Flowmon Networks

Driving Network Visibility

Seznam modelů Flowmon ADS verze ISP

Platné od 1.5.2017

ISP verze systému Flowmon ADS jsou speciálně navrženy a optimalizovány pro poskytovatele datových služeb a datová centra pro zvýšení bezpečnosti datové sítě a odhalení potenciálně nežádoucích aktivit. Pro dosažení vyššího výkonu je u těchto verzí možné použít vzorkování (samplování).

Flowmon ADS ISP		ISP 1	ISP 4	ISP 10	ISP 40	ISP 100	ISP 400
ZPRACOVÁNÍ DAT	**Datové toky**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	Externí datové zdroje	Reputační databáze (IP, host name, domain name, URL)					
REPORTOVÁNÍ UDÁLOSTÍ	**Reportování a alertování**	E-mail, PDF, Syslog, SNMP, spuštění záchytu paketů, spuštění skriptu					
	Podpora SIEM systémů	Události v CEF (Syslog), SNMP trap					
VÝKONNOSTNÍ PARAMETRY	**Výkon (toků/s) po samplování**	5000	5000	10000	10000	15000	15000
	Šířka pásma	1 Gbps	4 Gbps	10 Gbps	40 Gbps	100 Gbps	400 Gbps
	Podpora vzorkování	ANO, na úrovni toků					
	FCP instance	1	2	2	3	3	4
UŽIVATELSKÉ ROZHRANÍ	**Vizualizace událostí**	Dashboard, Detaily, Interaktivní, Důkazy					
	Audit změn konfigurace	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.

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.

Detekční metody zahrnují kontrolu konzistence vstupních dat, detekci infikovaných zařízení, odhalování slovníkových útoků na síťové služby, anomálie poštovný komunikace a rozesílání SPAMu, skenování portů, anomálie DNS provozu, zneužití služby Telnet, anomálie ICMP provozu, nedostupné služby, přenos velkého množství dat, anomálie v provozu na síťové vrstvě, tzv. reflection/amplification DoS/DDoS útoky, komunikaci na potenciálně závadné IP adresy vč. honeypot komunikace.

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.