OS RISCOS CIBERNÉTICOS NA AGENDA DAS CORPORAÇÕES BRASIL E GLOBAL

Cyber Insurance

10 DE MARÇO DE 2018

AGENDA

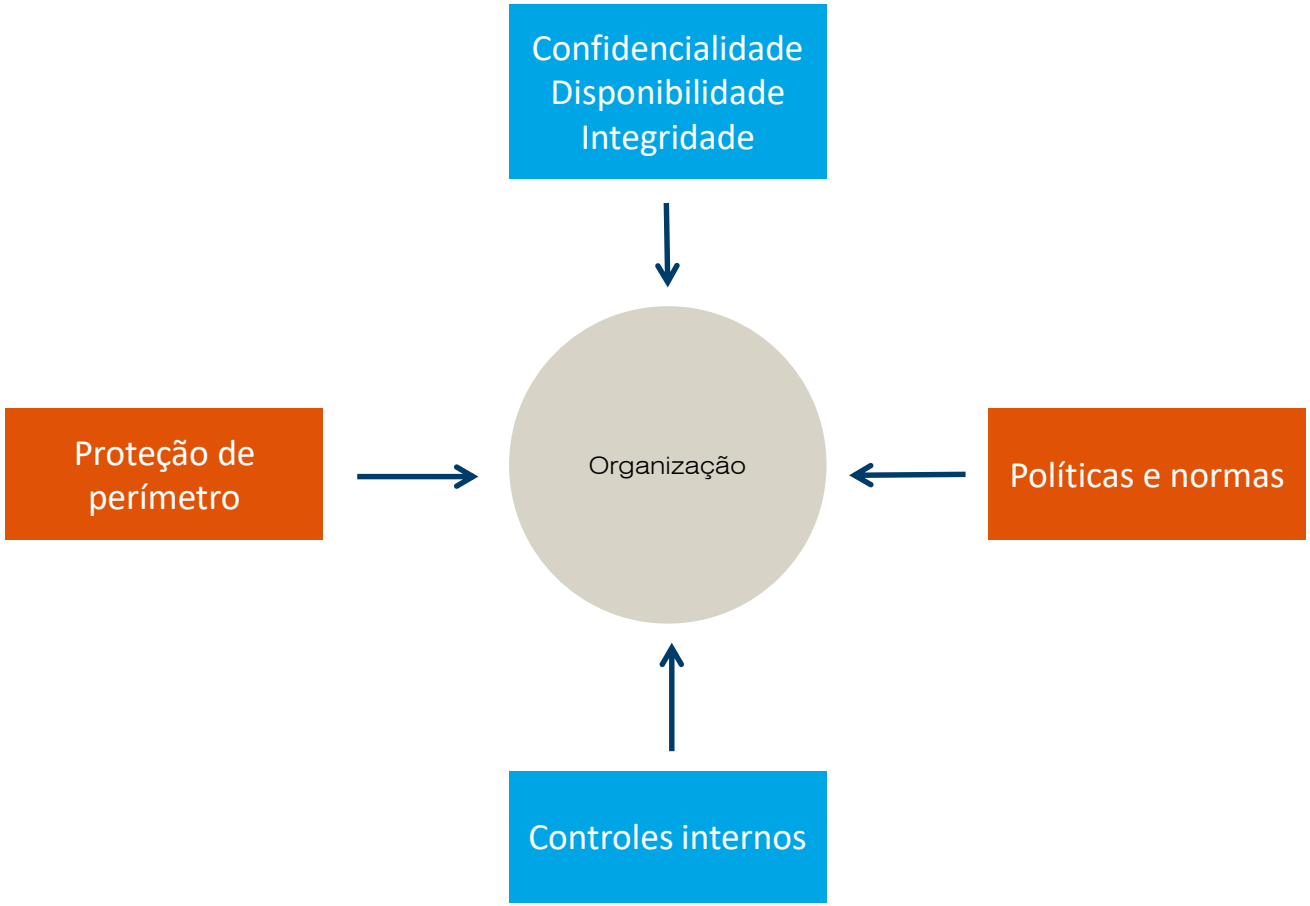
1. SEGURANÇA CIBERNÉTICA
2. DADOS DA PESQUISA
3. CENÁRIO REAL
4. CYBER INSURANCE
5. ABORDAGENS CONSULTIVAS
6. PERGUNTAS?

SEGURANÇA CIBERNÉTICA

Kroll

O QUE MUDOU?

