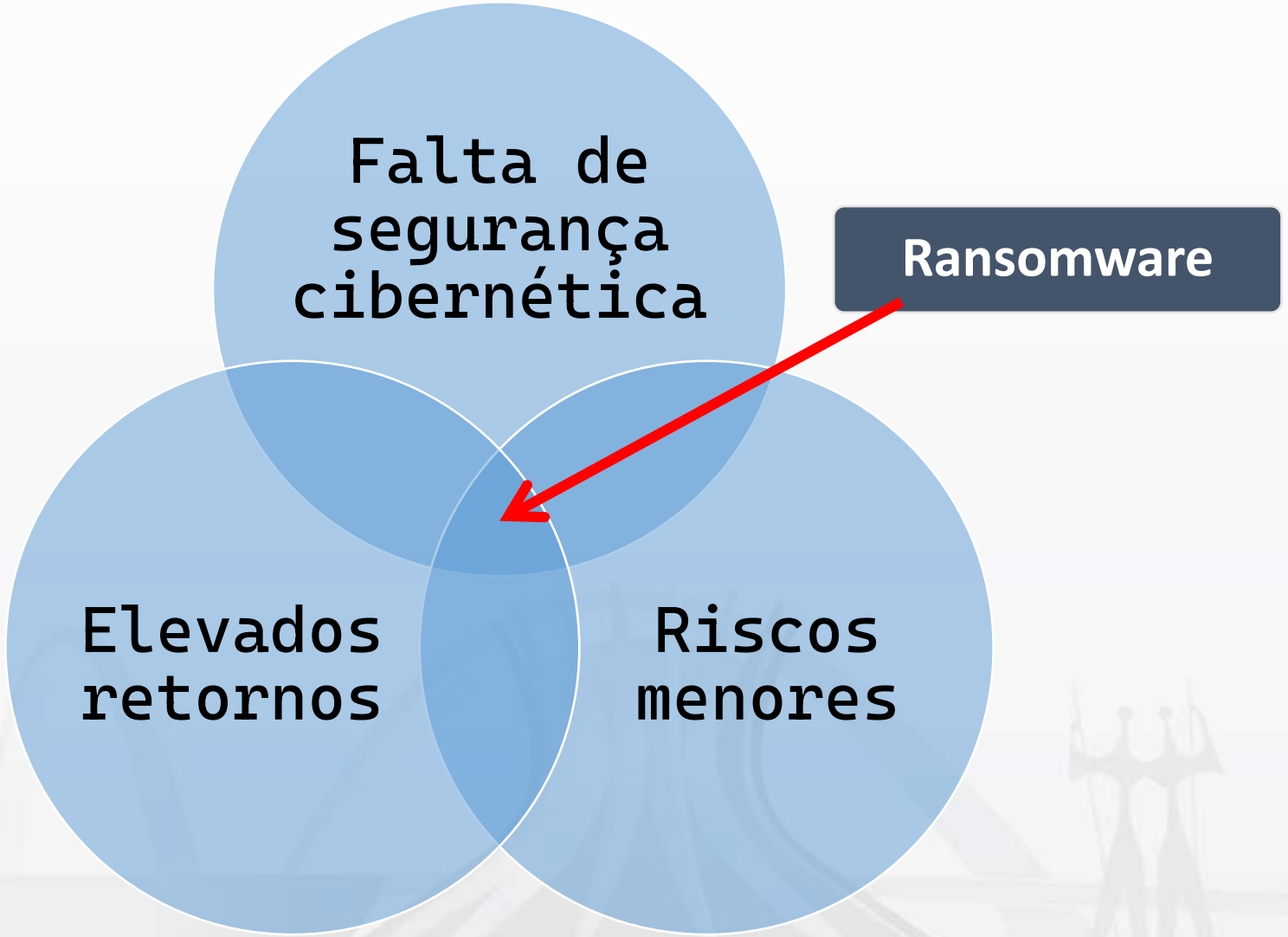
Aviso Legal

Todas as opiniões apresentadas aqui são exclusivas do orador, apenas para fins ilustrativos, e são pessoais e não representam as de pessoas, instituições ou organizações com as quais o apresentador possa estar associado em capacidade profissional ou pessoal, a menos que explicitamente declarado. Quaisquer opiniões ou pontos de vista não são recomendações técnicas e nem jurídicas, e não têm a intenção de difamar qualquer religião, grupo étnico, clube, organização, empresa ou indivíduo.

Sobre

- Mestre em Ciência da Computação (UnB)
- Pós-graduado em Gestão Pública (FGV)
- Perito em TIC / MPF
- Cyber Forensics Analyst / BlackBerry
- Professor (INSPER, IDESP, IPOG e WB)
- Coautor dos livros Cyber Risk e Técnicas Avançadas de Investigação
- Idealizador e mantenedor do http://dfir.com.br/

Crime organizado



Russia arrests alleged hacking group members

Prevenir

- Conscientização de usuários
- Segurança de rede e de dispositivos
- Estratégia de resiliência cibernética

