Partnerské školení

Flowmon ADS

Martin Ševčík, Presales Engineer

Flowmon
Driving Network Visibility

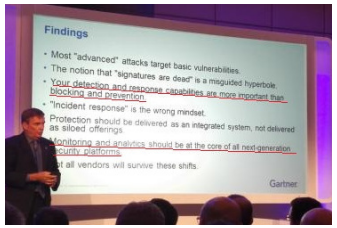
Flowmon ADS

Detekce anomálií & analýza chování sítě (NBA)

Flowmon
Driving Network Visibility

NBA – doporučená technologie

Gartner



Neil MacDonald
VP Distinguished Analyst
Gartner Security & Risk Management Summit

Recommendation

After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques.

- *Detekce a reakce jsou mnohem důležitější než blokování a prevence*
- *Monitorování a analýza by měla být jádrem všech bezpečnostních platforem příští generace*

Flowmon
Driving Network Visibility

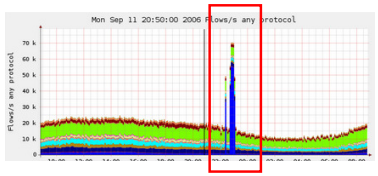
NBA

- **Pokrývá bezpečnostní mezeru** mezi koncovými body a perimetrem
- **Automaticky identifikuje hrozby**, útoky, incidenty a problémy s konfigurací
- **Doplňuje tradiční bezpečnostní nástroje** založené na podpisech
- **Aktivně upozorňuje** na neočekávané chování v síti

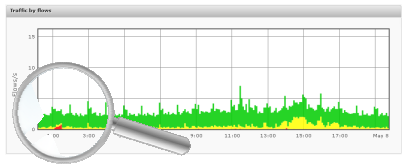
Flowmon
Driving Network Visibility

Detekce anomálií

- V čem se lišíme od ostatních nástrojů?



Běžné nástroje „detekce anomálií“ používají pouze statistické metody k detekci dopravních špiček a odchylek



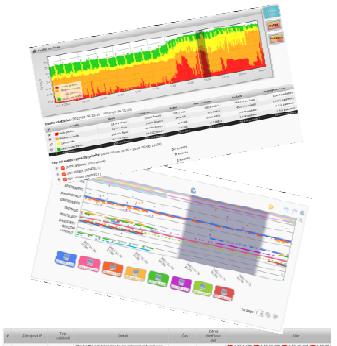
Flowmon analyzuje každý flow, detekuje i objemově nevýznamné anomálie a přesahuje tak tradiční statistické algoritmy

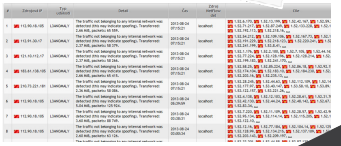
Flowmon
Driving Network Visibility

Technologie Flowmon ADS

Flowmon ADS

- Strojové učení
- Adaptivní baselining
- Heuristika
- Vzory chování
- Reputační databáze

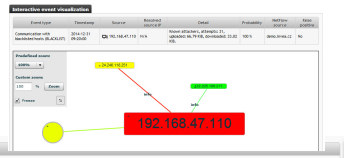


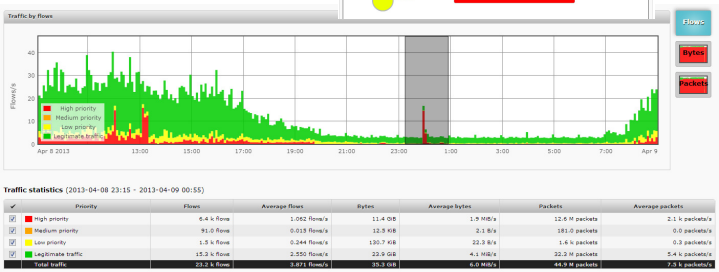


Flowmon
Driving Network Visibility

Vizualizace událostí

- Grafické rozhraní pro analýzu detekovaných událostí
  - Dashboardy a reporty
  - Interaktivní vizualizace

