



## **Anexo – AvantPortal**

Portal informativo sobre AvantData.

Disponibilidade de modelos e arquivos.

## Sumário

<b>1</b>	<b>Introdução</b>	<b>3</b>
<b>2</b>	<b>Acesso:</b>	<b>3</b>
<b>3</b>	<b>Ferramentas</b>	<b>5</b>
3.1	AvantAgent	6
3.1.1	Monitores	9
3.1.2	Perfis	10
3.1.3	Scripts	11
3.2	Marketplace	13
3.2.1	API	14
3.2.2	Coletores	16
3.2.3	Dashboard	18
3.2.4	Parser	20
3.2.5	Regras	22
3.2.7	Relatórios	24
3.2.8	Templates	27
<b>4</b>	<b>Suporte</b>	<b>30</b>
3.1.	Licença	30
3.2.	Documentos	31

## 1 Introdução

No AvantPortal é possível ter acesso a uma biblioteca de artefatos com uma variedade de casos de usos nativos e homologados pelo fabricante, que podem ser diretamente importados na ferramenta, de acordo com as tecnologias existentes na infraestrutura. Atualmente estão disponíveis uma variedade de Dashboards, regras, monitores, scripts, APIs, modelos de relatórios e outros artefatos, de diferentes produtos e fabricantes, como firewalls (Fortigate, Sophos, ForcePoint, PFSense, PaloAlto), switches (Cisco, Intelbras, HPE, Mikrotik, Huawei), serviços de nuvem (Google, Microsoft 365 e serviços relacionados), serviços de Infraestrutura (Active Directory, Eventos do Windows, logs do Linux e serviços) e vários outros produtos que podem ser integrados ao AvantData. O AvantPortal é constantemente atualizado com novos casos de uso e artefatos, de acordo com as demandas e produtos observados nos diferentes clientes.

## 2 Acesso:

Para acessar o AvantPortal o usuário deverá abrir o seu browser de preferência e digitar o seguinte endereço: <https://avantdata.avantsec.com.br/portal/login/> onde realizará o login.

Caso o usuário não tenha as credenciais, deverá solicitar entrando em contato com suporte em: [suporte@avantsec.com.br](mailto:suporte@avantsec.com.br)

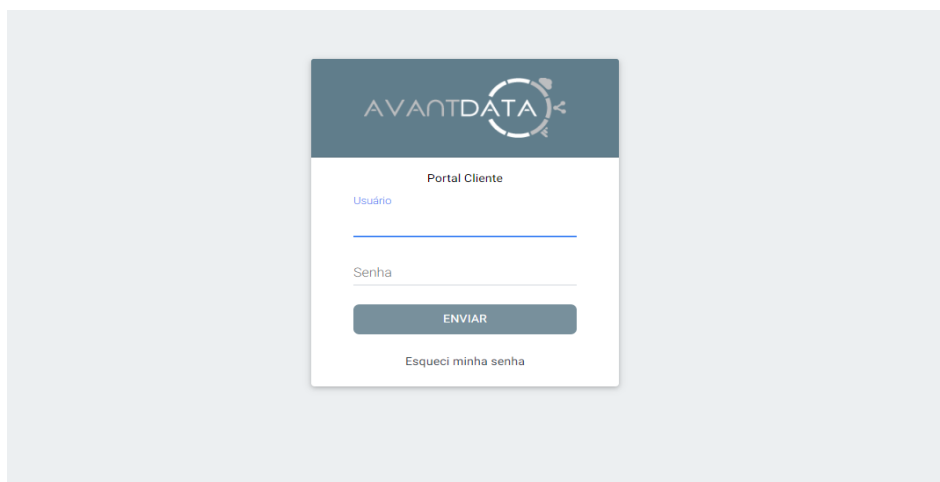


Figura - 1 Página de login

Após a autenticação com as credenciais enviadas pela AvantSec o operador terá acesso as áreas de Ferramentas e Suporte, disponíveis no menu superior da tela – MegaMenu, conforme a imagem abaixo:

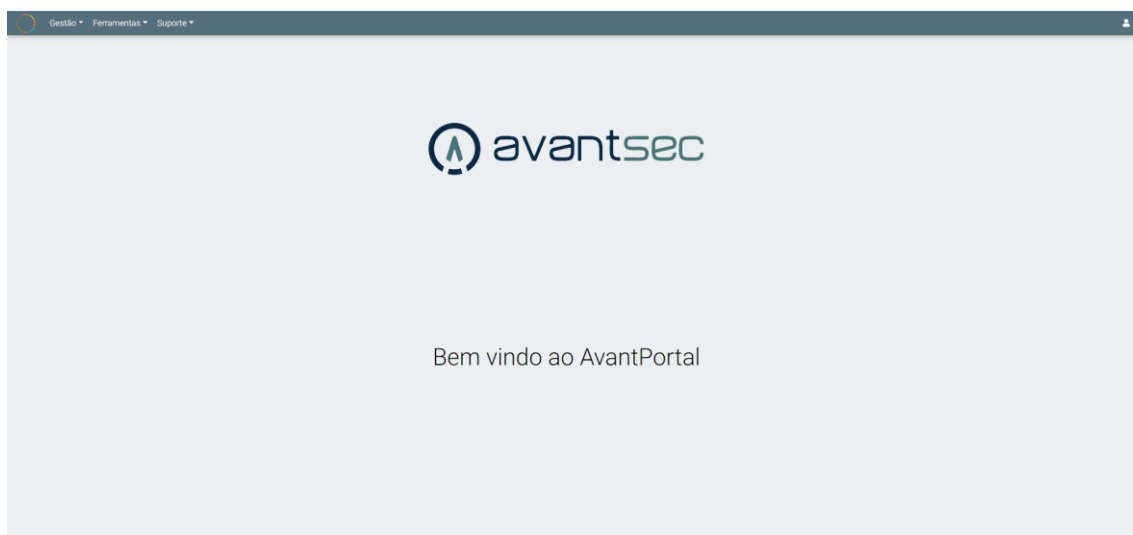


Figura 2 - Janela Principal

### 3 Ferramentas

No menu Ferramentas há diversas opções do Marketplace, assim como do AvantAgent e podem ser acessadas via MegaMenu, conforme a imagem abaixo:

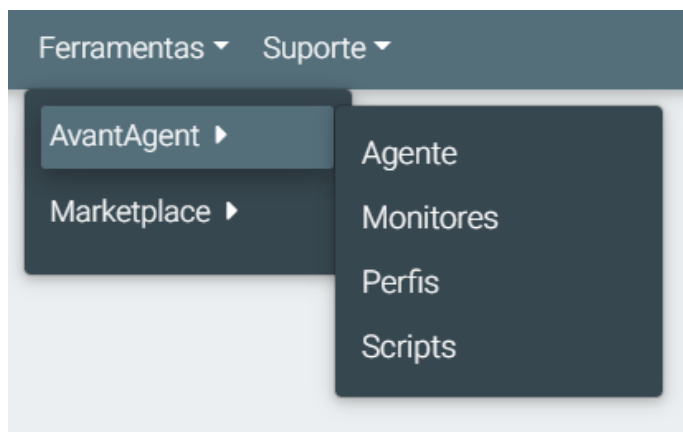


Figura 1 - AvantAgent

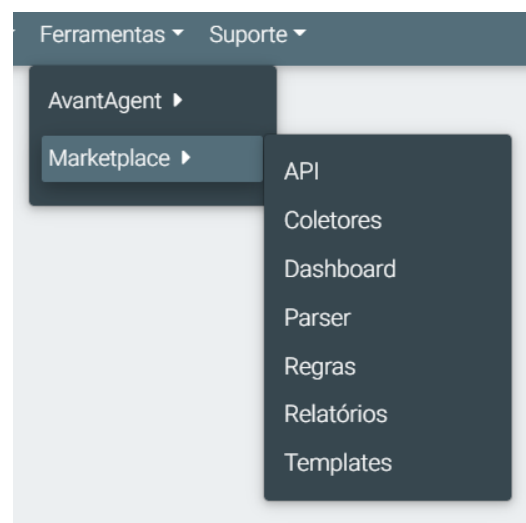


Figura 2 - MarkerPlace

### 3.1 AvantAgent

Nesse menu é onde são disponibilizados arquivos e modelos, com o objetivo do operador possa importar para AvantData, funcionalidades disponíveis no portal como modelos de regras, coletores, relatórios, visualizações e etc;

O AvantData permite que ao clicar com o botão direito do mouse o operador possa buscar objetos diretamente do AvantPortal. Facilitando a operação da ferramenta, pois isso não obriga o usuário a entrar no AvantPortal para fazer o download dos elementos selecionados.

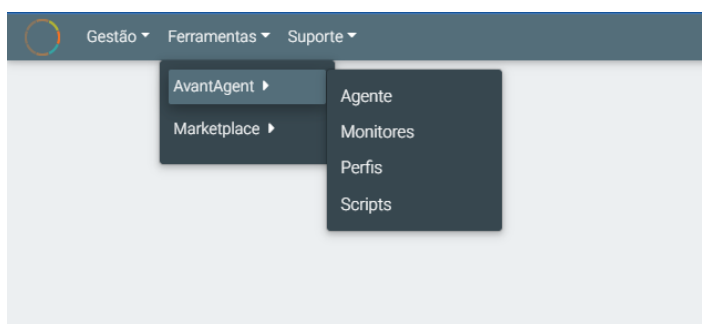


Figura 4 - Menu>Ferramentas>AvantAgent



Figura 5 - Buscar objetos diretamente do AvantPortal

Lista de Queries do AvantPortal

Nome	Tipo	Descrição
Administradores locais	OsQuery	Lista os administradores locais. TAG: Local Account - T1136/001
Administradores locais II	OsQuery	Verifica os Administradores locais II. TAG: T1136/001
Auto executáveis	OsQuery	Verifica os auto executáveis em itens de inicialização e registro do Windows. TAG: Boot or Logon Autostart Execution - T1547
Criptografia de disco via BitLocker	OsQuery	Verifica o status de criptografia de disco via BitLocker. TAG: Hardware - T1592/001
Eventos Malware Windows Defender	OsQuery	Query para buscar dados de malware no Windows Defender. Detecta eventos no Windows Defender (EventID: 1116 e 1117. Para duplicação dos eventos, usar a função select hex(mcs(CAMP01+CAMP02+...)) para o JOI do documento TAG: Import Indefinite - T1362/004
HazhFile	OsQuery	Calcula hash de arquivo para submeter ao Virus total ou outro motor de análise de malware. TAG: Exploitation for Client Execution - T1203
Patches do windows	OsQuery	Verifica a instalação dos patches do Windows. TAG: Patch System Image - T1601/001

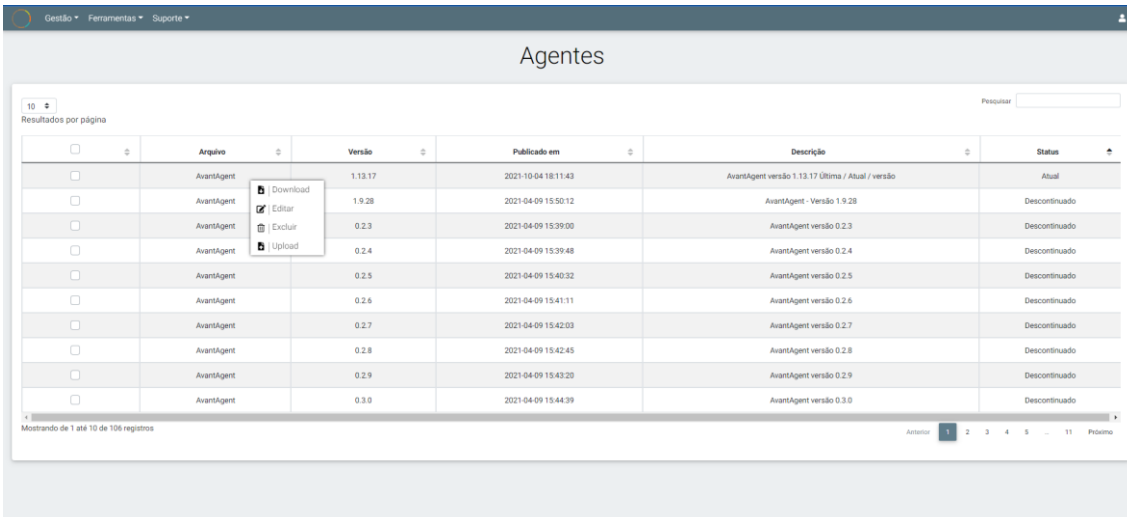
Figura 3 - Exemplo de Busca de OSQueries no AvantPortal

## Agentes

Na janela Agentes a visualização da tabela com o registro de todas as versões de agentes utilizadas até a atual, com data de publicação e seu status.

É possível fazer o download do agente atualizado, clicando com o botão direito do mouse no agente desejado, onde aparecerá uma janela de menu com as opções, “Download”.

Faça sempre o download da versão marcada como ATUAL.



	Arquivo	Versão	Publicado em	Descrição	Status
<input type="checkbox"/>	AvantAgent	1.13.17	2021-10-04 18:11:43	AvantAgent versão 1.13.17 Última / Atual / versão	Atual
<input type="checkbox"/>	AvantAgent	1.9.28	2021-04-09 15:50:12	AvantAgent - Versão 1.9.28	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.3	2021-04-09 15:39:00	AvantAgent versão 0.2.3	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.4	2021-04-09 15:39:48	AvantAgent versão 0.2.4	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.5	2021-04-09 15:40:32	AvantAgent versão 0.2.5	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.6	2021-04-09 15:41:11	AvantAgent versão 0.2.6	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.7	2021-04-09 15:42:03	AvantAgent versão 0.2.7	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.8	2021-04-09 15:42:45	AvantAgent versão 0.2.8	Descontinuado
<input type="checkbox"/>	AvantAgent	0.2.9	2021-04-09 15:43:20	AvantAgent versão 0.2.9	Descontinuado
<input type="checkbox"/>	AvantAgent	0.3.0	2021-04-09 15:44:39	AvantAgent versão 0.3.0	Descontinuado

Figura 8 –Página Agentes

Para importar o arquivo para o AvantData após o download, deverá seguir “Configurações”> “Entrada de Dados”> “AvantAgent” (Figura 7)

Na página Agentes, com o botão direito do mouse na opção de tabela “Agentes” aparecerá a opção de “Importar”. (Figura 10)

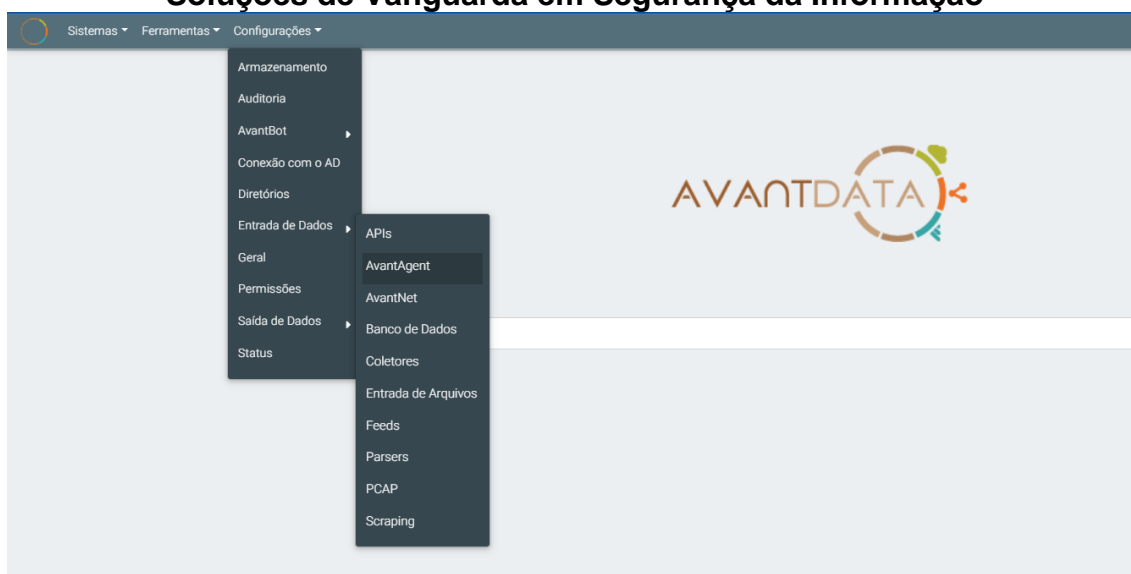


Figura 9 AvantData Configurações>Entrada de dado>AvantAgent

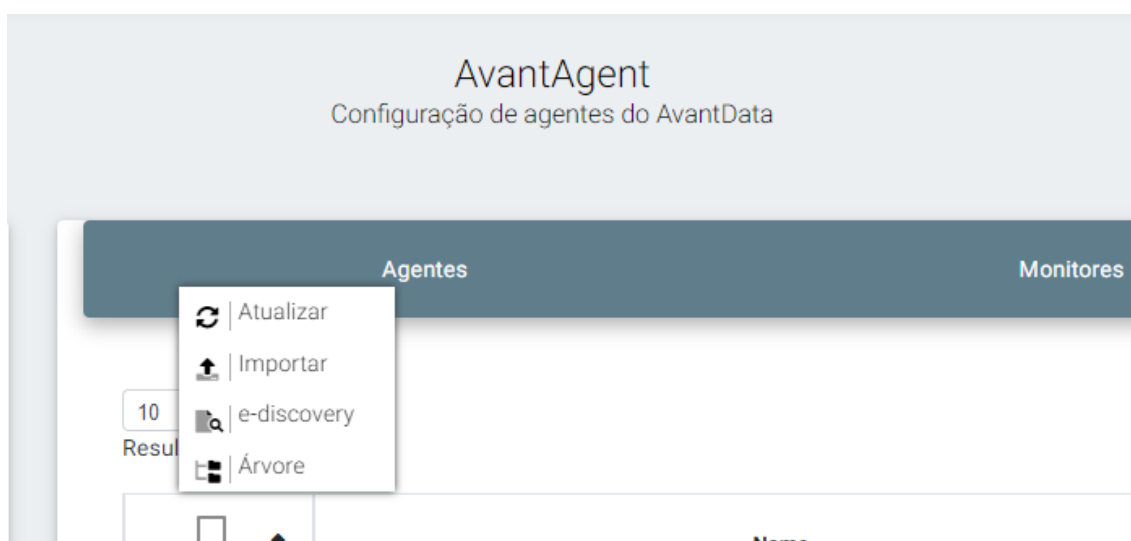


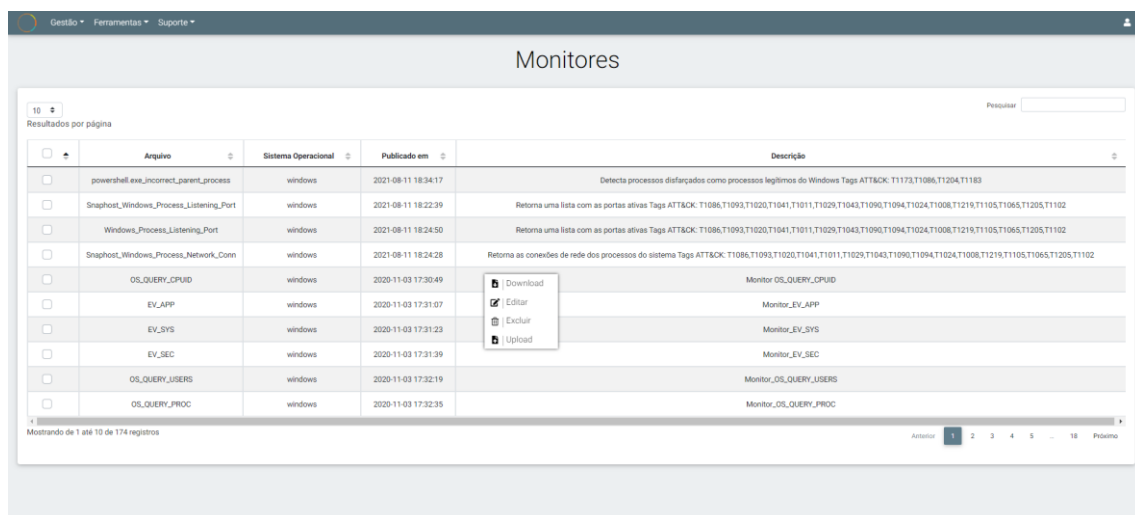
Figura 10 Importar Agente



### 3.1.1 Monitores

Na página de monitores há a visualização de uma tabela com modelos de monitores disponíveis para o AvantData, tendo sua descrição e o tipo de sistema operacional que suporta.

Para fazer o download, clique com o botão direito do mouse no monitor desejado, onde aparecerá uma janela de menu com as opções, “Download”.



Arquivo	Sistema Operacional	Publicado em	Descrição
powershell_exe_incorrect_parent_process	windows	2021-08-11 18:34:17	Detecta processos disfarçados como processos legítimos do Windows Tags ATT&CK: T1173,T1086,T1204,T1183
Snapshot_Windows_Process_Listening_Port	windows	2021-08-11 18:22:39	Retorna uma lista com as portas ativas Tags ATT&CK: T1086,T1093,T1020,T1041,T1011,T1029,T1043,T1090,T1094,T1024,T1008,T1219,T1105,T1065,T1205,T1102
Windows_Process_Listening_Port	windows	2021-08-11 18:24:50	Retorna uma lista com as portas ativas Tags ATT&CK: T1086,T1093,T1020,T1041,T1011,T1029,T1043,T1090,T1094,T1024,T1008,T1219,T1105,T1065,T1205,T1102
Snapshot_Windows_Process_Network_Conn	windows	2021-08-11 18:24:28	Retorna as conexões de rede dos processos do sistema Tags ATT&CK: T1086,T1093,T1020,T1041,T1011,T1029,T1043,T1090,T1094,T1024,T1008,T1219,T1105,T1065,T1205,T1102
OS_QUERY_CPUID	windows	2020-11-03 17:30:49	Monitor OS_QUERY_CPUID
EV_APP	windows	2020-11-03 17:31:07	Monitor_EV_APP
EV_SYS	windows	2020-11-03 17:31:23	Monitor_EV_SYS
EV_SEC	windows	2020-11-03 17:31:39	Monitor_EV_SEC
OS_QUERY_USERS	windows	2020-11-03 17:32:19	Monitor_OS_QUERY_USERS
OS_QUERY_PROC	windows	2020-11-03 17:32:35	Monitor_OS_QUERY_PROC

Figura 11 –Página Monitores

Para importar o arquivo para o AvantData após o download, deverá seguir “Configurações”> “Entrada de Dados”> “AvantAgent” (Figura 7)

Na página Agentes, com o botão direito do mouse na opção de tabela “Monitores” aparecerá a opção de “Importar”. (Figura 12)

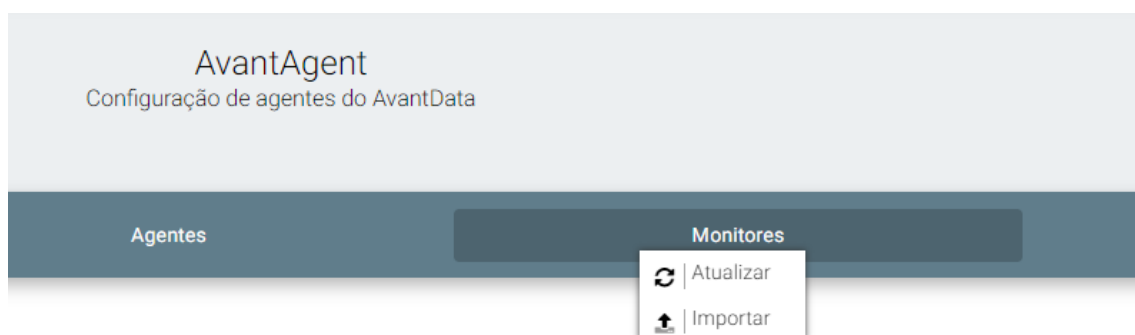


Figura 12 Importar Monitores

### 3.1.2 Perfis

Na página Perfis a visualização da tabela com modelos de perfis, perfis esses que são grupamentos de agentes e monitores.

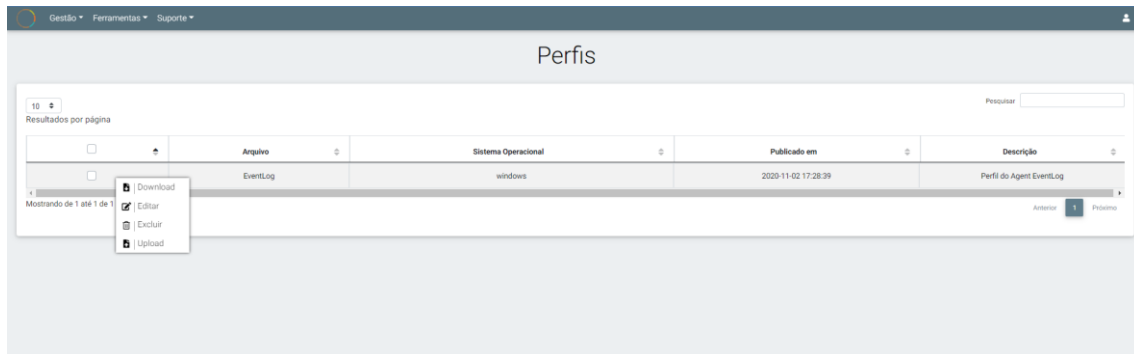


Figura 13 –Página Perfis

Para importar o arquivo para o AvantData após o download, deverá seguir “Configurações”> “Entrada de Dados”> “AvantAgent” (Figura 7)

Na página Agentes, com o botão direito do mouse na opção de tabela “Perfis” aparecerá a opção de “Importar”. (Figura 14)

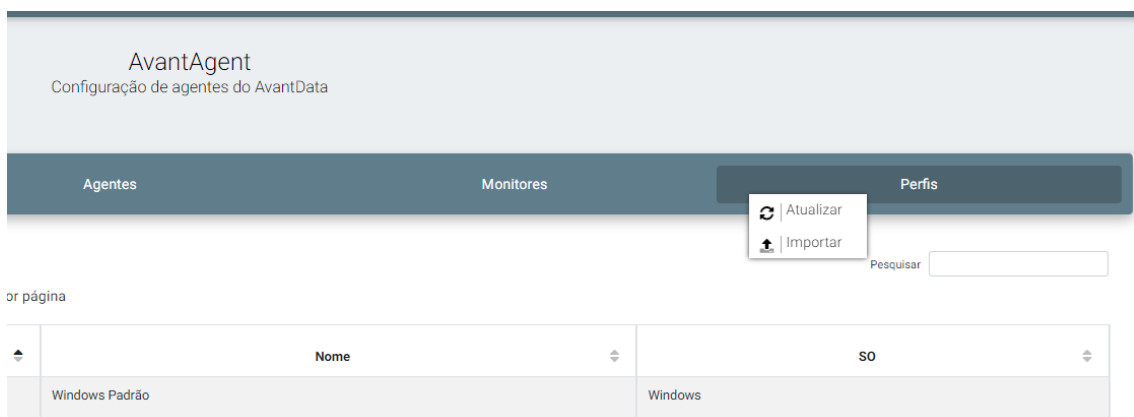
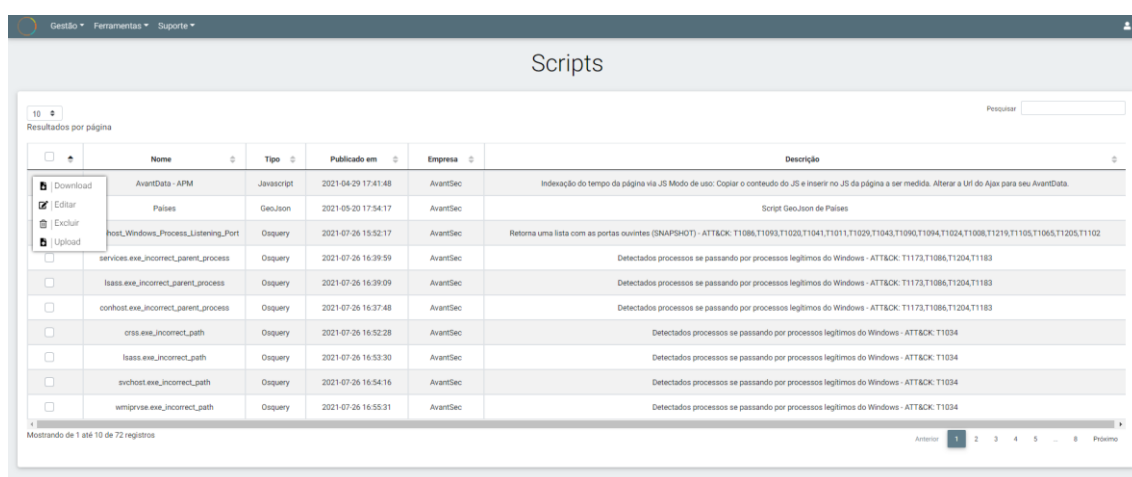


Figura 14 Importar Perfis

### 3.1.3 Scripts

Na página de scripts a visualização da tabela com todos os scripts disponibilizados pela Avantsec, seus tipos e descrição de uso, scripts esses que compõem o monitor.

Para fazer o download, clique com o botão direito do mouse no monitor desejado, onde aparecerá uma janela de menu com as opções, “Download”.



	Nome	Tipo	Publicado em	Empresa	Descrição
Download	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 do Ajax para seu AvantData.
Editar	Países	GeoJson	2021-05-20 17:54:17	AvantSec	Script GeoJson de Países
Excluir	Host_Windows_Process_Listening_Port	Osquery	2021-07-26 15:52:17	AvantSec	Retorna uma lista com as portas abertas (SNAPSHOT) - ATT&CK: T1086, T1093, T1020, T1041, T1011, T1029, T1043, T1090, T1094, T1024, T1008, T1219, T1105, T1065, T1205, T1102
Upload	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, T1183
	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, T1183
	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, T1183
	csrss.exe_incorrect_path	Osquery	2021-07-26 16:52:28	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1034
	lsass.exe_incorrect_path	Osquery	2021-07-26 16:53:30	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1034
	svchost.exe_incorrect_path	Osquery	2021-07-26 16:54:16	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1034
	wmiprvse.exe_incorrect_path	Osquery	2021-07-26 16:55:31	AvantSec	Detectados processos se passando por processos legítimos do Windows - ATT&CK: T1034

Figura 15 –Página Scripts

Outra forma, temos a opção de importar diretamente para o monitor no AvantData.

Indo em configurações > entrada de dados e AvantAgent (Figura 9).

Na página, à esquerda, em configuração, selecione “Monitor”, escolha o sistema operacional e o tipo de monitor que deseja criar. Em seguida na caixa posterior que aparecerá, com o botão direito do mouse, a opção “Importar query do AvantPortal” exemplificada na Figura 13.

Na nova janela contém a tabela com todos os scripts disponibilizados pelo portal e suas respectivas descrições (Figura 14) bastando escolher o desejado e clicar no botão de importar.

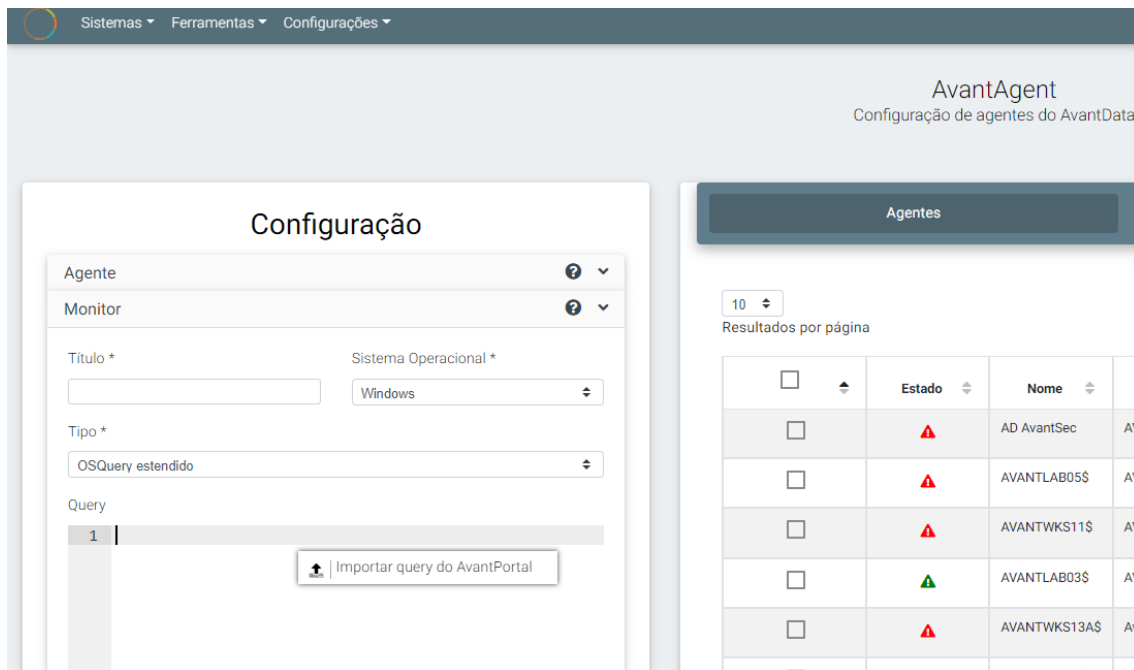


Figura 16 Importar monitor do AvantPortal

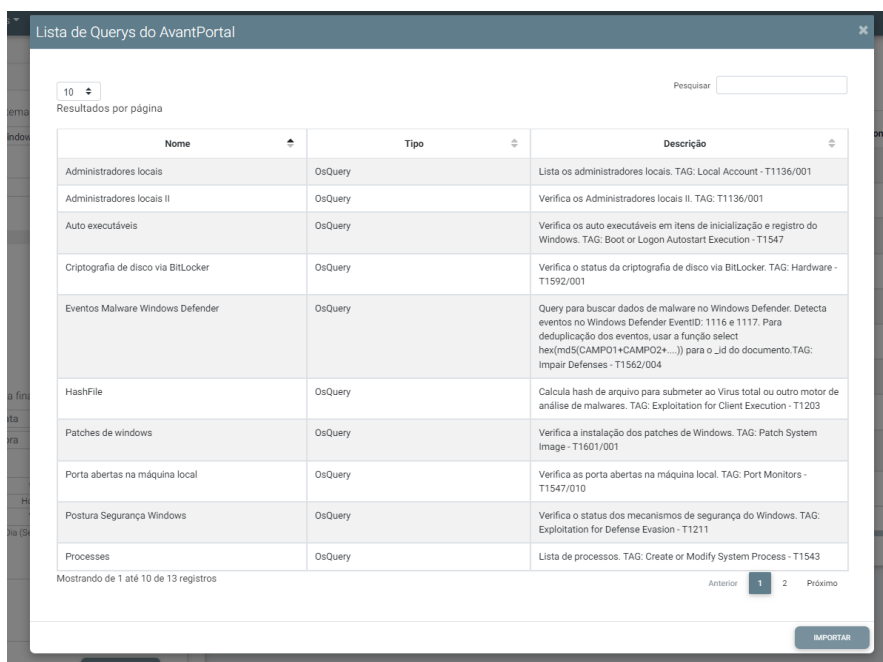


Figura 17 Janela Lista de Querys do AvantPortal no AvantData

### 3.2 Marketplace

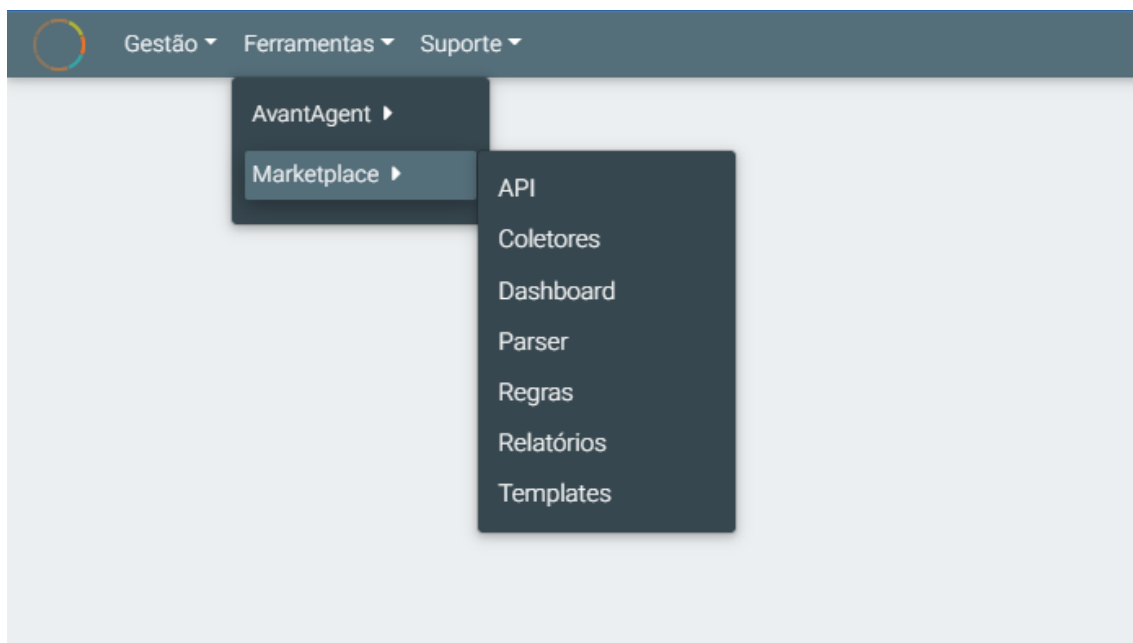
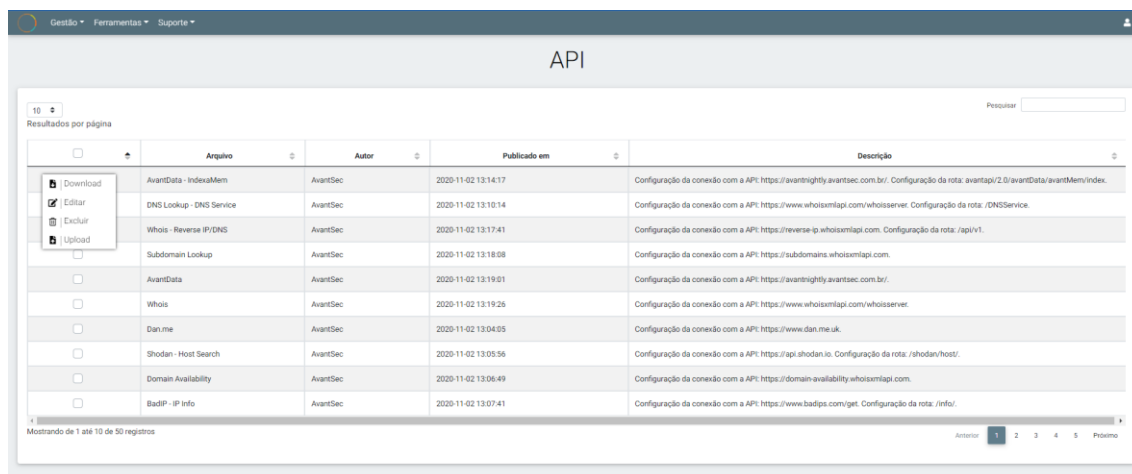


Figura 18 - Menu>Ferramentas>Marketplace

### 3.2.1 API

Na página de API a visualização da tabela contendo todas as configurações de conexão das API's disponíveis para utilizar na Entrada de Dados no AvantData, utilizado para enriquecimento de dados.

Para fazer o download, clique com o botão direito do mouse na API desejada, onde aparecerá uma janela de menu com as opções, "Download". (Figura 16)



	Arquivo	Autor	Publicado em	Descrição
<input type="checkbox"/>	AvantData - IndexMem	AvantSec	2020-11-02 13:14:17	Configuração da conexão com a API: https://avantrightly.avantsec.com.br/. Configuração da rota: avantapi/2.0/avantData/avantMem/index.
<input checked="" type="checkbox"/>	DNS Lookup - DNS Service	AvantSec	2020-11-02 13:10:14	Configuração da conexão com a API: https://www.whoismlapi.com/whoisserver. Configuração da rota: /DNSService.
<input type="checkbox"/>	Whois - Reverse IP/DNS	AvantSec	2020-11-02 13:17:41	Configuração da conexão com a API: https://reverse-ip.whoismlapi.com. Configuração da rota: /api/v1.
<input type="checkbox"/>	Subdomain Lookup	AvantSec	2020-11-02 13:18:08	Configuração da conexão com a API: https://subdomains.whoismlapi.com.
<input type="checkbox"/>	AvantData	AvantSec	2020-11-02 13:19:01	Configuração da conexão com a API: https://avantrightly.avantsec.com.br/.
<input type="checkbox"/>	Whois	AvantSec	2020-11-02 13:19:26	Configuração da conexão com a API: https://www.whoismlapi.com/whoisserver.
<input type="checkbox"/>	Dan.me	AvantSec	2020-11-02 13:04:05	Configuração da conexão com a API: https://www.dan.me.uk.
<input type="checkbox"/>	Shodan - Host Search	AvantSec	2020-11-02 13:05:56	Configuração da conexão com a API: https://api.shodan.io. Configuração da rota: /shodan/host/.
<input type="checkbox"/>	Domain Availability	AvantSec	2020-11-02 13:06:49	Configuração da conexão com a API: https://domain-availability.whoismlapi.com.
<input type="checkbox"/>	BadIP - IP Info	AvantSec	2020-11-02 13:07:41	Configuração da conexão com a API: https://www.badips.com/get. Configuração da rota: /info/.

Figura 19 - Página API

Para importar o arquivo para o AvantData após o download, deverá seguir "Configurações"> "Entrada de Dados"> "API" (Figura 17)

Na página, com o botão direito do mouse na opção de tabela "API – URL" aparecerá a opção de "Importar". (Figura 16)

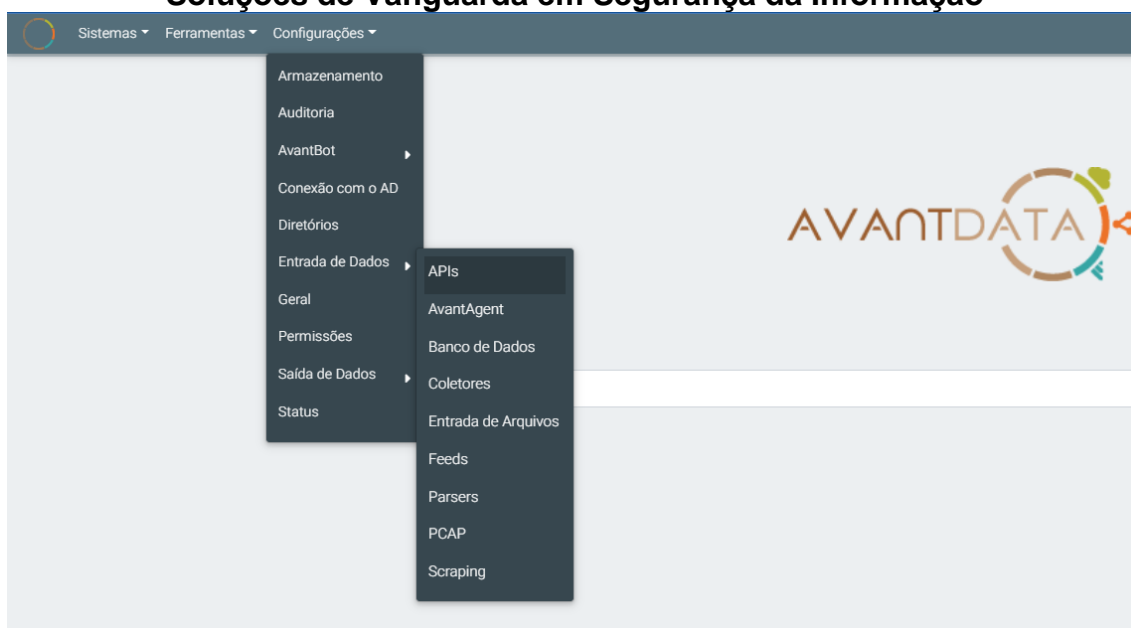


Figura 20 AvantData>Configurações>Entrada de Dados>APIs

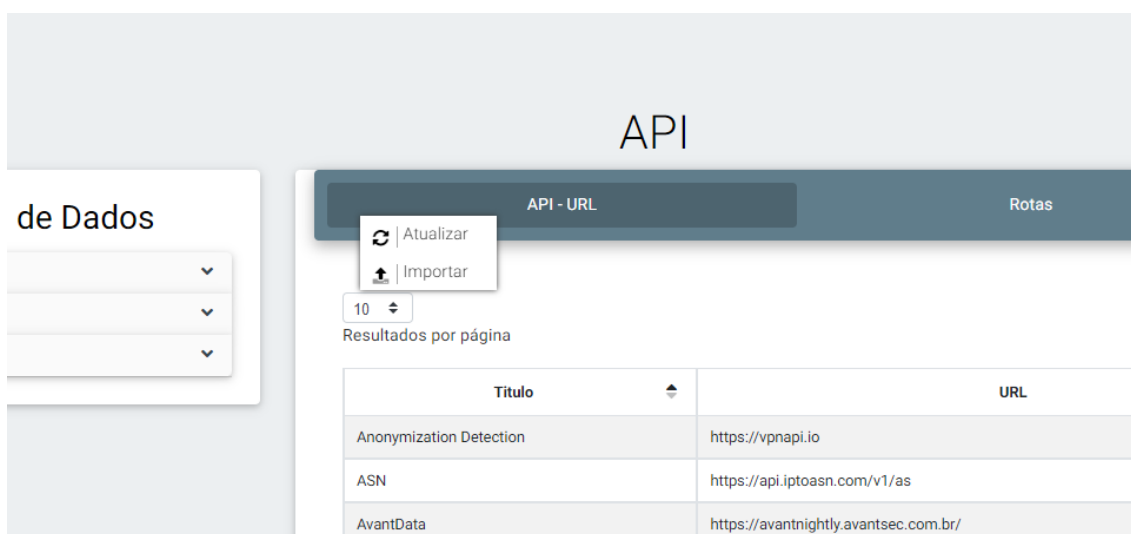


Figura 21 Importar API

### 3.2.2 Coletores

Em Coletores a visualização da tabela com todos os modelos de scripts para coletores, na utilização da Entrada de Dados do AvantData, e suas descrições.

