FlowMon – ADS – Behaviorální analýza sítě

Systém detekce anomálií pro vnitřní i vnější bezpečnost sítě

FlowMon ADS je řešení přinášející novou dimenzi využití statistik o provozu datové sítě (NetFlow, IPFIX, jFlow, NetStream). Díky unikátní technologii tzv. behaviorální analýzy (Network Behavior Analysis) je možné identifikovat hrozby, které překonaly zabezpečení na perimetru, byly zavlečeny do datové sítě jiným způsobem nebo pro ně dosud neexistuje signatura. Automatická detekce bezpečnostních incidentů, anomálií provozu datové sítě a konfiguračních problémů výrazně zjednodušuje správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.

Přínosy a výhody

- Automaticky identifikuje hrozby, útoky, incidenty a konfigurační problémy
- Vhodně doplňuje nástroje na bázi signatur a zvyšuje bezpečnost
- Pracuje na úrovni sítě bez nutnosti cokoliv instalovat na koncové stanice
- Odhaluje hrozby, útoky, úniky dat a incidenty, minimalizuje tak jejich finanční dopady
- Proaktivně identifikuje možné zdroje a příčiny problémů
- Detekuje nežádoucí aktivity uživatelů a zneužívání datové sítě
- Plugin pro řešení FlowMon, jednoduchá instalace a zhodnocení stávajících investic

Spojení bezpečnosti a správy sítě

FlowMon ADS kombinuje funkce důležité pro správce datové sítě, bezpečnostní nebo IT manažery do jediného nástroje schopného poskytovat velmi přesné a spolehlivé informace ve formě událostí. Díky automatickým notifikacím a reportingu je možné systém provozovat jako tzv. standalone řešení. Integrace s dohledovými systémy, incident handling systémy a systémy typu SIEM podporuje nasazení v prostředí rozsáhlých podnikových sítí.

Interaktivní dashboard poskytuje celkový přehled o stavu datové sítě s možností získat okamžitě ke každé události detailní informace o provozu, který danou událost způsobil. Alternativní pohledy na události, včetně jejich vizualizace formou orientovaných grafů, umožňují operátorovi analyzovat příčiny a relevantní okolí události. Samozřejmostí je integrace na síťové služby DNS, WHOIS nebo geolokace a vizualizace na mapě světa. Díky službě FlowMon Threat Intelligence získává FlowMon ADS informace z reputačních databází pro přesnější detekci infikovaných stanic nebo odhalení komunikace s botnet command & control centry.

Analýza signatur versus behaviorální analýza

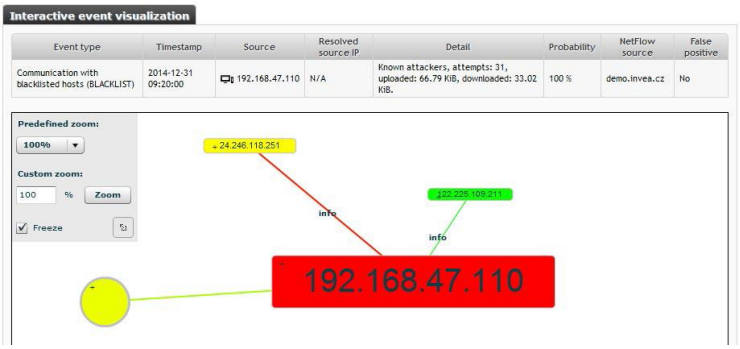
Systémy typu IDS, IPS nebo antiviry používané pro ochranu perimetru nebo koncových stanic identifikují hrozby a incidenty na základě tzv. signatur. Jedná se o definice známého malware a nežádoucího software. Oproti tomu behaviorální analýza umožňuje odhalovat dosud neznámé nebo specifické hrozby, pro které signatura neexistuje. FlowMon ADS implementuje desítky pokročilých algoritmů s prvky umělé inteligence, které vyhodnocují chování každého jednotlivého zařízení v síti, dynamicky stanovují profily očekávaného chování a upozorňují na nestandardní odchylky. Díky tomu představuje FlowMon ADS ideální nástroj pro odhalování pokročilých útoků a hrozeb typu APT (Advanced Persistent Threat).

Detekce incidentů a anomální chování

FlowMon ADS automaticky identifikuje celou řadu bezpečnostních a provozních incidentů, anomálie provozudatové sítě nebo nežádoucí chování uživatelů.

Typicky se jedná o:

- **Útoky na síťové služby** s cílem získat neoprávněný přístup k zařízení nebo službě.
- **Infikované stanice** a komunikaci s potenciálně nežádoucími IP adresami, mezi které patří botnet command & control centra, známí útočníci nebo systémy šířící nevyžádanou poštu a malware na základě pokročilých reputačních databází.



- **Anomálie DNS provozu** indikující infikované stanice, nežádoucí software nebo chybné konfigurace síťových služeb.
- **Anomálie DHCP provozu** indikující stanice pokoušející se o odposlech síťové komunikace, podvržené adresy (spoofing) nebo chybné konfigurace.
- **Skenování portů** a obdobné projevy infikovaných stanic nebo nežádoucích aktivit útočníků či interních uživatelů.
- **Potenciálně nežádoucí síťové aplikace** jako jsou P2P sítě nebo on-line komunikátory.
- **Anonymizační služby**, jako např. TOR (The Onion Router) nebo obcházení proxyserveru.
- **Výpadky nebo špatné konfigurace** síťových služeb.
- **Potenciální úniky dat** a využívání služeb pro výměnu dat na internetu.
- **Útoky na internetovou telefonii**, ústředny a přístroje připojené do IP sítě.
- **Nestandardní poštovní komunikace** a šíření spamu.
- **Zneužívání zranitelností** serverů a síťových služeb pro DDoS útoky.

Klíčové vlastnosti systemu

- Snadná instalace na sondu nebo kolektor
- Podpora NetFlow v5/v9, IPFIX, jFlow, NetStream, sFlow (částečně)
- Podpora NBAR2, analýza HTTP informací, MAC adres, VoIP informací
- Deduplikace a párování datových toků (RFC 5103)
- Multitenance a řízení uživatelských oprávnění pro separaci jednotlivých uživatelů
- Notifikace událostí e-mailem (variabilní formáty) a export událostí (syslog, SNMP, CSV)
- Modely pro korporátní sítě i rozsáhlé sítě poskytovatelů datové konektivity (ISP)

Snadné nasazení a rozšiřitelnost

Veškeré metody detekce anomálií jsou dostupné tzv. out-of-box, což umožňuje okamžité nasazení bez nutnosti náročné konfigurace nebo úprav pro dané prostředí. FlowMon ADS využívá pro analýzu provozu více než 50 různých algoritmů s prvky umělé inteligence (dynamické profilování standardního chování a detekce odchylek, dynamické rozhodovací stromy, strojové učení, prediktivní analýza časových řad, algoritmy shlukové analýzy), které analyzují provoz z různých úhlů pohledu a identifikují podezřelé stanice a události. Díky integrovanému konfiguračnímu průvodci, šablonám typických konfigurací pro různá prostředí a správě falešných poplachů (false positives) implementace nevyžaduje expertní znalosti.