VISÃO TRADICIONAL DE SEGURANÇA DA INFORMAÇÃO



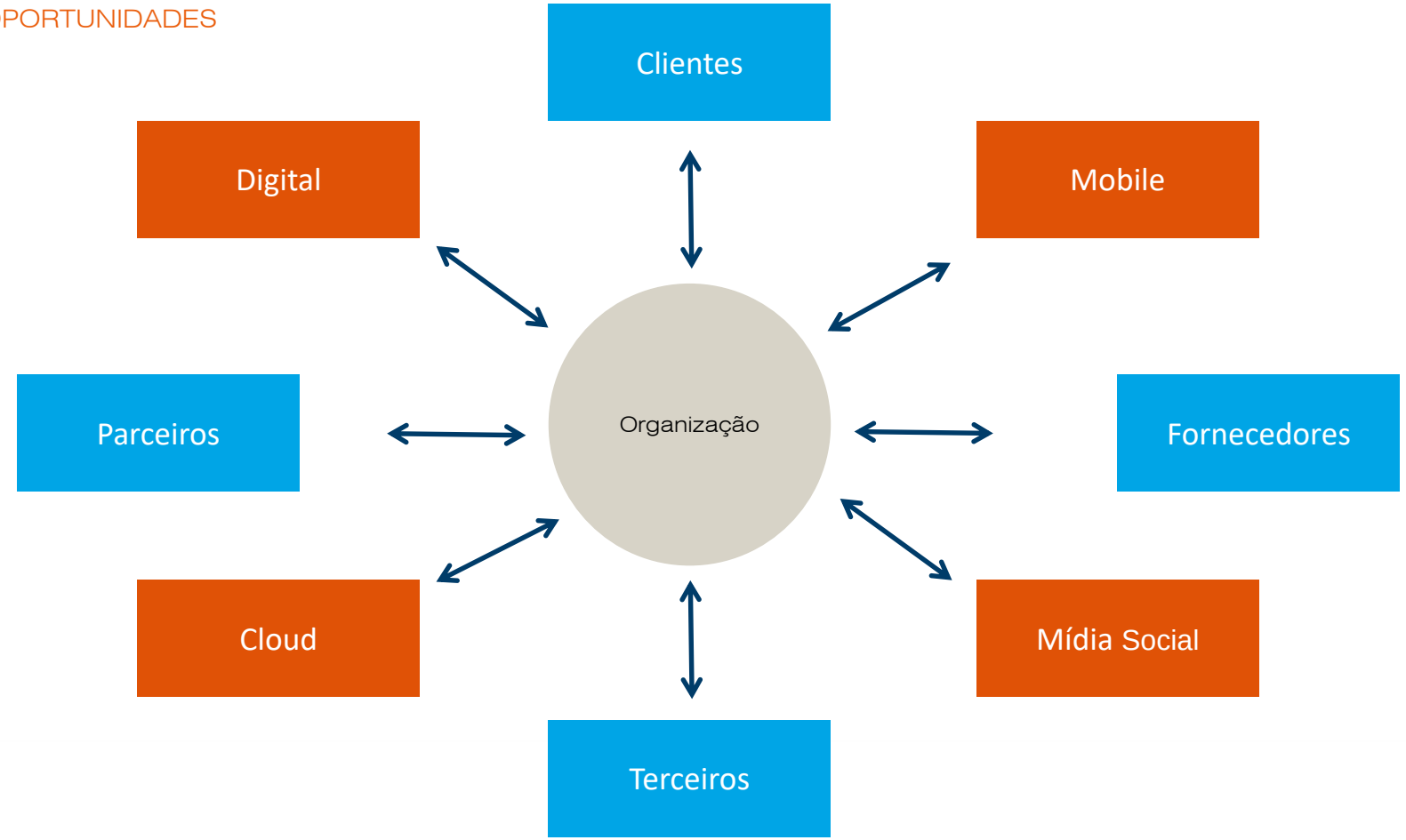
Kroll

O QUE MUDOU?

CYBER SECURITY – ECOSSISTEMA TECNOLÓGICO

NEGÓCIOS

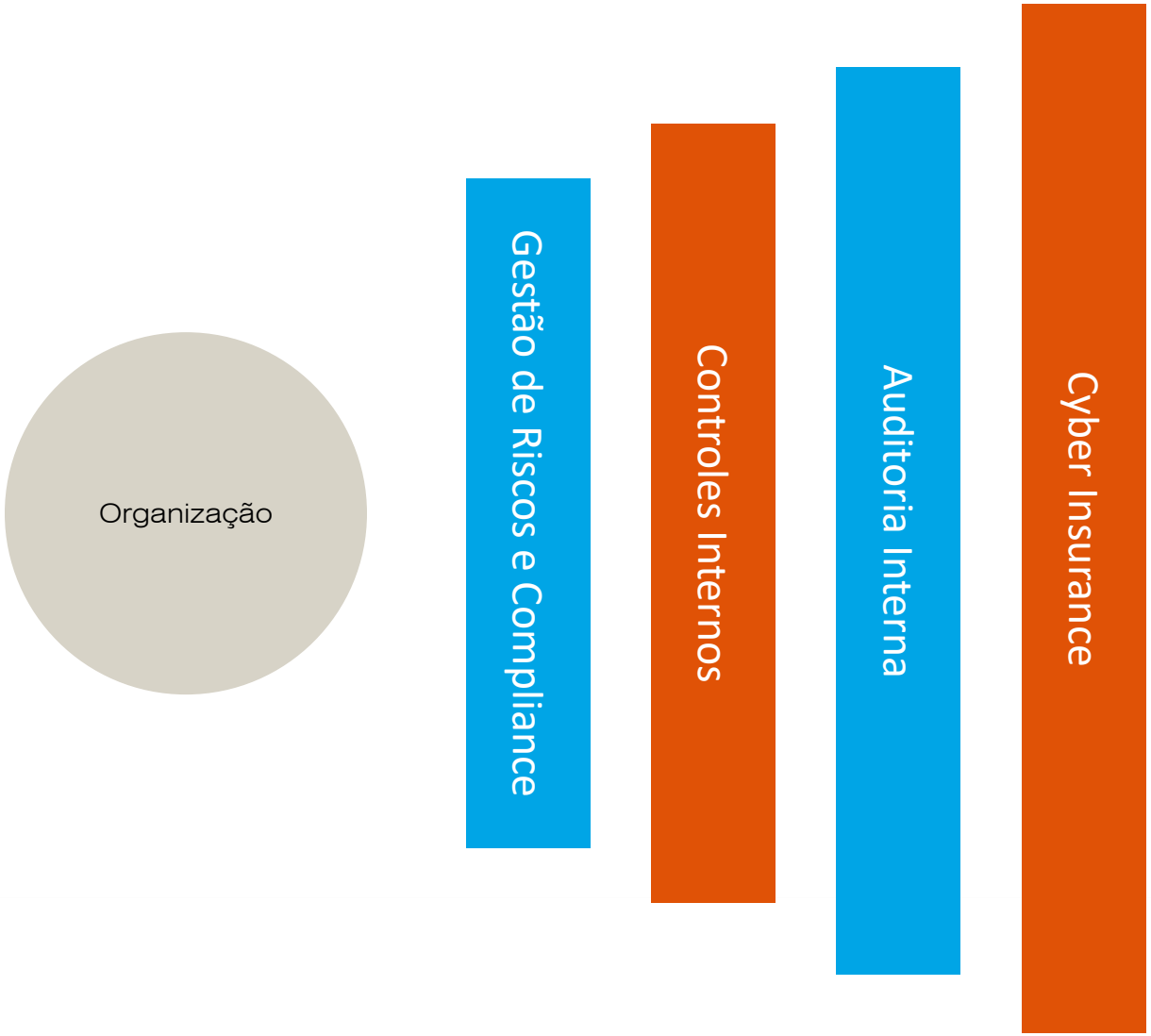
OPORTUNIDADES



Kroll

AS LINHAS DE DEFESA

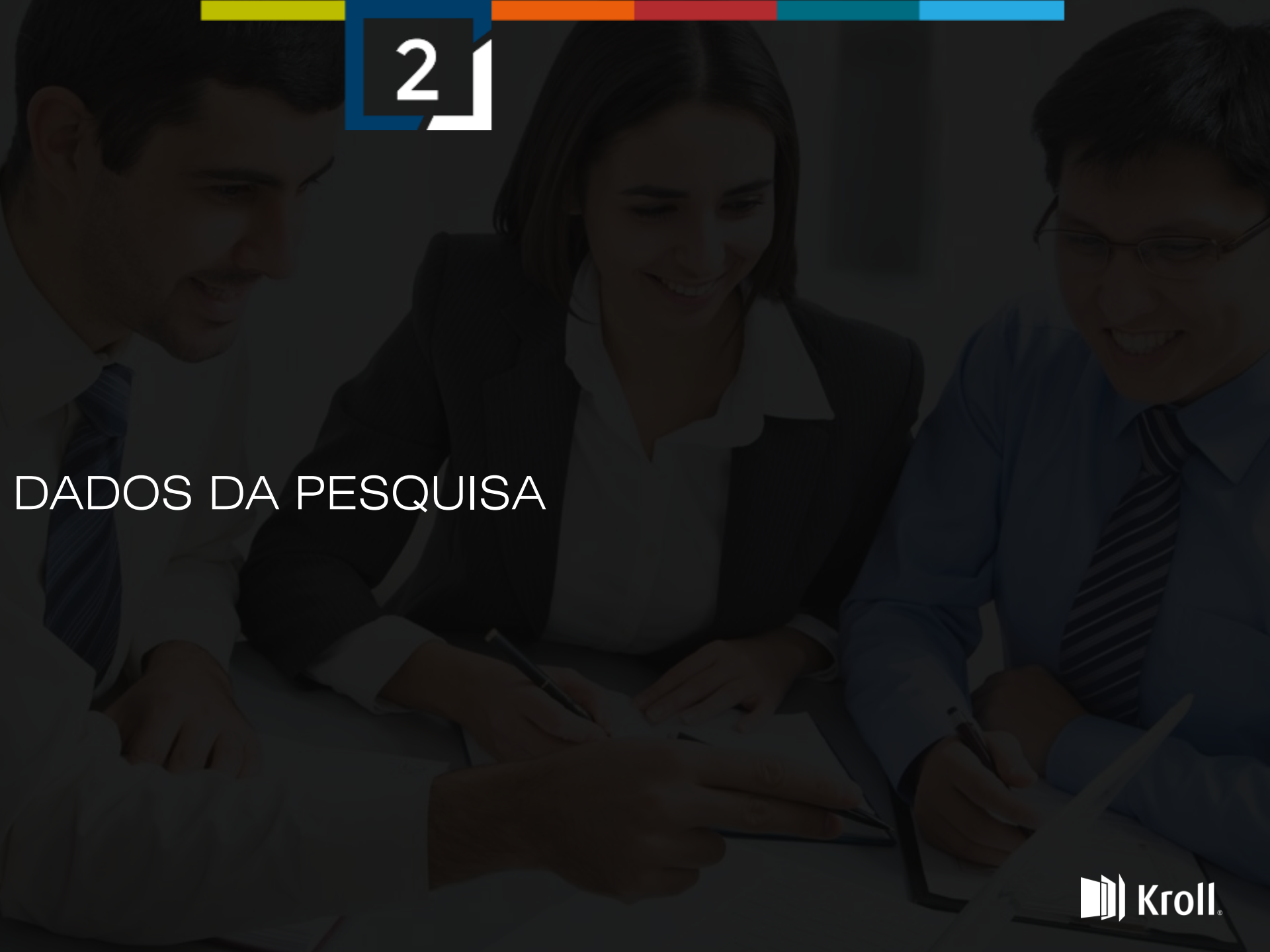
CYBER INSURANCE – NOVA LINHA DE DEFESA



Kroll

2

DADOS DA PESQUISA



Kroll

RESULTADOS DO BRASIL

REPORT CARD – ATAQUES CIBERNÉTICOS

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ 13% points above 2016
- ▲ 3% points above global average

CYBER SECURITY

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	45%	36%
Email-based phishing attack	37%	33%
MOST COMMON PERPETRATORS		**Global Avg.**
Ex-employees	32%	28%
MOST COMMON TARGET		**Global Avg.**
Customer records	47%	48%
Trade secrets/R&D/IP	44%	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		**Global Avg.**
IT service vendor	47%	35%

- No Brasil, **89%** dos respondentes afirmaram ter sido alvo de ataques cibernéticos, em relação à **76%** apontado no ano anterior.
- Este percentual é praticamente **o mesmo do resultado Global**.
- Estudos internos demonstram que a **detecção ainda é um problema**, mas o aumento da percepção está diretamente relacionado com o **surgimentos dos impactos**.
- Demanda de negócios relacionados com **Resposta a Incidentes, cresceu 63%**´em relação ao ano passado.
- As ações maliciosas buscas a **monetização** dos ataques.

