Komplexní bezpečnostní monitoring a detekce pokročilých hrozeb

Účel dokumentu

Množství IT systémů a zařízení v organizacích již přerostlo hranici, kdy je bylo možné sledovat člověkem. Je naprostou nezbytností mít zavedený pokročilý monitoring, aby správci byli co možná nejdříve informování, co se děje. Toto platí pro provozní monitoring systémů, ale dnes i stejnou měrou pro bezpečnostní monitoring, který byl dříve opomíjen. V případě bezpečnosti je třeba mít detailní přehled, co se na serverech, stanicích, aplikacích i bezpečnostních prvcích děje a to 24 hodin denně. Od takového řešení je navíc vyžadováno nejen, aby trvale kvalitně monitorovalo, co se děje, ale i uplatnilo jistou míru inteligence a tím pomohlo bezpečnostním technikům identifikovat ty nejzávažnější hrozby.

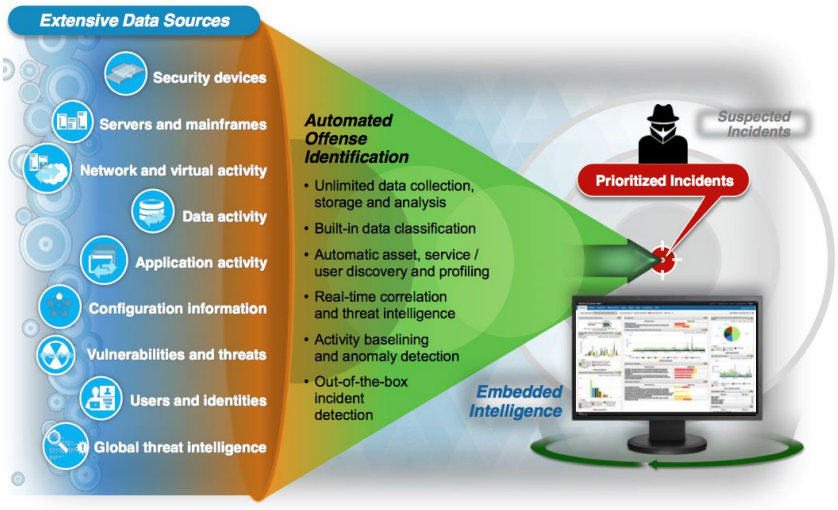
Tento dokument popisuje:

- Roli systému SIEM v bezpečnostním monitoringu
- Roli monitoringu provozu datové sítě pro detekci pokročilých útoků a anomálií

Výzva

Prvním krokem k bezpečné infrastruktuře je ochrana sítě na jejím perimetru. Blokovat nežádoucí provoz pouze pomocí pevně nastavených pravidel na firewallu již dlouho není dostatečné. Je nutné detekovat moderní hrozby, kontrolovat procházející data na aplikační úrovni, odhalovat zamaskovaný malware a další. Existuje mnoho bezpečnostních prvků, které řeší vždy úzce specializovanou oblast a chrání vždy jen proti danému způsobu útoků. Útočníci však využívají nejen technické zranitelnosti konkrétních produktů, ale kombinaci mnoha faktorů především principiálního rázu, a tím překonají systém ochrany jedním prvkem.

Proti takto pokročilým útokům vznikla ochrana v podobě systémů nazývaných jako *Security Intelligence and Event Management* (SIEM). Jedná se o jakýsi kokpit, zastřešení prvků v síti, jež systém monitoruje a pomocí zabudované inteligence se snaží odhalit nepatřičné chování.



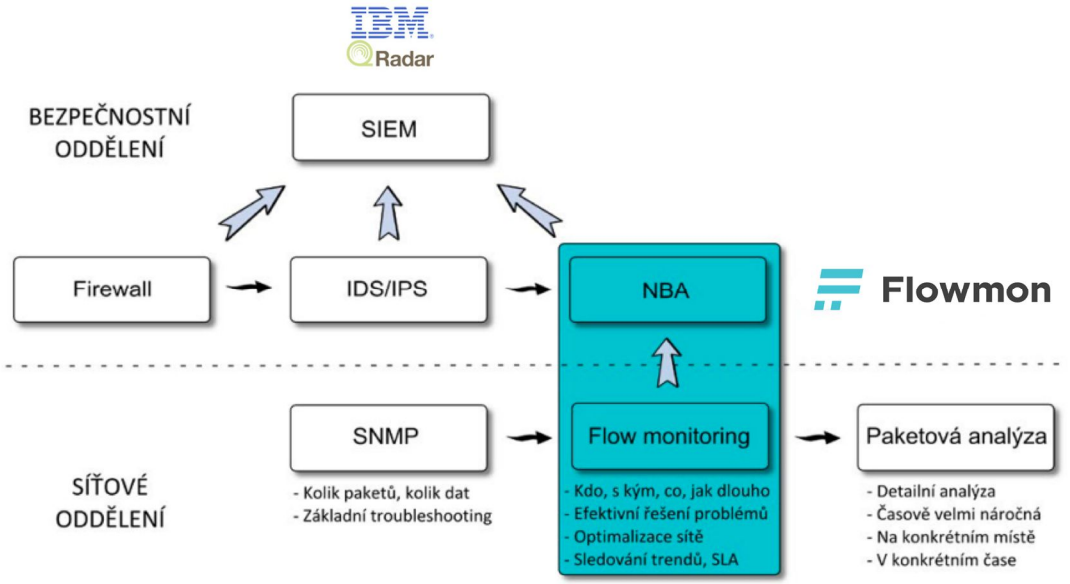
SIEM systém je díky informacím, které má o zařízeních v síti, schopen detekovat takové pokročilé hrozby, jako například přihlášení uživatele na lokální stanici, aniž by v docházkovém systému bylo evidováno, že by daný uživatel dnes přišel do kanceláře nebo pokus o přihlášení na administrátorský účet databázového serveru ze stroje, na který se minulý týden pokoušel někdo útočit a odhadnout heslo.

I přes to, že informace z prvků se zdá být dostatečná pro detekci pokročilých útoků, není tomu tak. Útočníci využívají taktiky, kdy svou nekalou činnost maskují za legitimní aktivitu tak, aby nebyla nápadná (maskování aplikace na jiném portu apod.) Pro takové případy je nutné doplnit systém SIEM o kvalitní monitorování síťové aktivity. Platí totiž tvrzení, že „síť nelže“. I když se podaří útočníkovi skrýt svůj průnik na databázový server, tak data, která se snaží odcizit, musí projít přes síť. Stejně tak i veškeré řídící pokyny v případě malware (BOT síť) jsou realizovány pochopitelně přes LAN i WAN.

Architektura řešení

Řešení proti moderním bezpečnostním hrozbám se skládá ze dvou pilířů – SIEM systému IBM QRadar SIEM a Flowmon s modulem ADS (Anomaly Detection Systém).

- IBM QRadar SIEM funguje jako centrální mozek, pro sběr a korelaci všech dostupných dat, a to jak z vlastních zařízení (logy), tak ze sítě.
- Viditelnost do interní sítě prostřednictvím monitorování síťového provozu zajišťuje řešení Flowmon společnosti Flowmon Networks podporující Cisco standardy Netflow v5, v9, NBAR2 ale i moderní standard IPFIX. Díky vlastním sondám a kompatibilitě se širokým okruhem síťových prvků je řešení možné nasadit do libovolné infrastruktury zákazníka.
- Automatickou detekci incidentů v interní síti provádí systém Flowmon ADS (Anomaly Detection System), který je součástí řešení Flowmon.



Díky tomuto spojení dvou bezpečnostních řešení v jedno ucelené získává zákazník schopnost detekovat neznámé hrozby, které jsou aktivní uvnitř sítě organizace. Zároveň detailní viditelnost do síťového provozu poskytuje přehled o provozních

problémech, anomáliích v síťovém provozu, či výskytu podezřelých aktivit v síti, které typicky předcházejí úspěšným útokům.

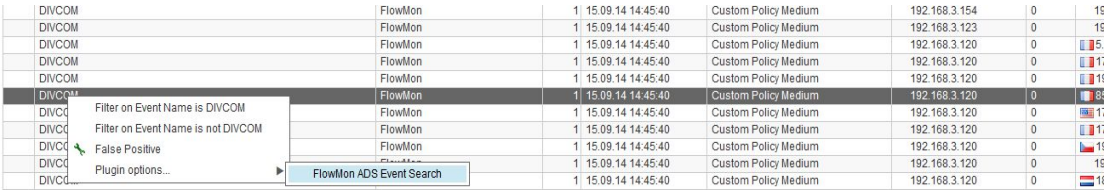
Přínosy řešení

Řešení pro bezpečnou a efektivní IT infrastrukturu je zaměřeno na poskytnutí komplexní ochrany sítě před známými i sofistikovanými hrozbami a zajištění bezpečné a stabilní infrastruktury. Klíčové přínosy řešení jsou:

