



Detecte, interrompa e elimine ameaças físicas e cibernéticas avançadas

Descubra conexões ocultas, obtenha inteligência acionável e acelere os dados para tomar decisões

Superando **DESAFIOS DE CAÇA A AMEAÇAS** no espaço físico e cibernético

Os atores de ameaças estão ficando mais sofisticados, enquanto os analistas estão sobrecarregados com o volume e a complexidade dos dados.

O cenário de ameaças está mudando constantemente. No mundo físico, novos círculos criminais e células terroristas continuam a se formar; no mundo cibernético, os atores de ameaças estão constantemente criando novas maneiras de roubar dados, interromper negócios e destruir reputações. Os responsáveis por caçar ameaças físicas e cibernéticas, seja o diretor de segurança da informação, o diretor de inteligência de ameaças, o diretor de detecção de fraudes, o chefe de polícia ou um líder de segurança nacional, têm um trabalho difícil a fazer.

Um dos maiores desafios que os analistas de segurança e inteligência enfrentam é estar sobrecarregado por grandes volumes de dados de diferentes fontes. E muitas vezes não possuem ferramentas que permitem prever e prevenir ameaças físicas e cibernéticas.

Essa é uma lacuna crucial, porque atrás de toda ameaça avançada há um humano. As soluções IBM® i2® oferecem uma plataforma de análise e inteligência de ponta que permite a caça avançada de ameaças com uma abordagem de humano contra humano. As soluções vão além dos recursos baseados



em políticas, para ajudar os analistas de segurança e inteligência não apenas a entenderem, mas também a anteciparem quando e onde o próximo agente de ameaças atacará, seja na rede de TI, na fronteira nacional ou nas ruas locais.

A solução capacita os caçadores de ameaças nos setores público e privado com as ferramentas de nível militar necessárias para superar os atores de ameaças, armando os analistas de

segurança e inteligência com ferramentas e tecnologia que permitem que eles detectem, interrompam e eliminem ameaças cibernéticas e físicas avançadas, correlacionando e analisando fontes de dados diferentes em tempo quase real.

[Assista ao vídeo para aprender como as soluções IBM i2 ajudam a identificar e prevenir ameaças cibernéticas avançadas.](#)



DETECTE, INTERROMPA E ELIMINE ameaças avançadas

As soluções IBM i2 fornecem aos analistas e caçadores de ameaças ferramentas avançadas para detectar, interromper e eliminar ameaças avançadas.

A detecção de ameaças não começa com dados. Ela começa com perguntas. Qual é o problema que um analista precisa resolver? Ele está procurando um insider malicioso que está removendo secretamente dados de propriedade intelectual de nossa rede? Estamos tentando eliminar um círculo de traficantes de drogas? Procura transações clandestinas que possam indicar lavagem de dinheiro? A identificação do problema ajuda a determinar os dados necessários e onde podem ser encontrados dentro ou fora da organização.

Depois que as origens de dados necessárias são determinadas, as ferramentas avançadas de análise e inteligência IBM i2 ajudam os analistas a transformar dados em decisões em tempo quase real, descobrir conexões ocultas com exibições visuais e transformar dados impressionantes e díspares, independentemente da fonte, em inteligência acionável.

Os aplicativos IBM i2 abrangem uma variedade de setores e necessidades de caça a ameaças, incluindo:

- *Agências nacionais de segurança e defesa* buscando obter insights imediatos e tomar decisões de segurança em velocidade e escala para apoiar operações críticas
- *Agências policiais* que precisam de uma imagem de inteligência comum, com análises projetadas para analistas de investigação, que otimizam a geração de oportunidade e o gerenciamento de crimes
- *Centros avançados de operações de segurança (SOCs)* em empresas que precisam encontrar ameaças mais rapidamente e mais cedo na rede de destruição e reduzir o tempo de detecção e os custos e o impacto de ataques cibernéticos
- *Líderes de prevenção de fraudes e crimes financeiros* em empresas comerciais que buscam enfrentar investigações complexas e descobrir conexões ocultas para detectar fraudes e ameaças internas em suas operações



DeliverFund usa o IBM i2 para interromper o tráfico de pessoas

A DeliverFund é uma organização de inteligência privada, sem fins lucrativos, comprometida em interromper redes de tráfico de pessoas. Em um caso, o tempo entre a detecção de uma rede e a prisão foi de apenas 27 dias. Segundo o fundador da DeliverFund, “no mundo do combate ao tráfico de pessoas, isso é inédito. Isso ocorreu em grande parte devido ao software de análise de inteligência IBM i2.”

[Assista ao vídeo sobre como a DeliverFund usa as soluções IBM i2 para combater o tráfico de pessoas.](#)

SUPERANDO OS INVASORES com uma abordagem de humano contra humano

As soluções IBM i2 combinam o poder da análise avançada com o poder dos recursos avançados de análise de inteligência liderados por humanos.



Soluções de segurança baseadas em políticas, como proteção de terminais, segurança de rede e gerenciamento de identidade e acesso, são formas necessárias de proteção contra ameaças. Mas essas soluções são ainda mais eficazes quando combinadas com o poder do insight humano sobre o comportamento humano, que pode ser desenvolvida por meio da análise multidimensional do IBM i2. Para ficar à frente das ameaças, os analistas de segurança e inteligência precisam pensar como os invasores que estão tentando derrotar, seja no mundo da segurança cibernética ou da inteligência de missão.

As soluções IBM i2 fornecem uma abordagem de humano contra humano para entender o inimigo. Análises poderosas podem ajudar os analistas a desenvolver formações de valor para entender e antecipar onde os atores de ameaças podem atacar. Ao conectar, analisar e visualizar fontes de dados diferentes, incluindo armazenamento de dados de software livre e de terceiros, seja de um sistema de recursos humanos, um banco de dados de crimes ou mídia social, a análise IBM i2 fornece insights em tempo quase real que podem ajudar a inteligência e os SOCs a detectar, interromper e eliminar atores de ameaças.



Por que as empresas estão adotando a caça a ameaças

Os recursos de análise do IBM i2 foram desenvolvidos no domínio das comunidades de defesa, aplicação da lei e inteligência. Hoje, à medida que as ameaças avançadas continuam a se sofisticarem, as empresas, especialmente nos setores de serviços bancários e financeiros, estão aproveitando esses recursos avançados de nível militar para detectar fraudes, identificar lavagem de dinheiro e antecipar ameaças cibernéticas.

-  [Assista ao vídeo para aprender como as soluções IBM i2 ajudam a evitar fraudes bancárias.](#)
-  [Assista ao webinar para saber mais sobre por que as empresas estão adotando a caça a ameaças.](#)

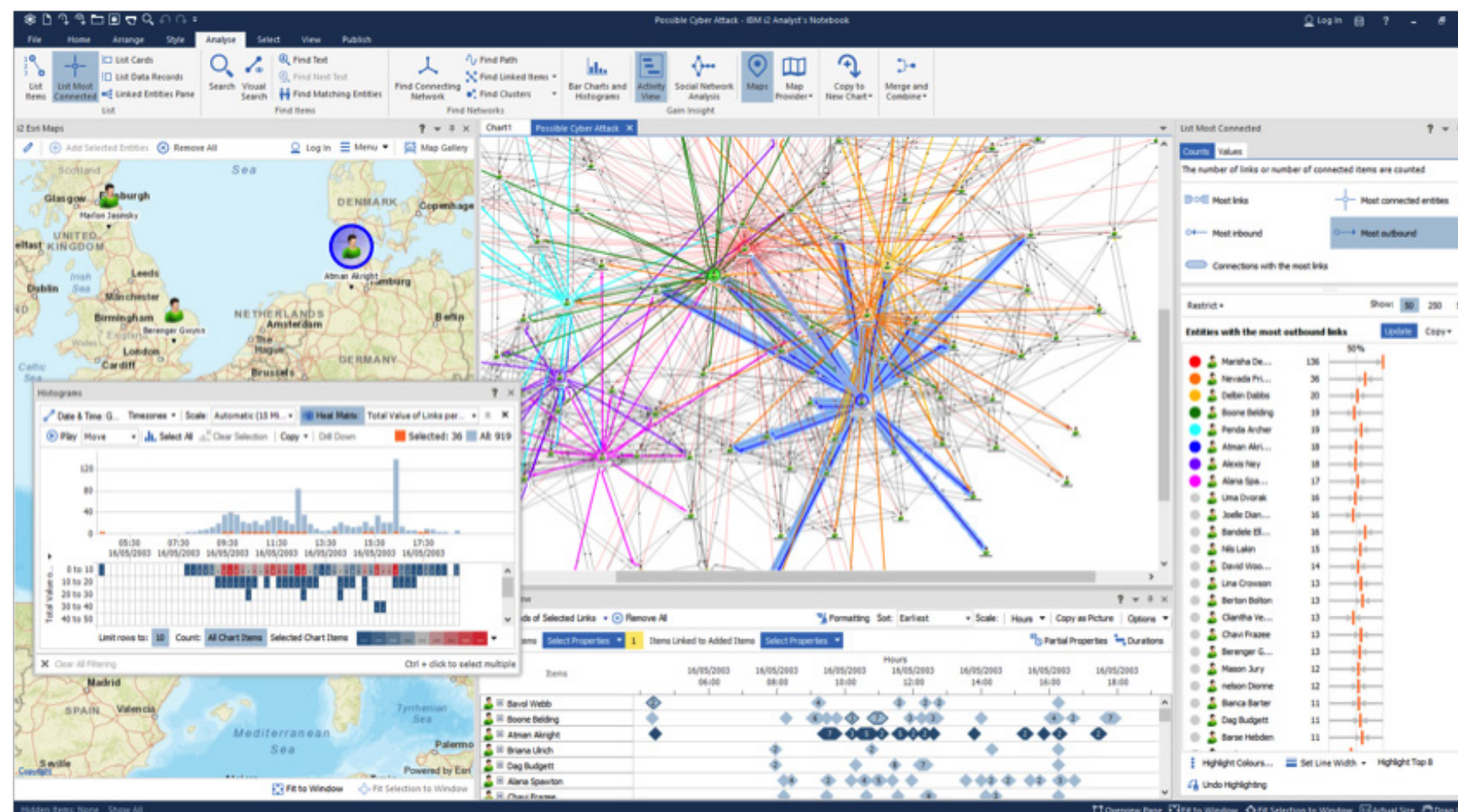
ARME SEUS ANALISTAS para combater adversários avançados

O IBM i2 multiplica os esforços de analistas que combatem adversários avançados no espaço físico e no ciberespaço.

Os dados de ameaças podem (e devem) ser extraídos de uma variedade de fontes. Mas, pesquisar manualmente bancos de dados, e-mails, vídeos, documentos, mídias sociais e dados de software livre para descobrir ameaças pode ser uma tarefa esmagadora para os responsáveis pela caça a ameaças.

As soluções IBM i2 são um “multiplicador de forças” para analistas de segurança e inteligência, trazendo dados estruturados e não estruturados de fontes internas e externas. A plataforma otimiza os dados aplicando um único modelo de dados a diferentes feeds de dados físicos e digitais, capacitando os analistas a realizar análises visuais, temporais e geoespaciais. Além disso, fornece aos analistas as ferramentas necessárias para conectar-se a novas fontes de dados ou de software livre, mesmo que as fontes ainda não tenham sido importadas para o armazenamento de dados IBM i2.

Os analistas podem usar algoritmos integrados ou criar consultas visuais para estabelecer conexões entre itens potencialmente correspondentes importados de fontes de dados diferentes e, em seguida, localizar e mesclar entidades correspondentes. Os analistas também podem criar e compartilhar gráficos com colegas, outros departamentos ou organizações de terceiros.



Ingira, funda e analise dados de diferentes fontes com análise visual multidimensional.

Como as soluções IBM i2 são construídas em uma arquitetura aberta e extensível, elas se integram facilmente aos investimentos em TI e são projetadas para lidar com consultas operacionais simultâneas de vários grupos de trabalho da organização, compartilhando um sistema central com a ingestão contínua de dados. As implementações podem variar de um único usuário implementado a um sistema em toda a organização conectado a várias fontes de dados e usado por muitos analistas.

Assista à demonstração para ver como as soluções IBM i2 podem ajudar os analistas a encontrar e combinar entidades aparentemente não relacionadas.