Kroll

RESULTADOS DO BRASIL

PRINCIPAIS TIPOS DE CIBERATAQUES

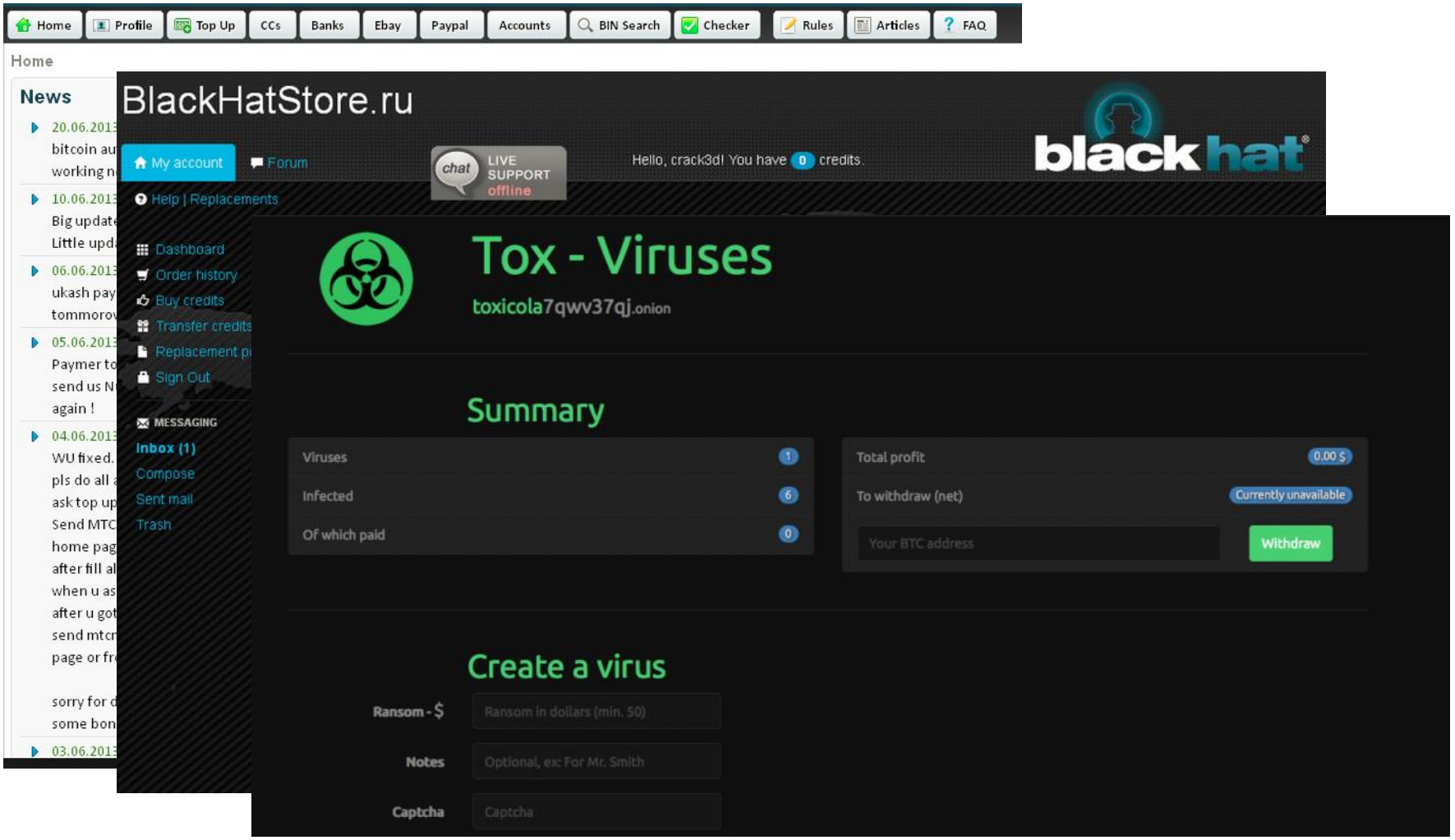
MOST COMMON TYPES OF CYBER INCIDENT		*Global Avg.*
Virus/worm attack	63%	62%
Email-based phishing attack	61%	57%
Alteration or change of data	55%	56%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	55%	55%
Ransomware attack	55%	55%
Denial of service attack	55%	52%

- Tanto no Brasil quanto globalmente, ataque por vírus/ *worm* foi mencionado como o principal preocupação das empresas. **Tratam-se de ataques em massa.**

Kroll

HAAS – HACKER AS A SERVICE

Terceirizando os ataques - Ransomwares



Kroll

RESULTADOS DO BRASIL

PRINCIPAIS TIPOS DE CIBERATAQUES

MOST COMMON TYPES OF CYBER INCIDENT		*Global Avg.*
Virus/worm attack	63%	62%
Email-based phishing attack	61%	57%
Alteration or change of data	55%	56%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	55%	55%
Ransomware attack	55%	55%
Denial of service attack	55%	52%

- Ataques de Phishing passaram da 6ª para a 2ª posição, em relação ao último ano.

Kroll

BEC - Attack

Business E-mail Compromise

Criminosos se passam por funcionários do alto escalão da empresa e utilizam suas contas de e-mail, ou sutilmente parecidas, para enganar funcionários responsáveis por movimentações financeiras.

Cibercriminoso se passa por executivo da empresa e envia e-mail para o departamento financeiro

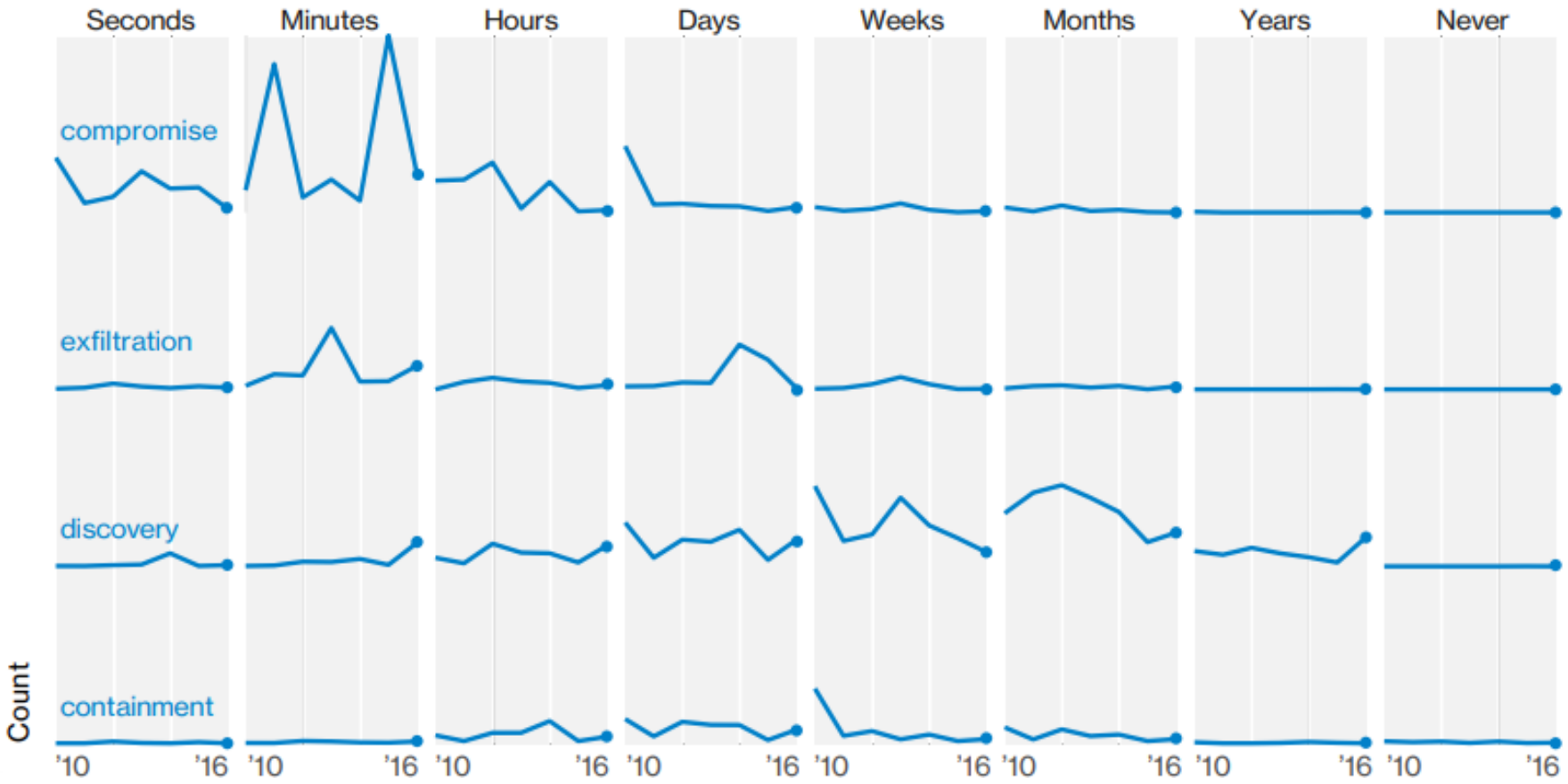
Financeiro realiza transação, conforme solicitação, para a conta do cibercriminoso.

