



## ***Anexo – AvantGraph***

Descrição e detalhes sobre análise de vínculos para segurança cibernética e combate a fraudes.

## Sumário

<b>1</b>	<b>Descrição:</b>	<b>3</b>
<b>2</b>	<b>Acesso:</b>	<b>4</b>
	Ontologia:	4
	Análises:	4
	Aparências:	5
	Categorias:	5
<b>3</b>	<b>Ontologias:</b>	<b>6</b>
<b>4</b>	<b>Análises:</b>	<b>12</b>
<b>5</b>	<b>Aparências:</b>	<b>19</b>
<b>6</b>	<b>Categorias:</b>	<b>20</b>

## 1 Descrição:

A análise de vínculos é uma técnica utilizada para entender o relacionamento entre nós ou também denominados entidades.

A descrição das características dos relacionamentos e dos nós é chamada de ontologia.

O projeto *DBPedia Ontology* - <https://www.dbpedia.org/resources/ontology/> é um repositório que contém diversos exemplos de classes e instâncias para a análise de dados, recurso fundamental da análise de vínculos. O DBPedia traz uma amostra do alcance dos *schemas* com suas classes e instâncias.

Com o uso de ontologia é possível realizar análises visuais complexas de áreas como:

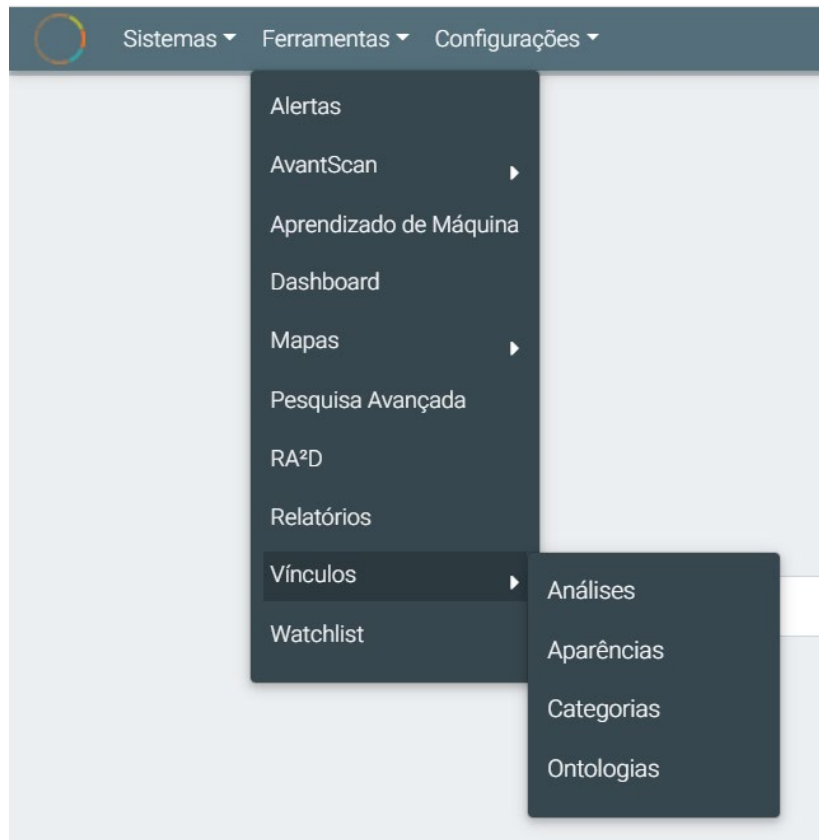
- Detecção de fraudes
- Ataques cibernéticos
- Threat Intelligence
- Threat Hunting
- Topologias de redes
- Mídias sociais

O AvantGraph é o módulo do AvantData, responsável pela preparação e análise de vínculos. O AvantGraph faz parte do módulo CORE e não exige licença adicional para o seu uso.

Qualquer uma das fontes de dados disponíveis no AvantData pode ser usada para a descrição de entidades e seus atributos, assim como dos relacionamentos e suas características. A etapa de preparação dos dados de entrada é feita na Ontologia e será detalhada nesse anexo.

## 2 Acesso:

Para acessar o AvantGraph o analista deverá clicar em Ferramentas -> Vínculos no MegaMenu do AvantData, conforme a imagem Figura 1 – AvantGraph:



*Figura 1 – AvantGraph*

O AvantGraph contém as seguintes opções principais:

Ontologia:

Descrição das ontologias e suas entradas de dados.

Análises:

Ambiente para a interação com os grafos, ou seja, a análise de vínculos propriamente dita.



## **Soluções de Vanguarda em Segurança da Informação**

### **Aparências:**

Definição das formas de visualização dos grafos, com suas respectivas características visuais, assim com o catálogo de aparências disponíveis na ferramenta.

### **Categorias:**

As análises, aparências e ontologias são agrupadas em categorias e nessa parte da ferramenta é possível gerenciar as categorias disponíveis para os analistas.

### 3 Ontologias:

Na ontologia é onde estão disponíveis as técnicas de classificação e relacionamentos dos dados. A partir do momento que as estruturas dos dados foram definidas, o AvantGraph consegue, automaticamente, criar visualizações interativas com os elementos selecionados.

Além de permitir a visualização dos vínculos, é possível realizar novas consultas baseadas nos nós, seus marcadores, atributos ou relacionamentos e suas características. Tudo isso é feito em interface visual, com cliques de mouse e eventos de arrastas e soltar. Porém, caso seja necessária uma análise mais aprofundada, a ferramenta também disponibiliza uma linguagem de pesquisa especialmente desenvolvida para trabalhar com grafos.

