Seznam modelů Flowmon ADS

platné od 1.5.2017

Flowmon ADS		Lite FPC-ADS-L	Standard FPC-ADS-S	Business FPC-ADS-B	Corporate FPC-ADS-C	Enterprise FPC-ADS-E	Ultimate FPC-ADS-U
ZPRACOVÁNÍ DAT	**Datové toky**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	Externí datové zdroje	NE	Reputační databáze (IP adresy, domény, hostname, URL)				
	Detekční metody	Základní	Rozšířené	Kompletní			
	Detekce VoIP/SIP anomálií	NE	ANO				
REPORTOVÁNÍ UDÁLOSTÍ	**Reportování a alertování**	E-mail notifikace, PDF		E-mail, SMS, Syslog, SNMP, spuštění záchytu paketů, spuštění skriptu			
	Podpora SIEM systémů	NE		Události v CEF (syslog), SNMP trap			
VÝKONNOSTNÍ PARAMETRY	**Výkon (toků/s) na každou FCP instanci**	100	1000	2000	3000	4000	5000
	Velikost sítě (počet IP adres)	250	1000	5000	10000	20000	50000
	FCP instance	1	1	2	3	3	3
UŽIVATELSKÉ ROZHRANÍ	**Vizualizace událostí**	Dashboard Detaily, Důkazy	Dashboard, Detaily, Interaktivní, Důkazy				
	Agregované události	NE	ANO				
	Integrace s nástroji třetích stran	Web. odkazy, diagnostika (ping, tracert)		+ LDAP/AD dotazy	+ McAfee ePo dotazy		
	Audit změn konfigurace	NE		ANO			

FCP instance (flow collection & processing instance) představuje počet nezávislých instancí zpracovávající flow data s možností vytvoření instance detekční metody se specifickou konfigurací. Každá FCP může mít vlastní konfiguraci zpracování flow statistik v rámci dané FCP. Ve verzi Flowmon ADS Ultimate lze upravit počet FCP instancí i výkon na každou instanci.

SIEMy HP Arcsight, IBM QRadar, Enterasys nebo Juniper jsou podporovány přímo (CEF formát zpráv). Ostatní (Trustwave, RSA, atd.) je možné integrovat na základě analýzy Syslog zpráv nebo SNMP notifikací. Integrace není zahrnuta v ceně produktu. Pro více informací o podporovaných SIEM systémech viz dokument Flowmon & SIEM – Seamless Integration.

Flowmon Threat Intelligence je prémiová cloudová služba, která získává informace o aktuálních útočnících, infikovaných stanicích či command & control centrech. Tyto informace využívá pro detekci jakékoliv podezřelé komunikace v síti. Služba Flowmon Threat Intelligence také umožňuje aktualizaci vzorů chování detekčních metod a tím detekovat nejnovější hrozby. Tato služba je dostupná pro všechny zákazníky s platnou službou Gold Support.

Seznam detekčních metod pro jednotlivé verze Flowmon ADS je v popsán v dokumentu „List of Flowmon ADS Detection methods“ na support portálu, který přístupný po registraci. Výkon jednotlivých verzí Flowmon ADS je uváděn pro smysluplnou konfiguraci a odpovídající dostupné výpočetní zdroje na Flowmon sondě a Flowmon kolektoru.

Flowmon Networks a.s.

info@flowmon.com