Cibercriminoso recebe o pagamento e limpa rastros do ataque.

Kroll

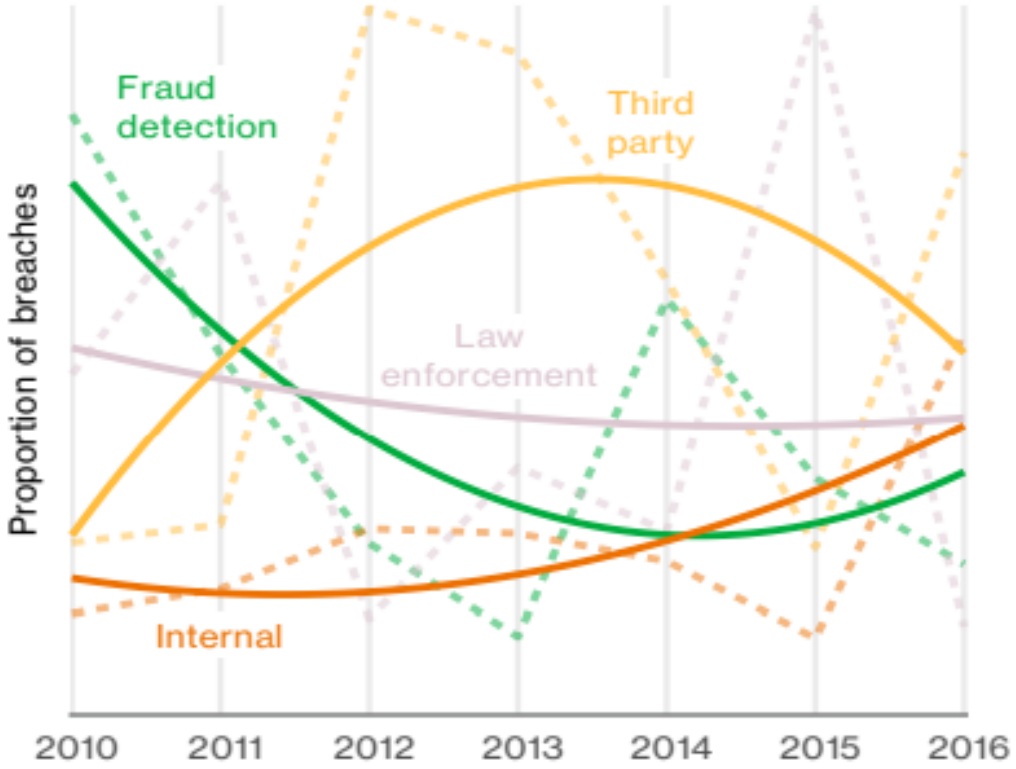
RESULTADOS DO BRASIL

INDICADORES DE OUTRAS PESQUISAS



DETECÇÃO DOS ATAQUES

Mudança de panorama



- Detecções ainda ocorrem através de terceiros;
- Controles internos e mecanismos de detecção de fraude aumentando a eficiência.

