2026 WTR WORKSHOP DE TECNOLOGIAS DE REDES PoPBA

28 A 30 SETEMBRO

VOCÊ FAZ PARTE DESSA CONEXÃO

REALIZAÇÃO

REMESSA

PoP BA

RNP

MINISTÉRIO DA CULTURA

MINISTÉRIO DA DEFESA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DAS COMUNICAÇÕES

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Do SIEM ao XDR: como a cibersegurança está mudando o jogo contra ataques modernos

Willian Oliveira, CISSP, Solution Sales Manager LATAM, Kaspersky

Geraldo Vasconcelos, Presales Manager Brazil, Kaspersky

Quando seu EDR básico finalmente gera o alerta… mas o ransomware termina o trabalho.

As ameaças se transformaram em dores de negócio

Defesas isoladas (antivírus, firewall)	Ameaças coordenadas e persistentes
Foco em prevenção	Foco em detecção + resposta
Reação manual e lenta	Automação e resposta em tempo real
Protege apenas o dispositivo	Protege usuário, dado, nuvem e identidade
Alta dependência de equipe humana	Inteligência e correlação automatizada

As ameaças mudaram. E continuam evoluindo.

Ransomware como serviço (RaaS)

Criminosos alugam ataques prontos, com suporte técnico incluído.

Phishing e engenharia social avançada

Campanhas personalizadas que exploram o comportamento humano.

Ataques automatizados com IA

Modelos de IA testando vulnerabilidades e gerando e-mails falsos realistas.

Movimento Lateral

Após uma brecha, o atacante move-se internamente e alcança servidores críticos.

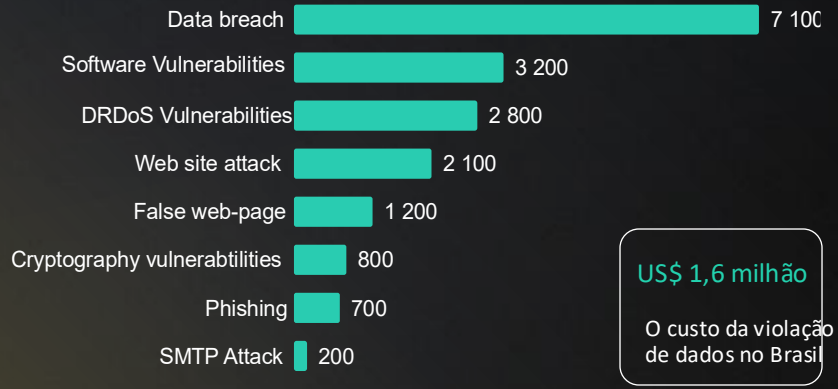
Comprometimento de credenciais e AD

Roubo de acessos e uso indevido de privilégios administrativos.

Panorama das ameaças no setor governamental brasileiro

Os incidentes cibernéticos no setor público brasileiro continuaram a aumentar ao longo de 2024 e em 2025.

A maioria dos incidentes está ligada a violações de dados e à exploração de vulnerabilidades de software.