Para fazer o download, clique com o botão direito do mouse no coletor desejado, onde aparecerá uma janela de menu com as opções, “Download”. (Figura 19).

Há diversos tipos de coletores disponíveis como templates, dessa forma, o operador pode selecionar modelos de UEBA, análise de tráfego de rede, Busca de Vulnerabilidade, dentre outros.

Coletores

10

Pesquisar

Resultados por página

<input type="checkbox"/>	Arquivo	Autor	Publicado em	Descrição
<input type="checkbox"/>	Email Teste	AvantSec	2020-11-02 15:46:25	Indexação coletor para teste de email
<input type="checkbox"/>	Ioc	AvantSec	2020-11-02 15:48:24	Indexação de IOC
<input type="checkbox"/>	Correlacionador Avançado AvantAgent e Banco de Dados	AvantSec	2020-11-02 19:56:44	Correlaciona dados do AvantAgent com Bancos de Dados, via conectores e AvantAPI, para gerar informações novas em tempo de indexação.
<input type="checkbox"/>	Monitoramento e ajuste de configuração de AvantAgent	AvantSec	2021-10-06 16:37:48	Busca os agentes com problemas de configuração inicial, normalmente por falhas de conectividade entre AvantAgent e AvantData. Executa u
<input type="checkbox"/>	Reindexação	AvantSec	2021-11-18 01:19:29	Reindexa os índices que seguem um padrão determinado pelo usuário em um novo índice.
<input type="checkbox"/>	Detector de anomalia - External Domain - Fit	AvantSec	2021-11-24 16:49:26	Código modelo para treinar um modelo para detectar anomalias relacionadas a um domínio externo. Alterar queries/índices/diretórios segun
<input type="checkbox"/>	Deleta Índice	AvantSec	2021-11-18 01:20:06	Deleta índices que seguem um padrão determinado pelo usuário.
<input type="checkbox"/>	Detector de anomalia - External Domain - Predict	AvantSec	2021-11-24 16:52:13	Código modelo para predição de anomalias relacionadas a um domínio externo. Alterar queries/índices/diretórios segundo a demanda
<input type="checkbox"/>	Monitoramento de link	AvantSec	2021-11-18 01:08:59	Exemplo de monitor de link de conectividade com teste de download e upload.
<input type="checkbox"/>	Controle de licença	AvantSec	2020-11-02 16:17:03	Indexação dos dados de licença.

Mostrando de 1 até 10 de 19 registros

Anterior

1

2

Próximo

Figura 22 - Página Coletores

Para fazer a importação para o AvantData, deverá seguir “Configurações”> “Entrada de Dados”> “Coletores” (Figura 20)

Na página do Coletor, no conteúdo à esquerda “script” a um campo de entrada, nele deve-se escolher o arquivo que deseja importar para a criação do novo coletor. (Figura 21)



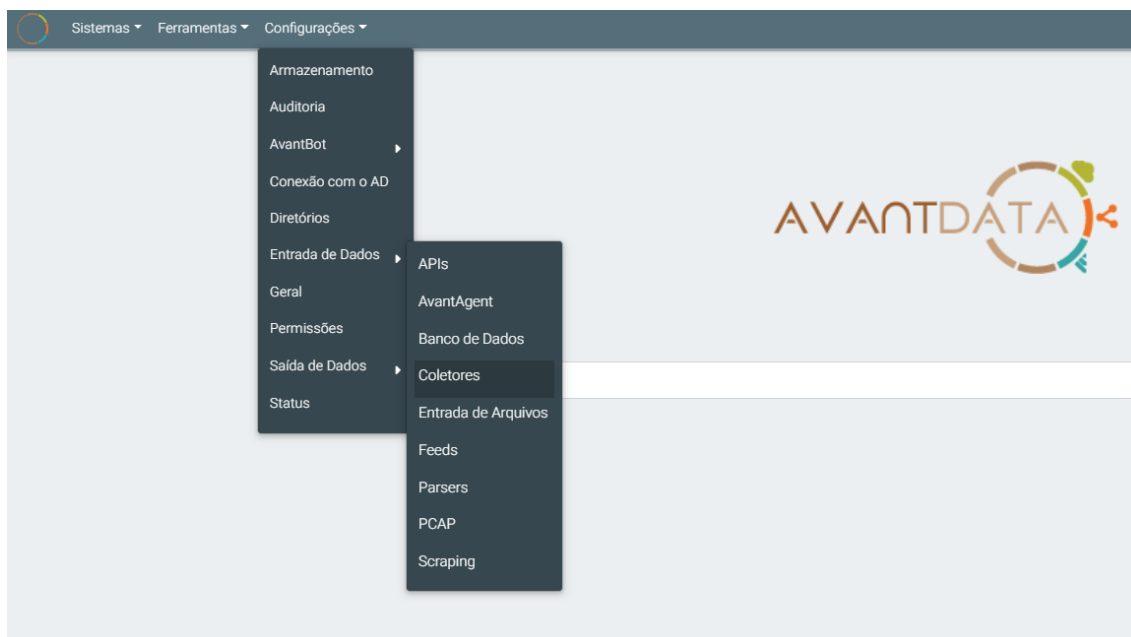


Figura 23 AvantData>Configurações>Entrada de Dados>Coletores

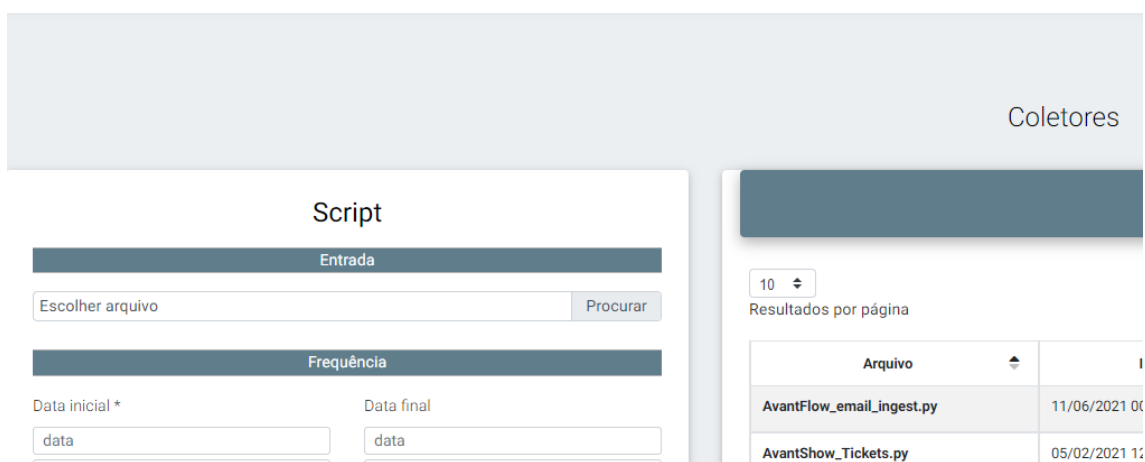
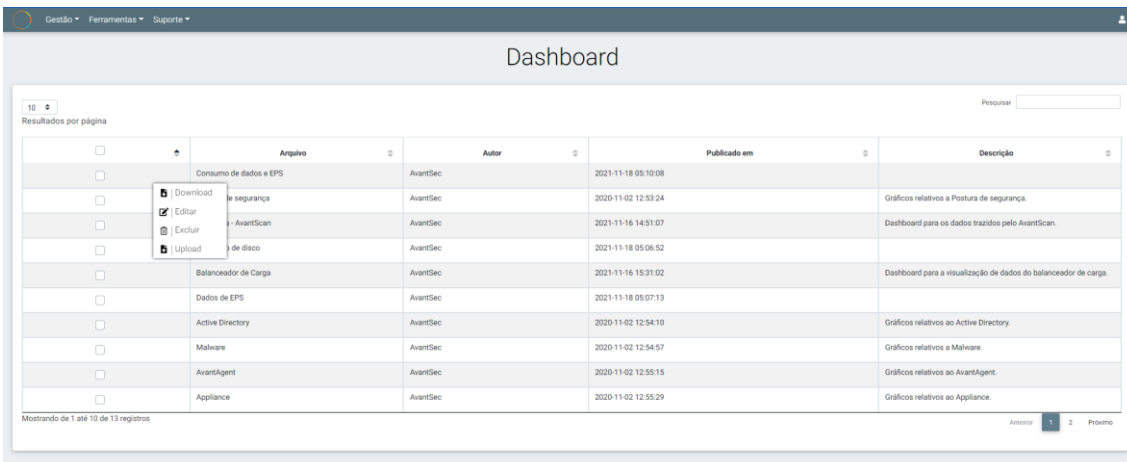


Figura 24 Importar arquivo coletor

### 3.2.3 Dashboard

Na janela de Dashboard a visualização da tabela com modelos de Dashboards, que são disponibilizadas para o uso no AvantData.

Para fazer o download, clique com o botão direito do mouse no modelo desejado, onde aparecerá uma janela de menu com as opções “Download”



The screenshot shows the 'Dashboard' page in the AvantSec application. At the top, there is a navigation bar with 'Gestão', 'Ferramentas', and 'Suporte'. Below it, the title 'Dashboard' is centered. A search bar is on the right. The main area contains a table with 5 columns: 'Arquivo', 'Autor', 'Publicado em', and 'Descrição'. A right-click context menu is open over the first row, showing options: 'Download', 'Editar', 'Excluir', and 'Upload'. The table lists various dashboard models like 'Consumo de dados e EPS', 'Postura de segurança', 'AvantScan', 'Balanceador de Carga', 'Dados de EPS', 'Active Directory', 'Malware', 'AvantAgent', and 'Appliance'. At the bottom, it says 'Mostrando de 1 até 10 de 13 registros' and has pagination controls for 'Anterior', '1', '2', and 'Próximo'.

	Arquivo	Autor	Publicado em	Descrição
<input type="checkbox"/>	Consumo de dados e EPS	AvantSec	2021-11-18 05:10:08	
<input type="checkbox"/>	Postura de segurança	AvantSec	2020-11-02 12:53:24	Gráficos relativos a Postura de segurança.
<input type="checkbox"/>	AvantScan	AvantSec	2021-11-16 14:51:07	Dashboard para os dados trazidos pelo AvantScan.
<input type="checkbox"/>	Balanceador de Carga	AvantSec	2021-11-18 05:06:52	
<input type="checkbox"/>	Balanceador de Carga	AvantSec	2021-11-16 15:31:02	Dashboard para a visualização de dados do balanceador de carga.
<input type="checkbox"/>	Dados de EPS	AvantSec	2021-11-18 05:07:13	
<input type="checkbox"/>	Active Directory	AvantSec	2020-11-02 12:54:10	Gráficos relativos ao Active Directory.
<input type="checkbox"/>	Malware	AvantSec	2020-11-02 12:54:57	Gráficos relativos a Malware.
<input type="checkbox"/>	AvantAgent	AvantSec	2020-11-02 12:55:15	Gráficos relativos ao AvantAgent.
<input type="checkbox"/>	Appliance	AvantSec	2020-11-02 12:55:29	Gráficos relativos ao Appliance.

