

ECHO

SISTEMA GLOBAL DE ADINT VIRTUAL

Descrição do Produto

Aviso Importante

Esse documento ("Documento") é entregue sujeito as seguintes condições e restrições:

- As informações fornecidas neste documento constituem "segredos comerciais do Grupo" Rayzone Group Ltd. ("Rayzone") e são confidenciais e de propriedade do Grupo Rayzone, suas afiliadas, e fornecedores. A Informação oferecido aqui, e qualquer Informação oferecido em promoção desse documento deve ser tratado em estrita confidencialidade.
- Qualquer reprodução não autorizada (eletrônico ou mecânico), uso, ou divulgação desse material, ou qualquer parte dele, é estritamente proibido. O conteúdo deste Documento ou qualquer parte dele pode ser usado somente para o propósito para o qual foi fornecido.
- Este documento destina-se exclusivamente ao uso de entidades expressamente autorizadas pela Rayzone.
- O material que descreve o Rayzone Group é para fins de informação geral e pode ser modificado pela Rayzone a qualquer momento, sem aviso prévio.
- O texto e os gráficos são apenas para fins ilustrativos e de referência. As especificações nos quais se baseiam estão sujeitos a alterações sem aviso prévio.
- As informações divulgadas neste Documento são divulgadas "como estão" e a Rayzone não deve ser responsável por sua precisão ou integridade.

Conteúdo

1. Sobre o Grupo Rayzone	3
2. Descrição do Produto ECHO	4
3. Componentes da solução	6
4. Recursos Avançados	18
5. Segurança	20

1. Sobre o Grupo Rayzone

Como líder global em soluções boutique baseadas em inteligência para agências nacionais em todo o mundo, O Grupo Rayzone se esforça para oferecer sistemas que melhorem a conscientização sobre ameaças potenciais, permitam mitigação à prova de falhas dessas ameaças e aumentar a eficiência das agências governamentais.

Com sua abordagem única à segurança, o Rayzone Group criou um ecossistema maleável e holístico que atende às necessidades dos clientes de forma coesa. O portfólio do Rayzone Group é composto por uma ampla gama de sistemas de proximidade e remotos, bem como a capacidade de construir e manter sistemas completos projetos governamentais de escopo. Nossa expertise deriva dos campos de Dataveillance, SIGINT, GEOINT, ADINT, OSINT, Cyber Celular, Cyber Intelligence, Fusion & Analysis, Counter intelligence e Cyber security levaram ao desenvolvimento de nossas soluções pioneiras que garantem os mais altos níveis de proficiência em todos os estágios do ciclo de inteligência.

O quebra-cabeça da inteligência não pode ser resolvido com uma única peça - portanto, o Rayzone Group oferece três tipos de soluções: sistemas autônomos, sistemas integrados e soluções nacionais completas e prontas para uso projetos.

Nossa equipe interdisciplinar, composta por especialistas em vários campos relevantes e internos engenheiros, cria sistemas revolucionários que respondem às necessidades em constante mudança dos clientes e projeta soluções personalizadas para desafios específicos. Antigos oficiais de operação e especialistas em segurança cibernética fornecem insights em primeira mão para garantir que nossas soluções sejam construídas com base nas tecnologias e metodologias mais recentes e relevantes.

Certificada pelas normas ISO 9001, ISO 14001, ISO 45001, ISO 27001 e com escritórios locais em vários países, o Rayzone Group vem fornecendo tecnologias para agências governamentais em dezenas de países por mais de uma década. O comprometimento total com a transparência completa, a verdadeira parceria e uma atitude positiva são elementos essenciais em cada envolvimento com os diversos parceiros da empresa. e uma ampla gama de clientes. Acreditamos que tanto nossa cultura centrada nas pessoas quanto nossa forte motivação para inovação tecnológica, aprimorar o desenvolvimento de nossas ferramentas e sistemas de inteligência cibernética e segurança, permitindo-nos assim fornecer aos nossos clientes as soluções mais avançadas para atender às suas necessidades específicas.

2. Descrição do Produto ECHO

2.1 Resumo Executivo

Echo é uma plataforma de investigação de coleta em massa baseada em ADINT, que permite que agências de inteligência e aplicação da lei conduzam análises aprofundadas de dados de usuários de internet móvel em um mundo global.

O Echo utiliza métodos de coleta de dados totalmente furtivos que não envolvem o alvo ou qualquer outra entidade. O sistema é agnóstico para tipos de dispositivos, sistemas operacionais e versões e, como tal, não requer pré-instalação de nenhum equipamento físico.

Este sistema reúne as pegadas digitais dos usuários móveis (metadados) e, usando o exclusivo Echo capacidades, extrai informações importantes e dados enriquecidos, como histórico de localização de um alvo, padrões comportamentais, perfil completo, capacidades de desanonimização e muito mais.

A plataforma baseada na web permite que os usuários realizem consultas simples, bem como investigações complexas. Os usuários se beneficiam de uma abordagem centrada no alvo (coleta de informações sobre pontos de interesse específicos) e uma abordagem centrada em dados (coleta em massa de tráfego da Internet em um nível nacional) com ferramentas de investigação adaptadas às suas necessidades e requisitos.

Principais recursos do ECHO incluem:

- Coleta em massa de tráfego de internet móvel
- Interceptação mundial contínua e retrospectiva
- Aquisição de alvos baseada em suposições
- Perfis de alvos íntimos (com base nas capacidades de melhor esforço)

¹¹ O Echo coleta dados na maioria dos tipos e versões de dispositivos. Pode haver exceções em dispositivos que usam tipos alternativos de identificadores de anúncio.

As principais vantagens do Echo incluem:

- Acesso imediato a dados históricos e em tempo real do alvo
- Coleta em massa de qualquer dispositivo móvel, independentemente de modelos ou sistemas operacionais
- Não requer instalação física
- Não é necessário envolvimento do alvo

2.2 A solução Echo

O Echo realiza a coleta em massa de pegadas digitais (metadados) de usuários móveis no país solicitado. O sistema coleta as seguintes informações com base no número de identificação exclusivo do usuário móvel:

- Tempo de atividade
- Localização histórica
- Operadora do celular
- Aplicativos usados no dispositivo
- Fabricante / modelo do dispositivo
- Versão do SO
- Tipo de conexão (2G/3G/4G/WIFI)
- Endereços IP

A quantidade massiva de informações coletadas, que podem ser armazenadas por até 6 meses, permite que o usuário investigue dados atuais e históricos. No âmbito da investigação, o usuário é capaz de investigar os dados em vários métodos, começando por locais conhecidos, IP endereços, IDs exclusivos e muito mais. Uma vez que os dispositivos suspeitos são identificados, cada um deles pode ser investigado mais detalhadamente e o usuário pode detalhar o histórico de localização, padrões de atividade, dispositivos usados, aplicativos, IP, etc.

3. Componentes da solução

3.1 Painéis de solução

No sistema, dois painéis fornecem resumos gráficos dos dados coletados:

- Painel do sistema – que apresenta uma visão geral dos dados atualmente visualizados no sistema implantado
- Painel de perfil – que apresenta todas as informações relevantes para um perfil específico

3.1.1 Painel Principal

O painel do sistema exibe dados estatísticos, incluindo:

- Aplicativos mais utilizados pelos usuários no sistema diariamente, semanalmente ou mensalmente
- Tipos de dispositivos móveis usados diariamente, semanalmente ou mensalmente
- Estatísticas relacionadas ao sistema: número de investigações, número de perfis criados no sistema, número de usuários do sistema conectados, taxa total de aquisição do sistema (número de pegadas digitais coletadas por segundo) e taxa de eventos do sistema (número total de pegadas digitais coletadas por dia)

Painel Principal



3.1.2 Painel do Perfil

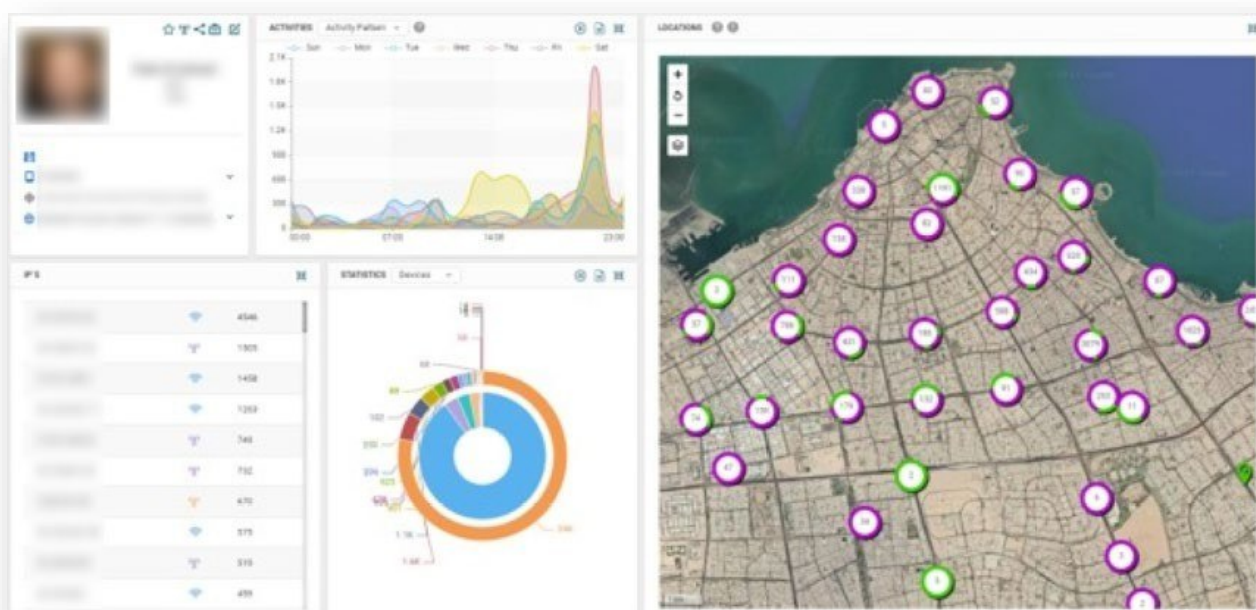
O painel de perfil resume informações sobre um único usuário de dispositivo móvel. O painel contém dados como e-mails, números de telefone, nomes e muito mais.

Em adição, o seguinte gráficos aparecer em cada perfil:

- Tipo e modelo do dispositivo usado no alvo
- Aplicações móveis utilizadas
- Histórico de geolocalização do usuário
- Endereços IP utilizados e frequência de utilização de cada um (capacidade de distinção entre conexões celulares e Wi-Fi)
- Operadoras de celular utilizadas
- Cronograma de atividades
- Resumo da atividade horário por dia na planilha semanal

Por meio do painel, e utilizando as informações disponíveis, o usuário pode localizar outros internautas com os mesmos endereços IP, filtrar o histórico de geolocalização por tempo, entre outras coisas.

Painel de Perfil



3.2 Grupos

Os usuários do sistema podem criar grupos de dispositivos móveis de acordo com três critérios:

1. Localização - O usuário do sistema pode criar um grupo de dispositivos móveis com base na área e no período de tempo.

O usuário deve criar um polígono da área de trabalho e definir o período de tempo relevante.

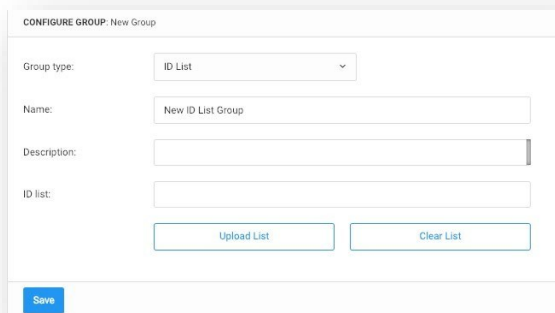
O usuário obterá então um grupo de dispositivos móveis que estavam neste local no momento relevante quadro. O sistema permite que o usuário inclua vários locais dentro de um grupo usando o relacionamento "ou" (o sistema mostrará todos os dispositivos móveis que estavam em um dos grupos definidos).

Criação de Grupo



2. Lista de IDs - o usuário cria esse grupo carregando os IDs dos usuários de dispositivos móveis no sistema (ou seja, uma lista de IDs que pertencem a um grupo terrorista grupo).

Lista de ID

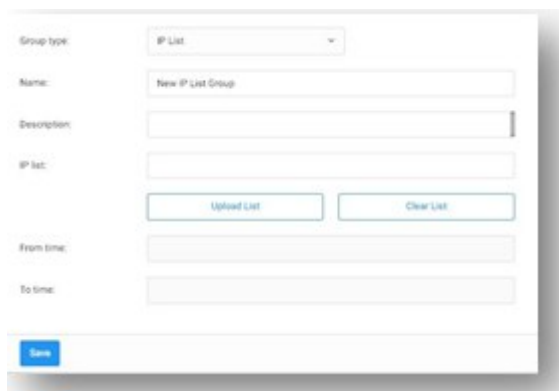


The screenshot shows a web form titled "CONFIGURE GROUP: New Group". It has the following fields and buttons:

- Group type:** A dropdown menu with "ID List" selected.
- Name:** A text input field containing "New ID List Group".
- Description:** A text input field.
- ID list:** A text input field.
- Buttons:** "Upload List" and "Clear List" buttons are positioned below the "ID list" field. A "Save" button is at the bottom left.

3. Lista de IPs - por meio desta lista de IPs, o usuário visualiza quais dispositivos móveis estão conectados aos IPs da lista em um momento específico.

Lista de IP



The screenshot shows a web form titled "CONFIGURE GROUP: New Group". It has the following fields and buttons:

- Group type:** A dropdown menu with "IP List" selected.
- Name:** A text input field containing "New IP List Group".
- Description:** A text input field.
- IP list:** A text input field.
- Buttons:** "Upload List" and "Clear List" buttons are positioned below the "IP list" field.
- From time:** A text input field.
- To time:** A text input field.
- Save:** A blue button at the bottom left.

3.3 Investigação

As investigações podem ser iniciadas de várias maneiras e podem se concentrar em:

1. Localização geográfica dentro de um período de tempo definido ou vários locais dentro de vários prazos.
2. Uma pessoa ou um grupo.
3. Um endereço IP ou vários.

Como o sistema coleta informações por até 6 meses, é possível investigar tendências e ações que aconteceram antes do evento principal e levaram a ele usando apenas tempo e lugar.

O processo de investigação pode ser dividido em duas abordagens diferentes:

1. Investigar um grupo (descrito na seção anterior) para descobrir quem está nele, estudar seu comportamento, etc.
2. Faça referências cruzadas entre diferentes grupos para entender quem está em ambos (independentemente do tipo de grupo) – localização/ID/IP).

Todos os resultados podem ser filtrados, classificados e reorganizados para permitir pesquisas adicionais e, eventualmente, levar a usuários específicos de dispositivos móveis.

Nova visão da investigação

CONFIGURE INVESTIGATION: New Investigation

Name:

Available groups:

>

Security

Security - London

Network

Computer Forensics (Linux)

File Investigation

OSINT tools

<

Save

Save and Investigate

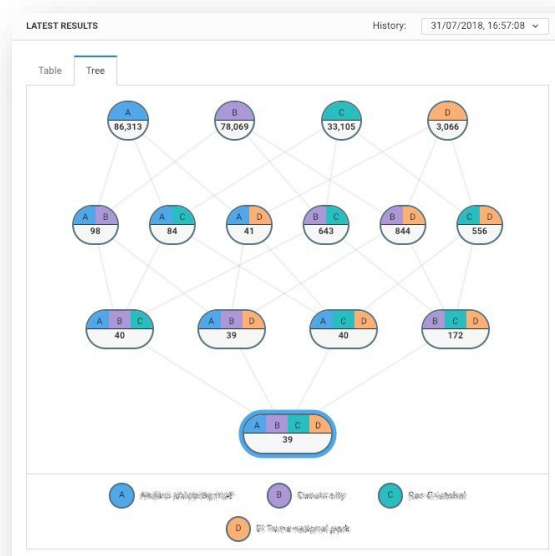
O resultado de uma investigação pode ser apresentado como uma lista de grupos com referências cruzadas e número relacionado de dispositivos móveis, ou em uma representação gráfica (visualização em árvore).

LATEST RESULTS History: 31/07/2018, 16:57:08

Table Tree

Group Name	Potential Profiles
América do Sul - Brasil	86,313
Europa - França	78,069
Ásia - Índia	33,105
América do Norte - Estados Unidos	3,066
América do Sul - Brasil + Europa - França	98
América do Sul - Brasil + Ásia - Índia	84
América do Sul - Brasil + América do Norte - Estados Unidos	41
Europa - França + Ásia - Índia	643
Europa - França + América do Norte - Estados Unidos	844
Ásia - Índia + América do Norte - Estados Unidos	556
América do Sul - Brasil + Europa - França + Ásia - Índia	40
América do Sul - Brasil + Europa - França + América do Norte - Estados Unidos	39
América do Sul - Brasil + Ásia - Índia + América do Norte - Estados Unidos	40
Europa - França + Ásia - Índia + América do Norte - Estados Unidos	172
América do Sul - Brasil + Europa - França + Ásia - Índia + América do Norte - Estados Unidos	39

Lista de visualização de grupos com referências cruzadas



Vista da Árvore

Além disso, o sistema fornece um resumo das informações relativas à cruz específica grupos referenciados como:

1. Aplicativos usados pelos usuários de dispositivos móveis no grupo
2. Operadoras de Internet – operadoras de telefonia móvel e WIFI
3. Modelos de dispositivo
4. Plataformas – tipos de SO
5. Endereços IP Usados
6. Atividade mensal
7. Atividade diária

3.3.1 Desanonimização

O Echo integra recursos de melhor esforço para desanonimizar o usuário do dispositivo móvel e fornecer mais dados de identificação pessoal, como gênero, faixa etária, número de telefone, e-mail, etc.

Esses dados permitem que o usuário aprenda mais profundamente sobre seu alvo e seus padrões.

Estes dados adicionais, nomeadamente idade ou sexo, simplificam o processo de eliminação quando se trata de um grupo de suspeitos.

3.3.2 Capacidades de Pesquisa

O Echo segue uma abordagem orientada para o alvo, permitindo que seu usuário mergulhe nos perfis alvo com apenas um identificador de usuário móvel.

Os usuários do sistema podem:

- Pesquise e encontre perfis de pessoas de interesse no sistema
- Mantenha-se atualizado com pessoas de interesse em relação a locais, padrões de comportamento e qualquer outra informação disponível no sistema

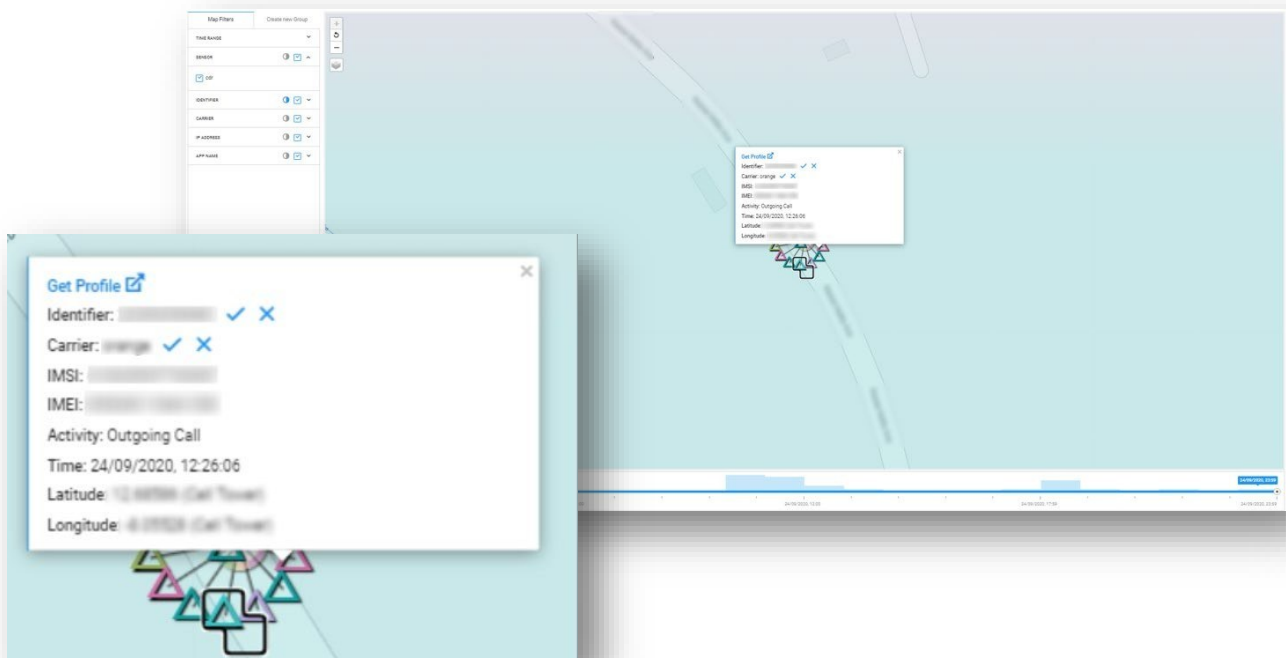
3.4 Capacidades Adicionadas

3.4.1 Registros de dados de chamadas

Os Registros de Dados de Chamadas (CDRs) são essenciais para uma investigação de inteligência bem-sucedida. O Echo é construído para suportar qualquer tipo de CDRs de qualquer fonte e permite que os analistas executem análises avançadas de dados de maneira simplificada e intuitiva. Através de CDRs, o sistema é capaz para fornecer:

- Correlação de localização e tempo
- Padrões históricos do MSISDN
- Pesquisas baseadas em IMSI
- Histórico de locais
- Análise de links entre MSISDNs

Dados produzidos por CDR



Observação: O formato do CDR deve ser definido previamente e será fornecido pelo cliente.

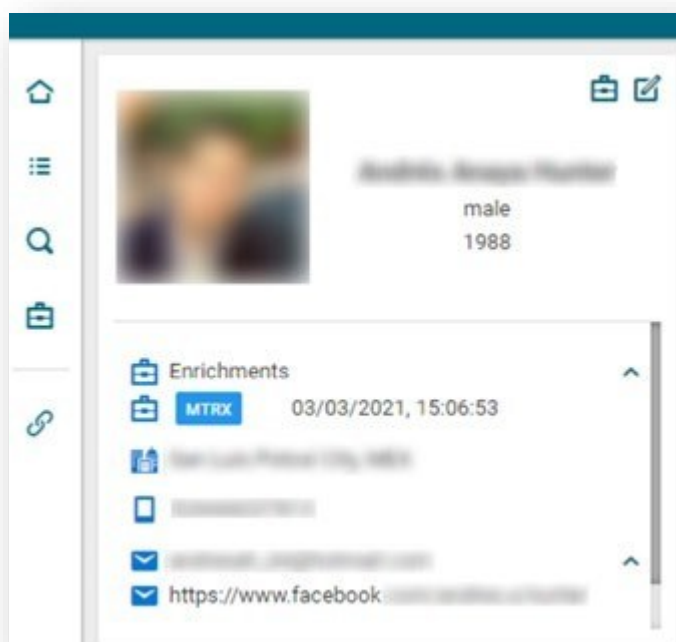
3.4.2 Enriquecimento de Dados de Código aberto

Um módulo adicional integrado ao Echo é o Optimus; a solução abrangente baseada em OSINT da Rayzone Group.

Usando o MSISDN do alvo, o Optimus envia rastreadores para capturar todos dados disponíveis de fontes abertas.

Uma vez que um alvo é designado, o Optimus é usado para enriquecer o perfil com dados extensos; sejam informações de perfil (nomes, imagens, sexo, idade, etc.) ou dados baseados em mídia social (e-mail, redes sociais). contas de mídia, etc).

Exemplo de dados de perfil obtidos do Optimus



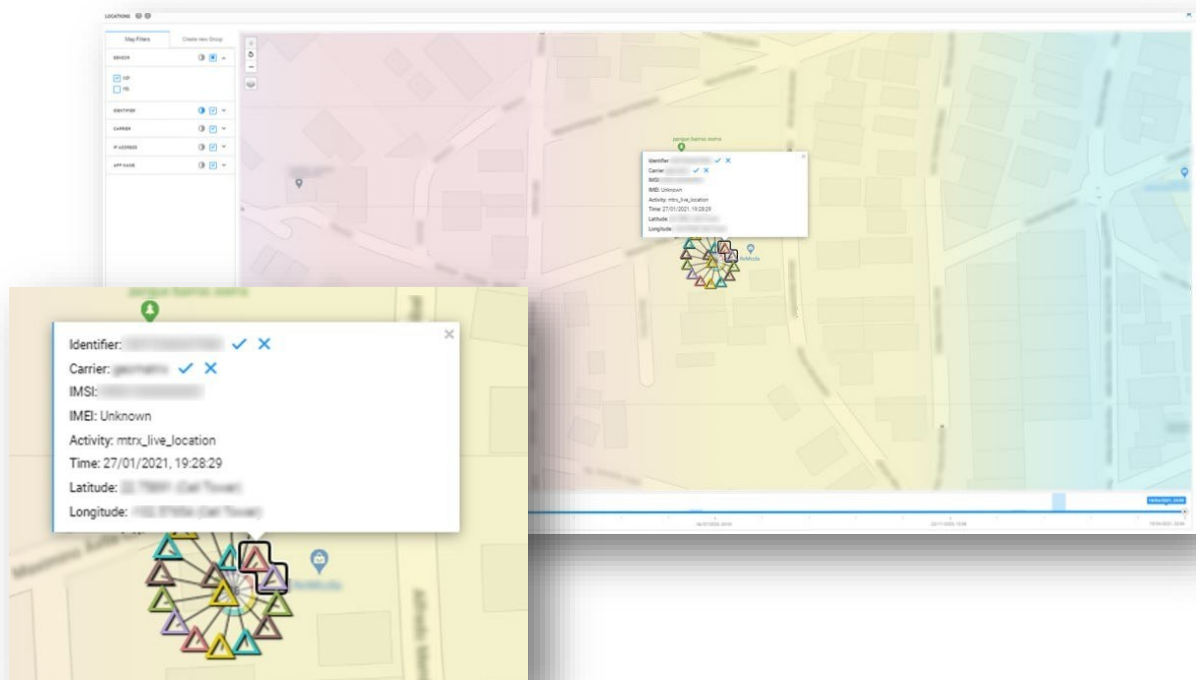
Observação: os recursos de enriquecimento estão sujeitos aos melhores esforços, bem como aos dados disponíveis publicamente, e são baseados na capacidade de converter o ADID de um alvo para um MSISDN.

3.4.3 Ativação de Localização Ao vivo

O Echo tem a capacidade de integrar módulos adicionais para monitoramento ativo de alvos. Por exemplo, a solução GeoMatrix do Rayzone Group, totalmente e perfeitamente integrada desde o início, fornece uma localização ao vivo com base no domínio celular usando o MSISDN de um alvo.

Além da localização, o usuário obtém informações adicionais relacionadas ao celular ambiente (ou seja, a operadora, IMEI e muito mais).

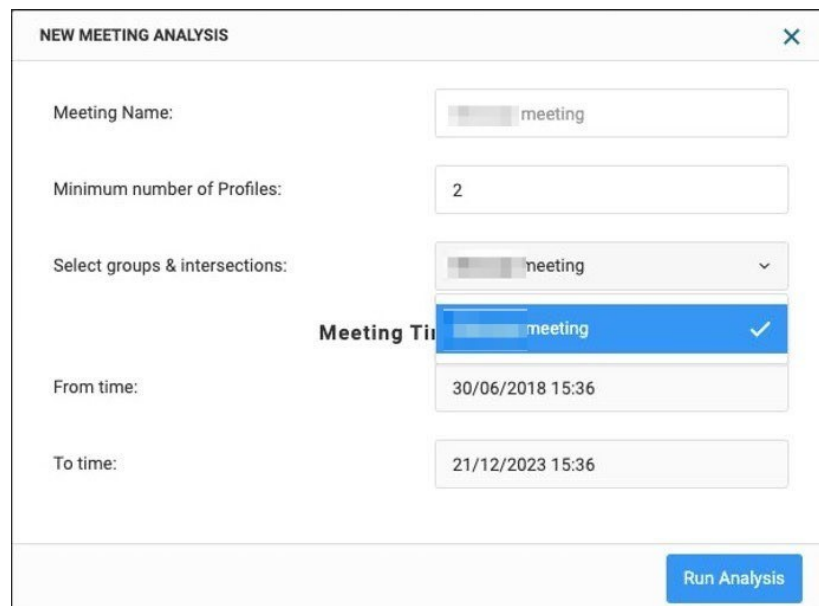
Localização ao vivo gerado pelo GeoMatrix



4. Recursos Avançados

4.1 Reunião de pessoas

Este recurso introduz uma camada analítica de perfis dentro de uma investigação, revelando instâncias quando dois ou mais perfis estavam presentes no mesmo local físico. O sistema fará a varredura de todos os locais históricos, identificando potenciais pontos de encontro com base na distância entre esses locais e um determinado período de tempo.



NEW MEETING ANALYSIS [X]

Meeting Name: [meeting]

Minimum number of Profiles: [2]

Select groups & intersections: [meeting] v

Meeting Time: [meeting] ✓

From time: [30/06/2018 15:36]

To time: [21/12/2023 15:36]

[Run Analysis]

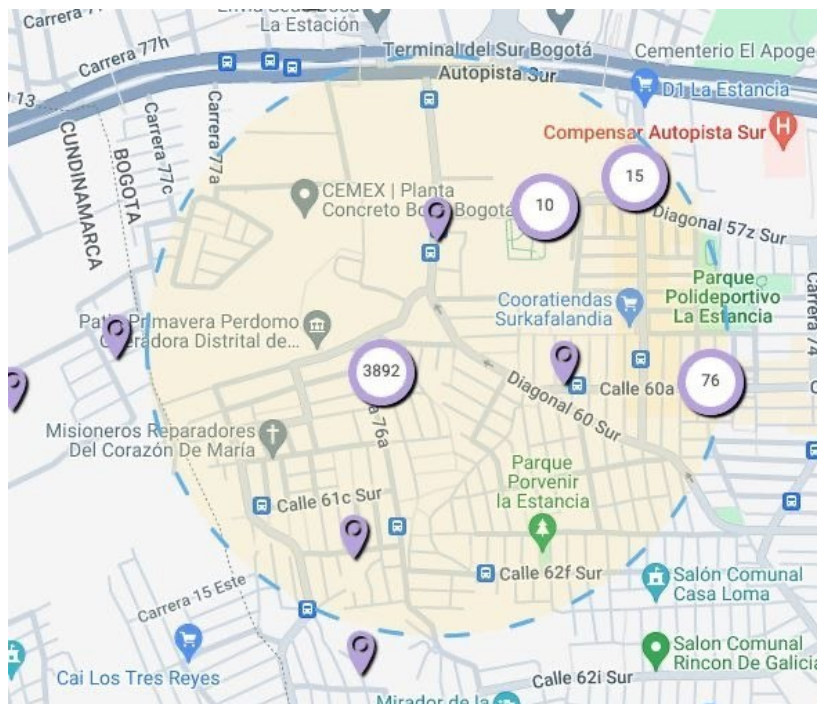
Definição da reunião



Potencial ponto de encontro identificado

4.2 Locais Frequentemente Visitados

Este recurso exibe os dois lugares mais visitados para cada perfil, utilizando todos os dados de localização disponíveis do perfil no Columbo.



Local frequentemente visitado - Indicação



Local visitado com frequência - Detalhes

5. Segurança

O Echo é implantado em dois ambientes separados – uma nuvem central segura; e um ambiente dedicado ao cliente que limita as interações do usuário do sistema e mantém todas as ações do usuário contidas. Tal separação impede que qualquer pessoa tenha acesso a informações confidenciais, como consultas conduzidas ou conclusões da investigação (registradas no sistema).

Quando implantado na nuvem, o ambiente do cliente seguro é protegido pelo acesso VPN, que criptografa todos os dados transmitidos entre as estações de trabalho do cliente e o sistema.

Uma estratégia é implantar o ambiente de cliente seguro nas instalações, em servidores próprios e administrado pelo cliente.

Essa estratégia permite que o cliente assuma o controle de questões de segurança, como proteção de dados.