Cyber Threat Intelligence x Cybercrime Investigations: aprendendo com o mercado e contribuindo com o futuro

GTS 2019

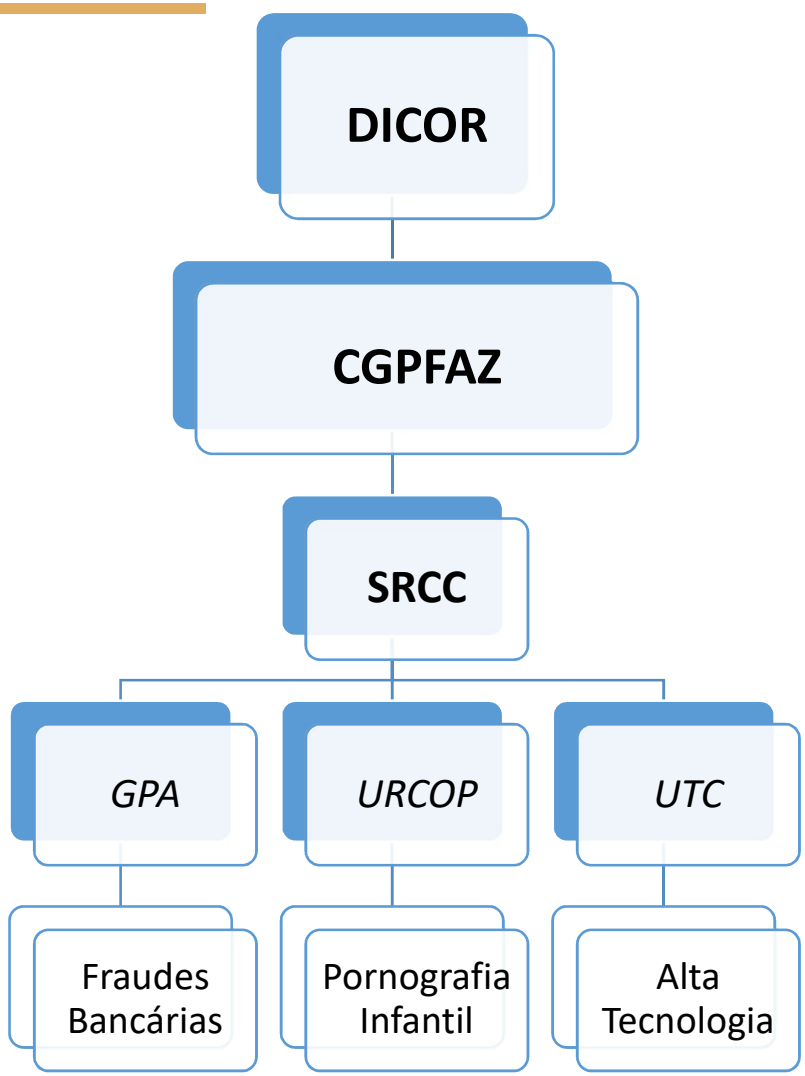
$ whoami

- PoP-BA/RNP (1994 – 2004)
- CAIS/RNP (2004-2007)
- Polícia Federal – Diretoria de TI (2007-2011)
- Polícia Federal - Serviço de Repressão a Crimes Cibernéticos (2011-2019)
- Triatleta e músico amador
- Pai “profissional”

Polícia Federal

- **Polícia judiciária da União**
- Infrações de repercussão interestadual internacional que exigem repressão uniforme
- Tráfico de drogas, contrabando e descaminho
- Polícia marítima, aeroportuária e de fronteiras
- Conflitos agrários

Introdução


DICOR
CGPFAZ
SRCC
GPA
URCOP
UTC
Fraudes Bancárias
Pornografia Infantil
Alta Tecnologia

Introdução

SRCC/CGPFAZ/DICOR/PF

Introdução

- Criada em 2003 e formalizada em 2011
- Atribuição de coordenação das ações de:
  - **Combate às fraudes eletrônicas (GPA – Grupo Permanente de Análise)**
    - **Internet banking**
    - **Clonagem de cartões de crédito/débito**
  - **Combate aos crimes de Alta Tecnologia (UTC)**
  - **Combate à pornografia infantil**
    - **URCOP criada em 2003 e incorporada à SRCC em 2014**

Missão

Coordenação	Capacitação e Treinamento	Desenvolvimento de Tecnologia de Investigação	Cooperação Internacional
• Combate às fraudes eletrônicas • Segurança cibernética • Crimes de alta tecnologia • Pornografia infantil • Apoio aos crimes cibernéticos impróprios	• Cursos a distância para difusão do conhecimento básico • Cursos presencias para aperfeiçoamento e especialização	• Ferramentas específicas para busca de informações e de investigação / inteligência policial • Apoio em investigações de alta complexidade	• Cooperação na área de crimes cibernéticos com outros países e forças policiais

UTC/SRCC

Crimes de Alta Tecnologia

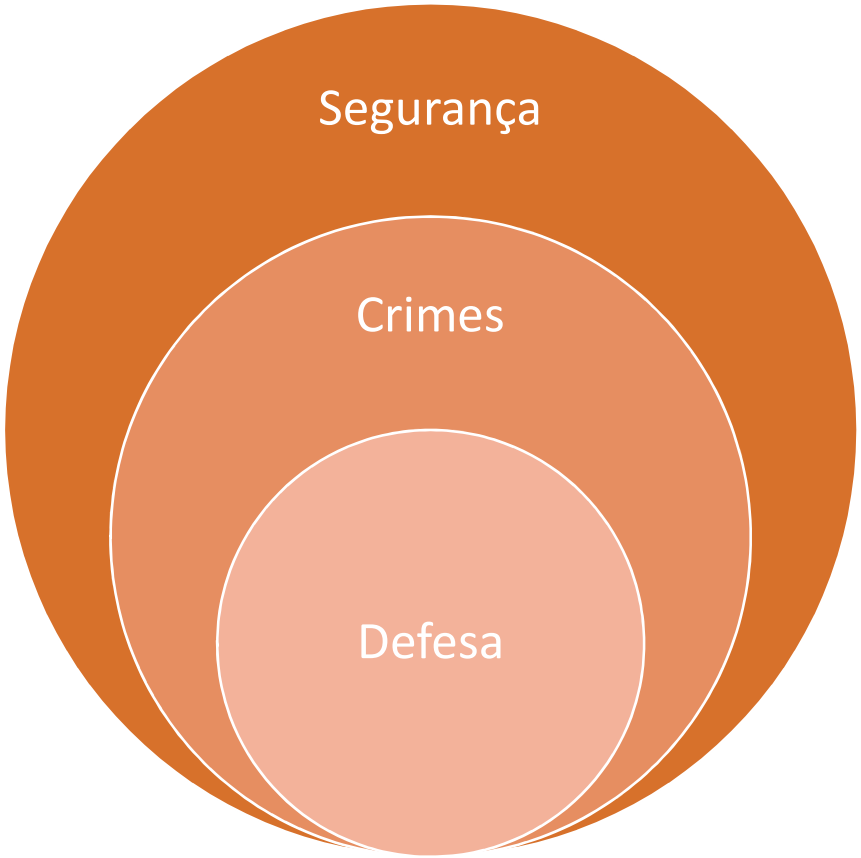
Prospecção e desenvolvimento de novas tecnologias

Capacitação

Crimes Cibernéticos

- Fraude Bancária
  - 3 bilhões de prejuízo em 2018
- Pornografia Infantil
  - 40 mil ocorrências por mês
- Crimes de Alta Tecnologia
  - Invasão
  - Vazamentos de dados
  - Sequestro de dados (*ransomware*)
  - Negação de serviço
  - Mineração clandestina de criptomoedas - *cryptojacking*

Crimes Cibernéticos



Segurança cibernética é responsabilidade de todos!

- Setor Privado e Setor Público!
  - Justiça
  - Polícia judiciária
  - CSIRTs
  - Agências de Inteligência
  - Terceiro setor
  - FFAA
  - Etc...