US$ 1,6 milhão

O custo da violação de dados no Brasil

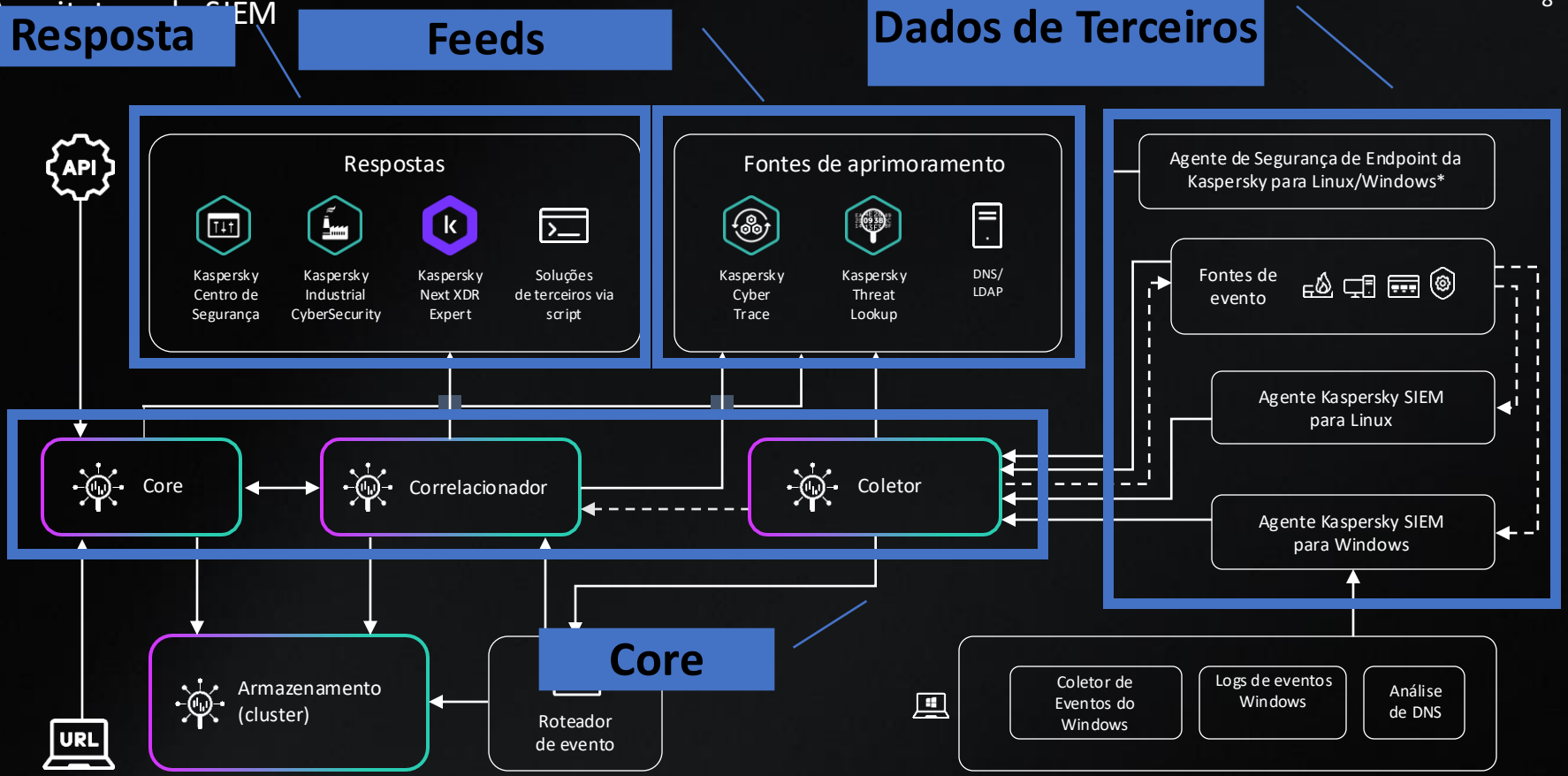
Fontes: Relatório do analista Kaspersky Incident Response, 2025 ; Relatório de Cibersegurança 2025, Brasscom

A maturidade em segurança é construída por camadas.

Correlação e Visibilidade total

Falta de visibilidade unificada entre ferramentas	Centraliza eventos e logs de múltiplas fontes.
Dificuldade em correlacionar incidentes complexos	Motor de correlação com mais de centenas de conectores.
Falta de priorização de riscos e ativos críticos	Dashboards e IA para risk scoring e contexto.
Necessidade de auditoria e compliance	Retenção de logs, relatórios e trilhas de conformidade.
Falta de continuidade operacional no SOC	SLA de incidentes e arquitetura resiliente.