Prevenir – Conscientização de Usuários

Prevenir – Segurança de Rede e de Dispositivos

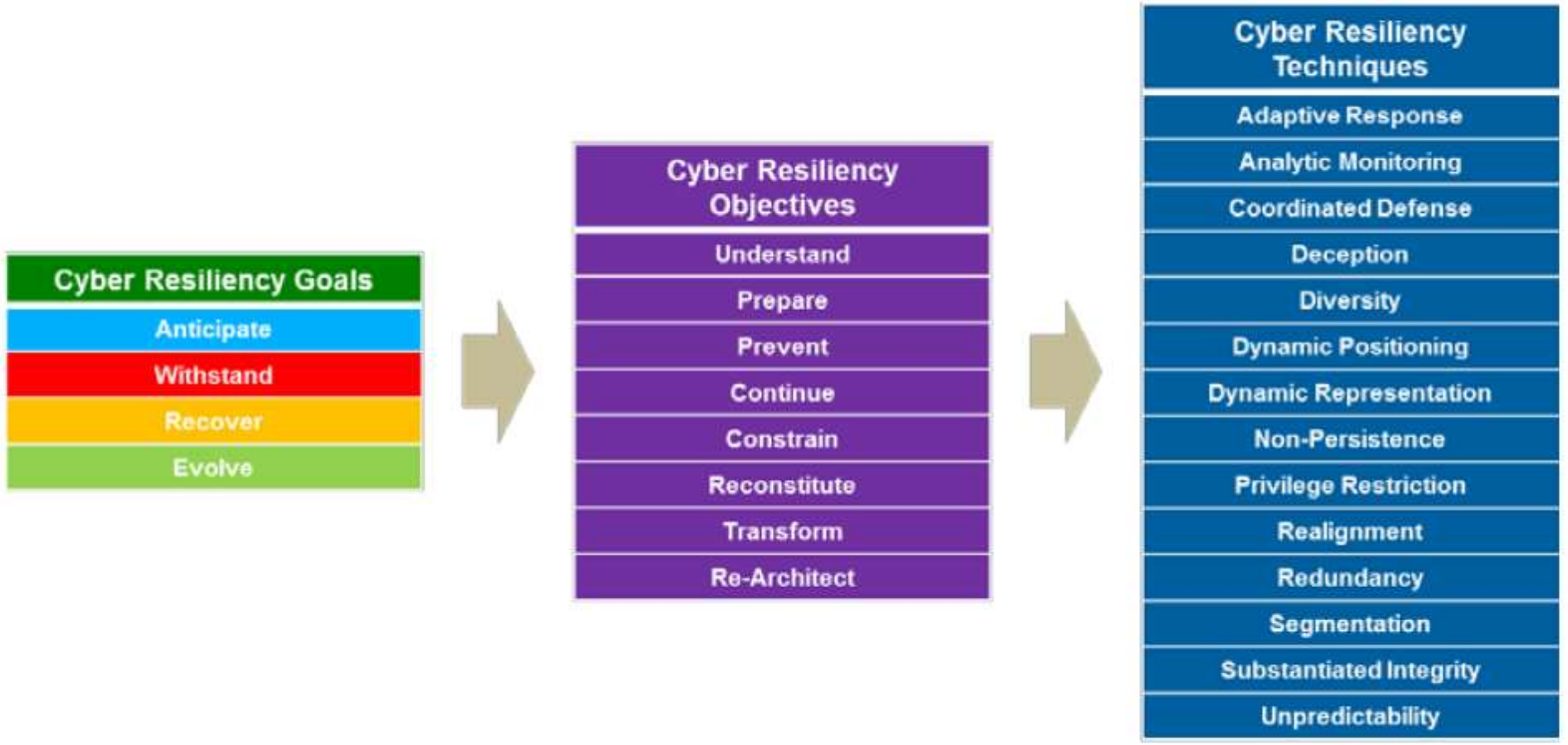


Figure 2. Cyber Resiliency Engineering Framework

Investigar

- Executar ferramentas de triagem
- Executar análise de causa raiz
- Seguir o dinheiro

Investigar – Ferramentas de Triagem e *Hunting*

Velociraptor

VIRUS TOTAL

MISP Threat Sharing

KAPE

Investigar – Ferramentas de Triagem e *Hunting*

Velociraptor

VIRUS TOTAL

MISP
Threat Sharing

KAPE

Investigar – Causa Raiz

Inter Forensics
CONFERÊNCIA INTERNACIONAL DE CIÊNCIAS FORENSES 2023

28 a 31 de
BRASÍLI

Investigar Siga o Dinheiro

Restaurar

- Empregar planos de recuperação de curto e longo prazos
- Usar ferramentas antivírus e antimalware
- Prevenir ataques futuros

Restaurar – Planos de Recuperação

Restaurar – Ferramentas

Restaurar – Prevenir Ataques Futuros

Referências

- Mitre ATT&CK: https://attack.mitre.org
- IPED: https://github.com/sepinf-inc/IPED
- CERT.br: https://cartilha.cert.br/ransomware/
- Ransomware Database: https://www.ransom-db.com
- Velociraptor: https://github.com/Velocidex/velociraptor
- SANS Digital Forensics: https://digital-forensics.sans.org
- Stop Ransomware: https://www.cisa.gov/stopransomware
- Eric Zimmerman's Tools (Kape): https://ericzimmerman.github.io
- Mitre Cyber Resiliency: https://www.mitre.org/sites/default/files/publications/13-4047.pdf
- NIST Tips & Tactics Ransomware: https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf

"O ransomware é um grande negócio, possibilitado por redes inseguras que permitem aos criminosos obter acesso às redes, em primeiro lugar, e por criptomoedas que permitem pagamentos que os governos não podem interditar. O ransomware tornou-se o modelo de negócio do crime cibernético mais lucrativo e, até resolvermos esses dois problemas, isso não vai mudar."

Bruce Schneier, maio de 2021

Contato

https://www.linkedin.com/in/caiado

http://dfir.com.br/about

WWW.INTERFORENSICS.COM

@InterForensics

REALIZAÇÃO:

APOIO INSTITUCIONAL: