Segurança e LGPD

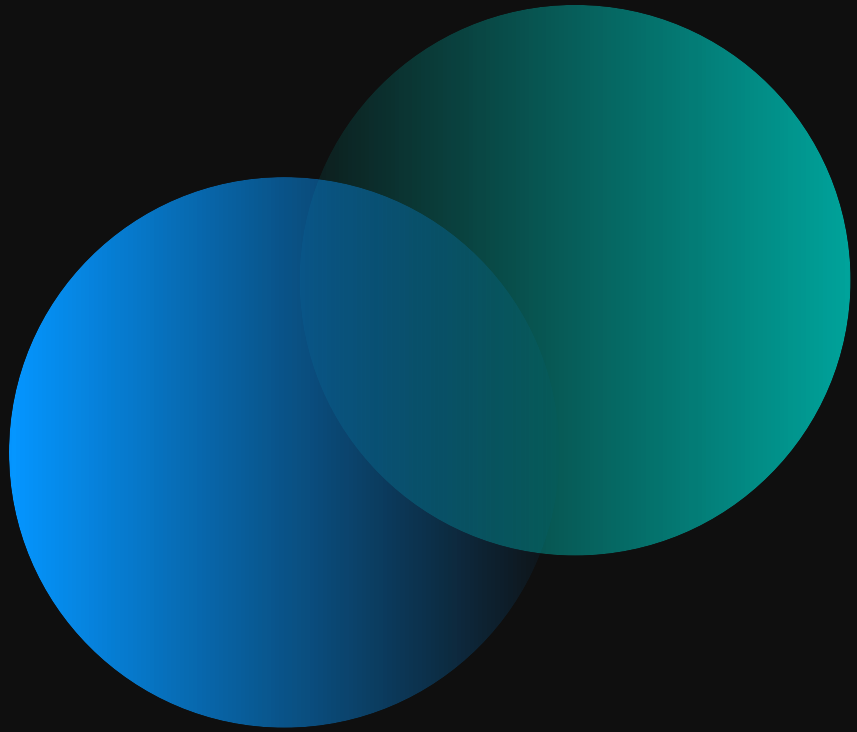
Como a Inteligência Artificial melhora a Detecção e Resposta de Segurança?

Américo Alonso
Chief Quality, Security & Data Protection Officer
SAM Head Digital Security & Mission Critical
02/12/2021

Atos

Visão geral

01. A Atos



Em poucas palavras

105.000 especialistas em 71 países

€11,2 bn de receita annual e **€1 bn** de margem operacional

Parceiro mundial de TI dos Jogos Olímpicos e Paralímpicos

Líder global em **cloud** e **digital workplace**

#2 em **serviços gerenciados de segurança** mundial (**#1** na Europa)

c.€235 m P&D no ano

85.000 novas certificações digitais

14,9 tCO2/m€ melhor da indústria

Atos: parceiro de confiança

6000+
Profissionais em Segurança

31 bilhões
Eventos de segurança processados por dia

15
Centros de Operações de Segurança

15 milhões
Cases de scan de vulnerabilidades

3,2 milhões
Endpoints protegidos pela Atos

300 milhões
pessoas protegidas pelas nossas soluções

+30 milhões
Equipamentos de rede e celulares

IDnomic
Identidades de confiança para pessoas e dispositivos

LEADER

IDC Analyze the Future
Managed Security Services Europe

LEADER

NelsonHall Success through insight
Cyber resilience services & EMEA
GDPR Services WW

Evidian
Gestão de accesos e identidades

NICHE PLAYER

Gartner
Identity Governance & Admin WW

NUMBER 2

Gartner
Managed Security Services WW Market share

Trustway
Proteção de dados em reposo e movimento

NICHE PLAYER

Gartner
Access Management WW

AIsaac
Plataforma de MDR patenteada

LEADER

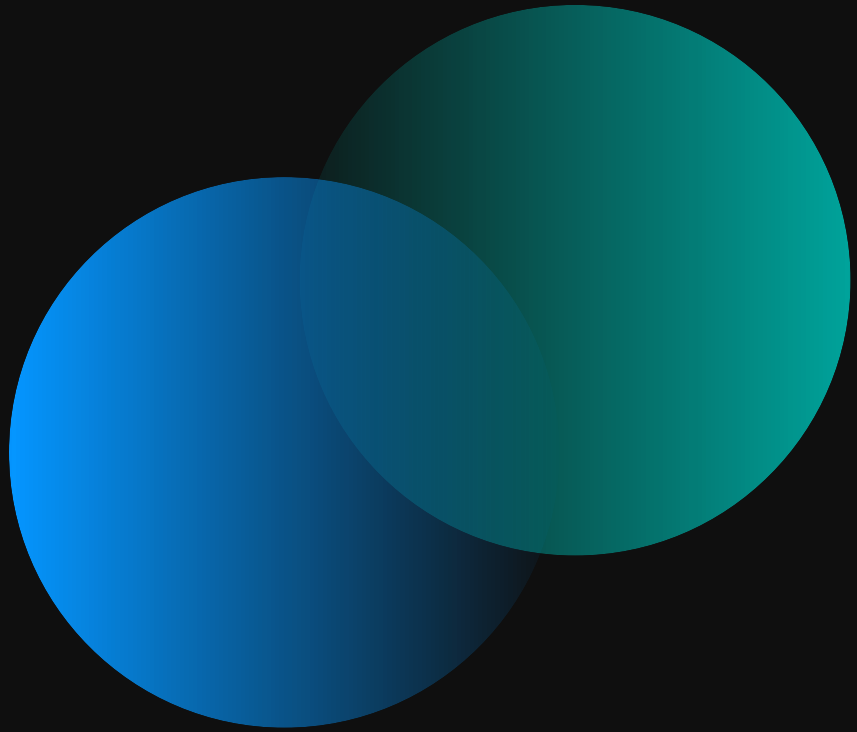
kuppingercole ANALYSTS
Identity Provisioning Global

LEADER

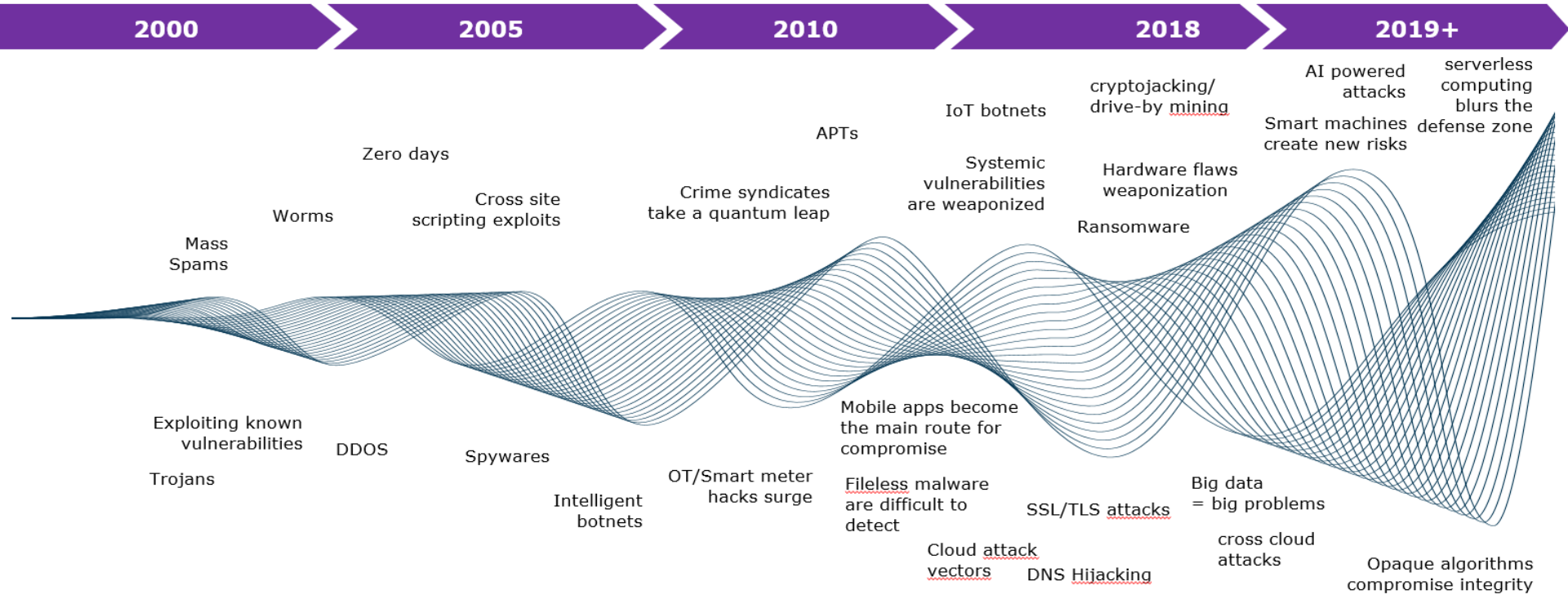
CXP Group
IARC · le CXP · PAC
IT Security Europe

Atos

02. Ecosistema de Ameaças

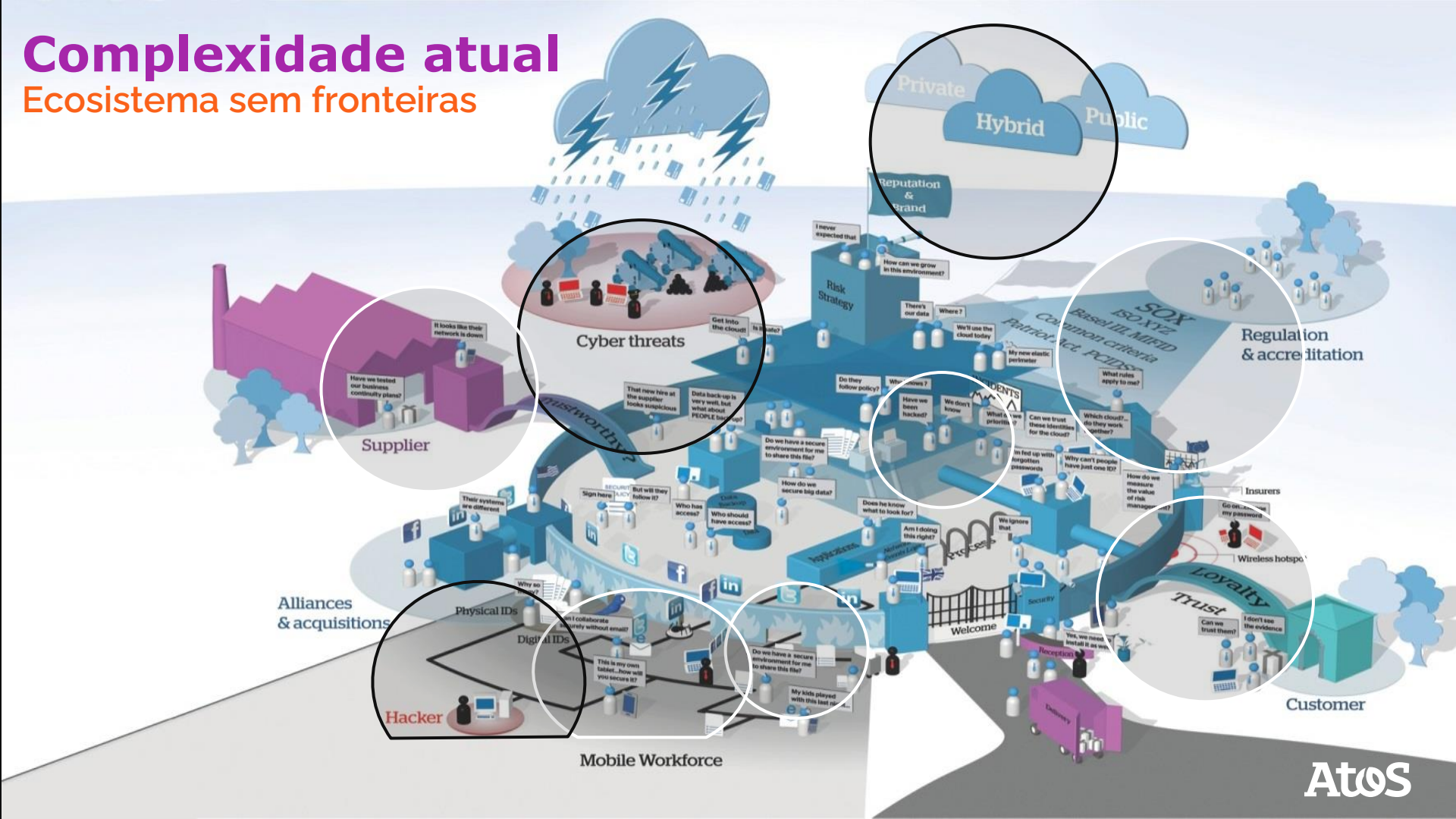


O sempre atualizado ecosistema de ameaças



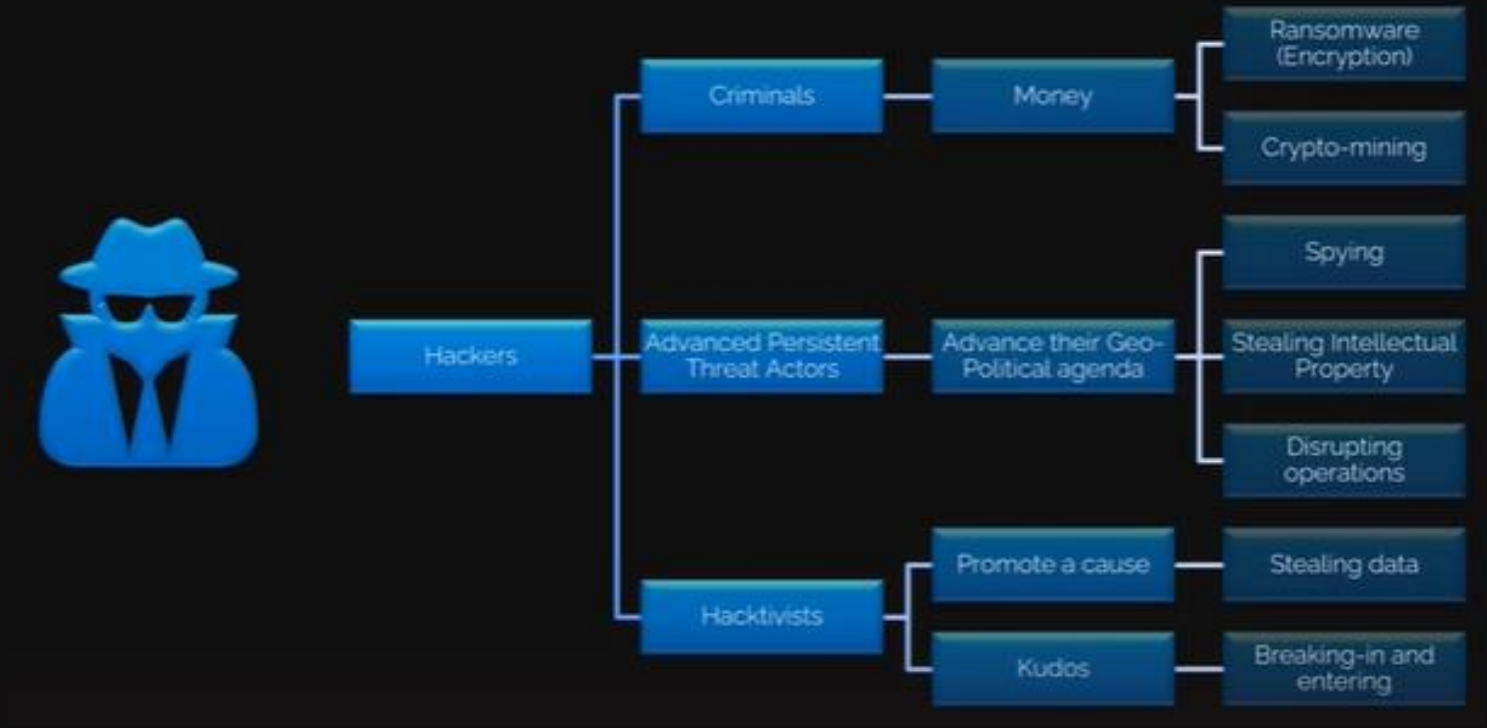
Complexidade atual

Ecosistema sem fronteiras

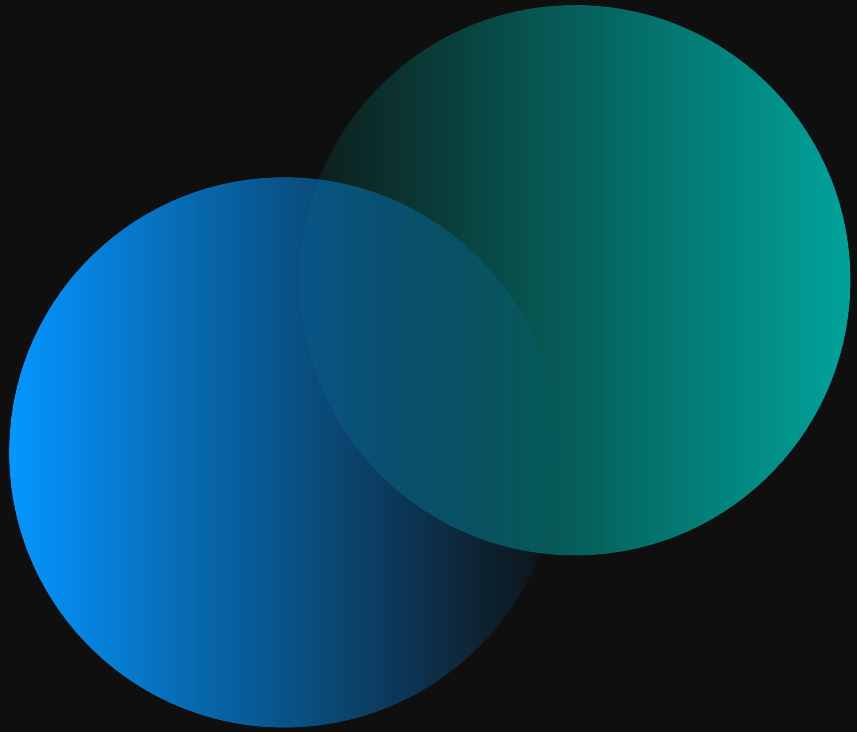


AtoS

A motivação dos Hackers



03. Atos e a Segurança de Tokyo 2020



O que os Jogos Olímpicos significam...

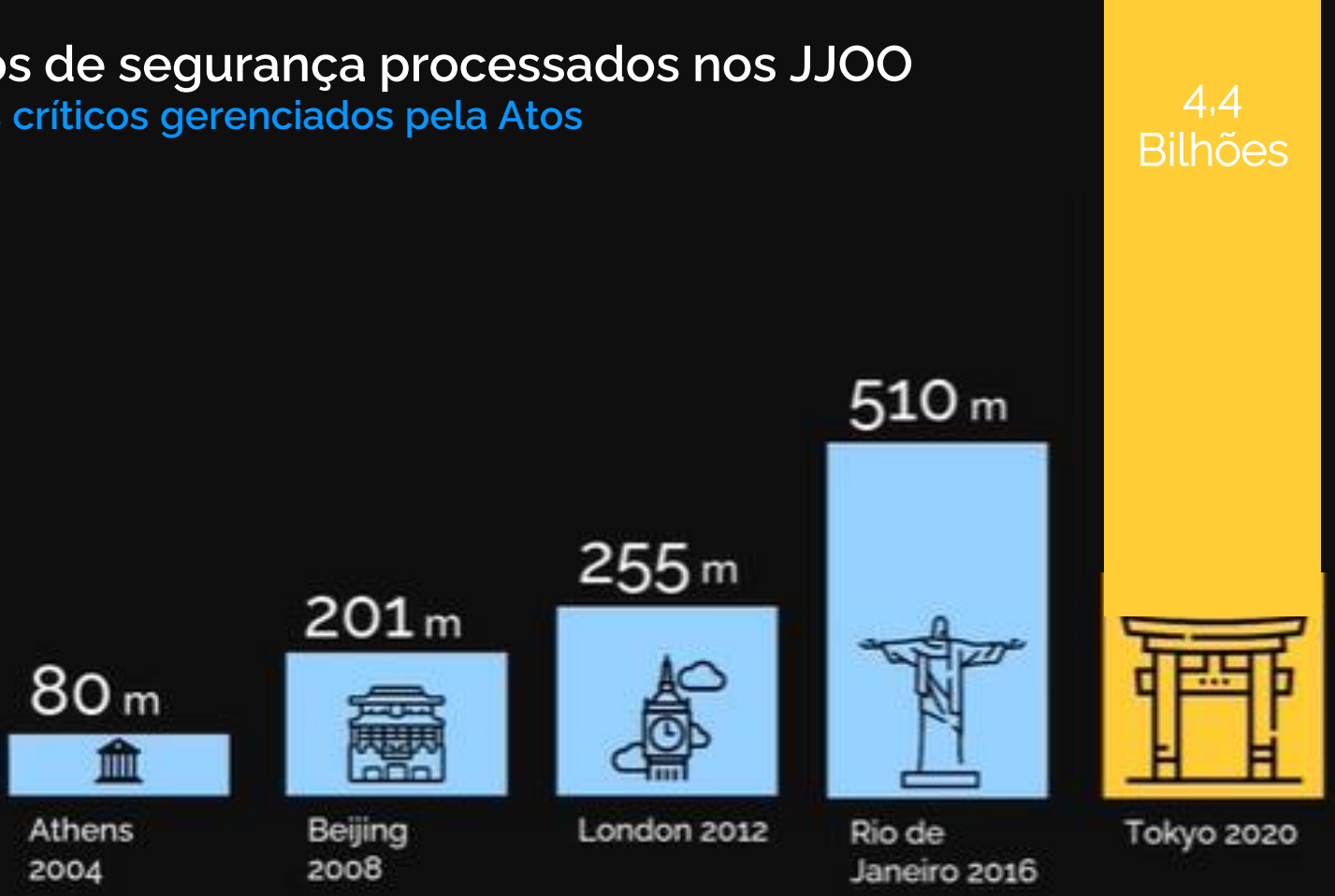
"...é como montar uma empresa nova, com 4 bilhões de clientes, 200.000 colaboradores, operando 24x7, em um novo território, a cada 2 anos, para trabalhar 15 dias..."

Tokyo 2020 em números

- Todas as aplicações críticas foram hospedadas **100% na nuvem** da Atos;
- **400 mil** credenciamentos emitidos (aumento de 30% desde Rio2016) – o que também serviu como um documento oficial de entrada seguro na fronteira do Japão;
- **41.724** voluntários aceitos por meio do portal do voluntariado;
- **339** eventos do programa olímpico com transmissão quase instantânea dos resultados para fãs, jornalistas e locutores;
- **Bilhões** de espectadores;
- **200 mil** horas de testes técnicos durante os preparativos – incluindo os primeiros métodos virtuais dos Jogos Olímpicos para completar os ensaios de tecnologia;
- Os servidores físicos foram reduzidos em quase **50%** em comparação com as edições anteriores – operando de 250 servidores no Rio 2016 para pouco mais de 130 em Tóquio 2020;
- Recorde de tráfego para plataformas digitais olímpicas **(+ 50%** de usuários em comparação ao Rio 2016);
- **5 milhões** de usuários do site olímpico oficial durante os primeiros dias dos jogos.

Eventos de segurança processados nos JJOO

Serviços críticos gerenciados pela Atos



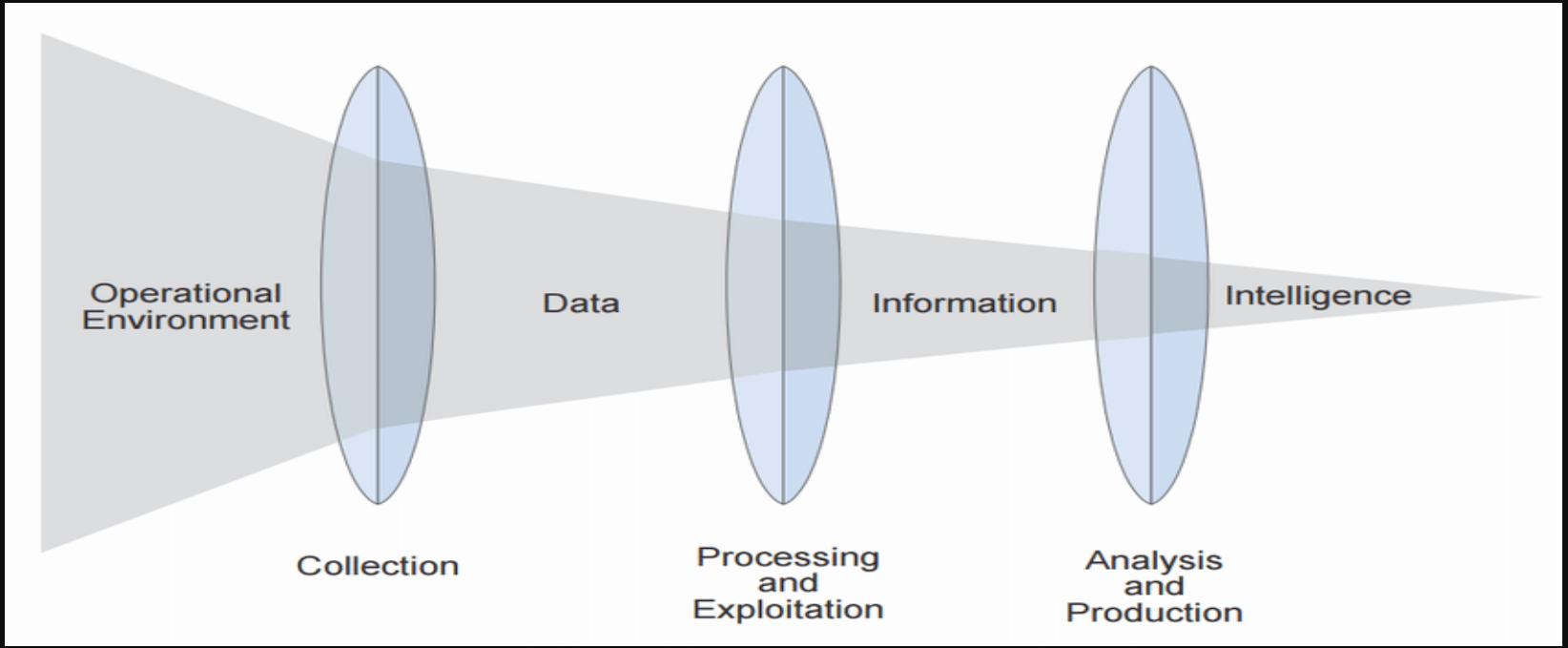
Enfrentando as ameaças

9 de Julio a 5 de Setembro

04. Prescritividade em Segurança Digital

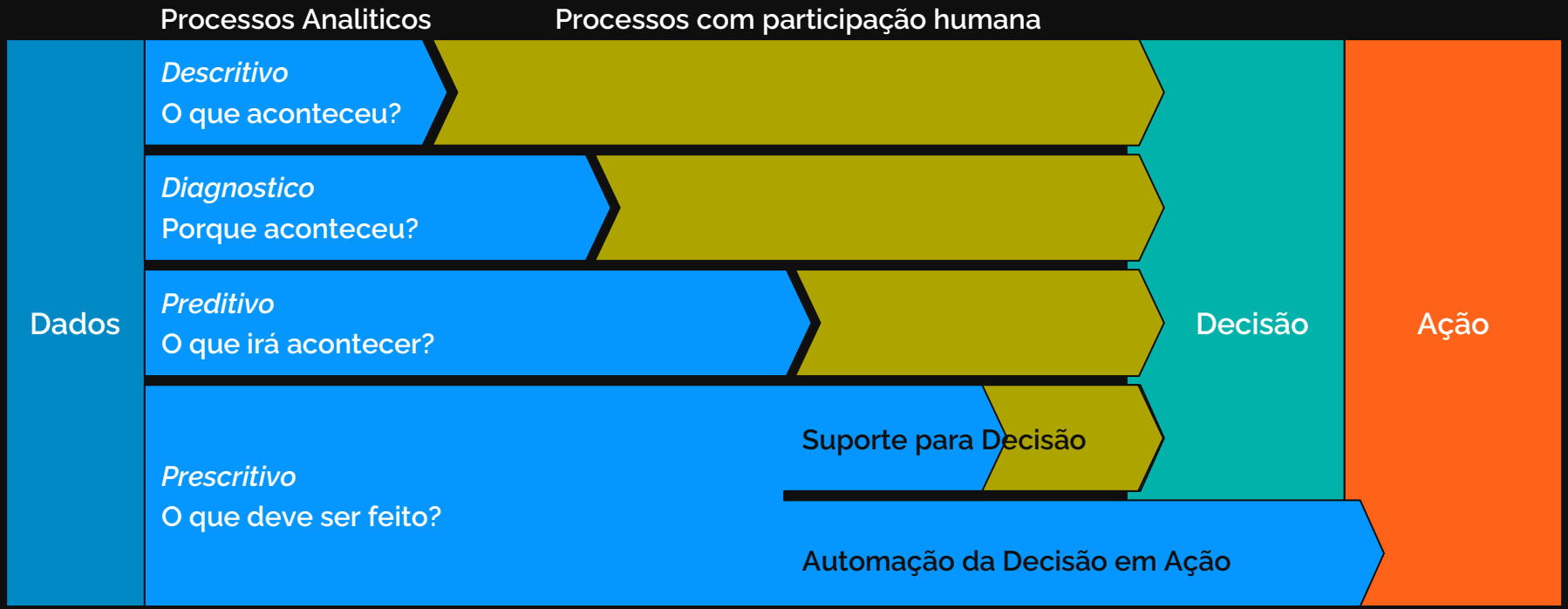
A jornada dos dados

Transformando o ruido em inteligência



Gartner – Segurança Prescritiva

Modelo conceitual



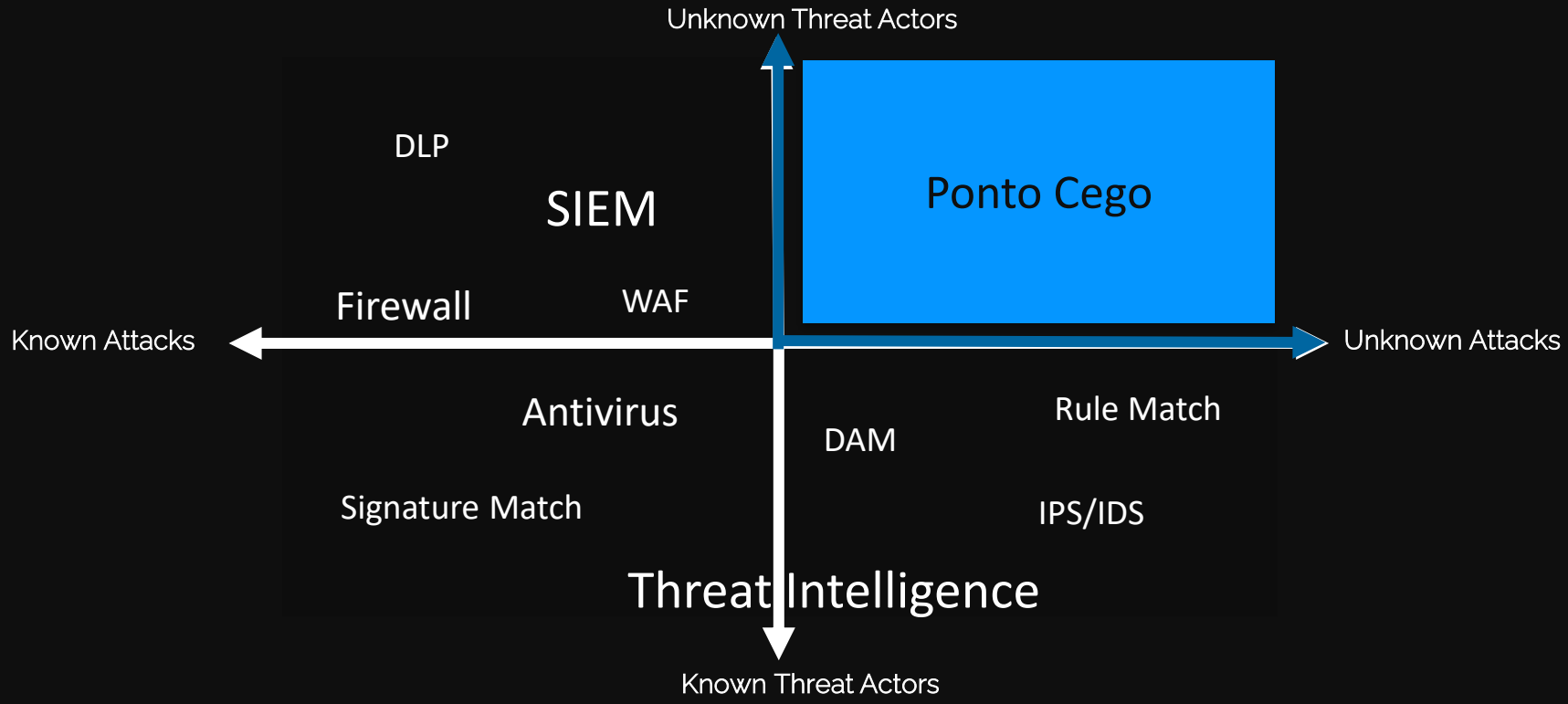
Source: Gartner, #G00254653 (September 2013)

Segurança Prescritiva

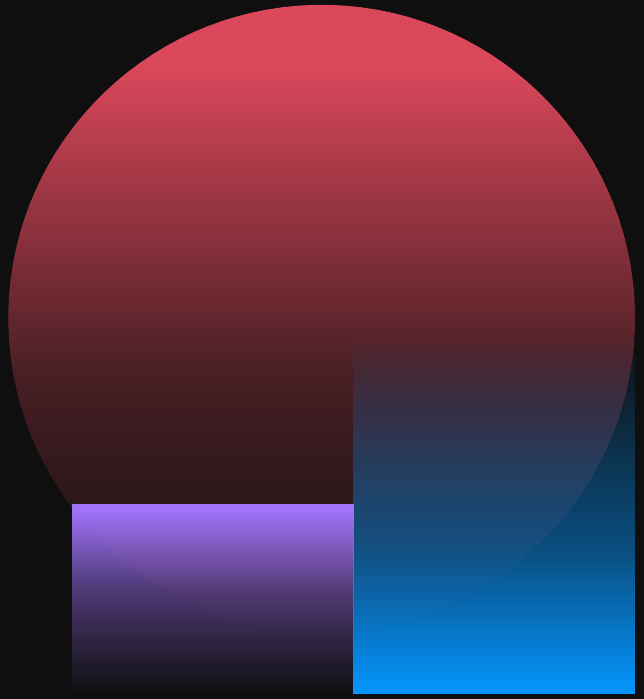
Não podemos encontrar aquilo que não estamos procurando

Inteligencia Artificial

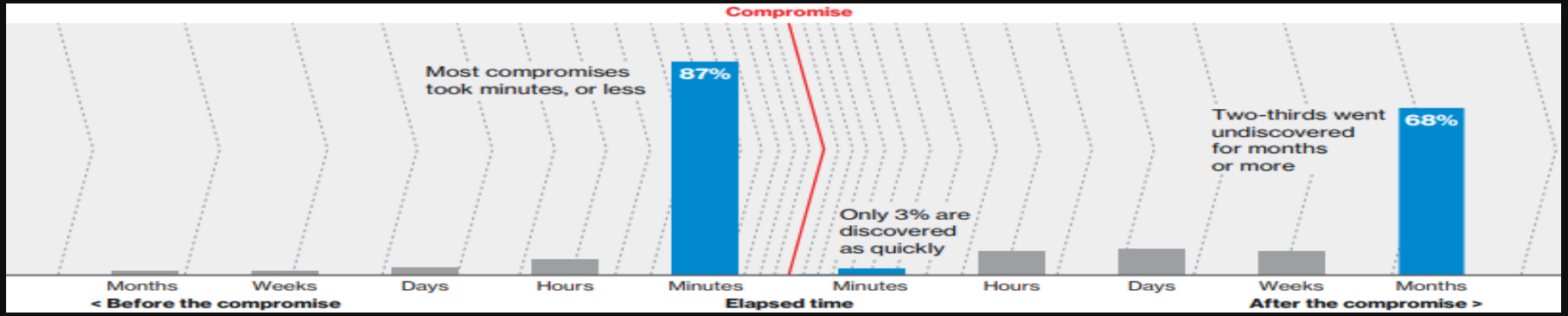
Quando não sabemos o que procurar...

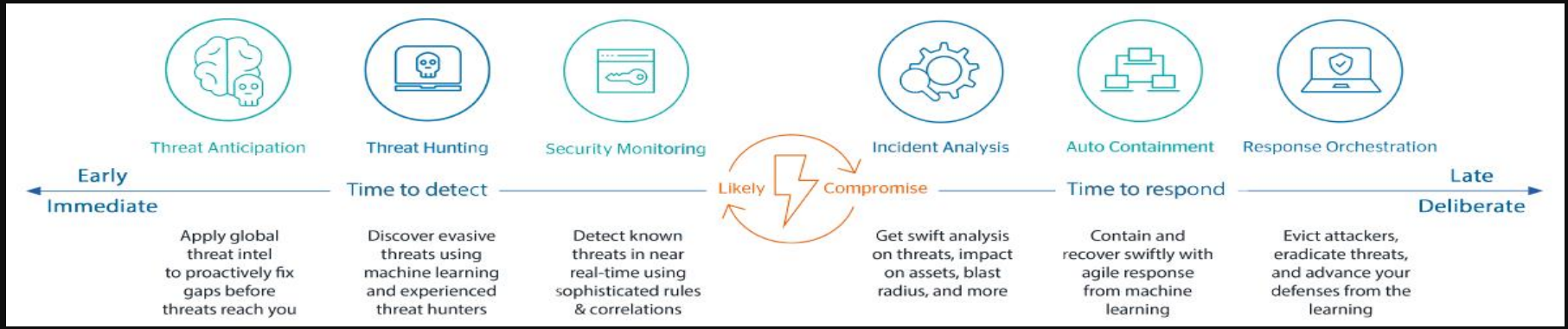


Uso de IA em Segurança Digital



Tempo de ação





Tempo de Permanência e Resposta

Fases de ataque – cenário tradicional

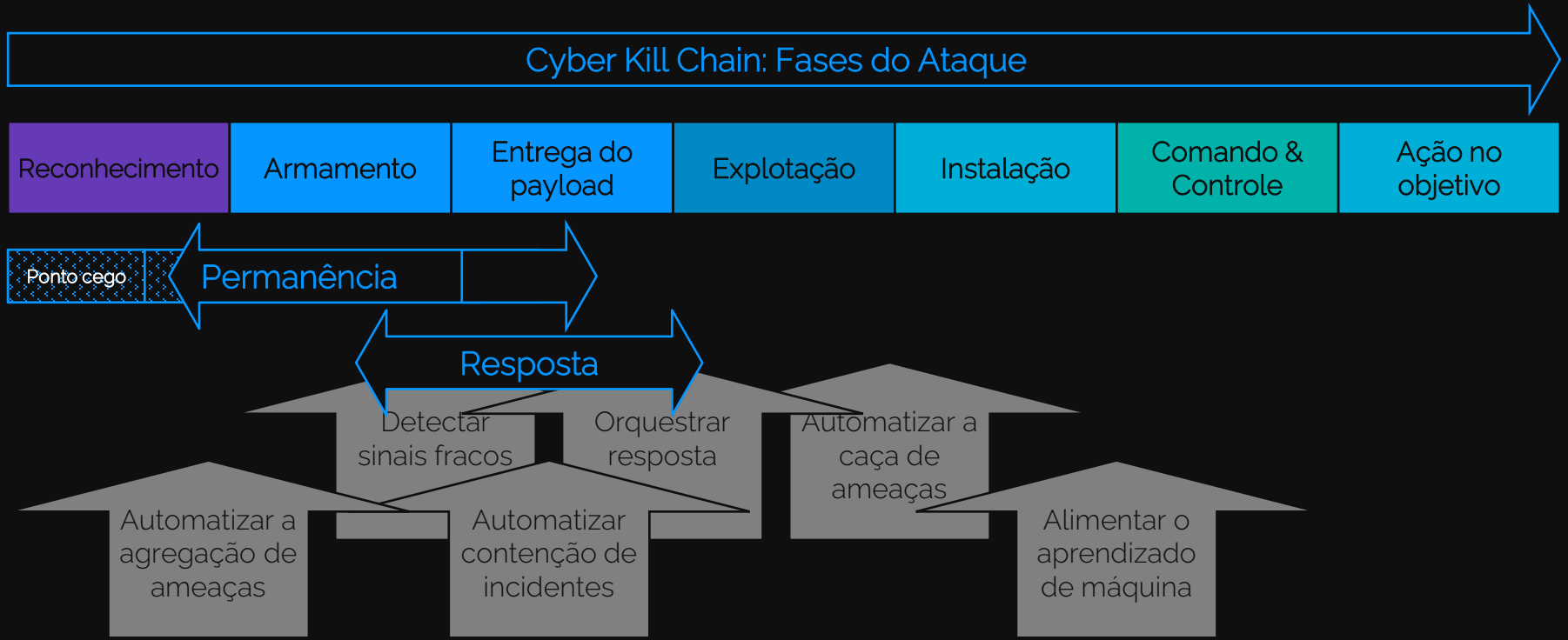
Tempo de permanência (Threat Discovery Time) ainda muito alto porque os ataques são mais penetrantes e difíceis de detectar
Tempo medio para descobrir ameaças: 191 días*

Tempo de Resposta

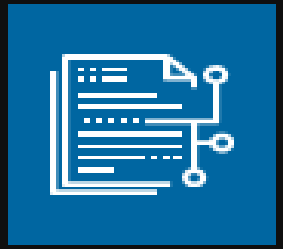
Tempo de Resposta em ascensão, à medida que investigação avançada de ataque, neutralização e recuperação exigem equipes CERT especializadas.
Tempo medio de contenção: 66 días*

Tempo de Permanência e Resposta

Fases de ataque – cenário com IA



Técnicas de Detecção



Regras & Assinaturas (SIEM)

Monitoração 24x7 do SOC
para ameaças conhecidas

Fontes de Inteligência de Ameaças (TI)

Antecipação de Ameaças 24x7
Para atacantes conhecidos

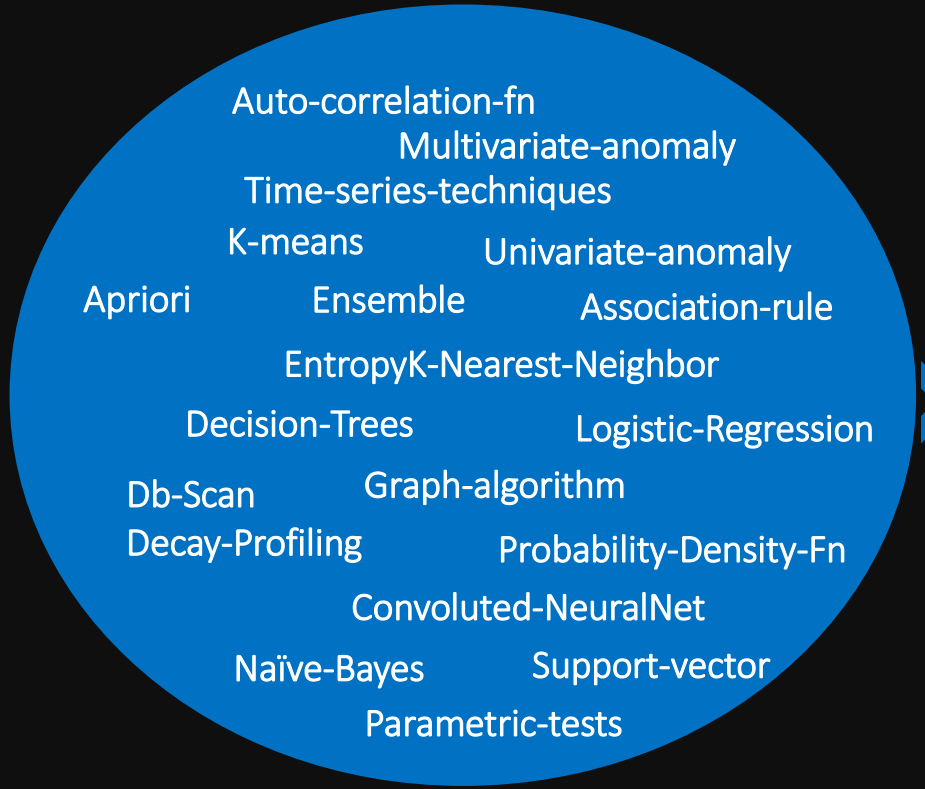
Modelos de Machine learning (TH)

Caça de Ameaças 24x7
Para ameaças/atacantes desconhecidos

Alguns algoritmos de Machine Learning

Multi-Mode
Data Ingestion

- Network
- endpoints
- users
- logs
- cloud



- Threat Hunting Models
- Investigation Models
- Response Models
- Threat Intel Models

Casos de sucesso de modelos de AI

Malware: Algoritmo de Geração de Domínio (DGA)

DGA é utilizado por malware para gerar domínios dinâmicos aleatórios, para entrar em contato com servidores CnC.

Lógica personalizada para processar solicitações e respostas DNS e identificar

Pontos chave:

- Tecnologias de detecção muito limitadas com foco em DNS.
- Não foi detectado por outras tecnologias.

Comprometimento de Ativo de nuvem

A maioria dos ativos de nuvem são inerentemente expostos à Internet e estão sob constante ataque

Lógica de criação de perfil que define a linha de base do comportamento de rede de cada ativo de nuvem e identifica comunicação anômala associada a tentativas de exfiltração e movimento lateral

Pontos chave:

- AWS GuardDuty não detectou o ataque.

Ataques a OT/IoT

Perfilamento dos padrões de comunicação (volume de dados, frequência de conexões e serviços acessados) de todos os ativos que interagem por meio do firewall para identificar movimento lateral, acesso CnC e tentativas de exfiltração

Pontos chave:

- Nenhuma das tecnologias existentes detectou qualquer vestígio do ataque.

Regra de FW sem aplicar

O modelo funciona em uma lógica customizada construída para detectar padrões de movimento lateral, especialmente aqueles que visam um serviço específico ou grupos de serviços

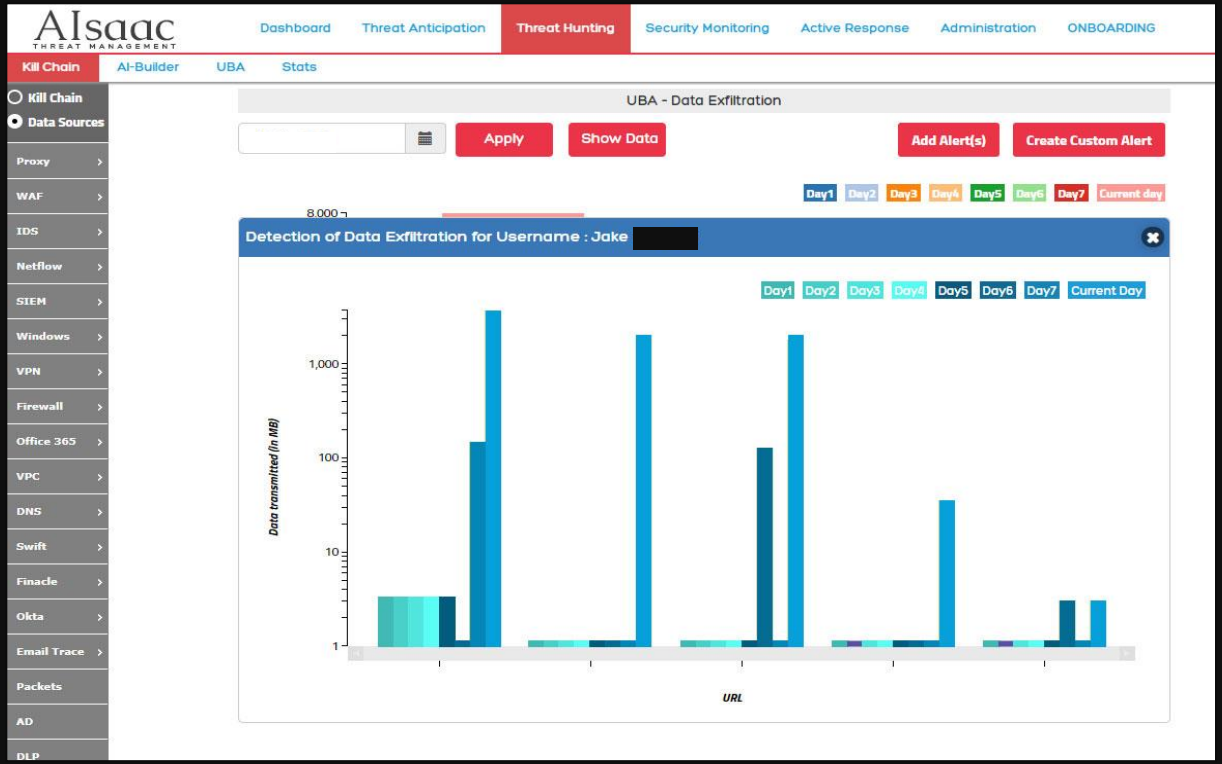
Pontos chave:

- Detectado pelo SOC. Uma regra (Block) foi implantada na rede; no entanto, um firewall faltou aplicar.

Exfiltração lenta de dados

Como o MDR detectou isso?

Um dos modelos do Threat Hunting sinalizou várias conexões automatizadas para o blog de um sistema específico por um longo período de tempo, o que revelou as tentativas de vazamento de dados. Os modelos procuram conexões não aleatórias de fontes internas para fontes externas, independentemente do tamanho do pacote. Como o insider estava usando um software para postar informações, o modelo identificou esse comportamento automático e não aleatório. O time de Threat Hunters investigaram à anomalia para confirmar o ataque.



Deteccção de Ransomware

Como o MDR detectou isso?

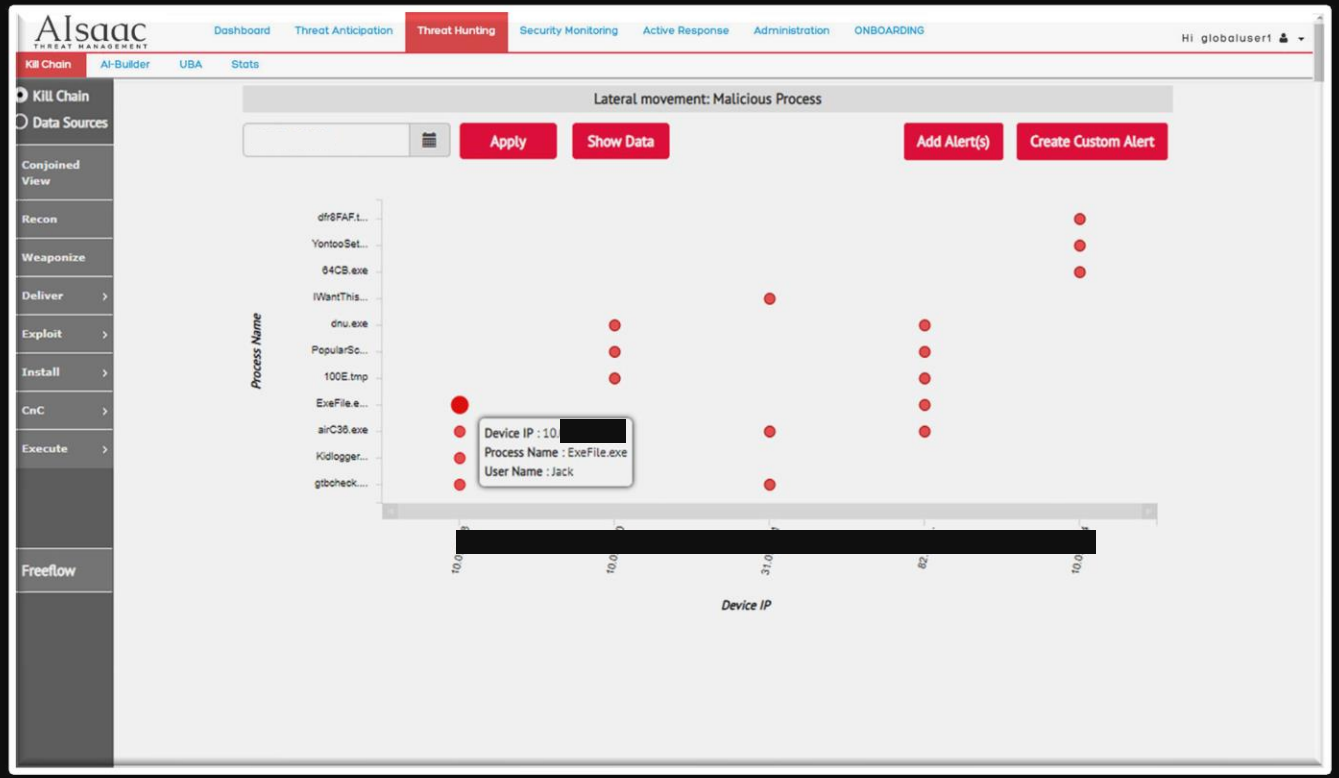
A equipe de Antecipação de Ameaças relatou o surgimento de kits de exploração Green Flash. A equipe de Threat Hunting começou a procurar especificamente por tráfego suspeito de sites semelhantes ao site do conversor de vídeo e identificou a ameaça.

Uma vez que o site do conversor de vídeo online é um site genuíno, nenhum dos proxies, Firewalls e EDR sinalizou esta comunicação.

Detecção de Trojan Racoon para roubo de informações

Como o MDR detectou isso?

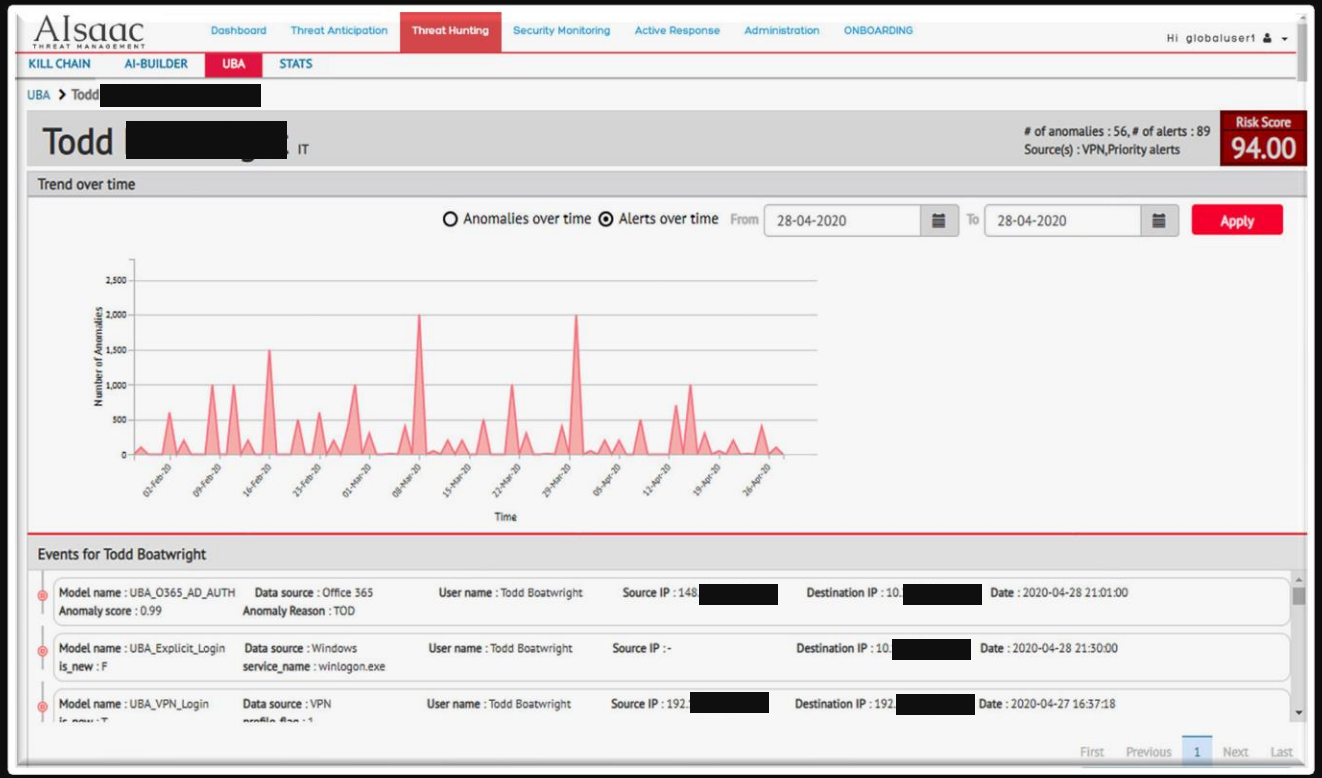
Usando o modelo analítico, fomos capazes de identificar a conexão persistente com o URL suspeito e, com a ajuda do feed da Inteligência de Ameaças, conseguimos comparar o URL suspeito com a infecção por Raccoon



Detecção de comprometimento de e-mail O365

Como o MDR detectou isso?

A solução traçou o perfil de comportamento do usuário com base em login múltiplo. O MDR procurou por anamolia no tempo de login, número de logins, duração do login, local do login, etc. A plataforma sinalizou o e-mail como suspeito, pois houve um evento de login para a conta do CEO de uma geografia atípica com base no perfil de autenticação anterior do CEO.



Dúvidas...

Obrigado !

For more information please contact:
M+ 55 11 98398 0604
americo.alonso@atos.net