Kroll

RESULTADOS DO BRASIL

PRINCIPAIS OBJETIVOS DOS ATAQUES

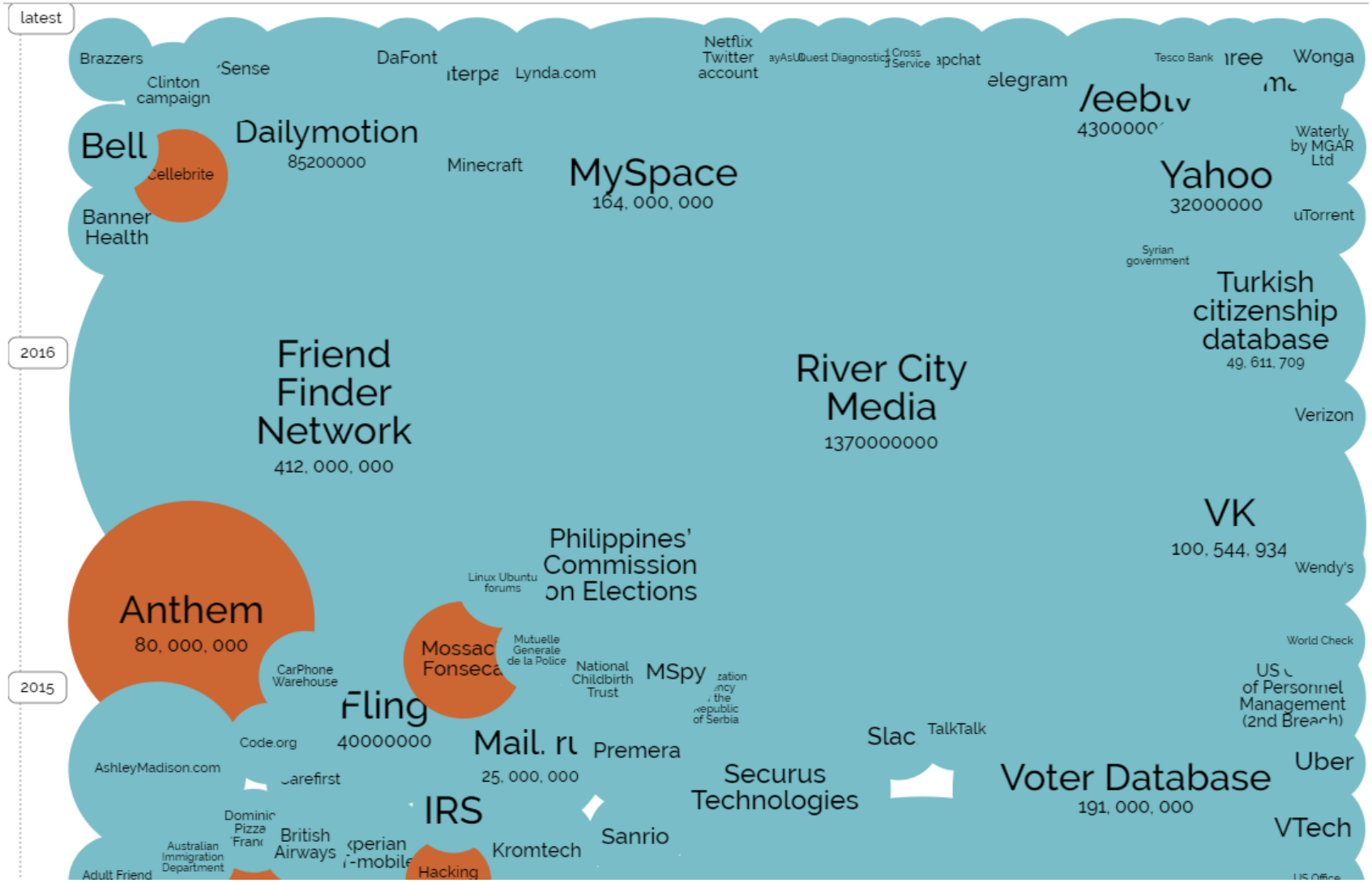
MOST COMMON TARGET		*Global Avg.*
Customer records	47%	48%
Trade secrets/R&D/IP	44%	40%

- Objetivo principal é obter acesso à informações sensíveis das empresas (informações sobre clientes, funcionários, identidade, segredos comerciais) e monetizar.

Kroll

CENÁRIO DOS ATAQUES – GLOBAL

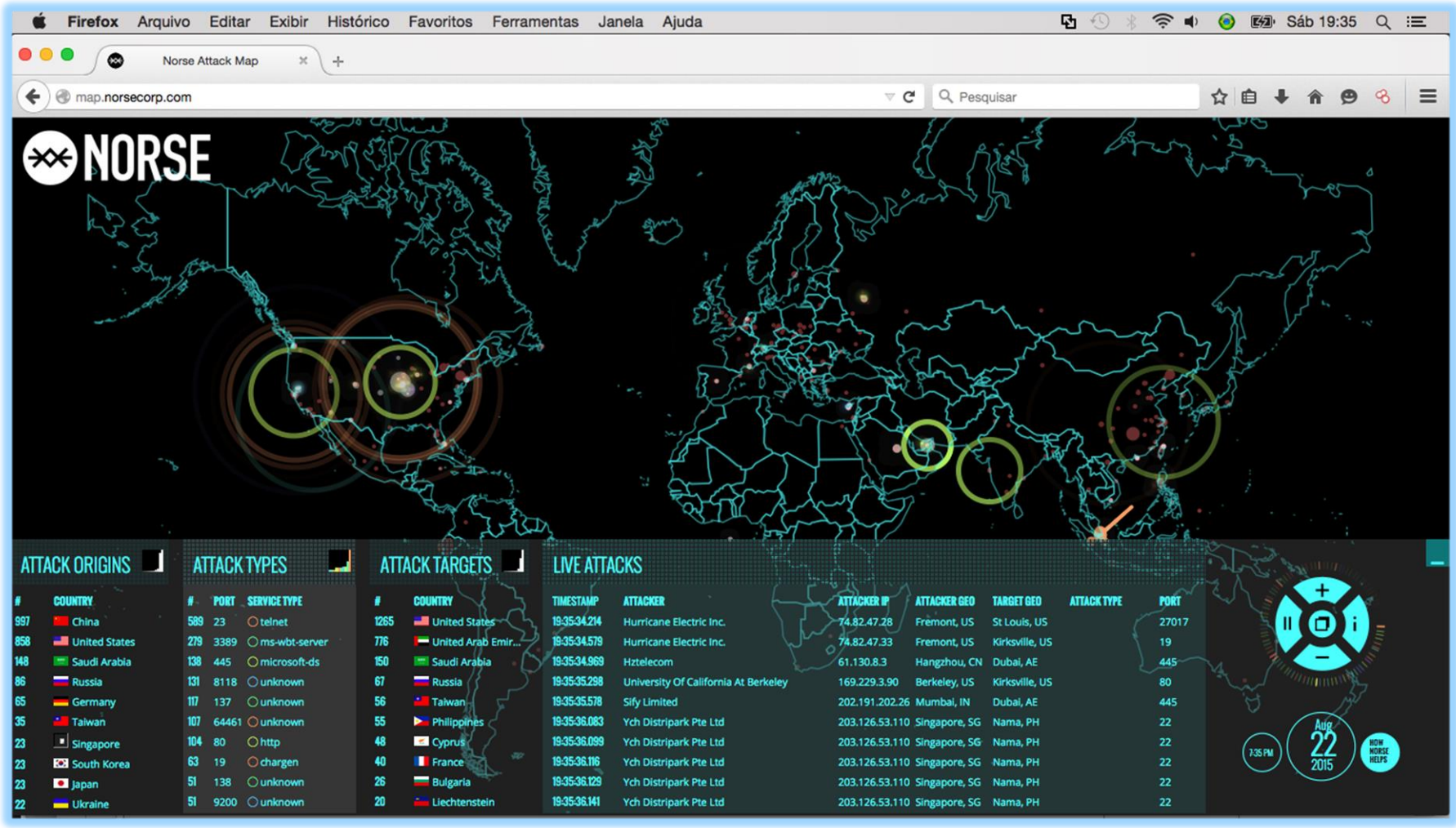
Informações sobre companhias comprometidas – "*data beautiful cyber*"