Crimes Cibernéticos

- Atores principais
  - ETIR/CSIRT – First Responder + Notificação de incidentes + Tendências
  - Polícia Judiciária/MP/Justiça – Investigação e responsabilização dos crimes cibernéticos
  - Empresas de Segurança da Informação – *Cyber Threat Intelligence*
  - Forças Armadas – Defesa Cibernética
  - Governo – Estratégia de Segurança Cibernética / Inteligência Cibernética
- **Integração entre os atores tem funcionado?**

Crimes Cibernéticos

O sistema de informática da Companhia de Docas do Ceará (CDC) foi invadido na madrugada de segunda-feira (28) e continua fora do ar

Na madrugada desta segunda-feira (28), o sistema de informática da Companhia de Docas do Ceará (CDC), que administra o porto de Mucuripe, em Fortaleza, foi vítima de um ataque cibernético ao ser invadido por um ataque hacker, segundo o *Portal do Bitcoin*. Os invasores exigiram um resgate em Bitcoin e a Polícia Federal foi acionada para resolver o caso, mas a CDC não informou o valor pedido.

Crimes Cibernéticos

Ataque ocorreu contra uma das mais antigas rádios espanholas, a Caderna SER, e uma empresa de tecnologia, a Everis

Duas das maiores companhias espanholas, a Sociedad Española de Radiodifusión (Caderna SER) e a Everis, empresa de TI da Nippon Telegraph e Telephone (NTT), se tornaram vítimas de um ataque de ransomware.

Veja também:

- Ransomware que exige R$ 10 mil para desbloquear PC já está na América Latina
- Entenda a falha do Windows que pode causar um 'novo WannaCry'

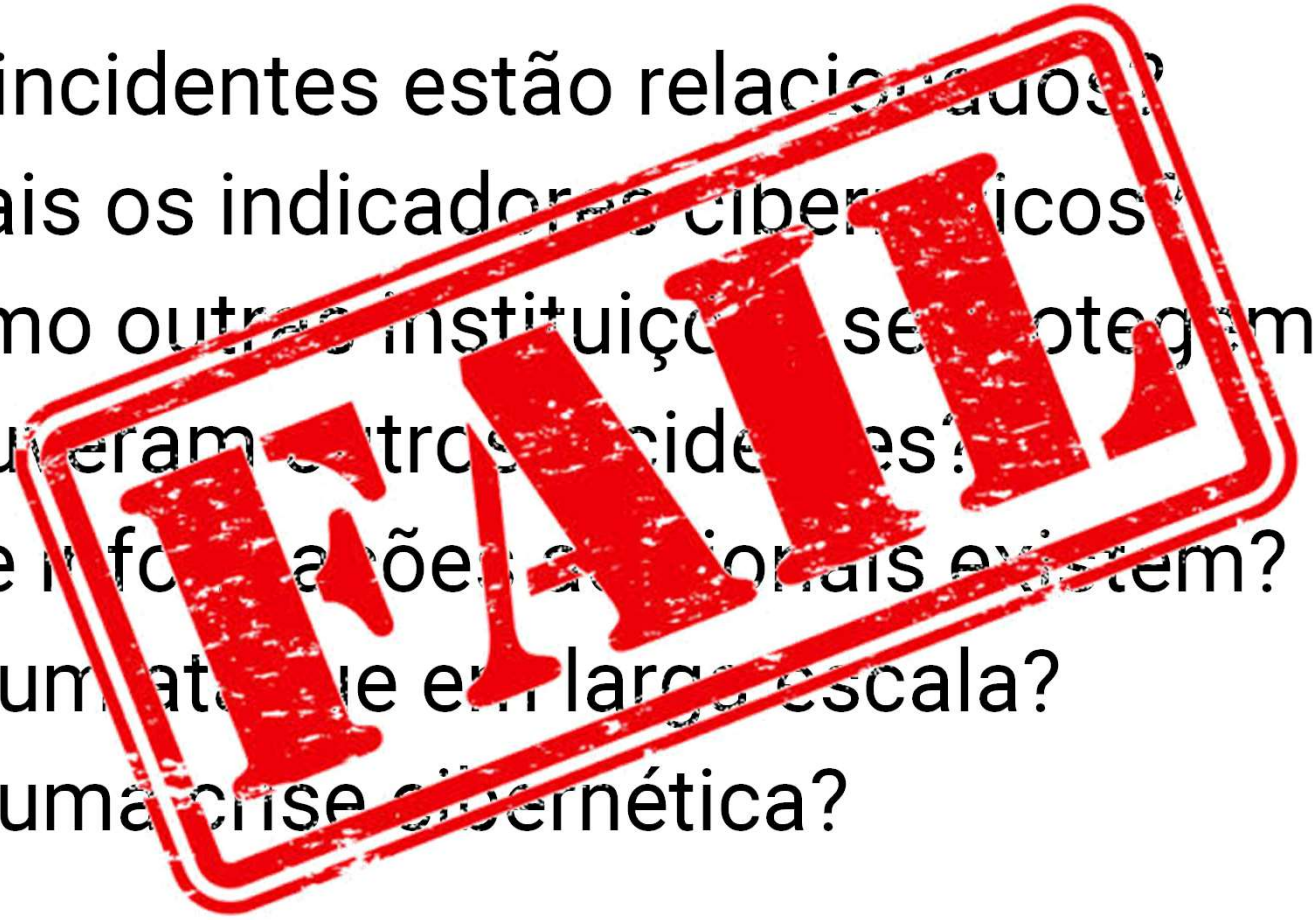
Um milhão de computadores Windows estão vulneráveis a ataque hacker BlueKeep

Por Thaís Augusto | 28 de Maio de 2019 às 18h40

Há duas semanas, a Microsoft disponibilizou um patch de segurança contra a vulnerabilidade BlueKeep, que permite a hackers executarem códigos de forma arbitrária para assumir o controle de um computador. Para ser executado, o BlueKeep não exige a interação do usuário com o código malicioso. Só que mesmo com o patch de segurança estando à disposição, cerca de 1 milhão de computadores Windows ainda não foram atualizados.

Crimes Cibernéticos

- Os incidentes estão relacionados?
- Quais os indicadores cibernéticos?
- Como outras instituições se protegem?
- Houveram outros incidentes?
- Que informações adicionais existem?
- Há um ataque em larga escala?
- Há uma crise cibernética?



Caso Wannacry

- Leia mais

  - Ataque cibernético muda rotina de equipes de tecnologia no País

Se no exterior o ataque cibernético WannaCry afetou grandes empresas, no Brasil quem sofreu mais foram os órgãos públicos. O Tribunal de Justiça de São Paulo (TJ-SP), por exemplo, teve mais de mil computadores afetados – 2% do total, segundo o órgão. O TJ-SP desligou parte de suas máquinas e interrompeu atendimentos na tarde dos ataques.

Outros órgãos da Justiça de São Paulo decidiram, preventivamente, desligar suas máquinas. “Quando recebemos a notícia de que o TJ tinha sido infectado, suspendemos toda a comunicação externa até que soubéssemos como lidar com o vírus”, explica Márcio Nisi, diretor da secretaria de TI do Tribunal Regional do Trabalho de São Paulo (TRT-SP).

A rede do TRT-SP ficou mais de 24 horas fora do ar – das 15h da sexta-feira até as 22h30 de sábado. Atitudes parecidas foram tomadas por ministérios como os do Trabalho e do Desenvolvimento Social.

Caso Wannacry

A Trend Micro liberou o estudo Round Up 2018, que mostra dados do cenário de ameaça cibernética e destaca os principais riscos aos usuários de internet. No estudo, a empresa descobriu que o Brasil foi um dos países que mais sofreram com ataques do ransomware WannaCry.

No total, foram cerca de 616 mil detecções do ransomware que sequestra os arquivos do computador e exige uma quantia em dinheiro para a liberação. Apesar do alto número, o estudo indica que muitos usuários conseguiram fugir da infecção ao atualizar o sistema operacional das máquinas.

Caso Wannacry

Há um ano, WannaCry infectava mais de 200 mil sistemas

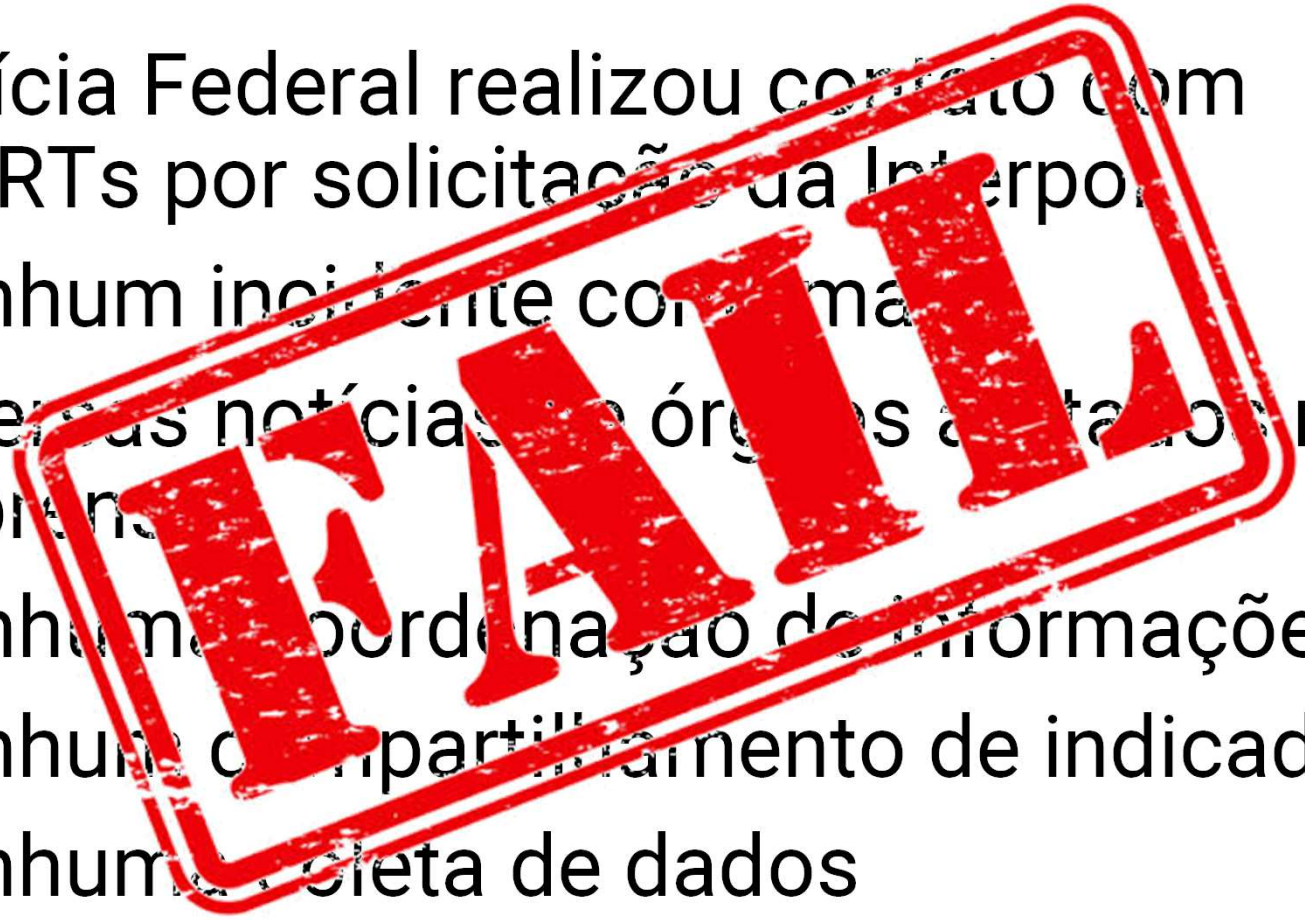
11 maio 2018

Na sexta-feira, 12 de maio de 2017, a comunidade global testemunhou o início da maior infecção de ransomware da história, que afetou mais de 200 mil sistemas em 150 países. A montadora Renault fechou sua maior fábrica na França e os hospitais do Reino Unido tiveram de rejeitar pacientes. Já no Brasil, o ataque causou a interrupção do atendimento do INSS, além de afetar empresas e órgãos públicos de 14 Estados mais o Distrito Federal.

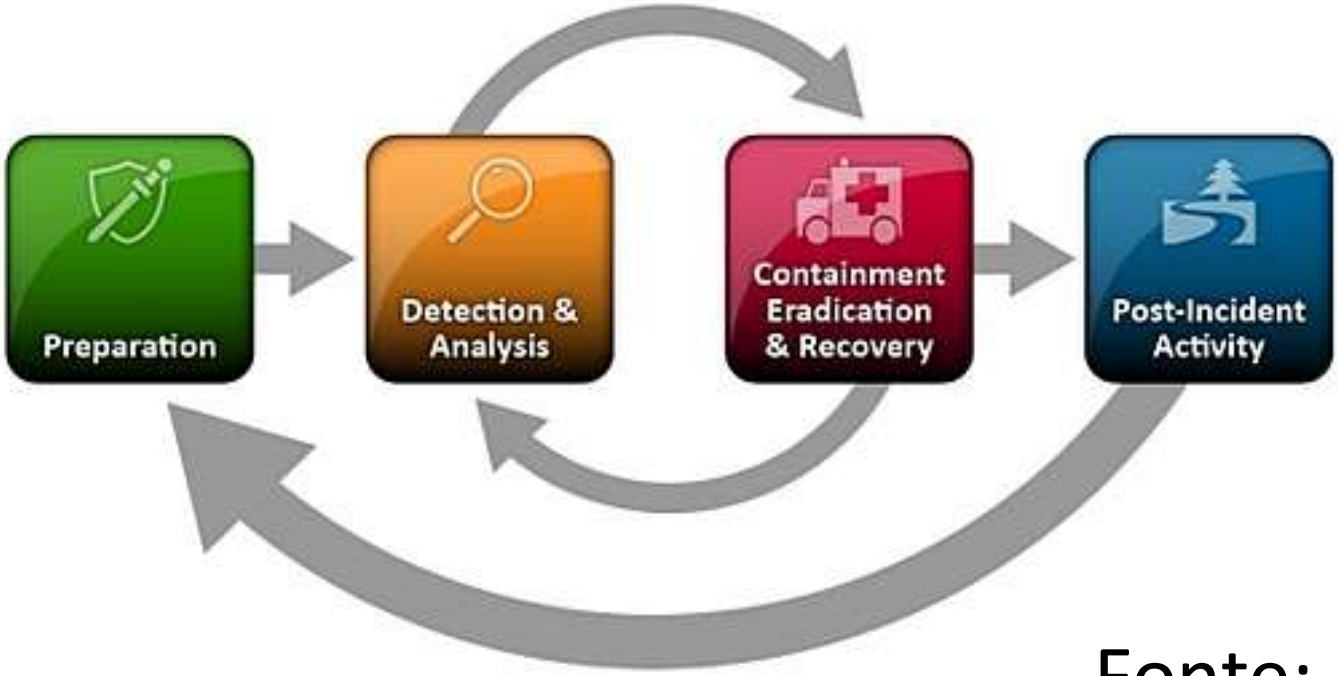
Nos dias após o ataque, os prejuízos foram se espalhando. O país mais afetado foi a Rússia, com 33,64% das empresas afetadas, seguido do Vietnã (12,45%) e Índia (6,95%). O Brasil foi o sexto mais atacado (4,06%).

Caso Wannacry

- Polícia Federal realizou contato com CSIRTs por solicitação da Interpol
- Nenhum incidente confirmado
- Diversas notícias em órgãos afetados na imprensa
- Nenhuma coordenação de informações
- Nenhum compartilhamento de indicadores
- Nenhuma coleta de dados



Dilema da ETIR



Fonte: NIST

Dilema da ETIR

- Norma Complementar 21/IN01/DSIC/GSIPR
- http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf
- Diretrizes para:
  - Registro de eventos
  - Coleta e preservação de evidências
  - **Comunicação às autoridades competentes**
- Problemas
  - Subnotificação
  - Falta de ETIR definida
  - Falta de triagem de informação

Exemplos internacionais (UK)

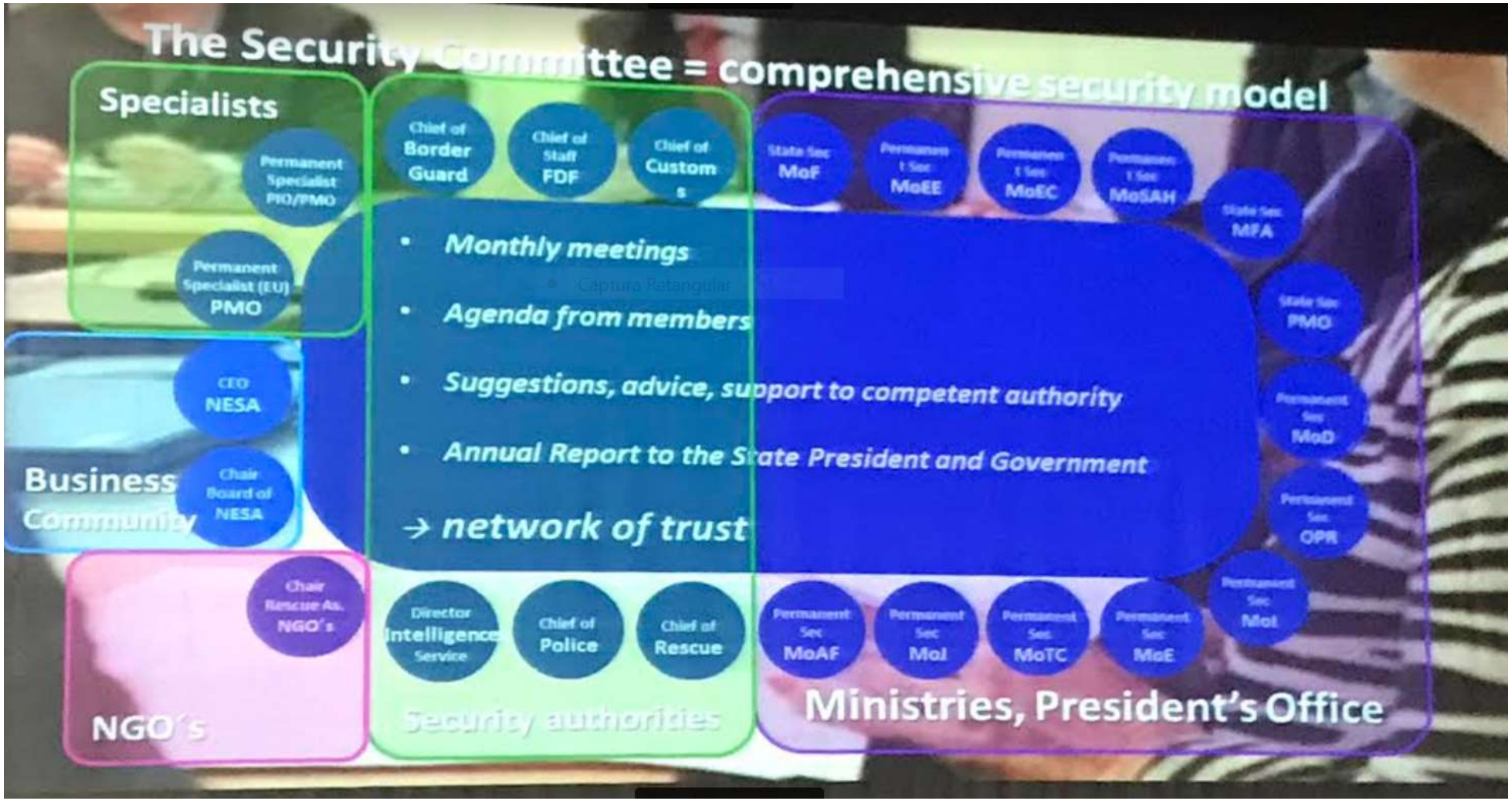
Embaixada Britânica
Brasília

Defence & Security Organisation

Caso de Estudo – CiSP

"É um Facebook Seguro para ameaças Cibernéticas"
UK Finacial Times

Exemplos internacionais (FI)



Crimes Cibernéticos

- Cooperação
  - **Ninguém tem uma visão completa do problema**.
  - Visibilidade é complexo: requer gente, tempo, tecnologia, armazenamento, etc.
  - Precisamos **trocar informações rapidamente**
  - **Rede de confiança nacional**
  - **Infelizmente tendemos a confiar em pessoas**
  - Pessoas passam, instituições ficam
  - Como resolver? **Tecnologia**?
- Exemplos atuais de redes de cooperação
  - FIRST (CSIRTs)
  - GTI / Febraban (Fraudes Eletrônicas)
  - SISBIN (Inteligência)
- **Transpor barreiras e pré-conceitos**

Crimes Cibernéticos

- Iniciativas do Governo Federal
  - Política Nacional de Segurnaça da Informação: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm
  - Estratégia Nacional: http://www.participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber
  - Exercício Guardião Cibernético
  - PLANO NACIONAL DE TRATAMENTO E RESPOSTA A INCIDENTES COMPUTACIONAIS – PNTIR
  - **Falta uma agência ou autoridade de segurança cibernética!**

Histórico

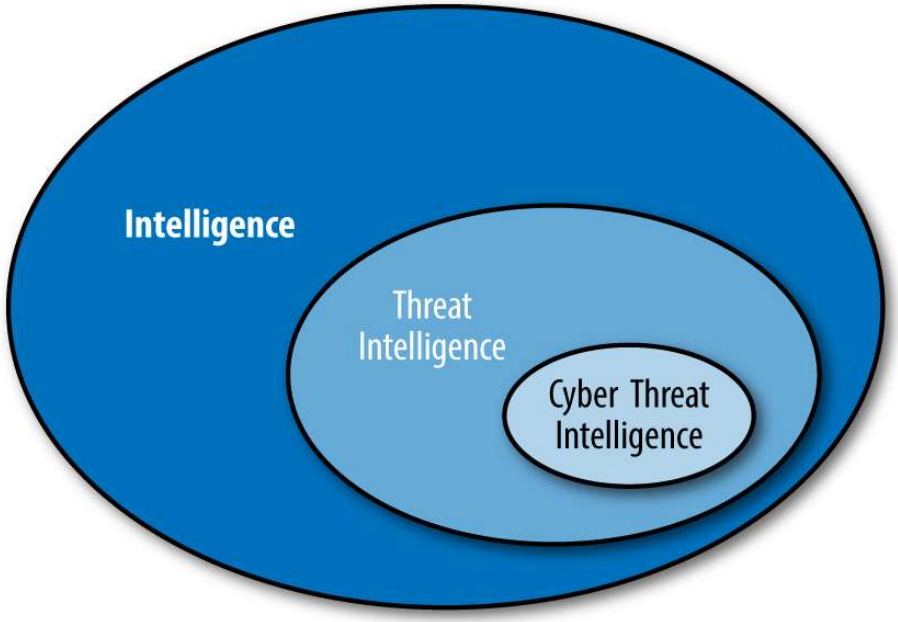
- 2010 – Projeto oráculo
  - Contexto dos grandes eventos
  - Experiência do projeto tentáculos
  - Crescimento dos crimes de alta tecnologia (DDoS, Invasão, *defacement*, *malware*, *botnets*, vazamentos)
  - Coleta massivas de dados e uso de tecnologia para prever **tendências** e ter dados **históricos**
- Problemas
  - Sabíamos onde queríamos chegar mas não sabíamos como
  - Falta de tecnologia
  - Falta de entendimento do problema
  - Foco excessivo em OSINT

Histórico

- Aftermath
  - Elaboração de uma especificação pelo CTI – Renato Archer
  - Criação de um piloto com coleta de redes sociais (twitter - demanda grandes eventos)
  - Migração do projeto para a SESGE (Colossus)
  - Foco em OSINT de redes sociais
- Outras iniciativas
  - Projeto EWS (USP/RNP) - https://gtews.ime.usp.br/
  - Ferramentas de empresas privadas
- Este assunto ficou dormente por um tempo..

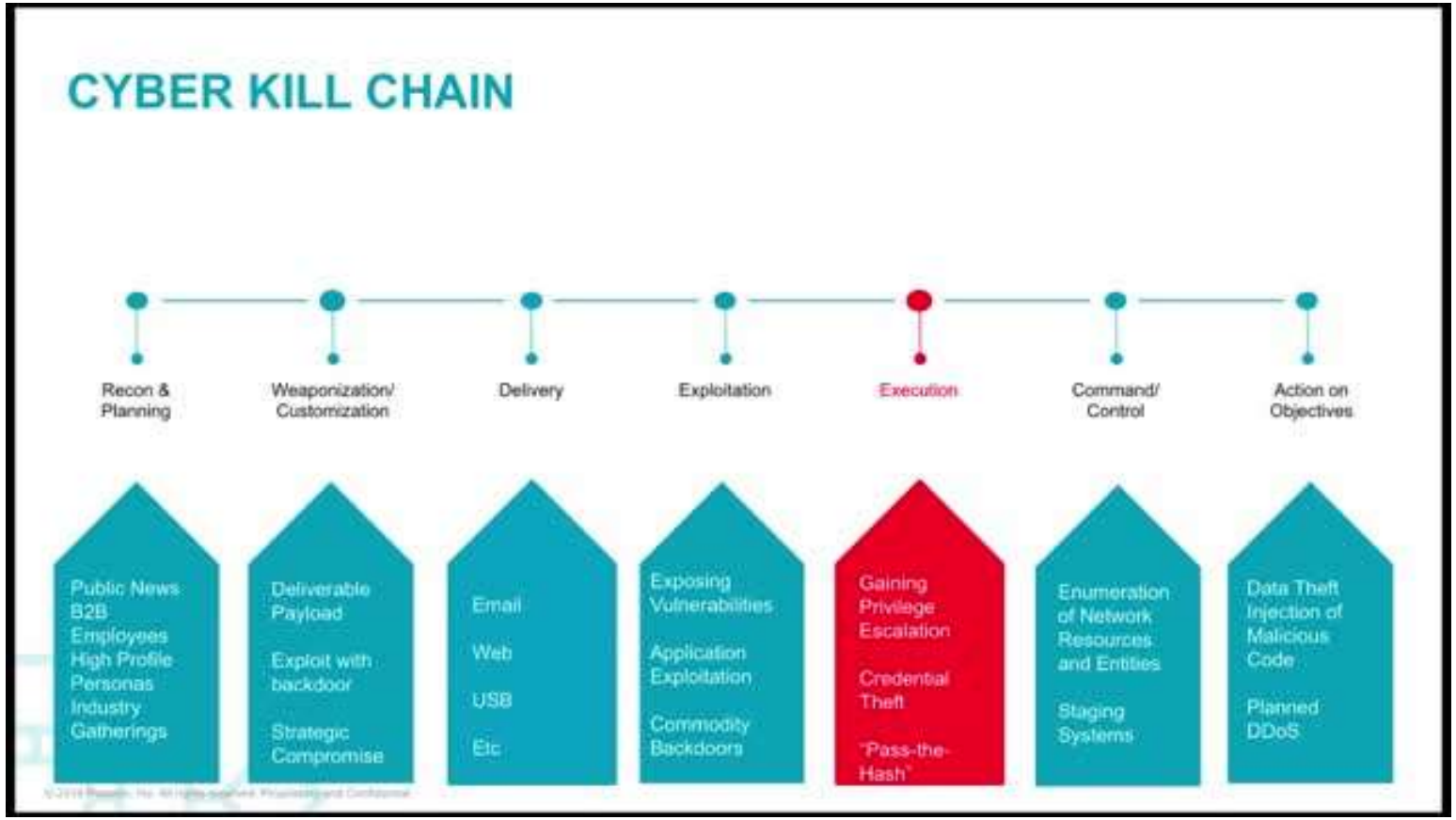
Novo Cenário

- *Cyber Threat Intelligence*
  - Inteligência de ameaças cibernéticas
  - Aplicação de doutrina de inteligência no campo cibernético
  - Evolução de resposta a incidentes (DFIR)
  - Análise de adversários, suas capacidades, motivações e objetivos