Essas visualizações podem ser alteradas em tempo de análise, por meio de *queries Cypher* - <https://neo4j.com/docs/cypher-manual/current/>, assim como interação do usuário com eventos de clique e arrastar do mouse, conforme a figura .Figura 2 - Threat Intelligence - Facebook

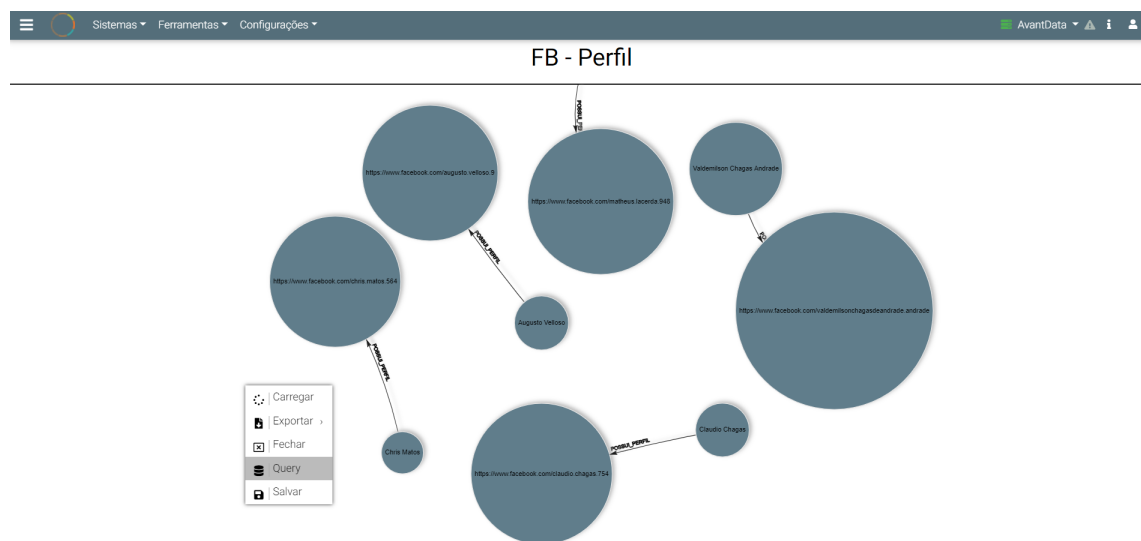


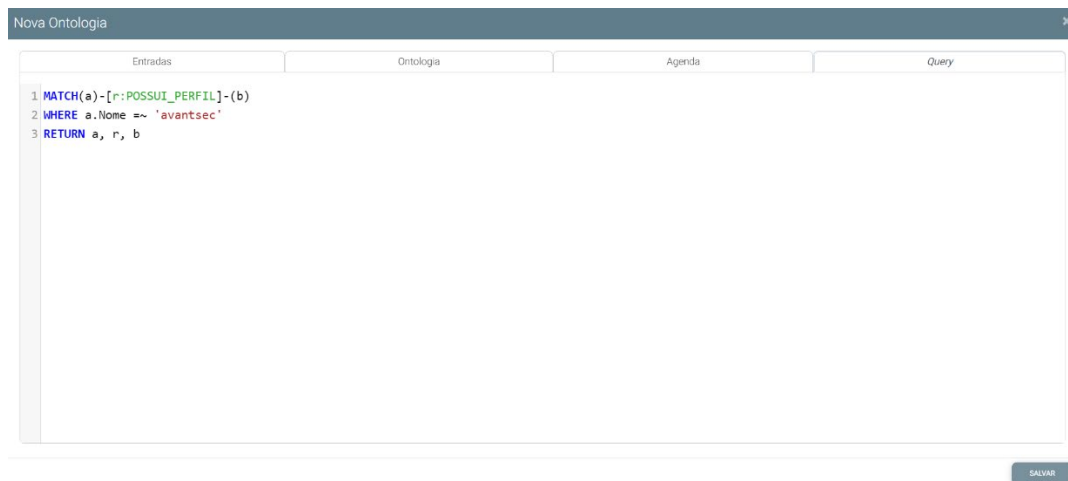
Figura 2 - Threat Intelligence - Facebook

Com as *queries Cypher* ( Figura 3 - Query Cypher ) é possível realizar análises baseadas em:

- Operadores Lógicos
- Agregações
- Propriedades dos nós e relacionamentos
- Operadores matemáticos

**Soluções de Vanguarda em Segurança da Informação**

- Comparações
- Operadores booleanos
- Operadores temporais
- Expressões regulares
- Operadores de mapas e listas



*Figura 3 - Query Cypher*

O AvantGraph utiliza, nativamente, um banco de dados especializado em grafos. Essa base de dados é alimentada e atualizada em tempo real, de acordo com a regra de extração de dados do AvantGraph. Com isso, é possível, por exemplo, que o AvantData receba dados para a construção de topologia de redes e de ataques relacionados a usuários ou entidades. Dessa forma, é possível a visualização não somente da topologia da rede, mas também da ação temporal do ataque ao ambiente investigado, assim como suas interações com ativos, usuários, domínios ou quaisquer outros elementos da rede analisada.