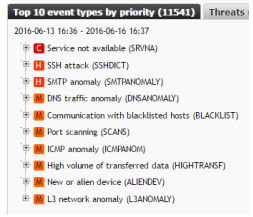


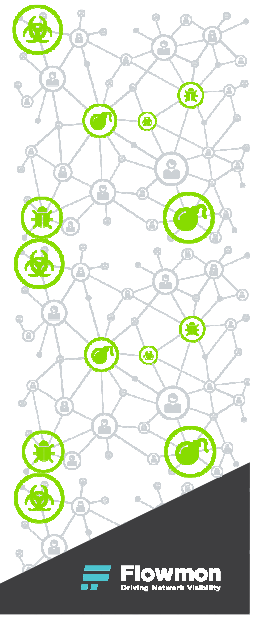


Flowmon
Driving Network Visibility

Detekční schopnosti ADS

- Útoky na síťové služby
- Infikovaná zařízení a komunikace s botnet C&C servery
- Skenování portů a dalších symptomů infikovaných zařízení
- Potenciální úniky dat a využívání služeb pro sdílení dat na internetu
- Výpadky síťových služeb nebo špatná konfigurace
- Nežádoucí aplikace jako jsou P2P, detekce obcházení PROXY, TOR
- Anomálie v provozu DNS, DHCP
- Útoky na VoIP, PBX, …
- Neočekávaný mailový provoz a SPAM





Flowmon
Driving Network Visibility

Uživatelsky definované metody pro detekci anomálií

- Za základě požadavků pokročilých uživatelů o možnost vytvářet vlastní detekční metody
- Detekce zaměřená na specifické scénáře následovaná standardním zpracováním událostí (priorita, notifikace, SIEM, …)
- Přínosy pro různá prostředí

Anomálie protokolu	HTTP UDP provoz	req_transferred > 104857600 AND protocol = 17 AND destination_port = 80
Specifický malware	Retefe2 banking trojan	http_url LIKE '/ICECVREU.js?%'
Regulární výrazy	SQL injection	Tools.re_match('.{1,4}[Oo][Rr].{1,4}\d.{1,3}\d', 'http_url') = 1
Detekce určitého OS	Windows XP	ua_os = 68 and ua_os_version = 5.1

Flowmon Driving Network Visibility

Uživatelsky definované metody pro detekci anomálií

- Definice vlastních detekčních metod pomocí syntaxe podobné SQL
- Popis syntaxe a příklady v uživatelské příručce

Uživatelský definovaný kód (unikátní ID) nebo behavior pattern

Popis účelu tohoto konkrétního behavior patternu

Popis události začne tímto textem

Zdroj události může být buď zdrojová nebo cílová IP adresa

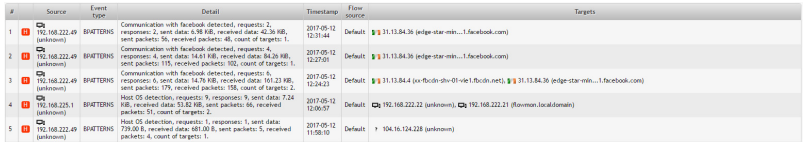
WHERE část SQL dotazu (povinná)

HAVING část SQL dotazu (nepovinná)

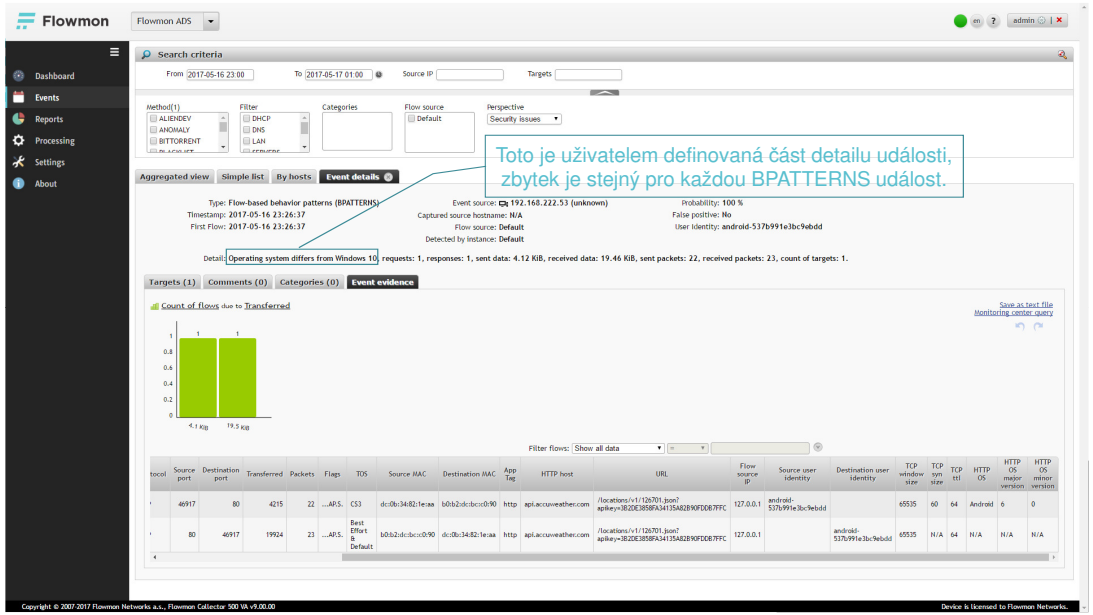
Flowmon Driving Network Visibility

Uživatelsky definované metody pro detekci anomálií

- Detekční metoda „Flow-based behavior patterns“ (**BPATTERNS**)
- Výsledkem detekce je **standardní událost**
  - Uživatelsky definované detaily, zahrnuje „Záznam události“
  - Přiřazení priority na základě perspektivy
  - Zahrnuty do emailových notifikací a PDF reportů
  - Export události do systémů třetích stran (syslog, SNMP trap)
  - Spuštění záchytu paketů nebo skriptu



Flowmon Driving Network Visibility



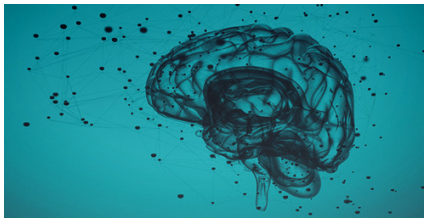
Příklady uživatelsky definovaných BPATTERNS

✓	Pattern code	Pattern description	Pattern detail	Pattern where clause	Pattern having clause	Active	Last change	Action
☐	FACEBOOK	Detection of communication with facebook	Communication with facebook detected	http_host LIKE '%facebook%' AND NOT destination_port = 53		Default	2017-05-11 22:04:47	
☐	INOUTRATIO	Detection of suspicious ratio in download/upload. Identification of potential data encryption via ransomware on shared hard drive.	Suspicious ratio between download and upload	req_transferred/rep_transferred BETWEEN 0.9 AND 1.1		Default	2017-05-12 06:00:38	
☐	NONWIN10	Detection of devices with different OS than Windows 10.	Operating system differs from Windows 10	#src_filter# AND ((ua_os <> 68 AND ua_os <> 65535) OR (ua_os = 68 AND ua_os_version <> 10.0))		Default	2017-05-12 14:20:18	
☐	OPENCONN	Detection of partially established connections.	Partially established connection	protocol = 6 and Tools.matchflags(req_flags, 'S', 'A') = 0 and Tools.matchflags(rep_flags, 'SA', '-') = 0		Default	2017-05-23 15:07:36	
☐	SQLINJECT	Detection of SQL injection using pattern like OR 1=1 in HTTP URL	SQL injection detected	#src_filter# AND destination_port = 80 AND protocol = 6 AND Tools.re_match('.{1,4}[Oo][Rr].{1,4}\d.{1,3}\d', 'http_url') = 1		Default	2017-05-11 22:17:42	
☐	UDPHTTP	Detection of HTTP protocol anomaly, traffic on UDP protocol. Web server IP is reported as event source.	HTTP protocol anomaly on UDP	#dst_filter# AND protocol = 17 AND destination_port = 80	SUM(req_transferred + rep_transferred) > 104857600	Default	2017-11-11 17:59:33	
☐	WANACRYPT0R	Detection of communication with known domain related to WanaCrypt0r.	WanaCrypt0r detected	http_host = 'aposdfjhgosurijfaewrwergwea.com'		Default	2017-05-15 14:54:40	
☐	WINXP	Detection of devices with unsupported operating system on the network	Device with Windows XP operating system detected	ua_os = 68 AND (ua_os_version = 5.1 OR ua_os_version = 5.2)		Default	2017-05-12 11:50:03	

- Příklady naleznete v ADS uživatelské příručce

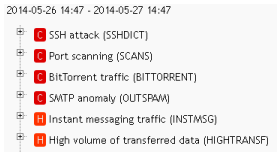
Flowmon Threat Intelligence

- IP a host reputační databáze
- Detekce C&C domén, P2P botnety, phishing
  - IP adresy (k dispozici)
  - HTTP host names (k dispozici, nutná sonda)
  - Doménová jména (nutná sonda)



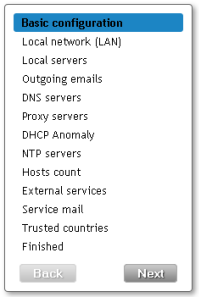
Alerty a integrace v ADS

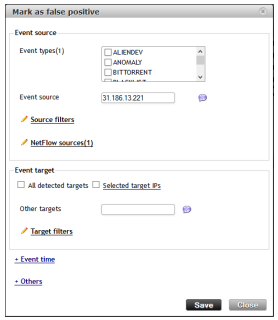
- **Perspektivy** pro nastavení priorit událostí
- **E-mail** reporty
  - Založeno na perspektivách
  - Různé formáty
- **PDF** reporty
  - Předdefinované a uživatelsky definované
- **SIEM/log** management
  - Syslog (CEF format)
  - SNMPv2 traps
- **Spuštění skriptu** nebo **záchytu provozu**



Konfigurace ADS

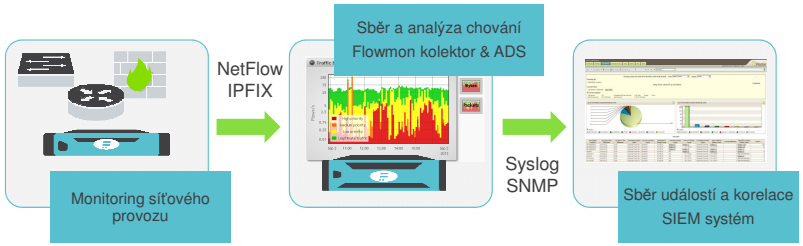
- Průvodce konfigurací pro počáteční nastavení
- Konfigurační šablony pro různá prostředí
- Správa false positive pro ladění systému





Integrace SIEM

- Export událostí pomocí syslog zpráv



- Propojení odkazy Flowmon <-> Log Management
- Zvláštní vztahy s dodavateli
  - IBM QRadar (whitepaper, integrace SW balíčku)
  - ArcSight nativní podpora prostřednictvím CEF

Verze ADS

- Flowmon ADS pro SMB/Enterprise segment
  - Navrženo pro tisíce toků za sekundu
  - Verze
    - Lite, Standard, Business, Corporate, Enterprise, Ultimate
  - Liší se podle výkonu a sady funkcí
- Flowmon ADS pro ISP/DC/operátory
  - Navrženo pro vzorkování na úrovni toku
  - Verze
    - ISP 1, ISP 4, ISP 10, ISP 40, ISP 100, ISP 400
  - Liší se podle výkonu

ADS pro SMB / Enterprise segment

	Lite	Standard	Business	Corporate	Enterprise	Ultimate
Přibližná velikost sítě do (není licencován parametr)	250 PC	1 000 PC	5 000 PC	10 000 PC	20 000 PC	50 000 PC
Výkon v tocích za sekundu	1 x 100	1 x 1000	2 x 2000	3 x 3000	3 x 4000	3 x 5000
Podpora SIEM (Syslog, SNMP)	NE	NE	ANO	ANO	ANO	ANO
Sada detekčních metod	Omezená	Standardní	Plná	Plná	Plná	Plná
Sběr toků a zpracování instancí	1	1	2	3	3	3

ADS pro ISP / DC / operátory

	ISP 1	ISP 4	ISP 10	ISP 40	ISP 100	ISP 400
Šířka pásma	1Gbps	4Gbps	10Gbps	40Gbps	100Gbps	400 Gbps
Celkový výkon v tocích za sekundu po vzorkování	5000	5000	10000	10000	15000	15000
Podpora SIEM (Syslog, SNMP)	ANO	ANO	ANO	ANO	ANO	ANO
Sada funkcí	Plná	Plná	Plná	Plná	Plná	Plná
Sběr a zpracování instancí	1	2	2	3	3	4

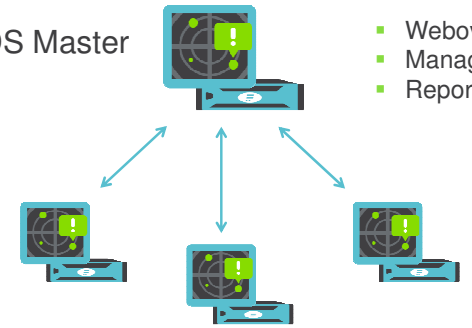
Distribuovaná architektura – Flowmon ADS

- Pro rozsáhlé a vytížené síťové infrastruktury
- Několik uzlů Flowmon ADS
  - Flowmon ADS Master – správa celé architektury, uživatelské rozhraní pro analýzu událostí a reporting
  - Flowmon ADS Slaves – nasazení v různých lokalitách pro detekci anomálií
- Výhody distribuované architektury
  - Load balancing a vyšší výkon
  - Centrální management a konfigurace
  - Centrální reporting a alerting

Flowmon
Driving Network Visibility

Distribuovaná architektura – Flowmon ADS

Flowmon ADS Master



- Webové rozhraní pro analýzu
- Management & konfigurace
- Reporting

Flowmon ADS Slaves

- Různé lokality
- Detekce anomálií
- Bez webového rozhraní

Flowmon
Driving Network Visibility

Děkuji za pozornost

Monitorování výkonu, viditelnost a bezpečnost s jediným řešením

Martin Ševčík, Presales Engineer
martin.sevcik@flowmon.com

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Česká republika
www.flowmon.com

Flowmon
Driving Network Visibility