Figura 25 – Página Dashboard

Para fazer a importação do modelo no AvantData, deverá seguir “Ferramenta”> “Dashboard”. (Figura 23)

Na página do Dashboard a extrema esquerda a um menu, nele a várias pastas, na designada com o botão direito do mouse, aparecerá uma janela menu com a opção “Importar”. (Figura 24)

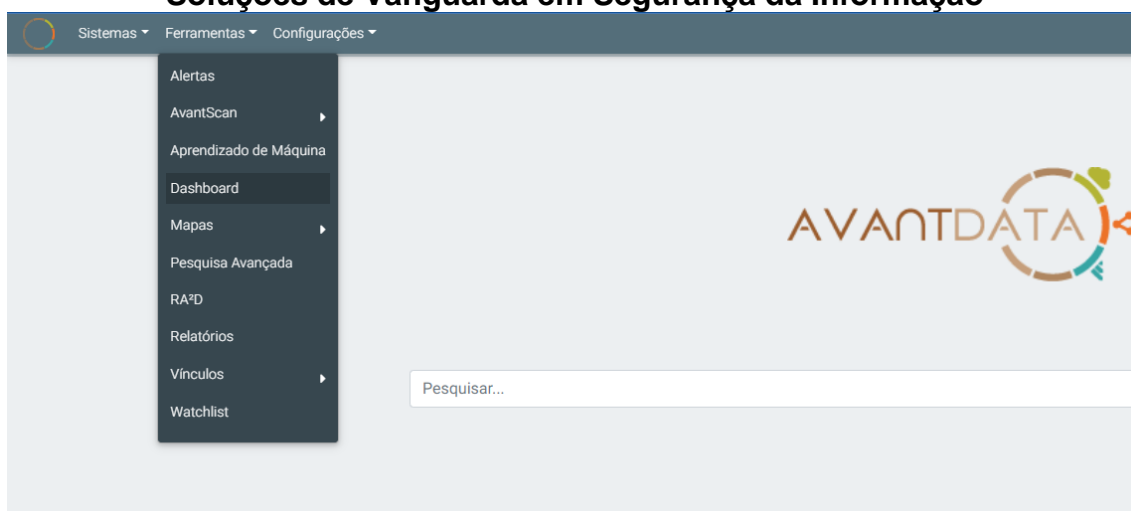


Figura 26 AvantData>Ferramentas>Dashboard

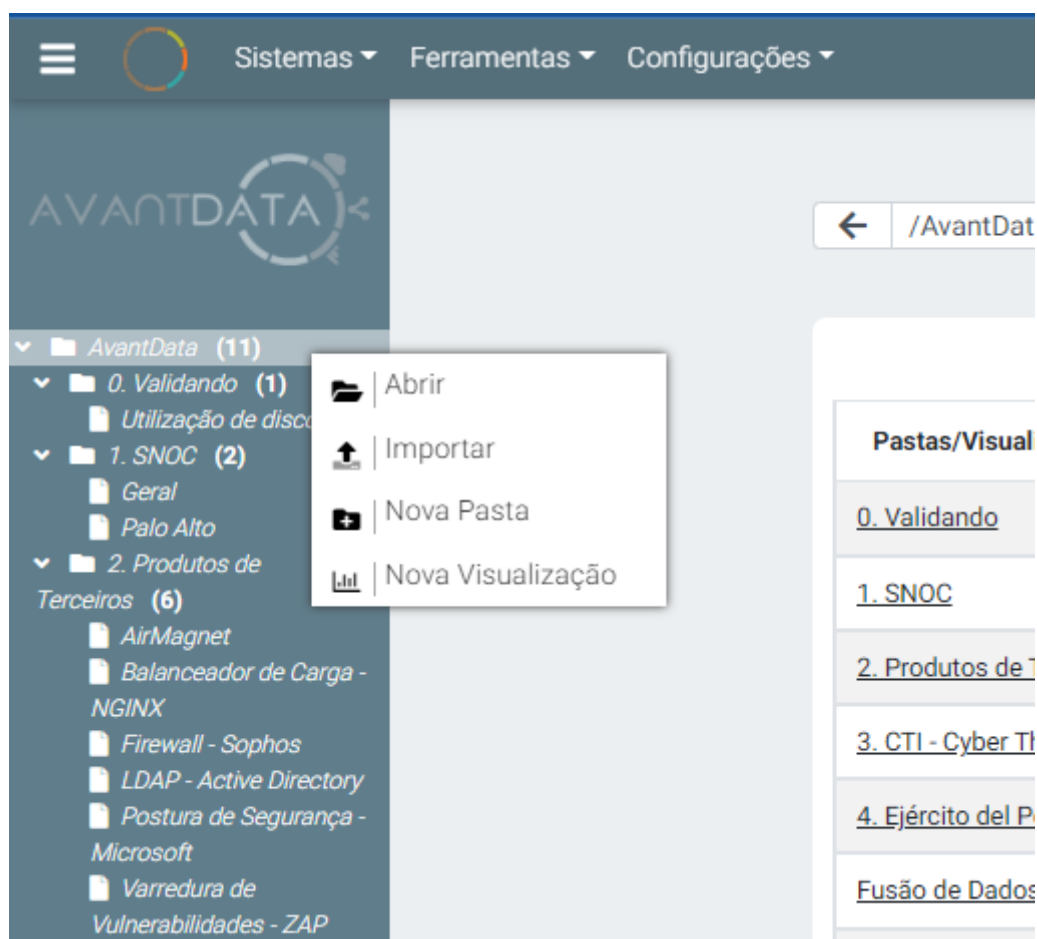
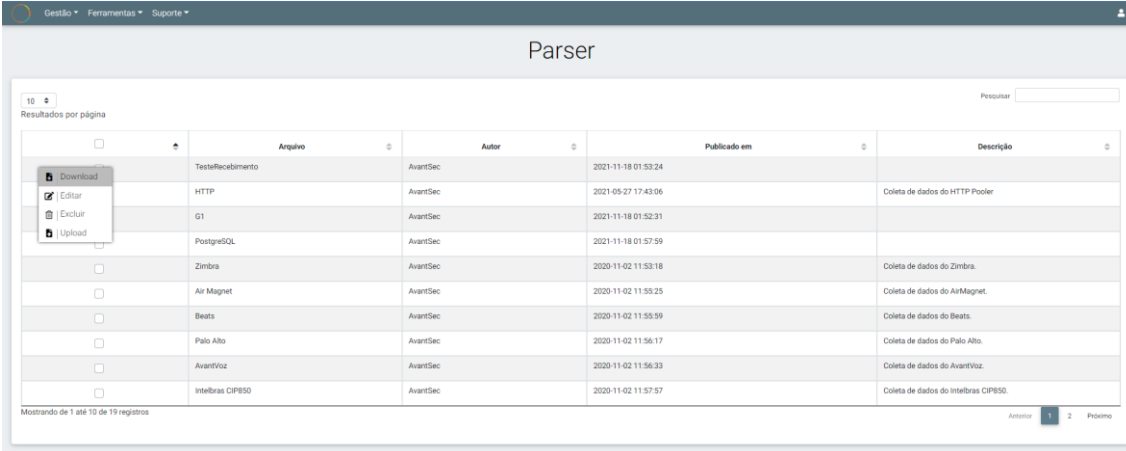


Figura 27 Importar dashboard

### 3.2.4 Parser

Na página Parser a visualização da tabela com todos os modelos de parser utilizados em busca e recebimento de dados no AvantData.

Para fazer o download, clique com o botão direito do mouse no parser desejado, onde aparecerá uma janela de menu com as opções, “Download”.



Parser

10 Resultados por página

	Arquivo	Autor	Publicado em	Descrição
<input type="checkbox"/>	TesteRecabimento	AvantSec	2021-11-18 01:53:24	
<input checked="" type="checkbox"/>	HTTP	AvantSec	2021-05-27 17:43:06	Coleta de dados do HTTP Pooler
<input checked="" type="checkbox"/>	G1	AvantSec	2021-11-18 01:52:31	
<input checked="" type="checkbox"/>	PostgreSQL	AvantSec	2021-11-18 01:57:59	
<input type="checkbox"/>	Zimbra	AvantSec	2020-11-02 11:53:18	Coleta de dados do Zimbra.
<input type="checkbox"/>	Air Magnet	AvantSec	2020-11-02 11:55:25	Coleta de dados do AirMagnet.
<input type="checkbox"/>	Beats	AvantSec	2020-11-02 11:55:59	Coleta de dados do Beats.
<input type="checkbox"/>	Palo Alto	AvantSec	2020-11-02 11:56:17	Coleta de dados do Palo Alto.
<input type="checkbox"/>	AvantVoz	AvantSec	2020-11-02 11:56:33	Coleta de dados do AvantVoz.
<input type="checkbox"/>	Intelbras CIPESD	AvantSec	2020-11-02 11:57:57	Coleta de dados do Intelbras CIPESD.

Mostrando de 1 até 10 de 10 registros

Figura 28 – Página Parser

Para fazer a importação do modelo no AvantData, deverá seguir “Configuração”> “Entrada de Dados”> “Parser”. (Figura 26)

Na página do Parser no conteúdo à esquerda “Arquivo” a um campo de entrada, nele deve-se escolher Upload e em seguida o arquivo que deseja importar. (Figura 27)

