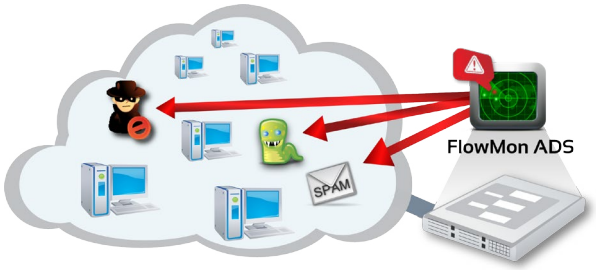
FlowMon ADS

Anomaly Detection System pro vnitřní i vnější bezpečnost sítě

Popis produktu

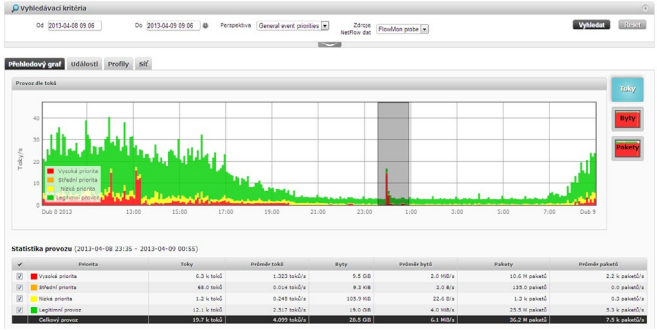
ÚVOD

FlowMon ADS je moderní systém detekce útoků, anomálií, pokročilých hrozeb a nežádoucího chování na síti založený na průběžném automatickém vyhodnocování a analýze statistik o provozu datové sítě (NetFlow/IPFIX) generovaných FlowMon sondami, aktivními prvky (přepínače, směrovače) či jinými nástroji (např. firewall). Cílem řešení je identifikace bezpečnostních incidentů, provozních problémů a celkové zvýšení bezpečnosti datové sítě. Hlavní výhodou proti běžným systémům detekce a prevence průniků 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 kombinuje řadu technik a metod umělé inteligence pro úspěšnou detekci bezpečnostních a provozních incidentů. Základními metodami jsou deduplikace a párování toků (RFC 5103), které zásadním způsobem zvyšují kvalitu primárních dat. Poté jsou aplikovány metody strojového učení a heuristické algoritmy, profilování chování a sledování jeho změny v čase, rozhodovací stromy pro sledování útoků a clusterovací algoritmy pro hledání shluků podobně se chovajících stanic a detekci tzv. outliers, tedy stanic, jejichž chování je v daném prostředí ojedinělé. Kombinací těchto metod je dosaženo vysoké spolehlivosti odhalení pokročilých útoků, moderních hrozeb a nežádoucích aktivit uživatelů.



KLÍČOVÉ VLASTNOSTI

- **Moderní NBA/NBAD systém pro detekci anomálií**
- **Desítky algoritmů pro identifikaci bezpečnostních a provozních incidentů**
- **Sledování dlouhodobých profilů chování zařízení na síti z pohledu služeb, objemů provozu a komunikačních partnerů**
- **Přehledný dashboard s okamžitou indikací incidentů a zobrazení top statistik**
- **Automatické detailní reporty**
- **Podpora NetFlow v5/v9, IPFIX, NetStream, jFlow včetně NBAR2, HTTP položek, MAC adres a další**
- **Deduplikace a párování toků**
- **Export událostí do SIEM systémů (syslog a CEF)**
- **Rozšiřující modul pro řešení FlowMon**
- **Jednoduchá instalace na sondu/kolektor**
- **Modely pro korporátní sítě i sítě ISP**

DETEKCE ANOMÁLIÍ A NEŽÁDOUCÍHO CHOVÁNÍ

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

Útoky - skenování portů, slovníkové útoky, denial of service, útoky prostřednictvím telnet protokolu a další,
Anomálie datového provozu - DNS, ICMP, DHCP, multicast, nestandardní komunikace,
Anomálie v chování zařízení - změna dlouhodobého profilu chování zařízení, změna chování sítě,
Nežádoucí aplikace - P2P sítě, Instant messaging, anonymizační služby, TOR, TeamViewer,
Bezpečnostní incidenty - viry, spyware, botnety, cizí zařízení v síti, komunikace s IP adresami na blacklistech,
Poštovní provoz - odchozí spam, chybná konfigurace,
Provozní problémy - zpoždění, nadměrná zátěž, reverzní DNS záznamy, nefunkční aktualizace,
Potenciální únik dat a informací - upload dat na veřejné servery, webová úložiště, podezřelé destinace.