Kroll

CENÁRIO DOS ATAQUES – GLOBAL

Fluxo de ataques em tempo real



Kroll

RESULTADOS DO BRASIL

PERPETRADORES DAS FRAUDES CIBERNÉTICAS

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	32%	28%

- Os principais responsáveis incidentes cibernéticos são funcionários e ex-funcionários das empresas, seguidos dos concorrentes.

Kroll

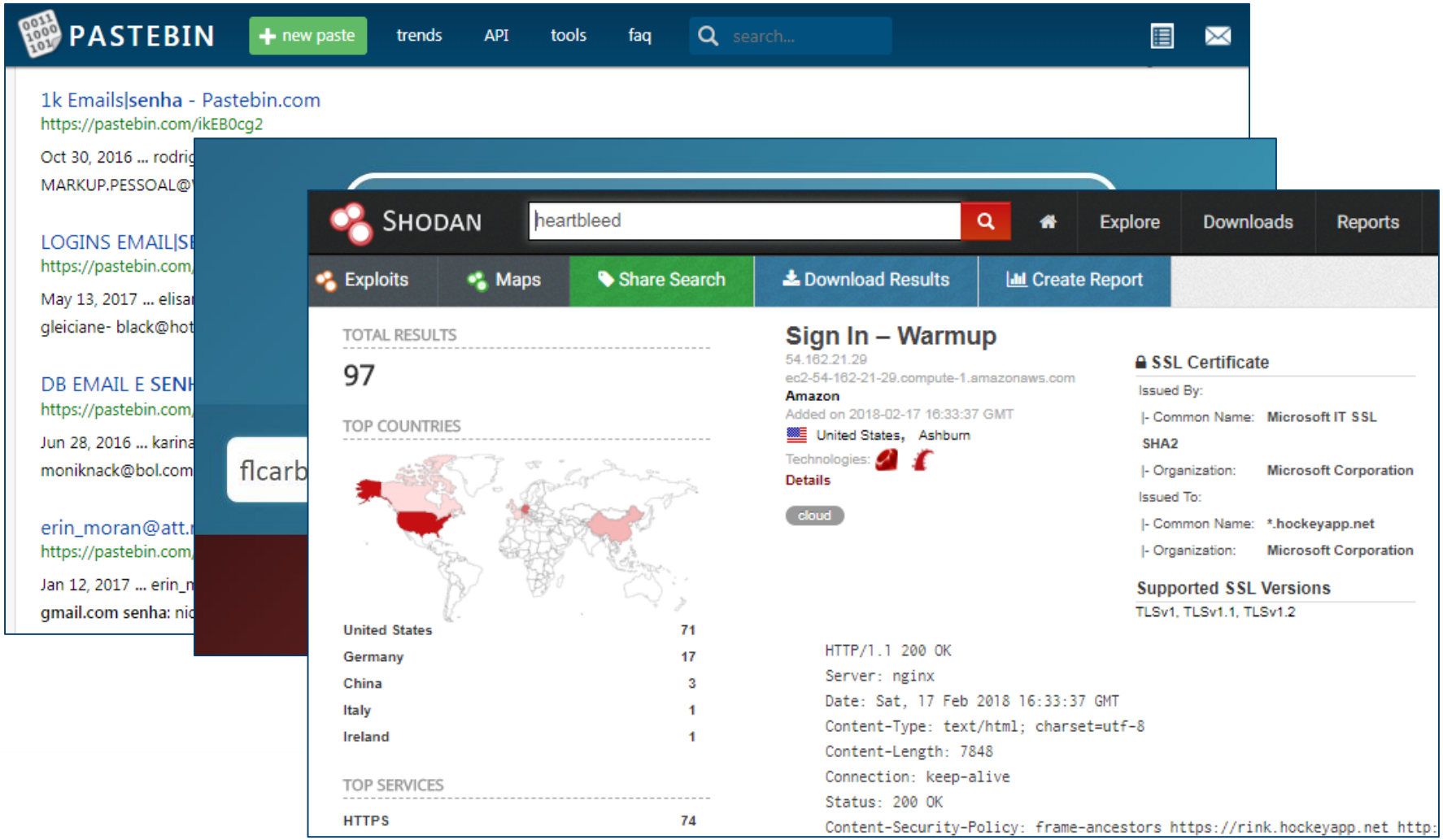
CENÁRIO REAL

DEMONSTRAÇÃO

COMO ISSO FUNCIONA NA VIDA REAL?

DEMONSTRAÇÃO

COMO ISSO FUNCIONA NA VIDA REAL?



Kroll

CYBER INSURANCE?

Seguro cibernético aparece em **13o lugar** das principais ações e controle de mitigação.

CYBER INSURANCE

Kroll

CYBER INSURANCE

NOVA LINHA DE DEFESA CIBERNÉTICA

Proteção dos negócios, contando com cobertura como:

- **Violação de dados / privacidade e gestão de crises**: Despesas relacionadas com a gestão do incidente, investigação, remediação, notificação, custos legais e procedimentos em tribunais.
- **Danos reputacionais**: Custos relacionados a **violação de propriedade intelectual**, direitos autorais, calúnia e difamação.
- **Extorsões cibernéticas**: Despesas relacionadas a casos de extorsões, mediando a **sequestro de dados** e servidores e criptografia de arquivos realizadas pelo crime organizado.
- **Riscos Operacionais**: Custos relacionadas a inoperância e/ou **indisponibilidade da rede** de computadores, além do roubo de dados.