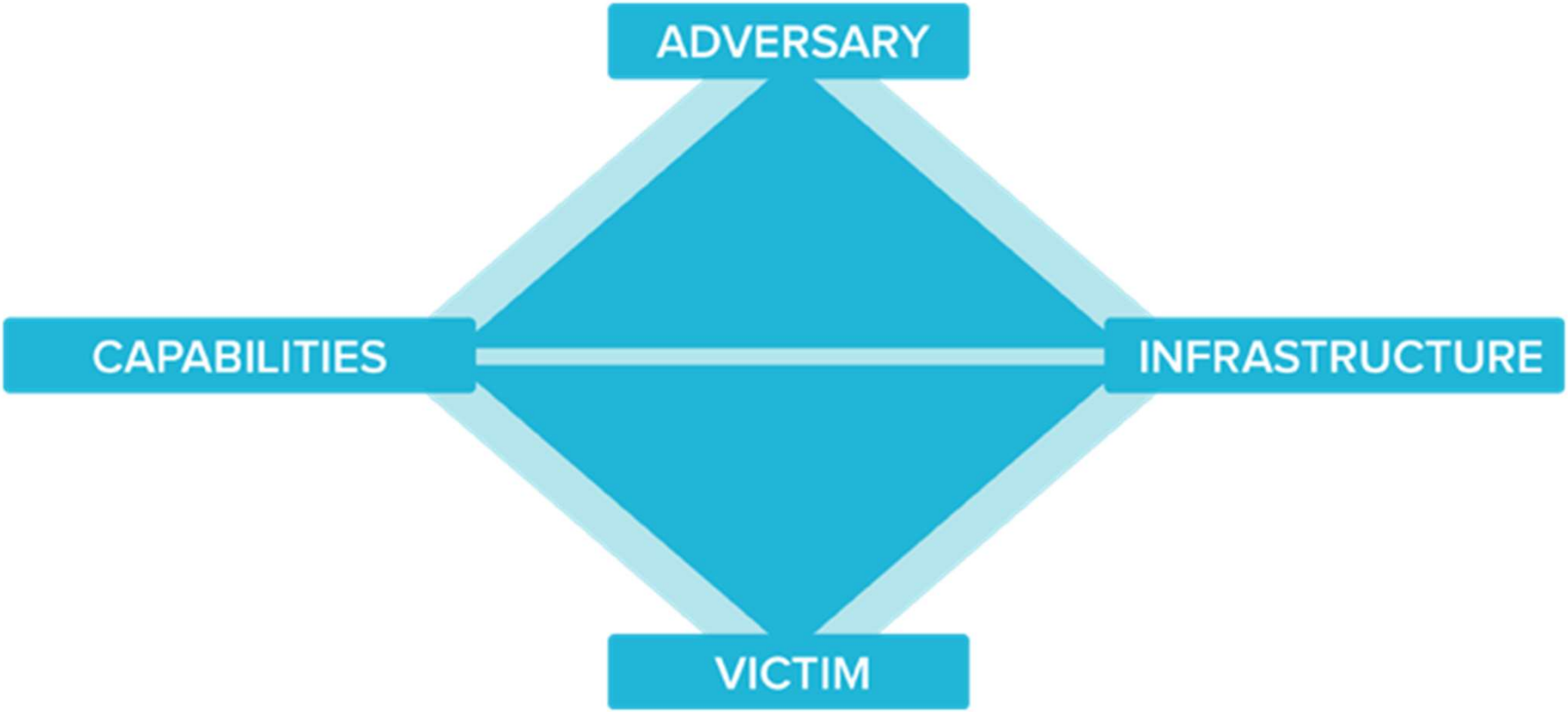
Novo Cenário

- Modelos
  - Cyber Kill chain



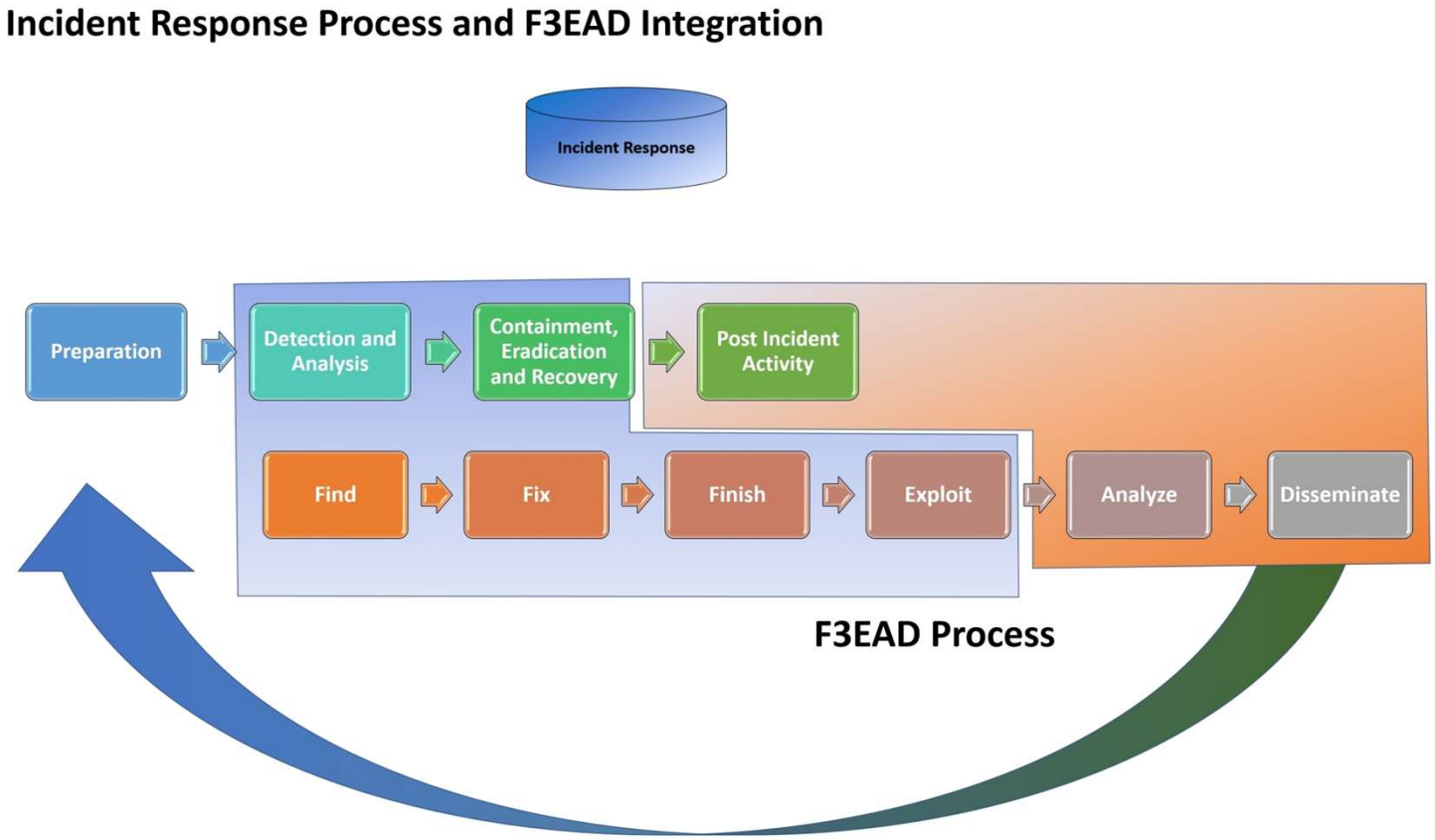
Novo Cenário

- Modelos
  - Diamond Model

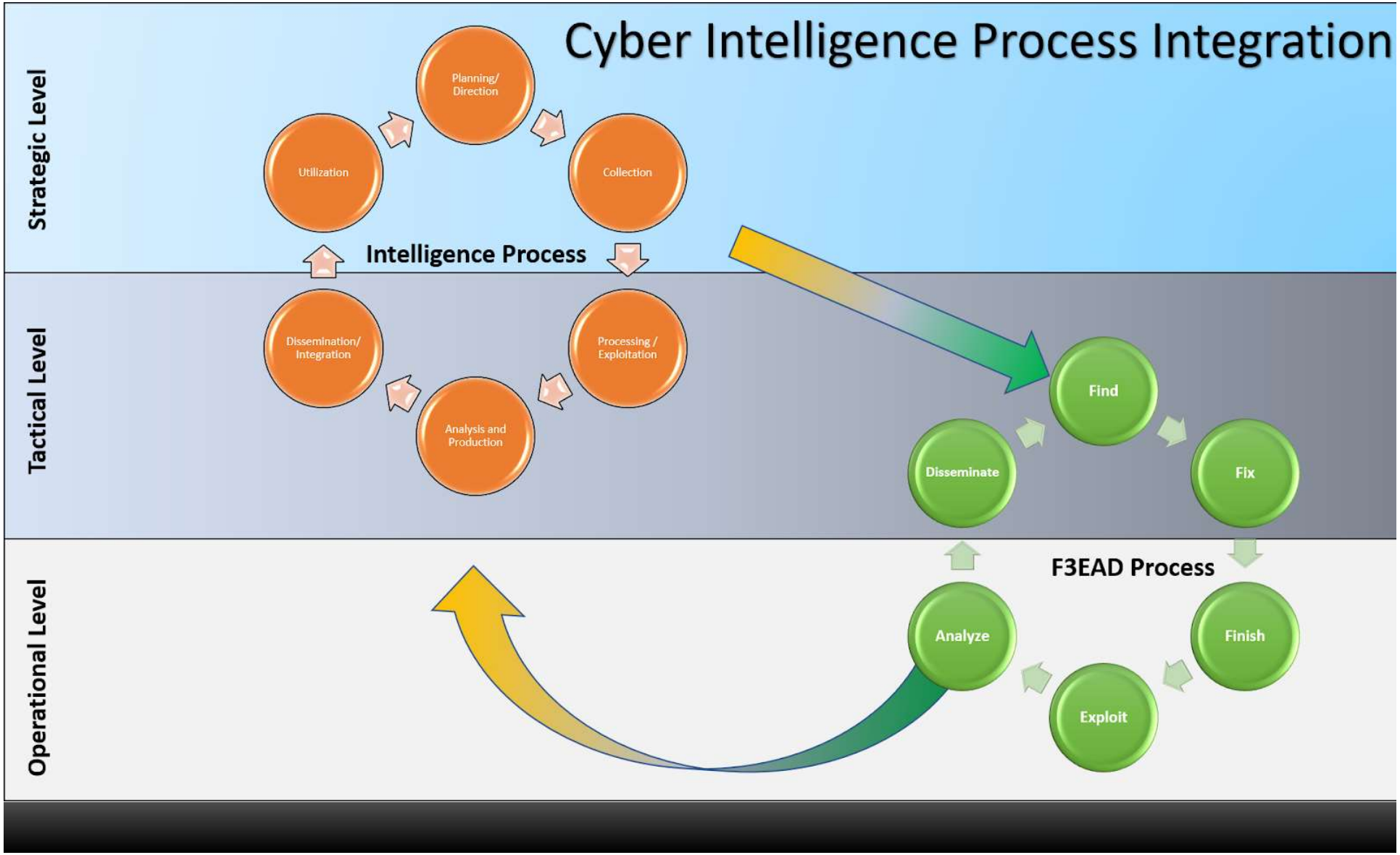


Novo Cenário

- Modelos
  - F3EAD



Novo Cenário



Novo Cenário

- *Cyber Threat Intelligence*
  - Setor privado avançando nesta área
  - Uso de doutrinas de inteligência militares/policiais
  - Mercado bastante promissor
  - Coleta massiva de informações de ameaçsa cibernéticas
  - **“Actionable intelligence”**
  - Diversas plataformas gratuitas e pagas
  - ... is expected to grow from USD 5.3 billion in 2018 to USD 12.9 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 19.7% during the forecast period.