Arquitetura do SIEM

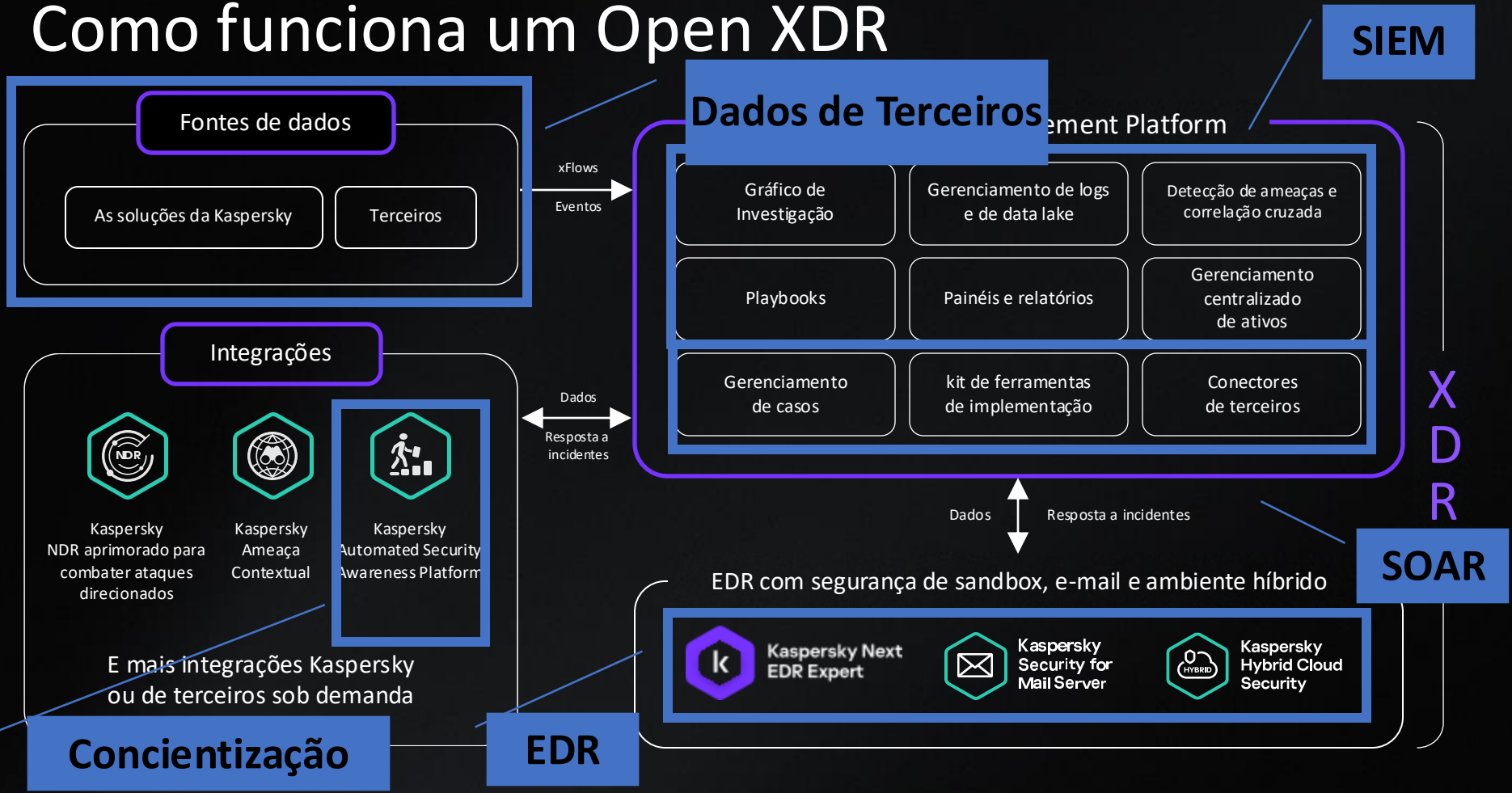


O Kaspersky SIEM apresenta uma arquitetura modular de microsserviços: é composta por vários serviços que interagem uns com os outros
*Se uma estação tem o Kaspersky Endpoint Agent (KES Win 12.6 ou Linux 12.2), ele pode ser usado para encaminhar eventos do Windows para o SIEM sem que seja necessário configurar uma fonte de dados adicional

Orquestração e automação completa

Falta de integração entre múltiplas camadas de segurança	Cross-correlation engine + orquestração total.
Dificuldade em investigar incidentes complexos	Investigation Graph com timeline visual.
Respostas lentas e dependentes de analistas	Playbooks automatizados e editor visual de resposta.
Necessidade de cobrir nuvem, e-mail e VDI	Proteção híbrida e integração nativa com múltiplas plataformas.
Exigência de alta disponibilidade e continuidade	SLA de incidentes e arquitetura resiliente.