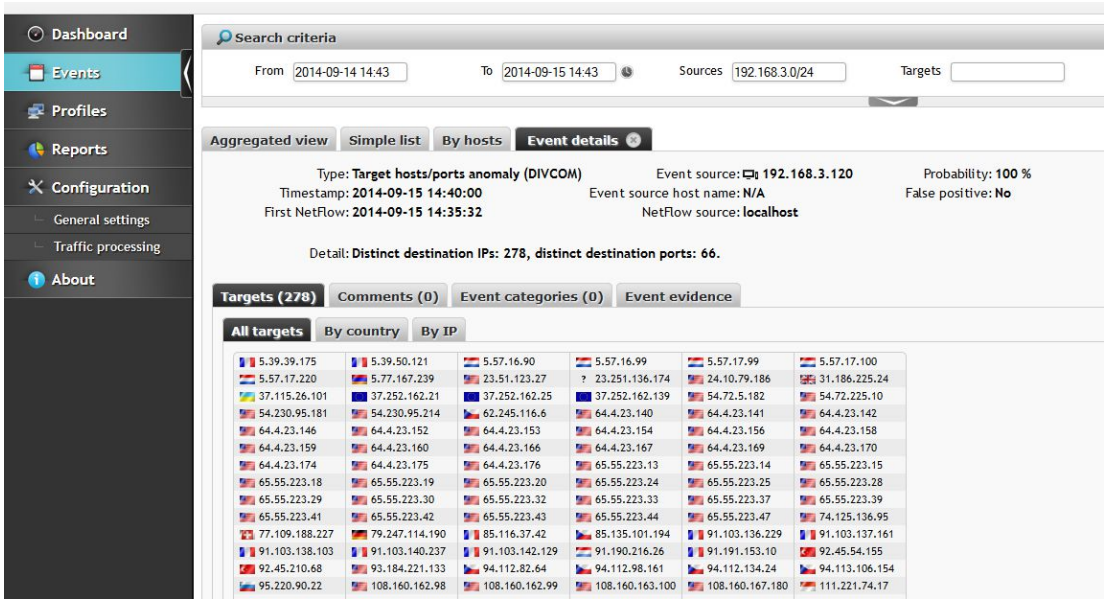
- detekce hrozeb ve vnitřní síti, pokud se jim do vnitřní sítě podaří proniknout,
- schopnost rozpoznat původní projevy hrozeb a jejich včasného zamezení,
- rychlé řešení incidentů v síti díky kompletní viditelnosti do aktivity jednotlivých prvků i síťového provozu,
- jednotný přístup pro uživatele,
- inteligentní korelační engine pro veškerá data, doplněný o pokročilý detekční modul síťové aktivity,
- škálovatelné a cenově příznivé řešení zajišťující komplexní ochranu sítě,
- zjednodušení a automatizace náročného a drahého manuálního procesu vyšetřování incidentů,
- snadná rozšiřitelnost řešení o řadu pokročilých modulů pro modelování útoků, správu rizik, scanner zranitelností, full-packet inspekci a dalších modulů,
- schopnost integrovat výstupy do jednoho centrálního dashboardu.

Integrace Flowmon řešení a IBM QRadar

Jednotného a vzájemně propojeného řešení je dosaženou obousměrnou integrací obou systémů. Flowmon ADS informuje SIEM systém o detekovaných incidentech a anomáliích prostřednictvím událostí doručovaných protokolem syslog, kde jsou tyto události automaticky analyzovány a korelovány s událostmi s ostatních prvků IT infrastruktury. V případě potřeby dalších informací přímo ze systému Flowmon je možné prostřednictvím kontextového menu v uživatelském prostředí QRadar přejít do systému Flowmon na detaily příslušné události a záznamy o síťovém provozu.



Integrace je připravena v podobě instalačního balíčku s průvodní dokumentací pro IBM QRadar a jeho implementace je tak otázkou několika přímočarých kroků.



Proč řešení pro bezpečnou a efektivní IT infrastrukturu?

Unifikované řešení pro detekci pokročilých i neznámých hrozeb, postavené na dvou ve světě uznávaných technologických řešeních, které jsou vzájemně integrovány, zvyšuje úroveň bezpečnosti IT infrastruktury a schopnost bránit se pokročilým hrozbám a moderním útokům. Provázanost komponent do jednoho celku poskytuje uživateli komfortní práci s incidenty bez nutnosti obsluhovat řadu oddělených systémů.

Pro více informací

Pro více informací, prosím, kontaktujte svého IBM nebo Flowmon Networks partnera.

IBM Česká Republika, spol. s r.o.
V Parku 2294/4
148 00 Praha 4
Česká republika
www.ibm.cz

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno
Česká republika
www.flowmon.com