Progress

Detection Methods and 3rd Party Flow Data

This document lists detection methods and their ability to work using high quality flow data from standard flow exported like routers, switches, or other flow exporters. It assumes that 3rd party flow data are accurate, does not miss any attribute including TCP flags, but are limited to L3 and L4 visibility. The methods and their sub methods that do not work or work partially with 3rd party flow data require additional information from application layer (L7) provided by Flowmon Probes.

Applicable for Flowmon ADS 12.1 or newer.

Method	Submethod	Working with standard quality flows
ALIENDEV	KnownSegment	Yes
ALIENDEV	IPBased	Yes
ALIENDEV	MACBased	No
ANOMALY	SentPackets	Yes
ANOMALY	ReceivedPackets	Yes
ANOMALY	SentBytes	Yes
ANOMALY	ReceivedBytes	Yes
ANOMALY	SentFlows	Yes
ANOMALY	ReceivedFlows	Yes
ANOMALY	Peers	Yes
ANOMALY	ActiveDevices	Yes
ANOMALY	Requests	Yes
ANOMALY	Responses	Yes
ANOMALY	CountUnpaired	Yes
ANOMALY	TCPFlow	Yes
ANOMALY	UDPFlow	Yes
ANOMALY	OtherFlow	Yes
ANOMALY	PercentUnpaired	Yes
ANOMALY	ProvidedServices	Yes
ANOMALY	UsedServices	Yes
BITTORRENT	General	Yes
BLACKLIST	Host	Yes
BLACKLIST	Service	Yes
BLACKLIST	Web	No
BLACKLIST	Domain	No
BLACKLIST	JA3	No
BPATTERNS	Depends on the sub method	Partially
BROKENSEN	Bytes	Yes
BROKENSEN	Duration	Yes
BROKENSEN	Packets	Yes
BROKENSEN	Period	Yes

COUNTRY	IncreasedCommunication	Yes
DHCPANOM	FakeServer	Yes
DHCPANOM	ServerOverloadIP	Yes
DHCPANOM	ServerOverloadNetwork	Yes
DHCPANOM	OversendingClientIP	Yes
DHCPANOM	OversendingClientNetwork	Yes
DHCPANOM	ServerChange	Yes
DICTATTACK	SMTPProtocol	Yes
DICTATTACK	SambaProtocol	Yes
DICTATTACK	VNCProtocol	Yes
DICTATTACK	IMAPProtocol	Yes
DICTATTACK	POP3Protocol	Yes
DICTATTACK	FTPProtocol	Yes
DICTATTACK	SSHProtocol	Yes
DICTATTACK	TelnetProtocol	Yes
DICTATTACK	RDPProtocol	Yes
DICTATTACK	HTTPProtocol	Yes
DIRINET	General	Yes
DIVCOM	VariousCommunication	Yes
DNSANOMALY	TCPHighTraffic	Yes
DNSANOMALY	ForbiddenServer	Yes
DNSANOMALY	UnusualServer	Yes
DNSQUERY	QueriesCount	Yes
DOHDET	BehavioralDetection	Yes
DOHDET	KnownServers	Partially
DOS	Volumetric	Yes
DOS	SYNFlood	Yes
DOS	FIN2WAIT	Yes
GEODIST	EnthropyChange	Yes
HIGHTRANSF	General	Yes
HONEYPOT	General	Yes
HTTPDICT	SameSize	Yes
ICMPANOM	DestinationUnreachIP	No
ICMPANOM	DestinationUnreachNetwork	No
ICMPANOM	SmurfAttack	No
ICMPANOM	ICMPScan	No
ICMPANOM	PingFlood	No
ICMPANOM	LargePayload	No
IPV6TUNNEL	TeredoTunnel	Yes
IPV6TUNNEL	6in4Tunnel	Yes
L3ANOMALY	IPSpoof	Yes
L3ANOMALY	SourceMulticast	Yes
L3ANOMALY	SameIPs	Yes
MULTICAST	MulticastDetection	Yes
NATDET	General	No
PEERS	PeersIncrease	Yes
RANDOMDOMAIN	General	No
RDPDICT	General	Yes

REFLECTDOS	Amplification	Yes
SCANS	PortBased	Yes
SCANS	UDP	Yes
SCANS	TCPSYN	Yes
SCANS	TCPFIN	Yes
SCANS	TCPNull	Yes
SCANS	TCPXmas	Yes
SCANS	ARP	No
SIPFLOOD	Invite	No
SIPFLOOD	Register	No
SIPPROXY	General	No
SIPSCAN	Register	No
SIPSCAN	Options	No
SIPSCAN	Invite	No
SMTPANOMALY	UndefinedServer	Yes
SMTPANOMALY	SpammingClient	Yes
SRVNA	TCPService	Yes
SRVNA	UDPService	Yes
SRVNA	TCPServiceReset	Yes
SSHDICT	General	Yes
TEAMVIEWER	General	Partially
TELNET	PortBased	Yes
TOR	ClientDirectAccess	Yes
TOR	ServerAccess	Yes
UPLOAD	General	Yes
VOIP	General	Yes
VPN	BehavioralDetection	Yes
VPN	OpenVPN	Yes
VPN	MSPPTP	Yes
VPN	IPSec	Yes
VPN	InternetTunnel	Yes
VPN	Hamachi	Yes
WEBSHARE	SiteVisit	Yes
WEBSHARE	SiteTransfer	Yes