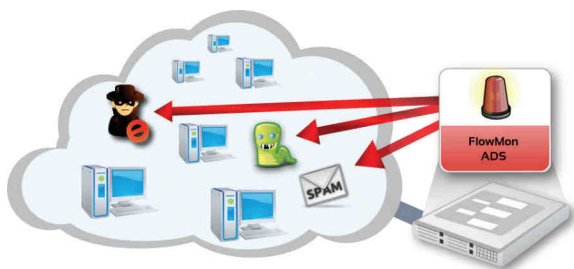


ÚVOD

Řešení FlowMon je možné rozšiřovat pomocí tzv. pluginů, které se instalují na FlowMon sondy či kolektory a přináší přidanou funkcionalitu. Velmi oblíbeným pluginem je FlowMon ADS, což je moderní systém detekce anomálií a nežádoucího chování na síti založený na permanentním vyhodnocování a analýze NetFlow dat. Hlavním cílem pluginu je odhalení provozních problémů a zvýšení vnější i vnitřní bezpečnosti datové sítě. Hlavní výhodou proti běžným IDS systémům je orientace na celkové chování zařízení na síti, což umožňuje reagovat na dosud neznámé nebo specifické hrozby, pro které není dostupná signatura.



HLAVNÍ FUNKCE A POUŽITÉ DETEKČNÍ METODY

FlowMon ADS plugin nabízí dva základní přístupy pro efektivní detekci anomálií a nežádoucího chování v síti. První přístup spočívá ve vyhledávání nežádoucího vzorů v komunikaci na síti. Avšak na rozdíl od jiných nástrojů není analyzován obsah jednotlivých paketů, ale komunikace jako celek (zdrojové a cílové IP adresy, použité porty, příznaky spojení, mezipaketové mezery, délka komunikace a mnoho dalšího). Díky tomu je možné snadno detekovat události, jakými jsou např. útoky (skenování portů, slovníkové útoky), nežádoucí aplikace (P2P síť, anonymizační služby), infikované počítače (viry, spyware) a řada dalších.

Druhý přístup je založen na vyhodnocování chování jednotlivých zařízení v síti a změně chování oproti jejich obvyklému stavu. Jedná se o moderní metodu označovanou jako behaviorální analýza. Hlavní výhodou spočívá v možnosti detekovat události, které jsou jinými systémy nezjistitelné a mohou se jevit jako legitimní – např. zcizená identita a hromadné kopírování důležitých firemních dat, nakažené zařízení (rozesílání spamu, snaha infikovat další stanice), provozní problémy (nefunkční aktualizace, nadměrná zátěž) a další.

KLÍČOVÉ VLASTNOSTI

- ▶ Plugin pro řešení FlowMon, jednoduchá instalace na sondu/kolektor
- ▶ Podpora NetFlow v5/v9, podpora IPv4 a IPv6
- ▶ Předdefinovaná sada pravidel pro odhalování nežádoucího vzorů chování
- ▶ Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti
- ▶ Budování dlouhodobých profilů chování zařízení na síti z pohledu služeb, objemů provozu a komunikačních partnerů
- ▶ Přehledný dashboard s okamžitou indikací problémů a top statistik
- ▶ Interaktivní vizualizace událostí
- ▶ Integrace informací ze služeb DNS, WHOIS, geolokační služby
- ▶ Implementace standardu Bidirectional flows (RFC 5103)
- ▶ Komplexní filtrování a prioritizování událostí s vazbou na reporting a alerty
- ▶ Automatizované výstupy prostřednictvím e-mailu

DETEKCE VNĚJŠÍCH I VNITŘNÍCH ÚTOKŮ

Prostřednictvím předdefinovaných vzorů chování a behaviorální analýzy systému FlowMon ADS je možné detekovat následující anomálie a nežádoucí chování v počítačové síti:

Útoky (skenování portů, slovníkové útoky, denial of service, protokol telnet)

Anomálie datového provozu (DNS, multicast, nestandardní komunikace)

Anomálie v chování zařízení (změna dlouhodobého profilu chování zařízení)

Nežádoucí aplikace (P2P síť, instant messaging, anonymizační služby)

Interní bezpečnostní problémy (viry, spyware, botnety)

Poštovní provoz (odchozí spam)

Provozní problémy (zpoždění, nadměrná zátěž, reverzní DNS záznamy, nefunkční aktualizace)

PROFILY CHOVÁNÍ

Na základě dlouhodobých statistik o provozu jednotlivých zařízení na síti plugin FlowMon ADS automaticky sleduje a informuje o jakékoliv změně v jejich chování nebo v chování celé sítě. Profily chování budované pluginem FlowMon ADS zahrnují:

Objemy datového provozu (přenesená data, počty spojení)

Struktura služeb (využívané a poskytované služby)

Komunikační partneři

Vyhledávání serverů a klientů v síti

Vyhledávání služeb v síti

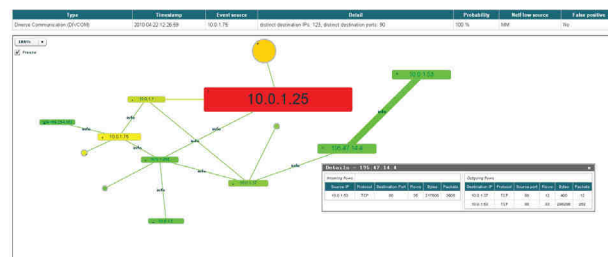
Celkový pohled na strukturu provozu

Detailní profil pro každou IP adresu, sledování trendů



INTERAKTIVNÍ VIZUALIZACE UDÁLOSTÍ

o detekovaných nežádoucích událostech je možné velmi snadno získat detailní informace, aby bylo možné provést taková opatření, která zamezí jejich dalšímu výskytu. Pro snazší a rychlejší práci jsou události vizualizovány ve formě orientovaných grafů, kdy se pomocí několika kliknutí uživatel dostane až na úroveň jednotlivých komunikací v síti.



Průzkum a vyhodnocení událostí formou orientovaných grafů sestavených na základě provozu na síti, který událost způsobil

Interaktivní průchod, zobrazení relevantního okolí události a drill-down až na úroveň jednotlivých datových přenosů

Export statistik o provozu na síti, které událost způsobil ve vhodné formě pro prokazování incidentů

HLAVNÍ PŘÍNOSY

- ▶ Detailní přehled o struktuře síťového provozu
- ▶ Kontrola dodržování bezpečnostních směrnic
- ▶ Odhalování vnitřních i vnějších útoků
- ▶ Rychlá diagnostika zpoždění sítě a služeb
- ▶ Prevence sdílení nelegálního obsahu
- ▶ Detekce nesprávných konfigurací sítě
- ▶ Monitoring kvality poskytovaných služeb
- ▶ Rychlá diagnostika zpoždění sítě, služeb a aplikací
- ▶ Odhalování infikovaných zařízení v síti
- ▶ Prevence používání ilegálního software
- ▶ Eliminace nežádoucích či škodlivých aplikací

SNADNÉ NASAZENÍ A ROZŠÍŘITELNOST

Plugin FlowMon ADS je navržen tak, aby jej bylo okamžitě možné nainstalovat a začít používat v různých prostředích. Je velmi operabilní díky tomu, že zahrnuje:

Šablony typických konfigurací pro různé typy sítě

Komplexní grafické reporty generované z aplikace na vyžádání

Upozorňování na nežádoucí stavy a situace prostřednictvím e-mailů

JAK ZÍSKAT PRODUKTY FLOWMON? →

Více informací o produktu FlowMon ADS získáte prostřednictvím výhradního distributora, kterým je společnost INVEA-TECH a.s.

www.invea.cz