Kroll

5

ABORDAGENS CONSULTIVAS

Kroll

ABORDAGEM CONSULTIVA

AVALIAÇÃO REAL DOS RISCOS CIBERNÉTICO

A grande maioria das empresas que operam no Brasil não sabem dimensionar os custos relacionados aos impactos dos **riscos cibernéticos**, devido a falta de consciência situacional e o baixo nível de maturidade em Cyber.

Um bom começo é a identificação dos riscos e quantificação dos impactos, através de um **Cyber Risk Assessment**.

Como resultado deste levantamento, a organização estará apta a determinar seu nível atual de maturidade em Cyber e saber qual o nível mínimo aceitável para o seu negócio, trabalhando nos **Gap´s** identificados.

ABORDAGEM CONSULTIVA

AVALIAÇÃO REAL DOS RISCOS CIBERNÉTICO

AVALIAÇÃO DE RISCOS DE TI

- Nível de consciência da organização
- Levantamento das políticas, procedimentos e controle
- Avaliação dos ativos e topologia de rede
- Avaliação dos processos de resposta e remediação

ANÁLISE DE VULNERABILIDADES

- Implanta variedade de ferramentas de código aberto e proprietárias para identificar vulnerabilidades
- Examina componentes da infraestrutura de rede nos perímetros interno e externo
- Prove análise de aplicações Web

TESTE DE INTRUSÃO

- Implantar ferramentas open source e proprietárias para explorar vulnerabilidades identificadas
- Intrusão“controlada" aos sistemas e ativos
- Criação dos cenários para Engenharia Social
- Relatórios detalhados sobre as ações e remediações

AVALIAÇÕES ESPECIALIZADAS

- Conformidade com orgãos reguladores
- Avaliação de Segurança em ambientes Wireless e VoIP
- Avaliação de Segurança em Terceiros
- Investigação e Computação Forense
- Avaliações customizadas

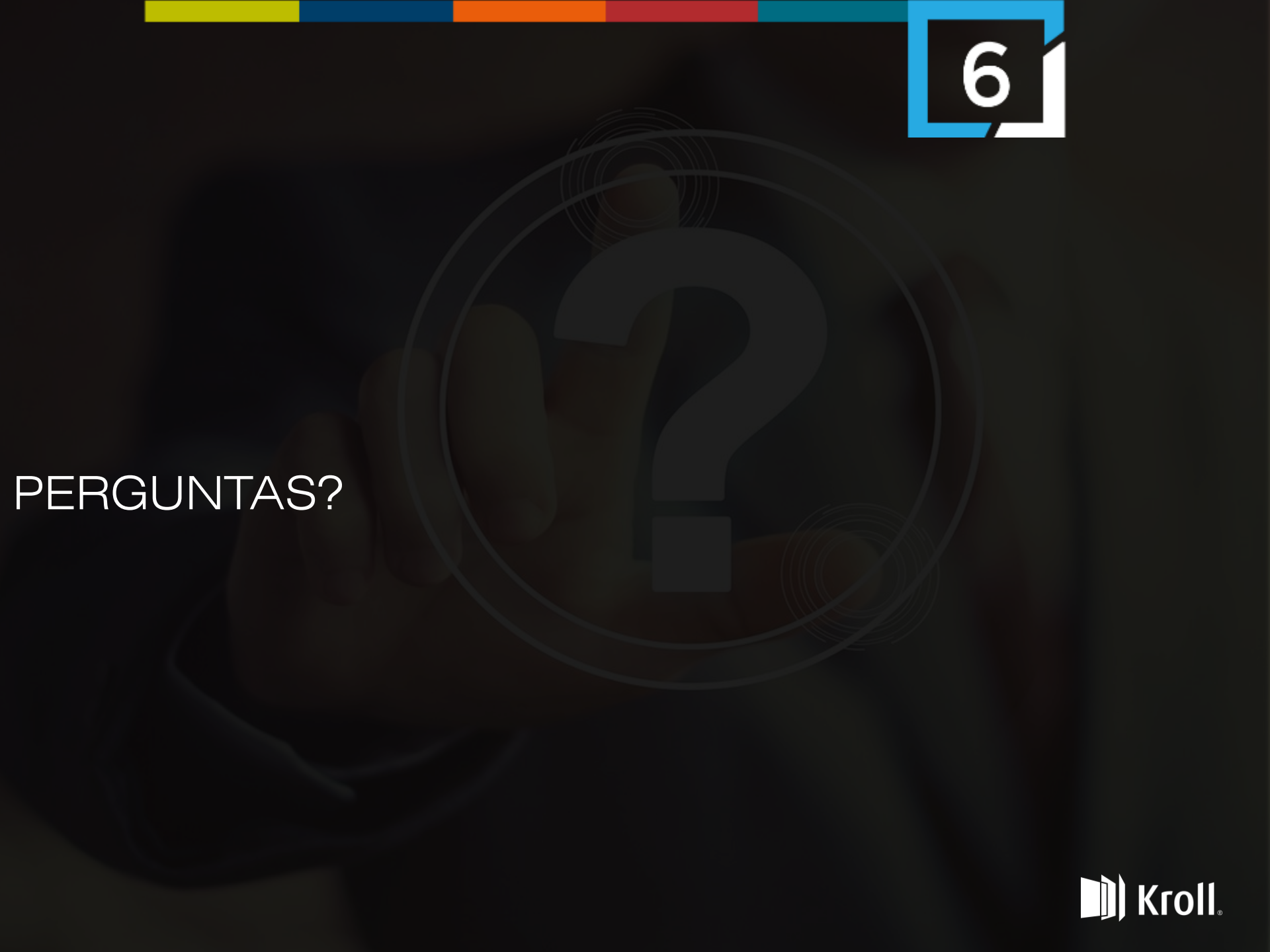
Kroll

ABORDAGEM CONSULTIVA
RESPOSTA A INCIDENTES

Capacidade de investigar aos incidentes, com o objetivo de:

- Erradicação do ataque
- Identificação da causa raiz
- Retroalimentação dos controles
- Atribuição de culpabilidade
- Retorno a normalidade

Kroll


6
PERGUNTAS?
Kroll

OBRIGADO

Kroll