Acelerar os DADOS PARA DECISÃO

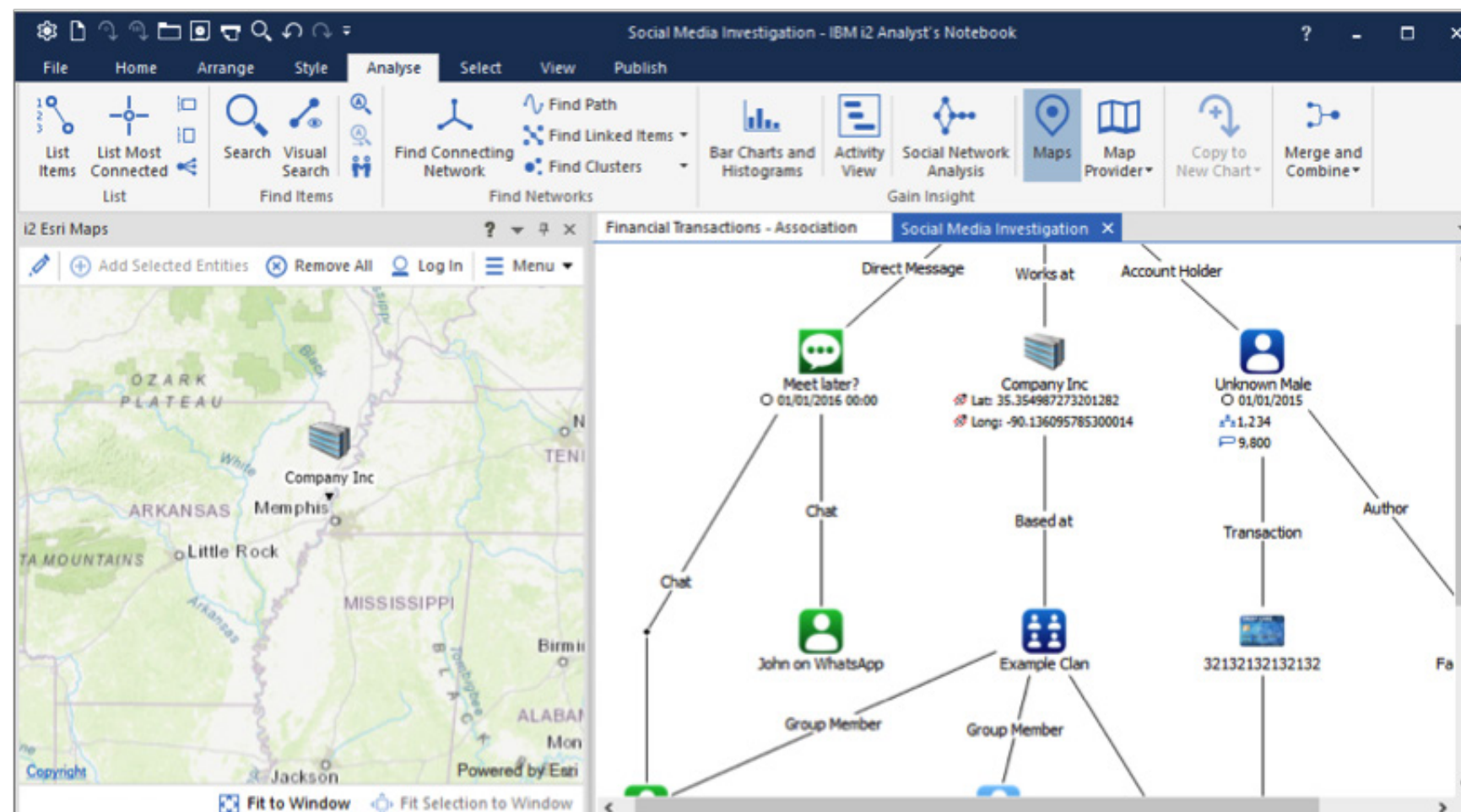
Ingira, funda e analise dados de diferentes fontes, incluindo dados estruturados, não estruturados, de inteligência de software livre (OSINT) e dark web, em tempo quase real.

Depois que os analistas determinam os dados que precisam analisar, o desafio é alavancar os dados de maneira a apoiar decisões imediatas. Para fazer isso, eles precisam da capacidade de entender rapidamente a substância e o significado das informações armazenadas e recebidas.

Com a capacidade de integração com outras fontes de dados, as soluções IBM i2 podem gerenciar centenas de consultas complexas simultâneas com ingestão contínua de dados, permitindo que as organizações carreguem dados dispersos por vários silos simultaneamente.

Os conectores de acesso a dados sob demanda ajudam os usuários a analisar dados em tempo quase real e:

- descobrir rapidamente padrões anormais, testar hipóteses e consultar terabytes de dados em segundos
- receber alertas automáticos quando os dados são incluídos ou alterados
- revelar hierarquias temporais, de rede e formações de valor geoespaciais críticos
- visualize dados de forma flexível em um formato histográfico ou temporal para identificar atividades anômalas, como o tunelamento do servidor de nomes de domínio



As soluções IBM i2 permitem que as organizações fundam dados de várias fontes internas e externas, incluindo mídias sociais.

A Building Society usa o IBM i2 para combater crimes financeiros

A Skipton Building Society, a quarta maior sociedade de construção do Reino Unido, precisava de uma maneira de ir além dos processos de análise manual para investigar crimes financeiros. A implementação das ferramentas de análise IBM i2 ajudou a acelerar as investigações em 80% e eliminou horas de análise baseada em planilha, apresentando dados visualmente.



Assista para descobrir como o IBM i2 transforma dados em decisão quase em tempo real.

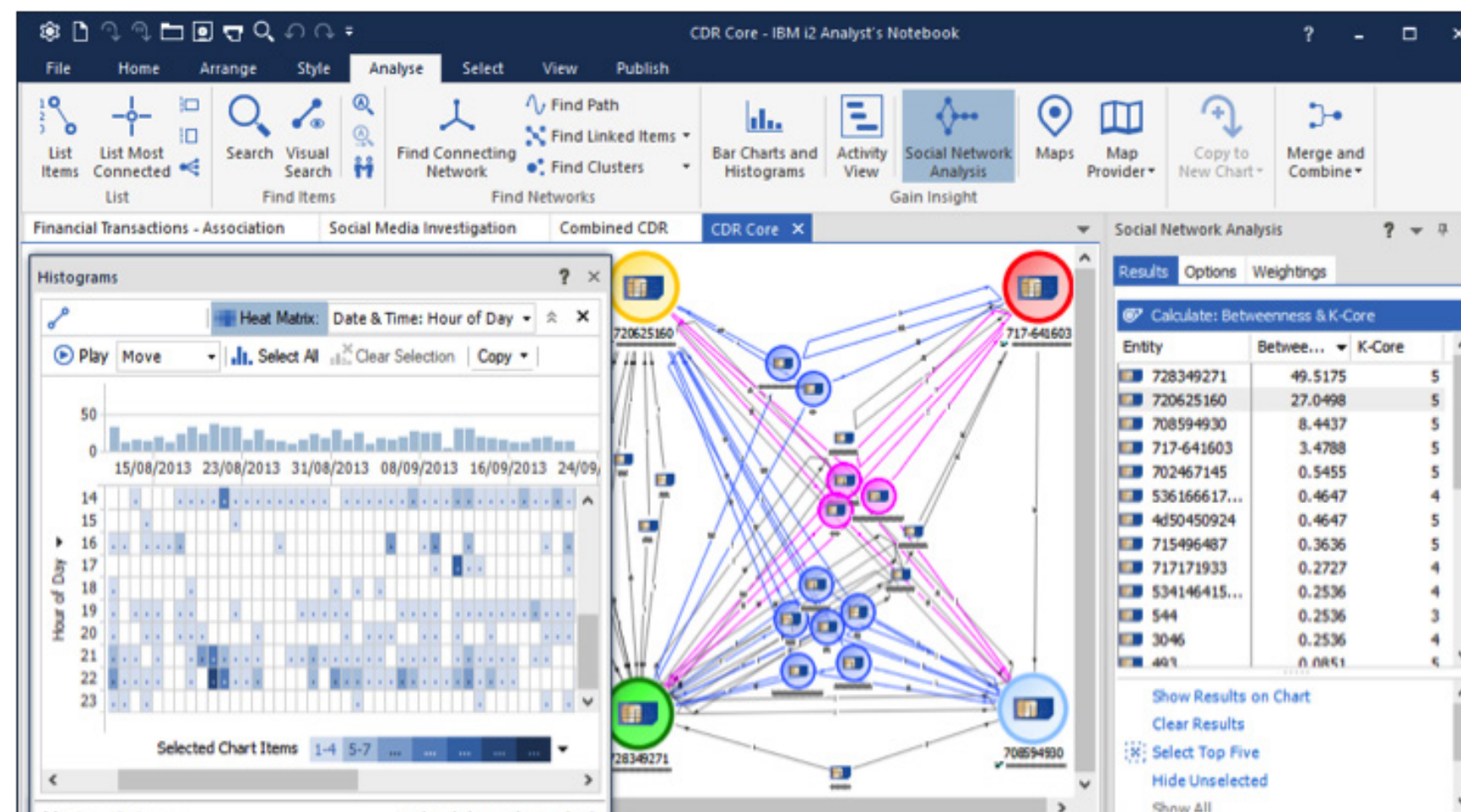
DESCUBRA CONEXÕES OCULTAS e obtenha novas insights

Os analistas podem fazer e responder perguntas complexas com recursos simples e fáceis de usar para descobrir conexões ocultas e encontrar o sinal no ruído.

Os analistas têm a tarefa de interpretar grandes quantidades de dados de várias fontes, incluindo bancos de dados, e-mails, vídeos, mídias sociais e fontes de dados abertas. Estejam eles procurando detectar, interromper e eliminar várias tentativas de login às 2 da manhã de um local remoto na China, o movimento no radar de armas através das fronteiras ou transferências suspeitas de fundos muito pequenas para desencadear uma revisão regulatória, é difícil para os analistas explorar esses enormes volumes de dados para conexões ocultas.

Com as soluções IBM i2, as informações coletadas podem ser integradas e visualizadas com informações de software livre para criar uma visão abrangente de padrões e conexões não óbvias. Os analistas também podem pedir ao sistema para “encontrar redes conectadas” para descobrir relacionamentos separados por vários graus.

Conexões e tendências enterradas em terabytes de dados podem ser visualizadas em tempo quase real com visualizações multidimensionais, incluindo análises geoespaciais, temporais e de relacionamento. Um mecanismo de resolução e recomendação de identidade fornece análise assistida, consolidando conjuntos de dados massivos e reconciliando



Os recursos de análise multidimensional ajudam a encontrar rapidamente conexões e padrões ocultos.

entidades duplicadas mascaradas por pseudônimos. Por meio do mecanismo, os usuários podem definir alertas para rastrear informações novas e críticas 24 horas.

Os analistas podem fazer perguntas complexas usando consulta visual, usando ícones para desenhar ou questões de diagrama sem necessidade de codificação ou suporte especial.

[Assista ao vídeo para aprender como as soluções IBM i2 podem ajudar a impedir ameaças internas.](#)

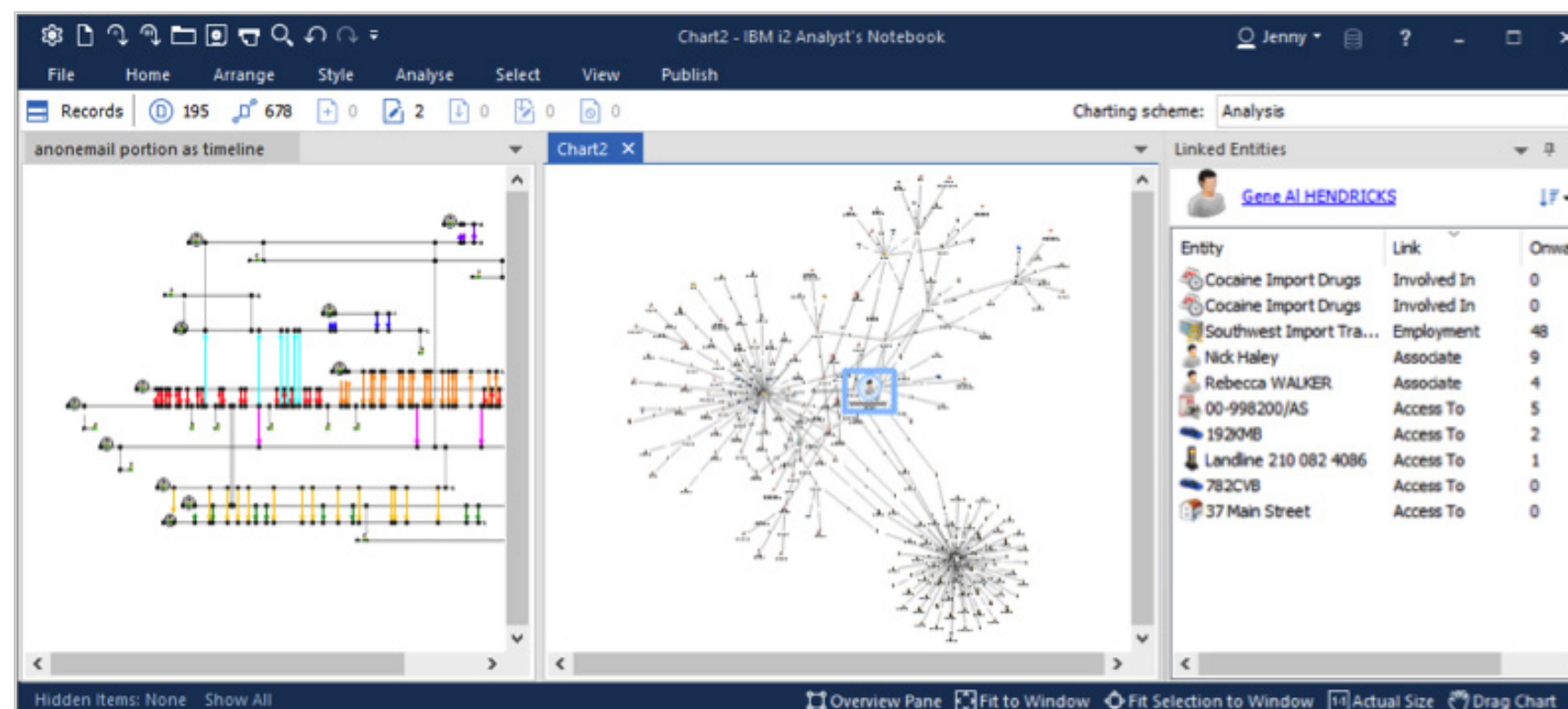


Transforme dados impressionantes e diferentes em **INTELIGÊNCIA ACIONÁVEL**

Tome decisões seguras e tome medidas confiantes transformando dados avassaladores e díspares em inteligência acionável em tempo quase real.

Para derrotar verdadeiramente as ameaças, a inteligência reunida sobre elas deve ser algo em que se possa agir, mesmo que isso signifique bloquear o acesso à rede para um usuário suspeito ou alertar as autoridades sobre atividades criminosas. No entanto, tecnologias como redes sociais, Internet das Coisas e nuvem produziram uma enorme quantidade de dados complexos os quais os agentes de ameaças estão ocupados usando para mascarar suas identidades e atividades. A rica extração, análise e visualização nas soluções IBM i2 podem transformar efetivamente a complexidade dos dados em inteligência acionável, ajudando a revelar quem está por trás das ameaças, qual é a ameaça, onde ela está, quando ela acontece e por que acontece.

As soluções IBM i2 podem vincular automaticamente entidades aparentemente não relacionadas, executando consultas complexas em centenas de terabytes de dados e aplicando análises avançadas tridimensionais simultaneamente. Com uma visão abrangente, os analistas podem desenvolver uma compreensão abrangente de suas superfícies e vulnerabilidades de ataque e desenvolver proativamente cenários de ataque físico e cibernético.



O IBM i2 capacita os analistas a aplicar análise visual, geoespacial e temporal para realizar consultas precisas e complexas que fornecem inteligência acionável.

Tornar a inteligência acionável também significa torná-la acessível à medida que sua organização faz a transição. Se o pessoal de segurança de uma empresa for mudado ou unidades militares e de inteligência forem transferidas, a evolução da força de trabalho poderá potencialmente interromper o fluxo de informações críticas sobre ameaças.

As soluções IBM i2 permitem que as organizações criem um repositório de dados robusto que permanece no local durante essas transições. Modelos predefinidos e personalizados podem ajudar a preencher rapidamente o repositório.

Devido ao seu design aberto, as soluções IBM i2 podem habilitar interfaces de programação de aplicativos (APIs) que permitem que as organizações personalizem análises que atendam às suas necessidades e requisitos específicos.

[Assista ao vídeo para saber como as soluções IBM i2 estão ajudando a comunidade de inteligência a criar um planeta mais seguro.](#)



Confiável para as missões mais críticas. QUAL É A SUA?

O IBM i2 é a plataforma confiável de análise de inteligência para o governo e o setor privado, abrangendo segurança e defesa nacional, aplicação da lei, investigações de fraude e caça a ameaças cibernéticas.

O software IBM i2 é baseado em quase três décadas de contribuição de analistas de mais de 4.000 organizações e é a plataforma confiável de análise de inteligência para o governo e o setor privado, abrangendo segurança nacional e defesa, aplicação da lei, investigações de fraude e caça a ameaças cibernéticas.

Respaldadas por um histórico de inovação em análise de inteligência, as soluções IBM i2 são construídas em uma arquitetura aberta e extensível com recursos de análise prontos para uso que oferecem aos clientes facilidade de escalabilidade e planejamento para necessidades futuras. Armandando analistas em todo o mundo com as ferramentas avançadas necessárias para detectar, interromper e eliminar ameaças físicas e cibernéticas avançadas, as soluções IBM i2 estão ajudando a criar um planeta mais seguro.

As soluções IBM i2 são apoiadas pelo poder da IBM, incluindo especialistas em análise de inteligência interna, serviços IBM e o ecossistema de parceiros IBM para design, instalação, suporte e treinamento para lidar até com os desafios mais complexos. O IBM i2 oferece experiência comprovada no assunto, experiência no mercado e experiência em implementações globais de todos os tamanhos que são incomparáveis.

Para mais informações

Para obter mais informações sobre soluções IBM i2, entre em contato com seu representante IBM ou Parceiro Comercial IBM ou visite: ibm.com/br/pt/marketplace/enterprise-insight-analysis

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

A página inicial da IBM pode ser encontrada em:
ibm.com

IBM, o logotipo IBM, ibm.com e i2 são marcas registradas da International Business Machines Corp., registradas em vários países no mundo inteiro. Outros nomes de produtos e de serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas registradas da IBM está disponível na internet em “Copyright and trademark information” em ibm.com/legal/copytrade.shtml

Este documento estava atualizado na data de publicação inicial e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países onde a IBM opera.

É responsabilidade do usuário avaliar e verificar a operação de outros produtos ou programas com produtos e programas IBM.

AS INFORMAÇÕES NESTE DOCUMENTO SÃO OFERECIDAS NO ESTADO EM QUE SE ENCONTRAM (“AS IS”) SEM QUALQUER GARANTIA, EXPLÍCITA OU IMPLÍCITA, INCLUINDO SEM QUAISQUER GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM PROPÓSITO ESPECIAL E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO VIOLAÇÃO. Os produtos da IBM têm garantia conforme os termos e condições dos contratos sob os quais são oferecidos.

O cliente é responsável por garantir a conformidade com as leis e regulamentações aplicáveis. A IBM não fornece conselhos jurídicos e não declara ou garante que seus serviços ou produtos irão assegurar que o cliente esteja em conformidade com qualquer lei ou regulamento. As declarações com relação aos objetivos e direções futuras da IBM estão sujeitas a mudanças ou retiradas sem aviso prévio e representam apenas objetivos e metas.

Declaração de Boas Práticas de Segurança: a segurança do sistema de TI envolve a proteção dos sistemas e informações através da prevenção, detecção e resposta ao acesso indevido de dentro e de fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação e mau uso de informações ou pode resultar em danos ou mau uso de seus sistemas, incluindo ataques a outras pessoas. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhuma medida exclusiva de produto, serviço ou segurança pode ser completamente efetiva na prevenção de uso ou acesso incorreto. Os sistemas, produtos e serviços IBM foram projetados para fazer parte de uma abordagem de segurança legítima e abrangente, a qual necessariamente envolve procedimentos operacionais adicionais e pode exigir que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE TODOS OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM LIVRES DE, OU QUE TORNARÃO A SUA EMPRESA LIVRE DE CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PARTE.

© Copyright IBM Corporation 2020