INVEA-TECH a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@invea.com
www.invea.com

FlowMon ADS

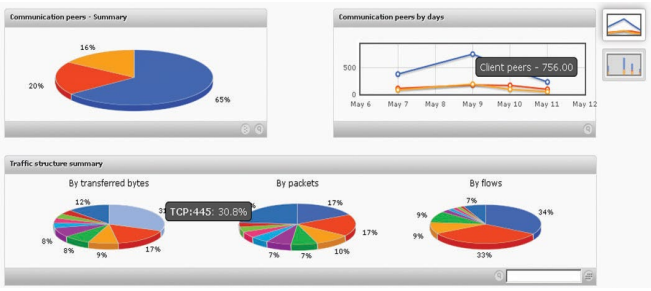
Anomaly Detection System pro vnitřní i vnější bezpečnost sítě

Popis produktu

PROFILY CHOVÁNÍ

Systém FlowMon ADS automaticky sleduje síť a na základě dlouhodobých statistik o provozu jednotlivých zařízení a informuje o změně v jejich chování nebo v chování celé sítě. Profily chování budované řešením FlowMon ADS zahrnují:

Objemy datového provozu - přenesená data, počty spojení,
Struktura služeb - využívané a poskytované služby,
Komunikační partneři - komunikující IP adresy,
Celková aktivita zařízení,
Detailní profil pro každou IP adresu, sledování trendů.



INTERAKTIVNÍ VIZUALIZACE UDÁLOSTÍ

Řešení poskytuje detailní informace o detekovaných nežadoucích událostech a bezpečnostních incidentech, 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.

Mezi další metody vizualizace událostí patří:

Interaktivní dashboard pro okamžitý přehled incidentů,
Průzkum a vyhodnocení událostí formou orientovaných grafů zobrazujících provoz na síti, který událost způsobil,
Interaktivní průchod, zobrazení relevantního okolí události a drill-down až na úroveň jednotlivých komunikací,
Export statistik o provozu na síti, které událost způsobily ve formě vhodné k prokazování incidentů.

HLAVNÍ PŘÍNOSY

- **Detekce provozních a bezpečnostních problémů**
- **Odhalování vnitřních i vnějších útoků, pokročilých hrozeb a chybných konfigurací sítě**
- **Kontrola dodržování bezpečnostních směrnic**
- **Odhalování potenciálních úniků dat**
- **Eliminace nežádoucích aplikací**
- **Odhalování infikovaných zařízení v síti**
- **Prevence používání nežádoucího software a sdílení nelegálního obsahu**
- **Kontrola odchozího provozu ze sítě, ochrana dobrého jména organizace**

SNADNÉ NASAZENÍ A ROZŠÍŘITELNOST

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

Šablony typických konfigurací pro různé typy sítí,
Konfiguračního průvodce pro okamžité nasazení,
Komplexní grafické reporty rozesílané automaticky nebo generované z aplikace na vyžádání,
Upozorňování na nežádoucí stavy a situace prostřednictvím pokročilého systému notifikací,
Integraci s dohledovými systémy a SIEM systémy prostřednictvím syslog (CEF formát) a SNMP,
Integraci s incident handling systémy prostřednictvím e-mailového rozhraní,
Řízení uživatelských oprávnění pro detailní nastavení přístup k datům,
Integraci informací ze služeb jakou jsou DNS, WHOIS a geolokační služby.

JAK ZÍSKAT PRODUKTY FLOWMON?

Obraťte se, prosím, na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či přímo navrhneme projekt monitorování Vaší sítě.

www.invea.com

INVEA-TECH a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@invea.com
www.invea.com