As entradas de dados podem ser oriundas de API, AvantAgent, Eventos de segurança, UEBA, WEB Scraping, Bancos de dados, Feeds, Tráfego de rede ou qualquer outra entrada de dados. Os dados estão disponíveis para a indexação automática, e diversas fontes distintas podem ser usadas para a mesma ontologia, conforme a imagem Figura 4 - Ontologia - Entrada de Dados:

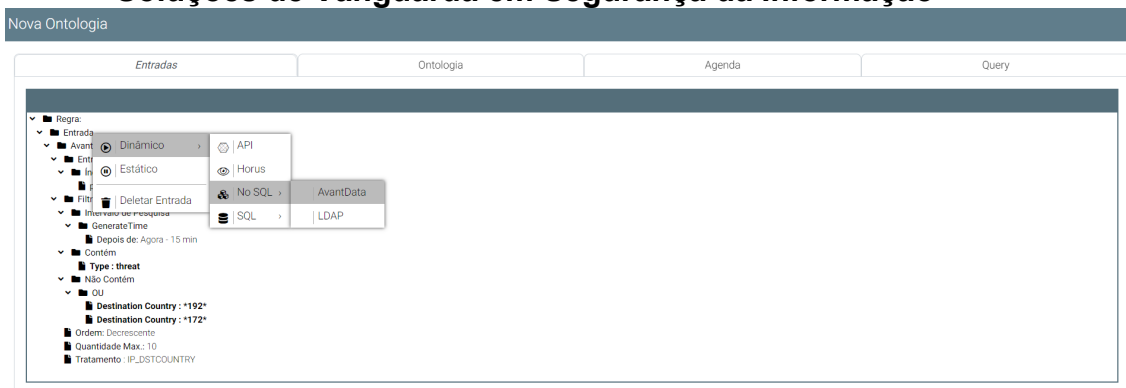


Figura 4 - Ontologia - Entrada de Dados

As análises podem ser acessadas diretamente o Dashboard, por meio de pivotamento de dados. Ou seja, a partir de um gráfico no Dashboard, o analista pode solicitar a visualização das análises de vínculos daqueles usuários, por meio de clique do botão direito do mouse, conforme a figura Figura 5 - Pivotamento para o AvantGraph:

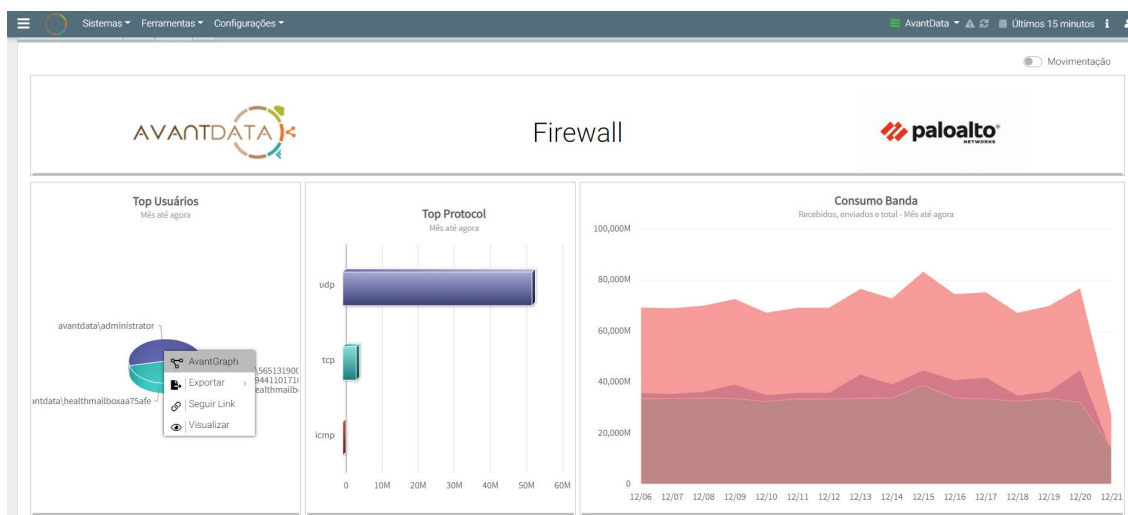


Figura 5 - Pivotamento para o AvantGraph

Caso exista uma base Neo4J disponível, o AvantGraph pode se conectar a esse *backend* para o processamento de vínculos relacionados aos dados previamente existentes. Para configurar o Neo4J o analista deverá ir em Configurações -> Geral -> AvantGraph, conforme a imagem Figura 6 - Neo4j backend:



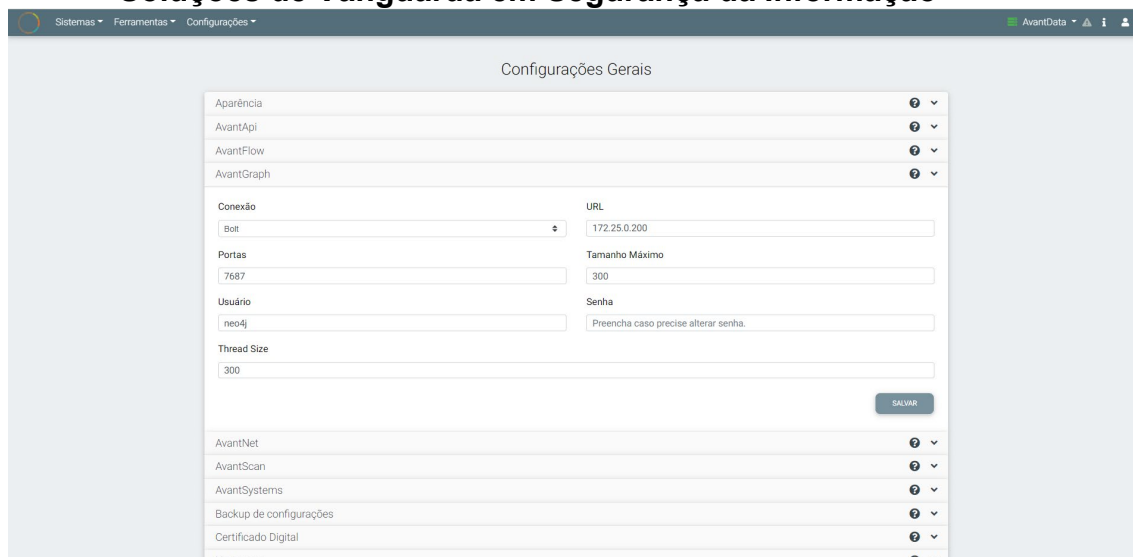


Figura 6 - Neo4j backend

A definição dos nós e relacionamentos é feita na aba Ontologia. Os nós podem ter marcadores e atributos.

Os marcadores e atributos servem como identificadores e são largamente usados para a criação e pesquisas nos grafos. Qualquer entrada de dados pode ser usada para a definição dinâmica e ou estática dos nós, marcadores e seus atributos, conforme a figura:

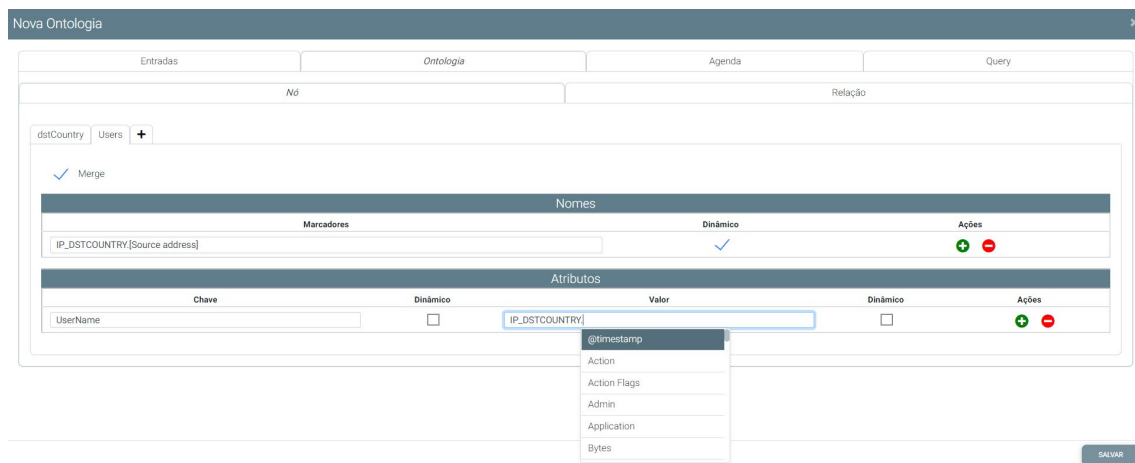


Figura 7 - Definição de nós e relacionamentos

Isso permite a atualização dos diagramas de vínculos em tempo real, ou seja, assim que uma ameaça ou fraude é sinalizada por um evento ou regra, o analista já possui a capacidade de realizar uma análise visual detalhada do incidente que está sendo tratado.

### Soluções de Vanguarda em Segurança da Informação

Para a alimentação de dados no AvantGrap é possível escolher os tempos e frequências para a ingestão de dados. Para isso basta clicar na aba Agenda, conforme a imagem Figura 8 - Agendamento para ingestão de dados e escolher a data inicial, data final e frequência de aquisição de dados.

Note que essa frequência é baseada no conceito de *CRONTAB* estendida, pois, ao contrário do Linux onde a menor unidade de execução de tempo da *CRONTAB* é de minutos, no AvantData é possível executar ação a cada segundo, assim como também em períodos anuais, definidos pelo analista.

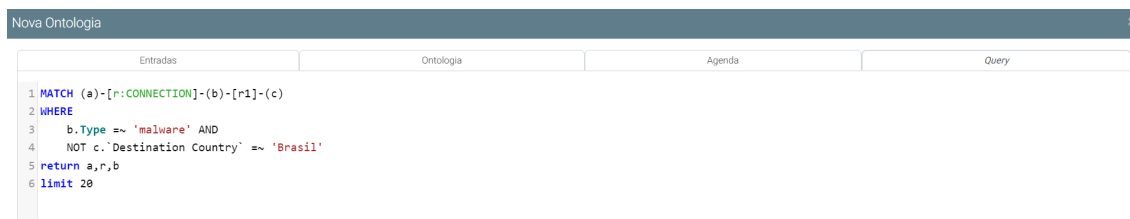


The screenshot shows the 'Nova Ontologia' window with four tabs: 'Entradas', 'Ontologia', 'Agenda', and 'Query'. The 'Agenda' tab is active, displaying a scheduling interface. It includes fields for 'Data Inicial' (01/05/2019 00:00), 'Data Final' (Data Hora), and 'Frequência' (0 0/5 \* \* \* \* \*). Below these are units: Segundo, Minuto, Hora, Dia, Mês, Ano, and Dia (Semana). There are also three status icons: a green plus, a red minus, and a blue checkmark.

Figura 8 - Agendamento para ingestão de dados

As ontologias podem ter definições de visualização padrão, baseadas em *queries Cypher*. Isso permite uma facilidade de entendimento dos dados pelo analista, pois os grafos já estão organizados e são automaticamente criados para agilizar a percepção do caso analisado e diminuir, por consequência, o tempo necessário para a consciência situacional do ambiente tratado.

Para a definição de uma visualização padrão o analista deverá selecionar a aba *Query* na ontologia e escrever a *query Cypher* adequada para o caso.



The screenshot shows the 'Nova Ontologia' window with the 'Query' tab active. It displays a Cypher query: 

```
1 MATCH (a)-[r:CONNECTION]-(b)-[r1]-(c)
2 WHERE
3   b.Type =~ 'malware' AND
4   NOT c.'Destination Country' =~ 'Brasil'
5 return a,r,b
6 limit 20
```

No AvantPortal existem diversas *queries*, *scripts* e ontologias disponíveis para a imediata aplicação das análises. Para isso, basta realizar o download e upload na ferramenta. Existe também um mapeamento das TTP baseadas no MITRE ATT&CK.

Gestão Ferramentas Suporte

Scripts

10

Pesquisar

Resultados por página

<input type="checkbox"/>	Nome	Tipo	Publicado em	Empresa	Descrição
<input type="checkbox"/>	Vínculo Aplicações	AvantGraph	2021-01-27 12:18:40	AvantSec	Retorna a análise de vínculos entre aplicações. Favor ajustar a query de acordo com a ontologia utilizada
<input type="checkbox"/>	Vínculo entre usuários e domínio	AvantGraph	2021-01-27 12:18:40	AvantSec	Análise de vínculo entre usuários e domínio. Favor ajustar a query de acordo com a ontologia utilizada
<input type="checkbox"/>	Vínculo Usuários Domínio	AvantGraph	2021-01-27 12:18:40	AvantSec	Retorna a lista de usuários distintos que estão se comunicando com o domínio selecionado. Favor ajustar a query de acordo com a ontologia utilizada
<input type="checkbox"/>	Países	Geo.Json	2021-05-20 17:54:17	AvantSec	Script Geo.Json de Países
<input type="checkbox"/>	Continente	Geo.Json	2021-05-20 17:54:47	AvantSec	Script Geojson de Continente
<input type="checkbox"/>	AvantData - APM	Javascript	2021-04-29 17:41:48	AvantSec	Indexação do tempo da página via JS Modo de uso: Copiar o conteúdo do JS e inserir no JS da página a ser medida. Alterar a Url
<input type="checkbox"/>	Snapshot_Windows_Process_Listening_Port	Osquery	2021-07-26 15:52:17	AvantSec	Retorna uma lista com as portas ouvintes (SNAPSHOT) - ATT&CK: T1086,T1093,T1020,T1041,T1011,T1029,T1043,T1090,T1094,T1024,T1025
<input type="checkbox"/>	services.exe_incorrect_parent_process	Osquery	2021-07-26 16:39:59	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1173,T1086,T1204,T1025
<input type="checkbox"/>	lsass.exe_incorrect_parent_process	Osquery	2021-07-26 16:39:09	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1173,T1086,T1204,T1025
<input type="checkbox"/>	conhost.exe_incorrect_parent_process	Osquery	2021-07-26 16:37:48	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1173,T1086,T1204,T1025

Figura 9 - AvantPortal

## 4 Análises:

As análises são a efetiva visualização dos grafos, com seus nós e relacionamentos, assim como os marcadores e atributos definidos nas ontologias.

Nas análises o AvantGraph plota os diagramas de vínculos, de acordo com a regra ontológica definida na etapa anterior. Porém, após a exibição dos grafos os analistas podem navegar nos diagramas, interagindo com os nós, relacionamentos, atributos, realizando novas consultas, criando tabelas exportando os dados e até mesmo imagens dos diagramas.

O objetivo das análises é permitir que os operadores possam ter uma rápida consciência situacional do tema investigado. Esse tipo de abordagem não é possível de ser realizada, de maneira simples, com bancos de dados relacionais ou mesmo com bancos não estruturados. Por isso o uso de uma estrutura dedicada e focada em diagramas de vínculos.

Os diagramas permitem a realização de pesquisas baseadas condições temporais, por saltos de relacionamentos, *full-text search*, expressão regular, ou seja, é possível identificar o grupo a que pertence um atacante (<https://avantapi.avantsec.com.br/#547b130f-0a19-424a-9a83-e482bedd9575>) e/ou ferramenta para exploração (<https://avantapi.avantsec.com.br/#e9909863-86e8-4018-bdd7-c2b6bc792332>) e vinculá-lo ao usuário ou entidade sendo ameaçada pelo vetor de ataque. Isso cruzando dados do MITRE ATT&CK e logs de firewall, Proxies e AD, por exemplo.

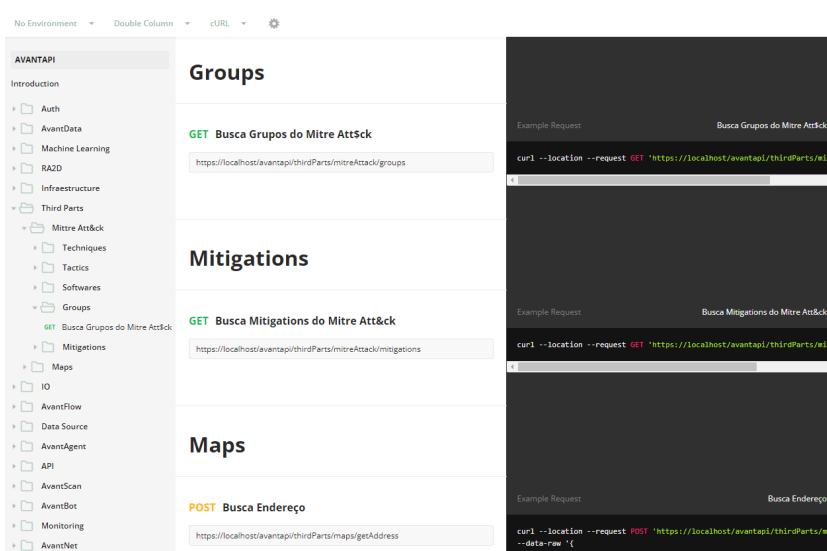


Figura 10 - Grupo de atacantes - MITRE ATT&CK - AvantApi

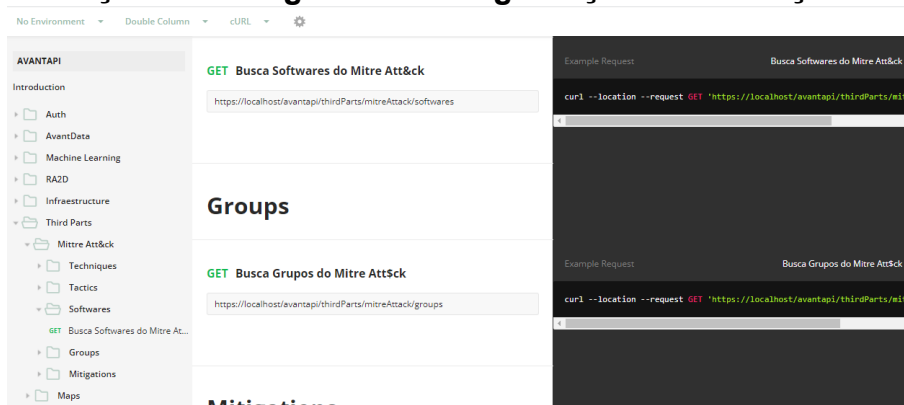


Figura 11 - Ferramentas de Ataque - MITRE ATT&CK – AvantApi

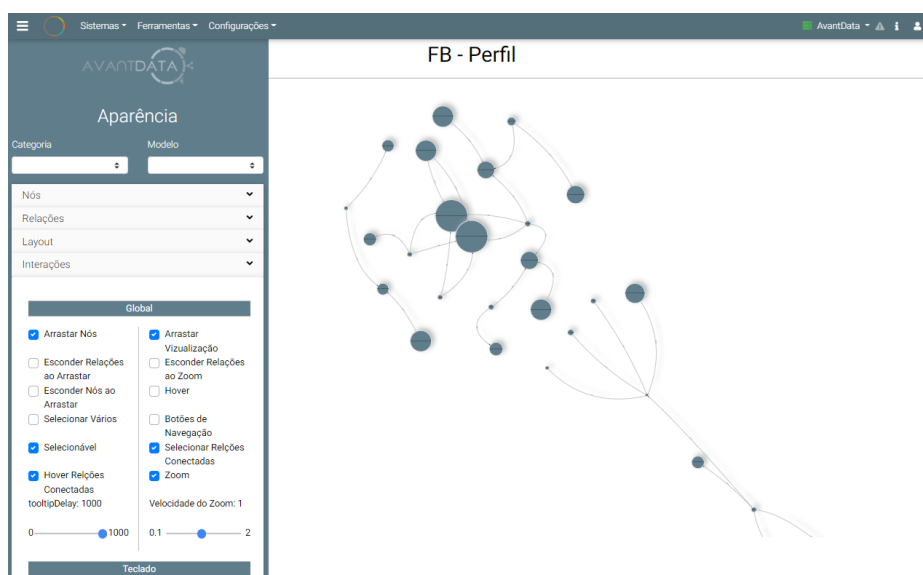


Figura 12 - Diagrama de vínculos com múltiplos saltos

As configurações dos elementos das análises podem ser alteradas há qualquer momento durante as pesquisas. As modificações de configurações dos parâmetros causam efeito imediato nos grafos e podem ser ajustas em tempo real para melhor entendimento do caso trabalhado.

As modificações são realizadas no menu lateral da esquerda, conforme as seguintes opções:

### Categoria

Agrupamento de análises que tem características comuns entre si. Essas categorias podem ser modificadas, incluídas e excluídas há qualquer momento pelo analista.

Modelo:

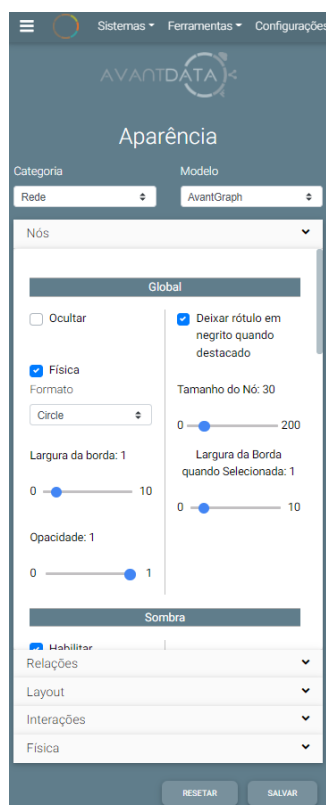
Conjunto de características previamente definidas e disponíveis no AvantGraph.

Os modelos carregam opções de interações, física da relação, nós, layout e todos os demais parâmetros que podem ser salvos em um modelo para facilitar as visualizações.

Com isso é possível, por exemplo, ter um formato de visão hierárquica e outro de visão em dispersão. Para isso basta selecionar um modelo pré-definido. Os modelos podem ser incluídos, modificados e deletados há qualquer momento.

Nós

Características de formato, fonte, cor, opacidade, sombreado e demais parâmetros relacionados aos nós.



*Figura 13 - Parâmetros de configurações dos nós*

## Relações

Formato dos traços, setas, fontes, cores e demais características das relações podem ser modificadas nessa tela.

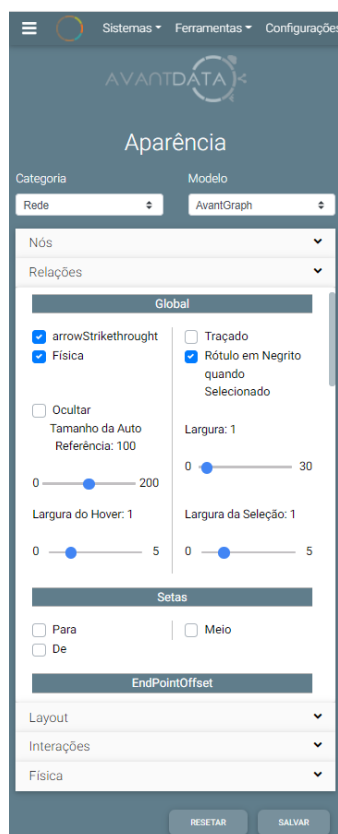
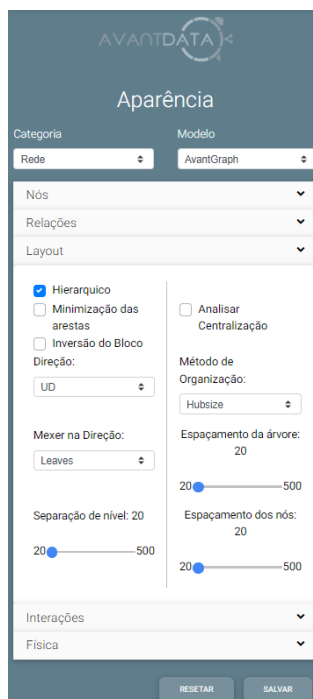


Figura 14 - Parâmetros de configurações das relações

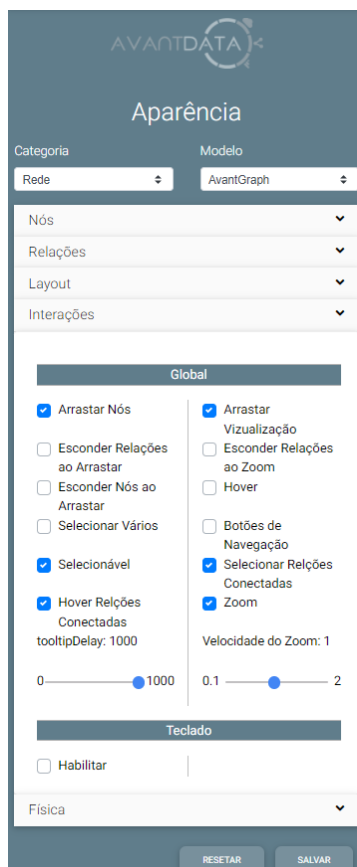
A maneira como os grafos serão apresentados. Podem ser em dispersão ou em hierarquia.



*Figura 15 - Parâmetros de configurações das layout*



Os nós e suas relações possuem parâmetros para serem arrastados, selecionados, suprimidos, dentre várias outras opções, relativas às interações entre os elementos apresentados na tela do analista. Essas configurações são feitas nessa área do AvantGraph.



The screenshot shows the 'Aparência' (Appearance) configuration window for the 'AvantGraph' model. It is divided into sections for 'Global' and 'Teclado' (Keyboard) settings. The 'Global' section includes checkboxes for 'Arrastar Nós' (checked), 'Esconder Relações ao Arrastar' (unchecked), 'Esconder Nós ao Arrastar' (unchecked), 'Selecionar Vários' (unchecked), 'Selecionável' (checked), 'Hover Relções Conectadas' (checked), and 'Arrastar Visualização' (checked). It also has a 'Velocidade do Zoom' slider set to 1. The 'Teclado' section has a 'Habilitar' checkbox (unchecked). A 'Física' dropdown is at the bottom. 'RESETAR' and 'SALVAR' buttons are at the bottom right.

Global
<input checked="" type="checkbox"/> Arrastar Nós
<input type="checkbox"/> Esconder Relações ao Arrastar
<input type="checkbox"/> Esconder Nós ao Arrastar
<input type="checkbox"/> Selecionar Vários
<input checked="" type="checkbox"/> Selecionável
<input checked="" type="checkbox"/> Hover Relções Conectadas tooltipDelay: 1000
<input checked="" type="checkbox"/> Arrastar Visualização
<input type="checkbox"/> Esconder Relações ao Zoom
<input type="checkbox"/> Hover
<input type="checkbox"/> Botões de Navegação
<input checked="" type="checkbox"/> Selecionar Relções Conectadas
<input checked="" type="checkbox"/> Zoom
Velocidade do Zoom: 1

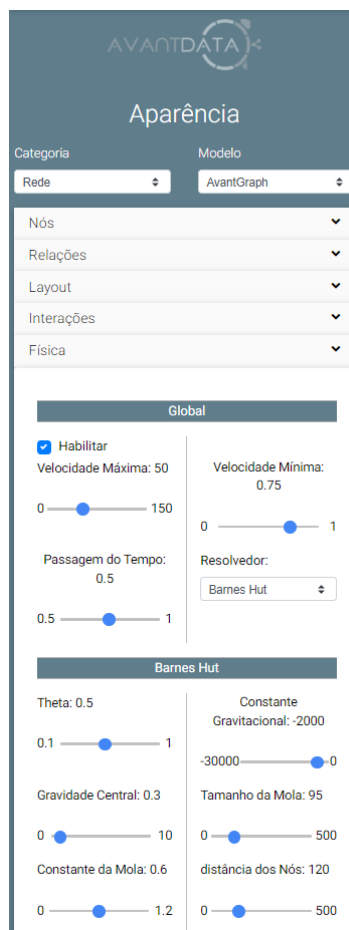
Teclado
<input type="checkbox"/> Habilitar

Física

RESETAR SALVAR

Figura 16 - Parâmetros de configurações das interações

A relação de repulsão, efeito de mola, velocidade, densidade de nós em um espaço da janela, caracterizam algumas das configurações de física entre os elementos. Esses valores podem ser modificados para exprimir a melhor visualização para os analistas, de acordo com as suas preferências pessoais.



AVANTDATA

### Aparência

Categoria: Rede Modelo: AvantGraph

Nós  
Relações  
Layout  
Interações  
Física

**Global**

☒ Habilitar

Velocidade Máxima: 50 Velocidade Mínima: 0.75

Passagem do Tempo: 0.5 Resolver: Barnes Hut

**Barnes Hut**

Theta: 0.5 Constante Gravitacional: -2000

Gravidade Central: 0.3 Tamanho da Mola: 95

Constante da Mola: 0.6 distância dos Nós: 120

Figura 17 - Parâmetros de configurações das física

## 5 Aparências:

As aparências são modelos personalizáveis para a visualização de dados no AvantGraph. A possui alguns templates nativos, porém nada impede que o analista configure os parâmetros de acordo com o que for de melhor conveniência para o entendimento dos cenários escolhidos.

Os catálogos são os conjuntos de aparência e nesse local o usuário pode escolher várias aparências distintas e agrupá-las de maneira que sejam usadas de maneira conveniente nas investigações.

Uma das aparências no catálogo deve ser definida como padrão, para isso, basta clicar com o botão direito do mouse e selecionar qual deverá ser a aparência padrão de um catálogo.

Todas as configurações disponíveis nas análises podem ser usadas na definição de modelos de aparências, conforme a imagem Figura 18 - Configuração de aparências

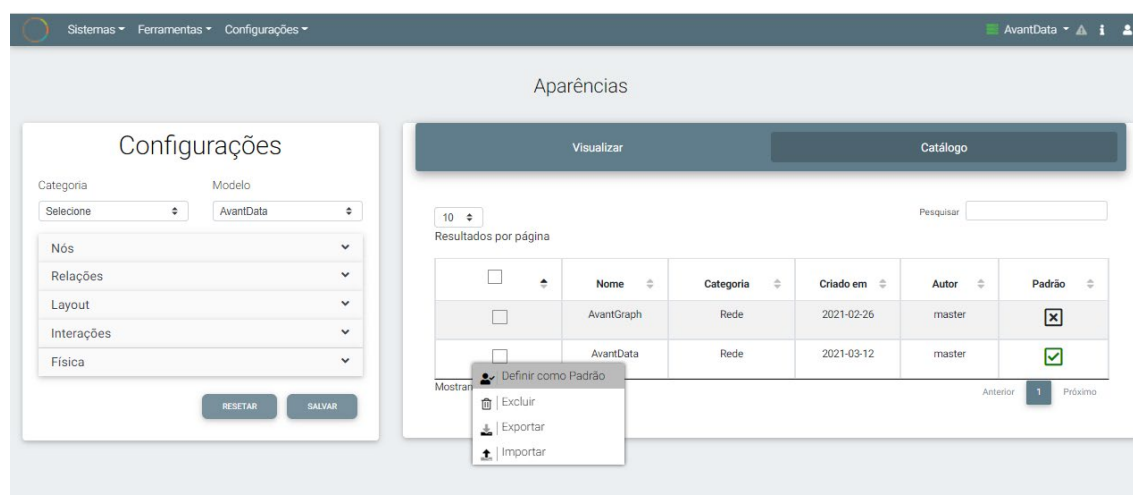


Figura 18 - Configuração de aparências

## 6 Categorias:

As categorias servem para consolidar análises, aparências e ou ontologias em grupos lógicos que contenham alguma característica em comum. O objetivo é diminuir a quantidade de clique de mouse para navegar e entender o comportamento das relações nos diagramas de vínculos.

O analista pode alterar ou excluir quaisquer uma das categorias disponíveis na ferramenta, assim como também tem a opção de incluir novas categorias há qualquer momento.



	Nome	Criado em	Autor
<input type="checkbox"/>	Rede	2021-02-26 16:41:12.562903-03	master