Como funciona um Open XDR




Um não simplesmente ...
...detecta TTPs avançados sem IOA e MITRE ATT&CK.

Indicadores de Ataque (IoA)

Busca por indicadores de ataque (IoA) em eventos em hosts protegidos

Automação

Os IoAs são mapeados no banco de dados MITRE ATT&CK para oferecer informações detalhadas, incluindo a técnica definida pela ATT&CK utilizada, uma descrição e as estratégias de atenuação

Regras integradas de IoA

dos especialistas da Kaspersky

Crie e importe

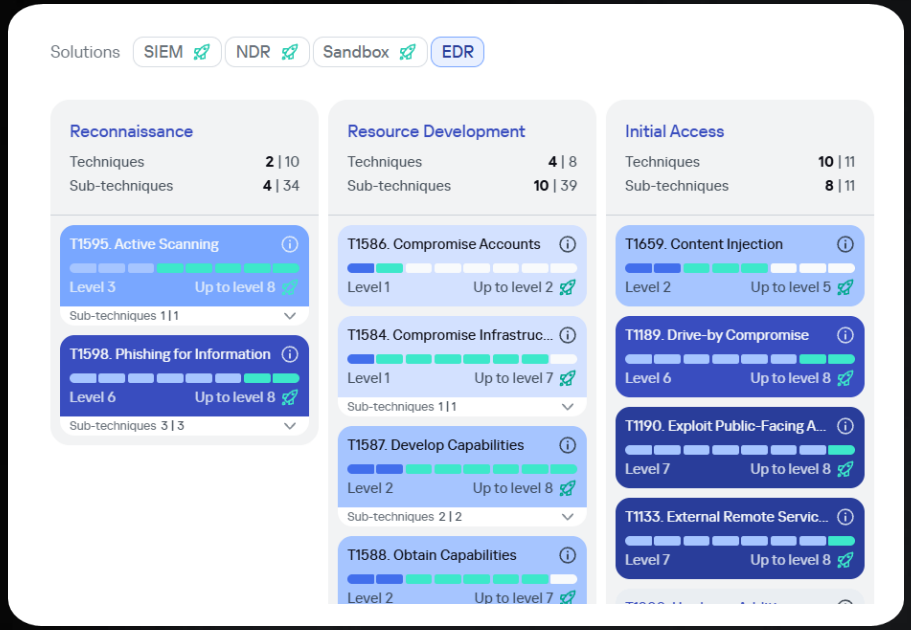
suas próprias regras de IoA

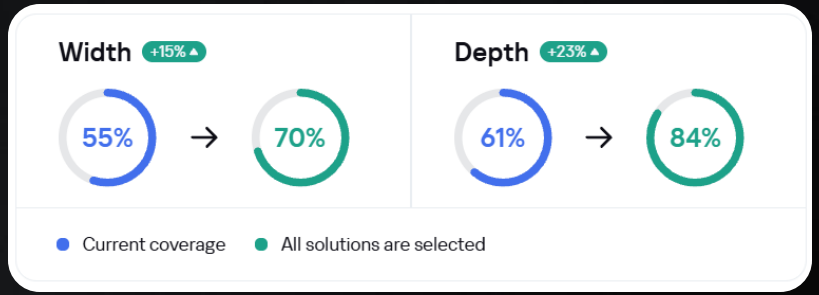
Descobre ações suspeitas usando o conjunto exclusivo de IoAs gerados pelos caçadores de ameaças.

Após a detecção de um evento suspeito pelo IoA, você receberá:

- Uma descrição dos eventos
- Recomendações sobre como mitigar o risco
- Confiança no veredito, incluindo a gravidade, para facilitar a classificação e agilizar a resposta

Cobertura do MITRE ATT&CK





Cenário de Demonstração

Etapa 1

O usuário recebe um e-mail com um link de URL de phishing.

Etapa 2

O usuário abre o link de URL de phishing no navegador.

Etapa 3

Foi baixado um arquivo malicioso adicional que se parece com um documento do Word para Windows.