Tecnologia

- https://www.misp-project.org/index.html
- **MISP - Open Source Threat Intelligence Platform &**
  Open Standards For Threat Information Sharing
- https://www.misp-project.org/communities/

Tecnologia

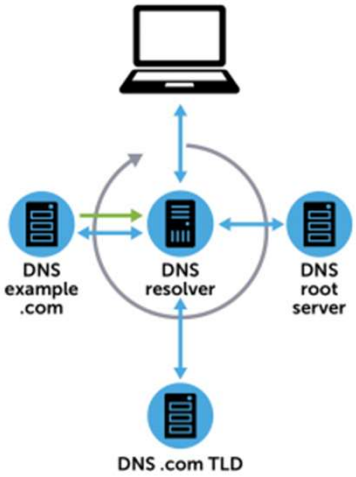
- Passive DNS
  - Dados históricos de consultas DNS
  - Fundamentais para “preencher os vazios”
  - Campanhas de *malware*
  - Histórico de hospedagens
  - Coleta acima do *resolver* de DNS
  - Visibilidade depende de regionalização da coleta
  - **Necessidade de uma coleta e disponibilização nacional**

Tecnologia

- Passive DNS

CIRCL Passive DNS

PDNS

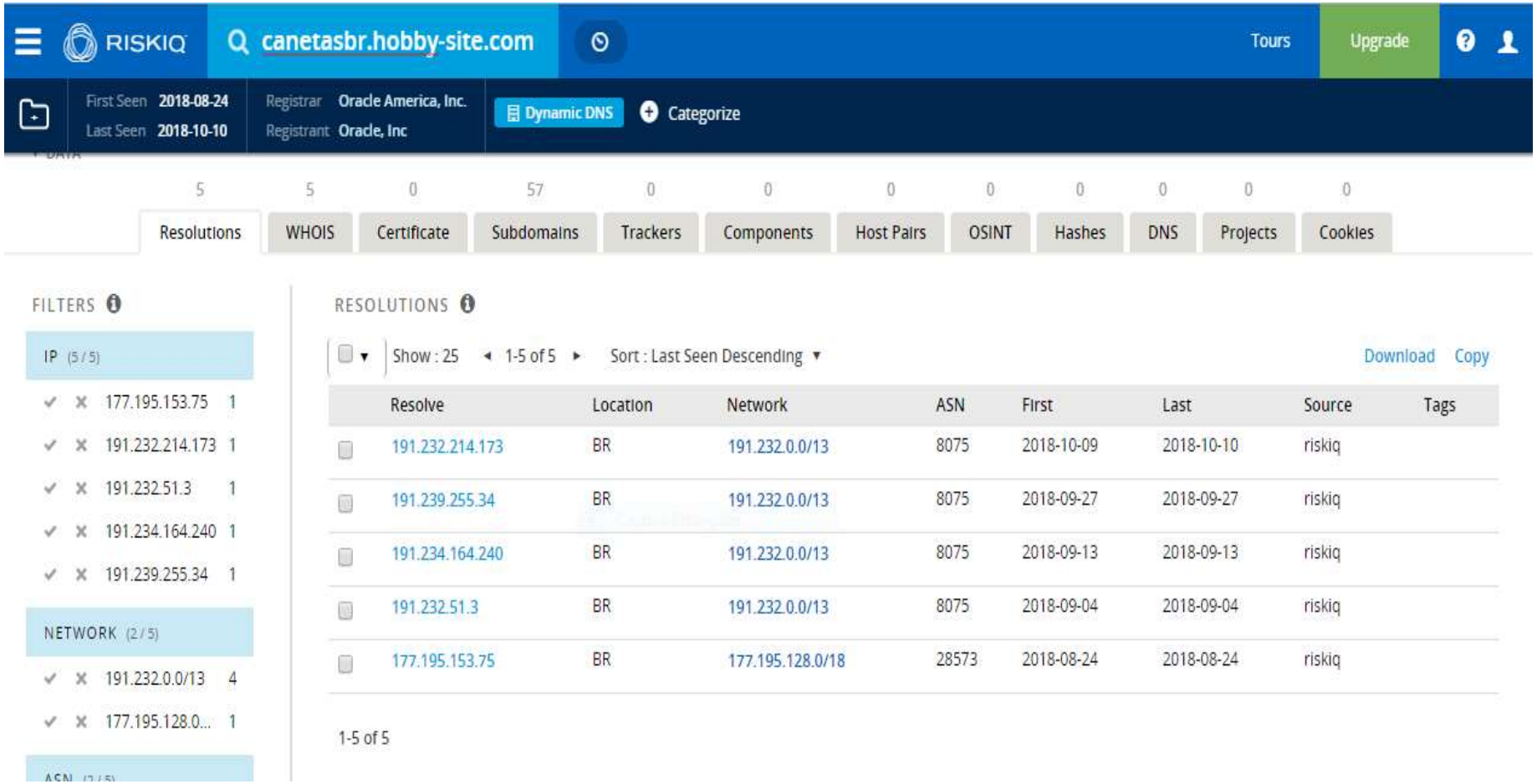


FARSIGHT SECURITY

Tecnologia

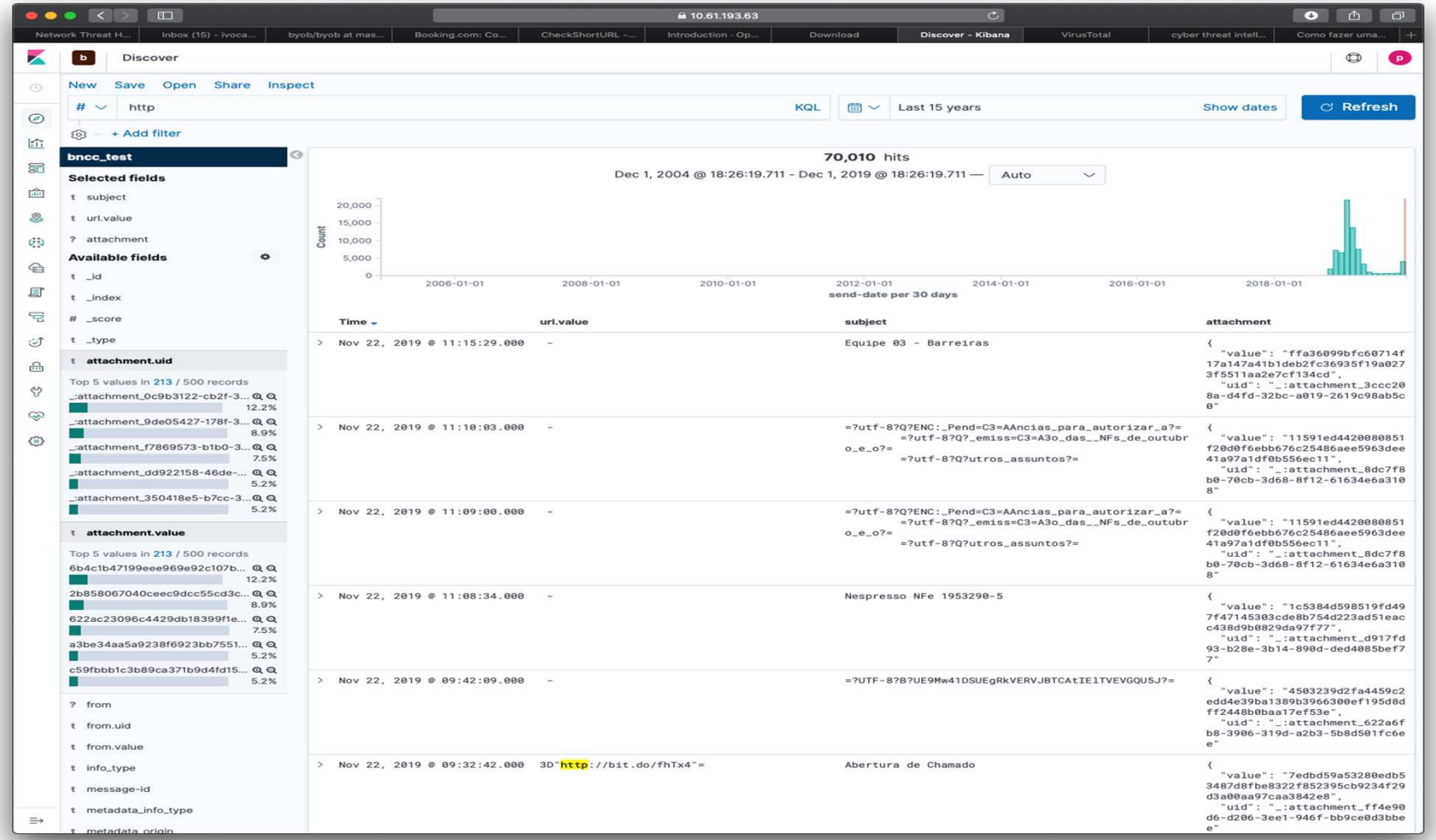
- Passive DNS

Tecnologia


RISKIQ
canetasbr.hobby-site.com
Tours
Upgrade
First Seen 2018-08-24
Last Seen 2018-10-10
Registrar Oracle America, Inc.
Registrant Oracle, Inc
Dynamic DNS
Categorize
5 5 0 57 0 0 0 0 0 0 0 0
Resolutions
WHOIS
Certificate
Subdomains
Trackers
Components
Host Pairs
OSINT
Hashes
DNS
Projects
Cookies
FILTERS
IP (5 / 5)
177.195.153.75 1
191.232.214.173 1
191.232.51.3 1
191.234.164.240 1
191.239.255.34 1
NETWORK (2 / 5)
191.232.0.0/13 4
177.195.128.0... 1
RESOLUTIONS
Show : 25
1-5 of 5
Sort : Last Seen Descending
Download
Copy
Resolve Location Network ASN First Last Source Tags
191.232.214.173 BR 191.232.0.0/13 8075 2018-10-09 2018-10-10 riskiq
191.239.255.34 BR 191.232.0.0/13 8075 2018-09-27 2018-09-27 riskiq
191.234.164.240 BR 191.232.0.0/13 8075 2018-09-13 2018-09-13 riskiq
191.232.51.3 BR 191.232.0.0/13 8075 2018-09-04 2018-09-04 riskiq
177.195.153.75 BR 177.195.128.0/18 28573 2018-08-24 2018-08-24 riskiq
1-5 of 5

Tecnologia

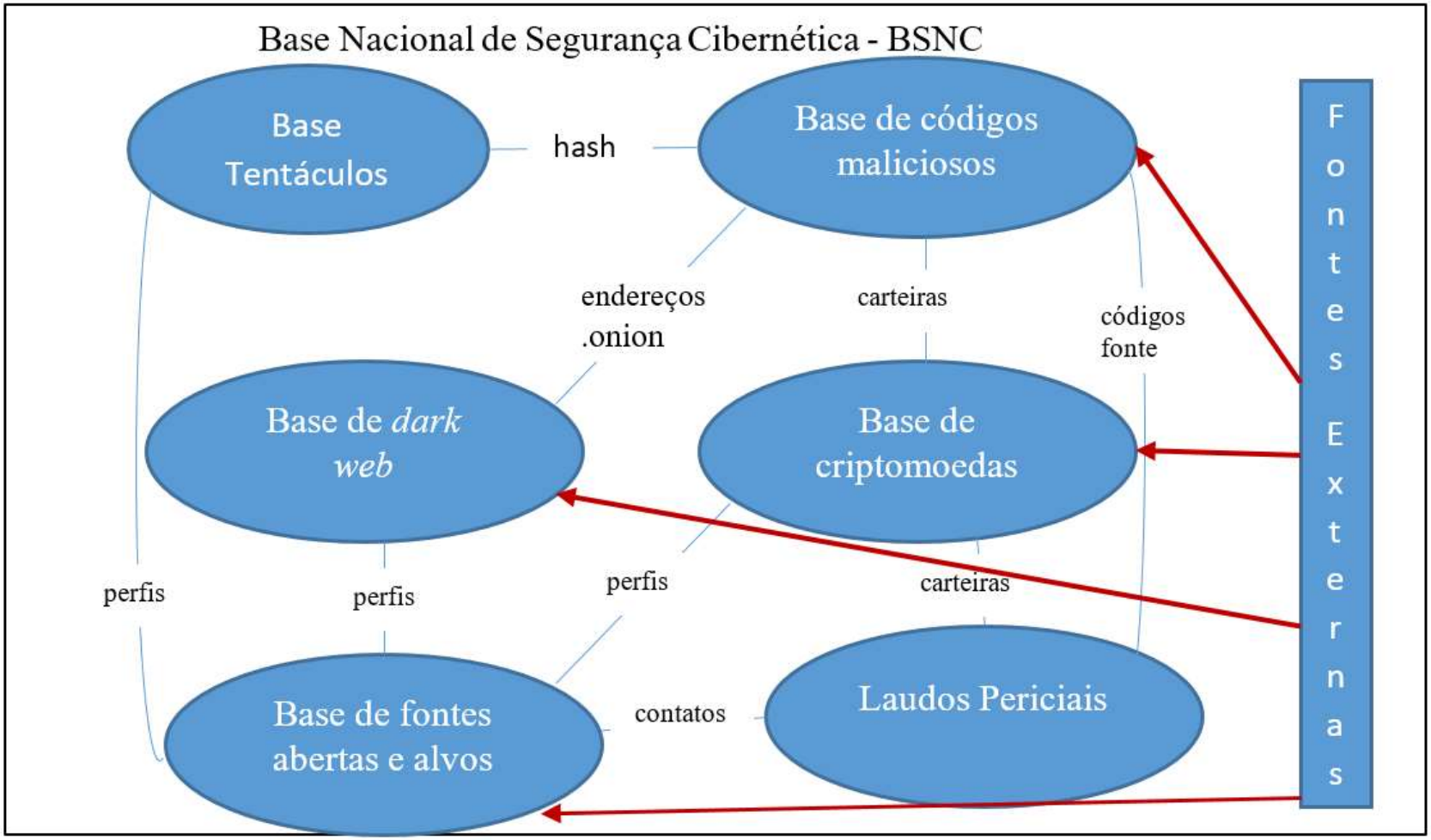
- Elasticsearch



Novo cenário

- **O cenário mudou!**
  - O setor privado evoluiu e passou a usar inteligência na proteção de suas redes – Cyber Threat Intelligence
  - Uso de modelos de inteligência militares e policiais
  - A tecnologia avançou e hoje existem padrões e ferramentas para viabilizar o que vislumbramos em 2011
  - STIIX/TAXII/Cybox, OpenIOC, ELK, Neo4J, Maltego, MISP, Cuckoo Sandbox, Passive DNS, Feeds de CTI, Machine Learning, etc...
  - Diversas empresas coletando e indexando dados sobre crimes cibernéticos
- **Oportunidades de parcerias e troca de experiências.**

Visão SRCC - BSNC



Cooperação SRCC

- Fraudes bancárias eletrônicas
  - Projeto tentáculos (Caixa / Febraban)
- Cooperação internacional
  - Dark0de / Wall Street Market / DeepDotWeb (FBI / Europol)
- Pornografia Infantil
  - Bases de *hashes* de arquivos conhecidos (Interpol / INHOPE / Project VIC / NCMEC)
- Crimes de alta tecnologia
  - Notificação e coordenação (Interpol / CSIRTs)
  - Ransomware (Empresas de AV)
  - Malware bancário (Caixa / BB / Itau)
  - Cyber Threat Intelligence (Kaspersky, Microsoft)
- **O que você / sua empresa tem em comum para trabalharmos juntos?**

Operação Código Reverso

Episódio na série crimes.com – Discovery Channel

Desafios

- **Cooperação**
  - Internacional (MLAT / Cybercrime 24/7)
  - Convenção de budapeste
  - Setor privado (*threat intelligence / hunting*)
- Criptografia
  - Dispositivos criptografados
    - Smartphones, mídias
  - Tráfego cifrado
    - Tor, VPN, etc
- Estrutura organizacional
  - ETIR constituída e operacional
  - SoC / Cyber Threat Intelligence
- Cultura de cybersegurança
  - Normativos e padrões de segurança (IN 21 – DSIC/GSI/PR)
  - Entidade regulatória
  - Cooperação e notificação de incidentes
- Subnotificação

Desafios

- CGNAT
  - Pedidos de identificação de suspeitos requerem portas de origem em IPv4 com CGNAT
  - Prejudica ENORMEMENTE as investigações
  - Serviços no Brasil não estão em IPv4 em muitos casos – O cliente ter IPv6 não adianta.
- **Precisamos definir um prazo para migrar os serviços para IPv6.**
  - **Governo poderia dar o exemplo**
  - **E-Ping tem recomendação mas ninguém segue**

Conclusões

- Ameaças cibernéticas
  - Cada vez mais complexas
    - Organizações criminosas – Células
    - Ataques *state sponsored* (guerra cibernética)
    - Troca de informações entre diferentes países
  - Cada vez mais numerosas
    - Brasil na vanguarda de ameaças
    - Valores impressionantes em fraudes e prejuízos
- Necessidade de mudanças de cultura
  - Segurança como algo constante e dedicado
    - Monitoramento, times de resposta, testes de penetração, red/blue teams, conscientização, etc.
  - Novas metodologias
    - ***Threat hunting*** e ***threat Intelligence***
- **Compartilhamento de informações a nível nacional**
    - **Confiança e colaboração.**

Obrigado

Ivo de Carvalho Peixinho
Perito Criminal Federal

E-mail: peixinho.icp@dpf.gov.br