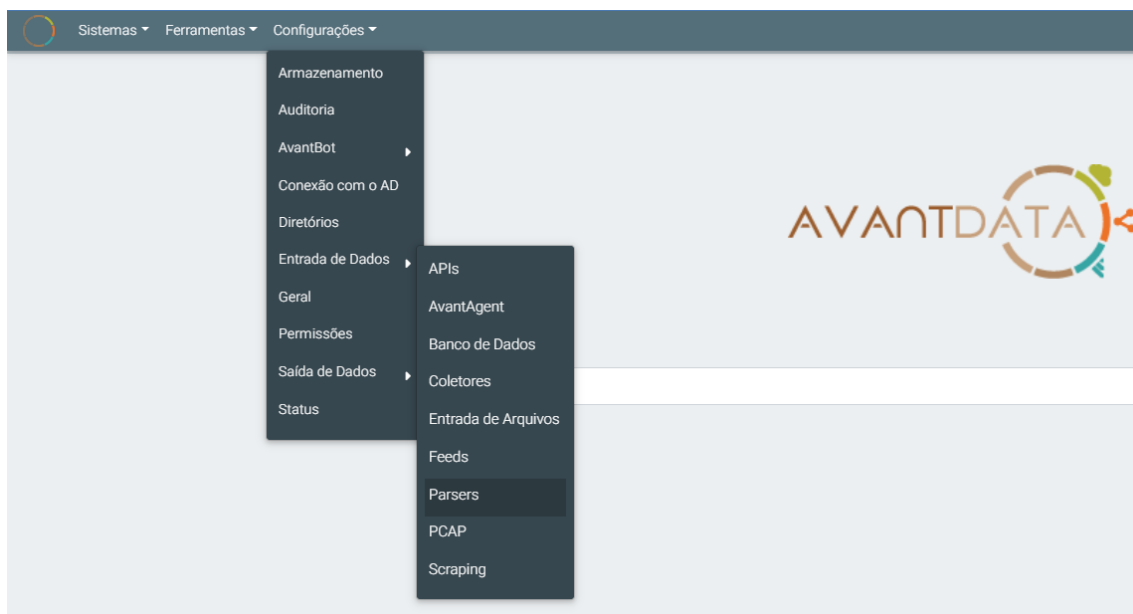


Figura 29 AvantData Configurações>Entrada de Dados>Parsers

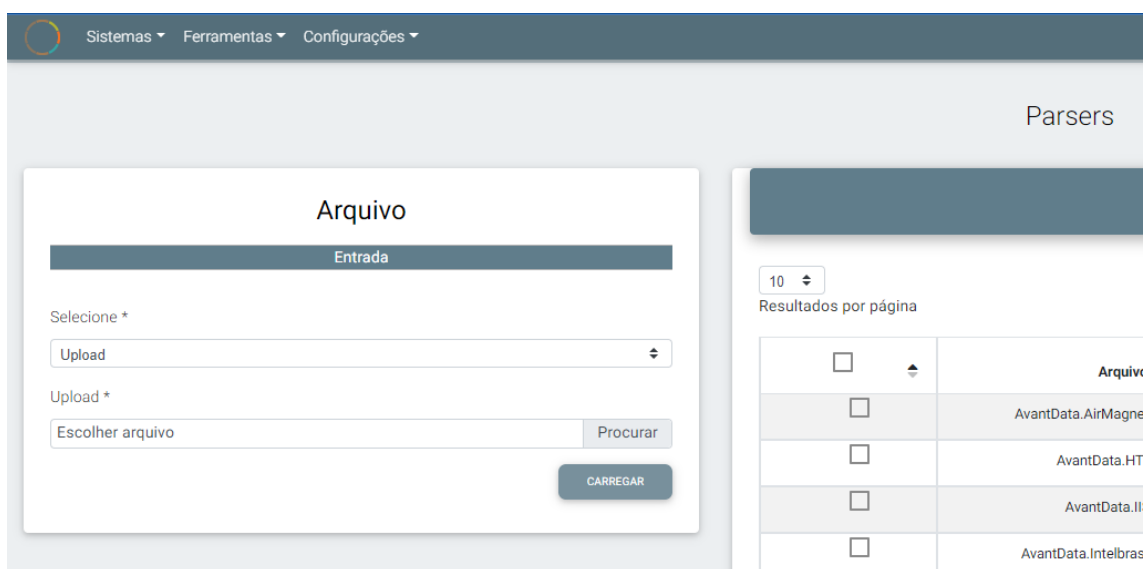
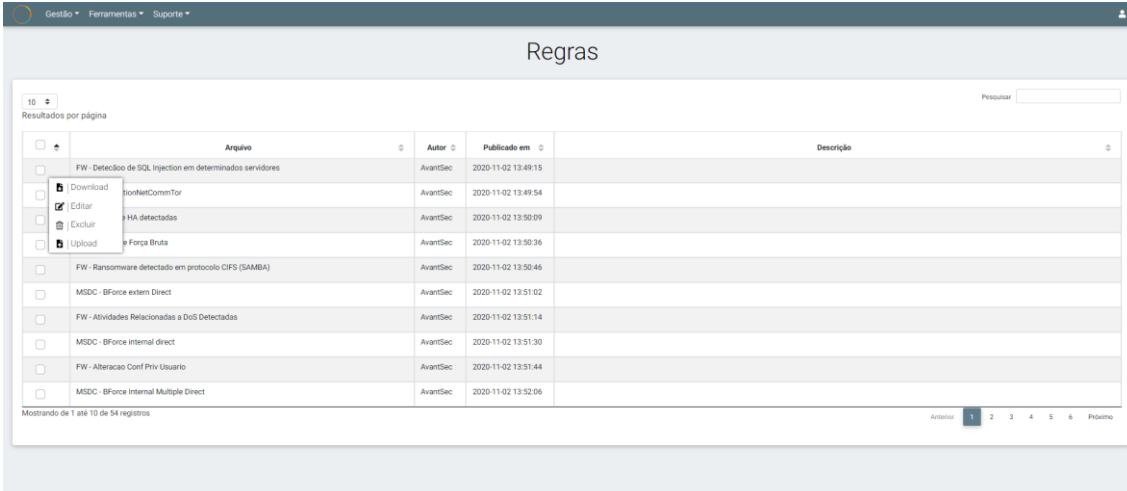


Figura 30 Upload

### 3.2.5 Regras

Na página Regras a visualização da tabela com os modelos de regras que podem ser utilizadas no AvantData em RA2D. Lá são publicadas regras que detectam padrões, anomalias ou atividades maliciosas

Para fazer o download, clique com o botão direito do mouse na regra desejada, onde aparecerá uma janela de menu com as opções, “Download”.



	Arquivo	Autor	Publicado em	Descrição
<input type="checkbox"/>	FW - Detecção de SQL Injection em determinados servidores	AvantSec	2020-11-02 13:49:15	
<input type="checkbox"/>	FW - Detecção de SQL Injection em determinados servidores	AvantSec	2020-11-02 13:49:54	
<input type="checkbox"/>	FW - Detecção de SQL Injection em determinados servidores	AvantSec	2020-11-02 13:50:09	
<input type="checkbox"/>	FW - Detecção de SQL Injection em determinados servidores	AvantSec	2020-11-02 13:50:36	
<input type="checkbox"/>	FW - Ransomware detectado em protocolo CIFS (SMB)	AvantSec	2020-11-02 13:50:46	
<input type="checkbox"/>	MSDC - BForce external Direct	AvantSec	2020-11-02 13:51:02	
<input type="checkbox"/>	FW - Atividades Relacionadas a DoS Detectadas	AvantSec	2020-11-02 13:51:14	
<input type="checkbox"/>	MSDC - BForce internal direct	AvantSec	2020-11-02 13:51:30	
<input type="checkbox"/>	FW - Alteração Conf Priv Usuario	AvantSec	2020-11-02 13:51:44	
<input type="checkbox"/>	MSDC - BForce Internal Multiple Direct	AvantSec	2020-11-02 13:52:06	

Figura 31 – Página Regras

Para fazer a importação do modelo no AvantData, deverá seguir “Ferramenta”> “RA2D”. (Figura 29)

Na página do RA2D, a extrema esquerda a um menu, nele a várias pastas, na designada com o botão direito do mouse, aparecerá uma janela menu com a opção “Importar”. (Figura 30)

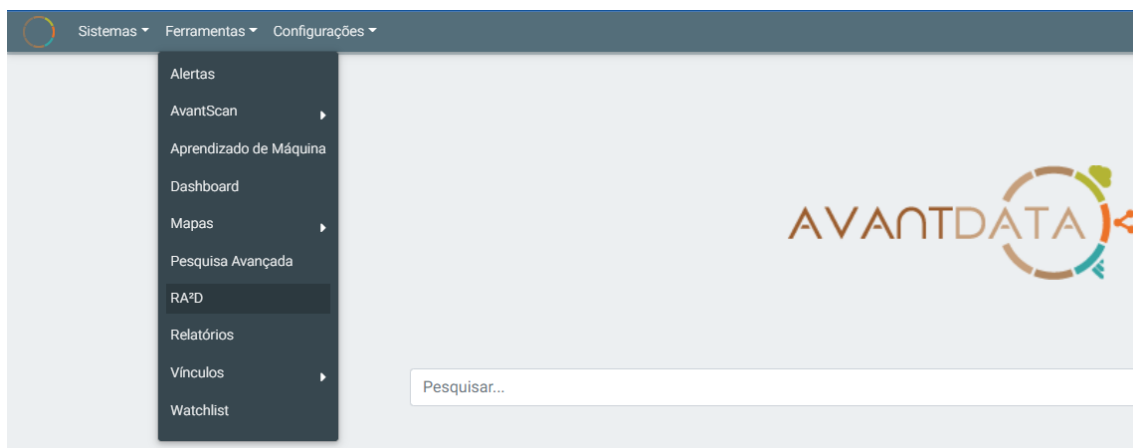


Figura 32 AvantData Ferramentas>RA2D



Figura 33 Importar Regras

### 3.2.7 Relatórios

Na página Relatórios a visualização da tabela com modelos de relatórios que podem ser utilizados no AvantData.

Para fazer o download, clique com o botão direito do mouse no monitor desejado, onde aparecerá uma janela de menu com as opções, “Download”.



The screenshot shows the 'Relatórios' page in the AvantSec interface. It features a table with columns for selection, file name, author, category, publication date, and description. The table lists various report templates such as 'Vulnerabilidade HTML', 'Ativos críticos apresentando falhas', 'Falha de Backup', etc. A search bar is located at the top right of the table area.

	Arquivo	Autor	Categoria	Publicado em	Descrição
<input type="checkbox"/>	Vulnerabilidade HTML	AvantSec	Vulnerability Management	2020-11-02 11:44:09	Modelo básico de relatório de Vulnerabilidades HTML.
<input type="checkbox"/>	Ativos críticos apresentando falhas	AvantSec	Failures/ Malfunction	2021-11-24 21:23:22	Modelo de relatório referente à falhas apresentadas em equipamentos críticos
<input type="checkbox"/>	Falha de Backup	AvantSec	Unintentional damage / loss of information or IT assets	2021-11-24 21:26:58	Modelo de relatório referente à falhas de backup de ativos críticos
<input type="checkbox"/>	Oscilações elétricas	AvantSec	LGPD	2021-11-24 21:30:32	Modelo de relatório referente à oscilações elétricas relatadas por ativos de energia elétrica.
<input type="checkbox"/>	Sítios fora do ar	AvantSec	Outages	2021-11-24 21:34:04	Modelo referente à sítios fora do ar.
<input type="checkbox"/>	Falha na gravação de disco de ativo crítico	AvantSec	LGPD	2021-11-24 21:28:01	Modelo referente à falha de gravação de dados críticos em ativos que possuem a mesma criticidade.
<input type="checkbox"/>	Relatório LATEX	AvantSec	UEBA	2021-08-09 00:08:41	AvantScan Relatório LATEX
<input type="checkbox"/>	Utilização indevida dos recursos	AvantSec	Eavesdropping/ Interception/ Hijacking	2021-11-24 21:35:32	Modelo referente à anomalias na utilização de recursos de ativos críticos.
<input type="checkbox"/>	Ativos indisponíveis	AvantSec	Outages	2021-11-24 21:31:47	Modelo de relatório referente à ativos críticos indisponíveis.
<input type="checkbox"/>	Acesso indevido aos compartimentos	AvantSec	Eavesdropping/ Interception/ Hijacking	2021-11-24 21:22:09	Modelo de relatório de acesso indevido à compartimentos disponibilizados através de sistemas de arquivos

Figura 34 –Página Relatórios

Para fazer a importação do modelo no AvantData, deverá seguir “Configuração”> “Saída de Dados”> “Relatório”. (Figura 32)

Na página do Relatório no conteúdo à esquerda “Configuração Modelo” a um campo “Modelo”, nele deve escolher “carregar” em seguida em Upload o arquivo que deseja importar. (Figura 33)



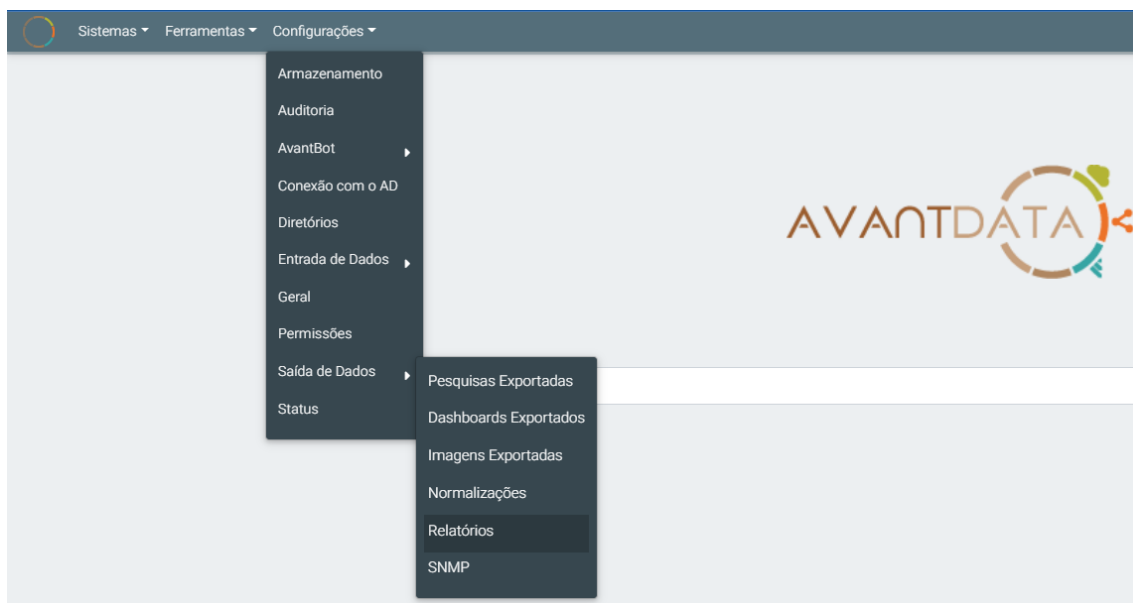


Figura 35 AvantData>Saída de Dados>Relatórios

Sistemas ▾ Ferramentas ▾ Configurações ▾

Relatórios  
Configuração de modelos d

### Configuração Modelo

Nome \*

Tipo \*

Modelo \*

Categoria \*

Upload

10 ▾  
Resultados por página

Nome	T
AvantScan	L
Relatório de Vulnerabilidade	H

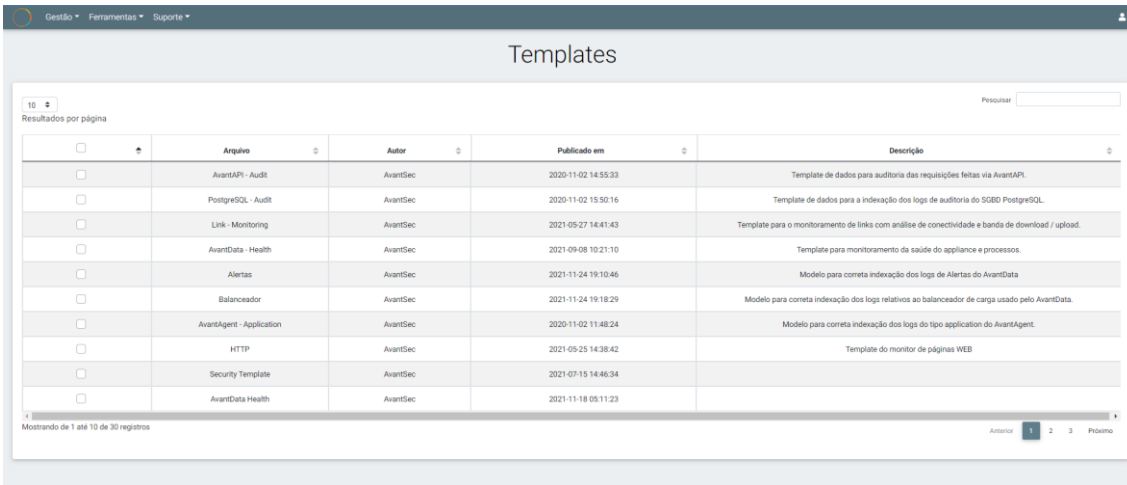
Mostrando de 1 até 2 de 2 registros

Figura 36 Upload modelo relatório

### 3.2.8 Templates

Na página Templates a visualização da tabela com modelos de templates para a utilização no AvantData.

Para fazer o download, clique com o botão direito do mouse no template desejado, onde aparecerá uma janela de menu com as opções, “Download”.



	Arquivo	Autor	Publicado em	Descrição
<input type="checkbox"/>	AvantAPI - Audit	AvantSec	2020-11-02 14:55:33	Template de dados para auditoria das requisições feitas via AvantAPI.
<input type="checkbox"/>	PostgreSQL - Audit	AvantSec	2020-11-02 15:50:16	Template de dados para a indexação dos logs de auditoria do SGBD PostgreSQL.
<input type="checkbox"/>	Link - Monitoring	AvantSec	2021-05-27 14:41:43	Template para o monitoramento de links com análise de conectividade e banda de download / upload.
<input type="checkbox"/>	AvantData - Health	AvantSec	2021-09-08 10:21:10	Template para monitoramento da saúde do appliance e processos.
<input type="checkbox"/>	Alertas	AvantSec	2021-11-24 19:10:46	Modelo para correta indexação dos logs de Alertas do AvantData.
<input type="checkbox"/>	Balancador	AvantSec	2021-11-24 19:18:29	Modelo para correta indexação dos logs relativos ao balancador de carga usado pelo AvantData.
<input type="checkbox"/>	AvantAgent - Application	AvantSec	2020-11-02 11:48:24	Modelo para correta indexação dos logs do tipo application do AvantAgent.
<input type="checkbox"/>	HTTP	AvantSec	2021-05-25 14:38:42	Template do monitor de páginas WEB.
<input type="checkbox"/>	Security Template	AvantSec	2021-07-15 14:46:34	
<input type="checkbox"/>	AvantData Health	AvantSec	2021-11-18 05:11:23	

Mostrando de 1 até 10 de 30 registros

Figura 37 – Página Templates

Para fazer a importação do modelo no AvantData, deverá seguir “Configuração”> “Status”. (Figura 35)

Na página Status na opção “Template” com o botão direito do mouse, aparecerá o menu de opções com “Importar”. (Figura 36)



Figura 38 AvantData Configurações>Status

Sistemas ▾ Ferramentas ▾ Configurações ▾

Status




Cluster

Nós

Alias

Template

10 ▾  
Resultados por página

 Atualizar  
 Importar  
 Novo Template

<input type="checkbox"/> Todos ▾	Template
<input type="checkbox"/>	avantagent_up_template
<input type="checkbox"/>	teste_campo2_template
<input type="checkbox"/>	mitre_teste_template

Figura 39 Importar modelo template

## 4 Suporte

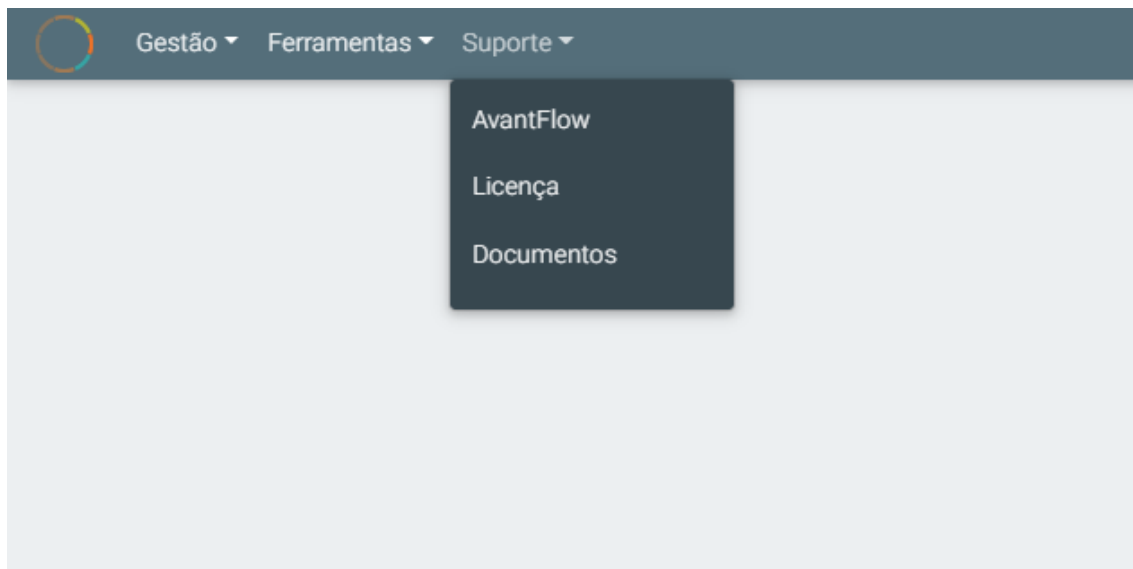


Figura 40 - Menu Suporte

### 3.1. Licença

Na página de Licença há a visualização da tabela com as licenças disponíveis na conta do usuário logado no AvantPorta.

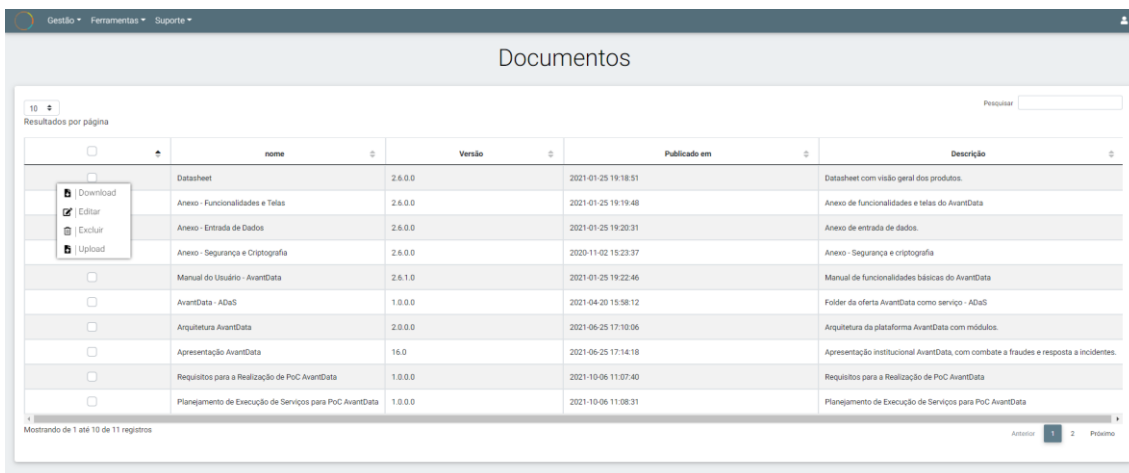


Figura 41 – Página Licença

### 3.2. Documentos

Na janela documentos a visualização de todos os documentos e suas descrições referentes ao produto AvantData disponibilizado pela Avantsec.

Para fazer o download do documento, clique com o botão direito do mouse no desejado, onde aparecerá uma janela de menu com as opções “Download”.



	nome	Versão	Publicado em	Descrição
<input type="checkbox"/>	Datasheet	2.6.0.0	2021-01-25 19:18:51	Datasheet com visão geral dos produtos.
<input type="checkbox"/>	Anexo - Funcionalidades e Telas	2.6.0.0	2021-01-25 19:19:48	Anexo de funcionalidades e telas do AvantData
<input type="checkbox"/>	Anexo - Entrada de Dados	2.6.0.0	2021-01-25 19:20:31	Anexo de entrada de dados.
<input type="checkbox"/>	Anexo - Segurança e Criptografia	2.6.0.0	2020-11-02 15:23:37	Anexo - Segurança e criptografia
<input type="checkbox"/>	Manual do Usuário - AvantData	2.6.1.0	2021-01-25 19:22:46	Manual de funcionalidades básicas do AvantData
<input type="checkbox"/>	AvantData - ADaS	1.0.0.0	2021-04-20 15:58:12	Folder da oferta AvantData como serviço - ADaS
<input type="checkbox"/>	Arquitetura AvantData	2.0.0.0	2021-06-25 17:10:06	Arquitetura da plataforma AvantData com módulos.
<input type="checkbox"/>	Apresentação AvantData	16.0	2021-06-25 17:14:18	Apresentação institucional AvantData, com combate a fraudes e resposta a incidentes.
<input type="checkbox"/>	Requisitos para a Realização de PoC AvantData	1.0.0.0	2021-10-06 11:07:40	Requisitos para a Realização de PoC AvantData
<input type="checkbox"/>	Planejamento de Execução de Serviços para PoC AvantData	1.0.0.0	2021-10-06 11:08:31	Planejamento de Execução de Serviços para PoC AvantData

Figura 42 – Página Documentos