Etapa 4

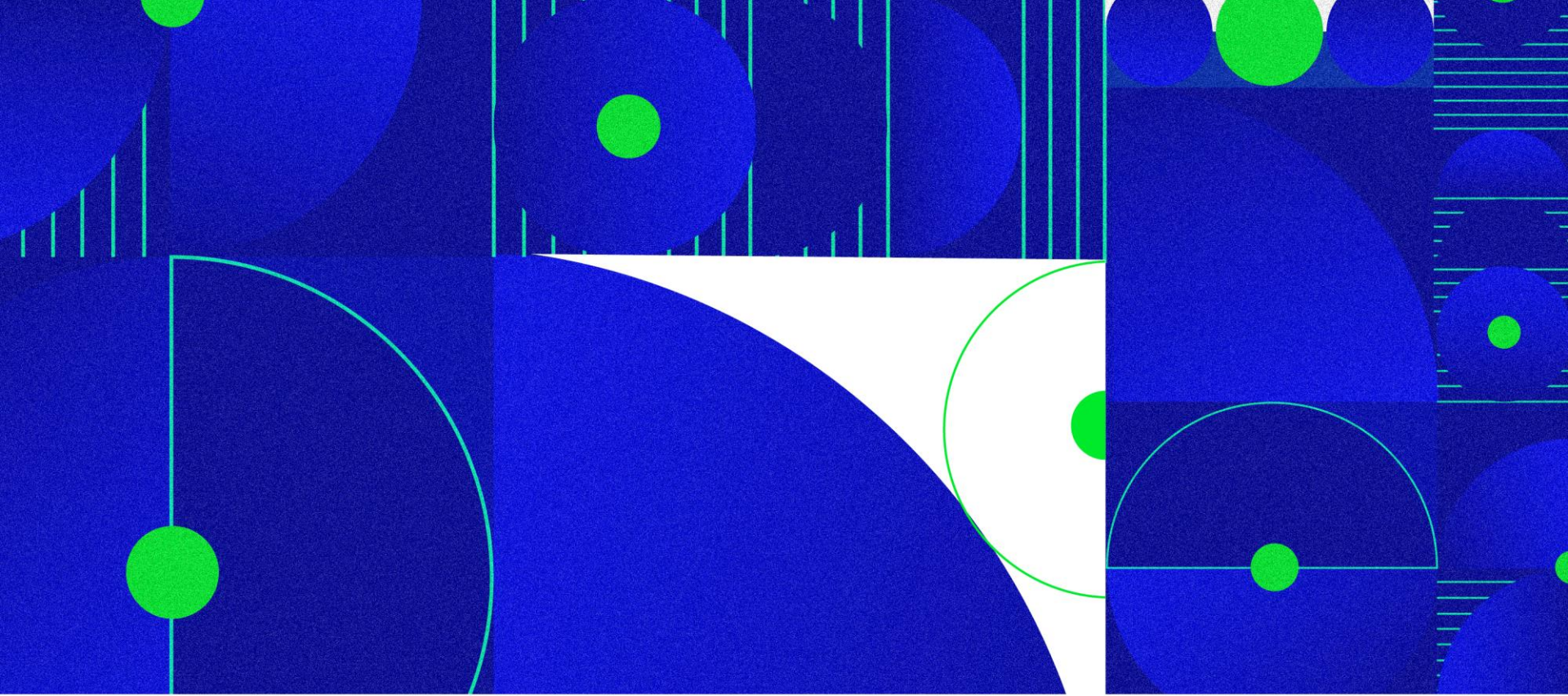
O arquivo executável malicioso foi executado e o PC do usuário foi infectado.

Etapa 5

Sequestro de processos avançado (Process Hollowing/Hijacking).

Etapa 6

Estabelecimento de conexão de saída C2 (Comando e Controle) e orquestração remota.



OURO

nic.br

Q13

Webfoco TELECOM

XSITE kaspersky

PRATA

InforTel

BRONZE

DISTRITO engenharia

FABIANI BORGES

KAIAK

IMTECH

infor barramar

PROBAHIA

SOFTDADOS

APOIO

cais

ESCOLA SUPERIOR DE REDES

nic.br

UFBA Universidade Federal da Bahia

REALIZAÇÃO

REMESSA

PoP BA

RNP

MINISTÉRIO DA CULTURA

MINISTÉRIO DA DEFESA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DAS COMUNICAÇÕES

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO