avantsec

Soluções de Vanguarda em Segurança da Informação

MANUAL AVANTDATA

Anexo - Entradas de Dados

O AvantData possui suporte, sem a adição de recursos externos à ferramenta, para recebimento e correlacionamento de dados vindos de fontes externas por meio dos seguintes protocolos, formas de acesso a SGBD, ou formatos de arquivos/dados:

1.Protocolos:
CIFS FTP LDAP HTTP(S) IPFIX J-Flow LDAP NetFlow SCP SFlow SNMP (v1, v2, v2c e v3) Syslog (UDP, TCP, TLS) TCP UDP
2.Bancos de dados:
Caché InterSystems Elasticsearch Hadoop HIVE

HBase JDBC MariaDB MEMCACHED MongoDB MSSQLServer MySQL Neo4j ODBC Oracle PostgreSQL REDIS GRAPH REDIS JSON REDIS KV SQLite
3.Formatos de arquivo/dados:
CSV (com seletor de delimitadores) Json Microsoft Office PCAP Texto (W3C, Logs *nix, Arquivos texto em geral) XML YAML Avro file
4.APIs
Pode ser feita a obtenção de dados de APIs REST cadastradas pelo usuário, como descrito na seção 7.7.9

Tabela 1 - Meios de recebimento de dados

Os dados a serem recebidos podem estar comprimidos (ou não) em diferentes formatos. A descompressão irá depender da configuração dos conectores. É mostrado como fazer a configuração dos diversos conectores em *7.7 Entrada de dados.*

Os coletores e conectores do AvantData podem ser configurados para recebimento de dados das seguintes fontes:

* Algumas das APIs exigem licença adicional

1. APIs*
Amazon Top Sites ASN BadIPs

BadIPs IPs Info
BadIPs por País
Brand Alert
Censys.io
Censys.io
CheckPoint (LEA)
CISCO Umbrella
Contatos dos WebSites
Cuckoo
CVE – https://cve.circl.lu/api
CWE
DNS Lookup
DNS Shodan
Domain Availability
E-mail Verification
FireEye Isight
FireEye iSight
GeoLocation por IP
GoogleMaps
Grey noise
HPE
IBM X-Force
IP Reverso
IPs
MAEC
MISP
MITRE ATT&CK
Office 365/Microsoft 365 (Microsoft Graph API)
OpenVAS
ProxyMesh
Registrant Alert
Reputação do domínio
Reverse MX
Reverse NS
Screenshot
Seclytics
Seclytics ASNs
Seclytics CIDRs
Seclytics Domínios
Seclytics IPs
Shodan
Shodan
Shodan Ips (Pesquisa por bloco de IPs)
SonarQube
SSLMate
SSLMate
STIX2
Tenable SC
Vírus Total IPs (Pesquisa por bloco de IPs)

Vírus Total Scan URLs Vírus Total URLs VirusTotal VPNIO WebSite Categorization Whois Whois History Whois URL e IP WHOISXML
2. Outros softwares:
3COM (SW/RO) Active Directory Airmagnet Aker Amazon S3 Apache Apache Drill Apache Kafka Apache SPARK API Restful Beyondtrust BitDefender CEF CheckPoint CISCO (SW/RO) Cisco ASA CiscoVPN Citrix Xenserver Cyberark Clamav CrowdStrike Dell (SW/RO) Enterasys (SW/RO) Extreme (SW/RO) F5 Big-IP AFM F5 Big-IP APM F5 Big-IP AWAF F5 Big-IP DNS / GTM F5 Big-IP LTM Fortinet Fortinet VPN ForeScout FreeBSD GlobalProtect VPN HAProxy Hauweii (SW/RO) HP (SW/RO)

Hyper-V
IBM (SW/RO)
IIS
IPFW
Jboss
Karspersky
KVM
Linux (AvantAgent / Syslog)
MACOS
McAfee Endpoit Security
McAfee ePolicy Orchestrator
Microsoft Active Directory
Microsoft Exchange
Microsoft Graph API
Microsoft IIS
Microsoft Office 365
Microsoft OneDrive
Microsoft Sharepoint
Microsoft Windows (eventos)
Microsoft Windows (PowerShell)
Microsoft Windows (Osquery)
NetSkope
Nginx
OpenLDAP
OpenVPN
OracleVM
Palo Alto
PAM - Privileged Access Management (Syslog)
PFsense
PFSense
PostFix
Qmail
Safe Orange (UTM)
Sendmail
Senha Segura (PAM)
Sophos
Sophos VPN
Squid
Symantec
Tenable SC
Tomcat
TrendMicro
VMware
Zimbra

Tabela 2: Fontes de dados nativas

O AvantData provê a funcionalidade de desenvolvimento/configuração de conectores customizados, visando a coleta de dados não suportados nativamente pela plataforma. Isso pode ser feito por meio de diversos métodos (e todos os serviços/protocolos previstos neste documento), incluindo: novos parsers, scripts de coleta em Python, cadastro/integração de APIs, etc.

Base Pré-Instalada

Com base na tabela de fontes de dados nativas acima, assim como o resultado das implantações da solução em ambiente diversos, segue lista da base pré-instalada de objetos (painéis, dashboards, gráficos, relatórios, regras de correlacionamento, alertas e APIs), por categoria, incrementada a cada atualização do produto (e também disponível na base de modelos, acessada via portal do cliente, disponível em – https://avantdata.avantsec.com.br/portal/login/:

1.Segurança e Infraestrutura de rede:
Firewall AntiMalware Autenticação (ambientes Microsoft e *Unix) Switches (Syslog) Balanceadores de Carga Proxies (forward e reverso) Roteadores (Syslog) Plataformas de Virtualização Conformidade Acesso Internet (Syslog)
2.Aplicações, Serviços e Sistemas:
Servidores WEB Bancos de Dados (SGBDs) Servidores de Aplicação

Esta estrutura, conforme atualizada, se reflete na pasta “Modelos”, encontrada na solução conforme o contexto (dashboards, regras de correlacionamento, etc):


AVANTDATA
AvantData
Modelos
Segurança e Infraestrutura
Firewall
AntiMalware
Autenticação
Switches
Balanceadores de Carga
Proxies
Roteadores
Plataformas de Virtualização
Conformidade
Acesso Internet
Aplicações, Serviços e Sistemas
Servidores WEB
Bancos de Dados
Servidores de Aplicação