VERSIM

Dystrybutor IT

LM/SIEM od Extreme Networks

Śniadanie Technologiczne z NGE Polska

16.03.2016

Tomasz Sroczyński, Versim S.A.

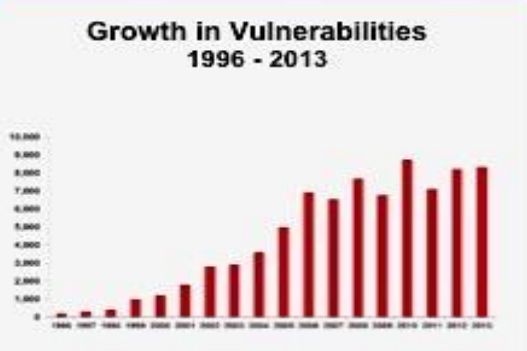
VERSIM

Dystrybutor IT

Coraz większy zasięg ataków oraz wyższy poziom zagrożeń

VERSIM
Dystrybutor IT

Rosnąca liczba niechronionych elementów



- Rośnie liczba luk w zabezpieczeniach
- Rośnie ogólny obszar ataków
- Patche nie mogą być wdrożone natychmiastowo lub nie istnieją

Ataki zero-day i ciągle mutujące zagrożenia

- Ataki ciągle ulegają zmianom w celu omijania sygnatur
- Rosnąca liczba ataków zero-day

Ataki wieloaspektowe / APT

- Dobrze skoordynowane ataki przez dobrze skoordynowane zespoły
- Atakujący uzyskują dostęp poprzez użytkowników
- Tradycyjne narzędzia bezpieczeństwa nie mogą wykryć lub ocenić zakresu naruszenia

Średnia strata z tytułu włamania do sieci wynosi 5.9 mln $
Coraz większe naciski na realizację zgodności

Extreme networks

NGE Polska

Historia Extreme Networks

VERSIM
Dystrybutor IT

Extreme networks

NGE Polska

Struktura zarządzania politykami i zabezpieczeniami

VERSIM
Dystrybutor IT

Kompleksowe rozwiązanie do zarządzania siecią, politykami i zgodnością

Transformacja logów, zdarzeń, przepływów, zarządzanie zagrożeniami i lukami w zabezpieczeniach poprzez produkty SIA-G2

Bezpieczeństwo i analityka

Widoczność, kontrola i automatyka sieci poprzez NetSight

Zarządzanie siecią

Zarządzanie tożsamością i dostępem przez NAC

Ludzie

Widoczność i zarządzanie aplikacjami przez Purview

Aplikacje

Ochrona sieci przez IPS-G2, WIPS, polityki SecureNetworks

Infrastruktura

Widoczność *Detekcja* *Egzekwowanie*

NGE Polska

Rozwiązania Extreme - analityka zabezpieczeń

VERSIM
Dystrybutor IT

Zarządzanie logami

- ✓ *Scentralizowana baza danych dla przechowywania logów (firewalle, serwer, przełączniki, oprogramowanie antywirusowe, itp.)*
- ✓ *Normalizacja logów – tłumaczenie na zrozumiały dla człowieka język*

SIEM

- ✓ *Korelacja logów i informacji o bezpieczeństwie*
- ✓ *Nadawanie priorytetów zdarzeniom typu Offense*

Risk Manager

- ✓ *Monitorowanie profili ryzyka urządzeń (hasło, konfiguracja, patche)*
- ✓ *Utrzymywanie topologii sieci i korelacja ryzyka urządzeń*

Vulnerability Manager

- ✓ *Skanowanie urządzeń pod względem znanych luk w zabezpieczeniach, określonych w bazie danych CVE*
- ✓ *Raporty dotyczące ekspozycji na zagrożenia oraz nadawanie priorytetów działaniom naprawczym*

X-Force/ IP Reputation

- ✓ *Ochrona przed atakami typu Day Zero dzięki aktywnemu monitorowaniu aktywności Internetowej*
- ✓ *Automatyczne przesyłanie zaktualizowanych sygnatur zabezpieczeń*

Informacje o zarządzaniu logami

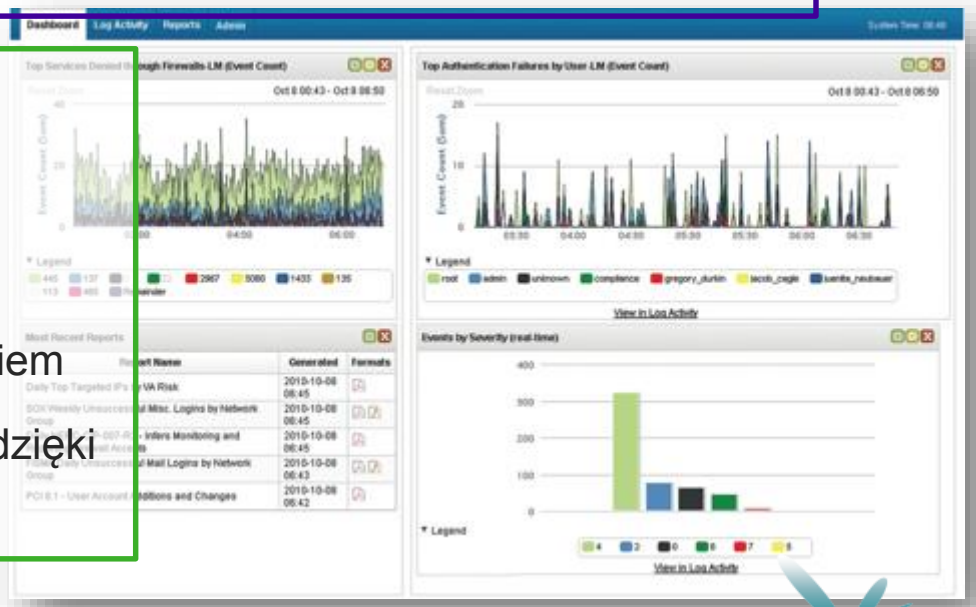
VERSIM
Dystrybutor IT

Log Manager zbiera, archiwizuje, analizuje i raportuje logi zdarzeń z całej infrastruktury - dotyczące sieci, bezpieczeństwa, hostów i aplikacji

- Rozproszone zbieranie logów, dane archiwalne, raportowanie i wyszukiwanie – dopasowane do rozmiarów każdej sieci
- Szablony raportów dla potrzeb realizacji zgodności z przepisami i audytowania
- Niezawodne i zapewniające integralność danych przechowywanie logów dla potrzeb analiz dochodzeniowych

Największe korzyści:

- Zapewnia zgodność z przepisami i wewnętrznymi zasadami użytkowania
- Zmniejsza liczbę manualnych zadań związanych ze zgodnością i raportowaniem
- Zmniejsza zagrożenia bezpieczeństwa dzięki wglądowi w aktywność sieci



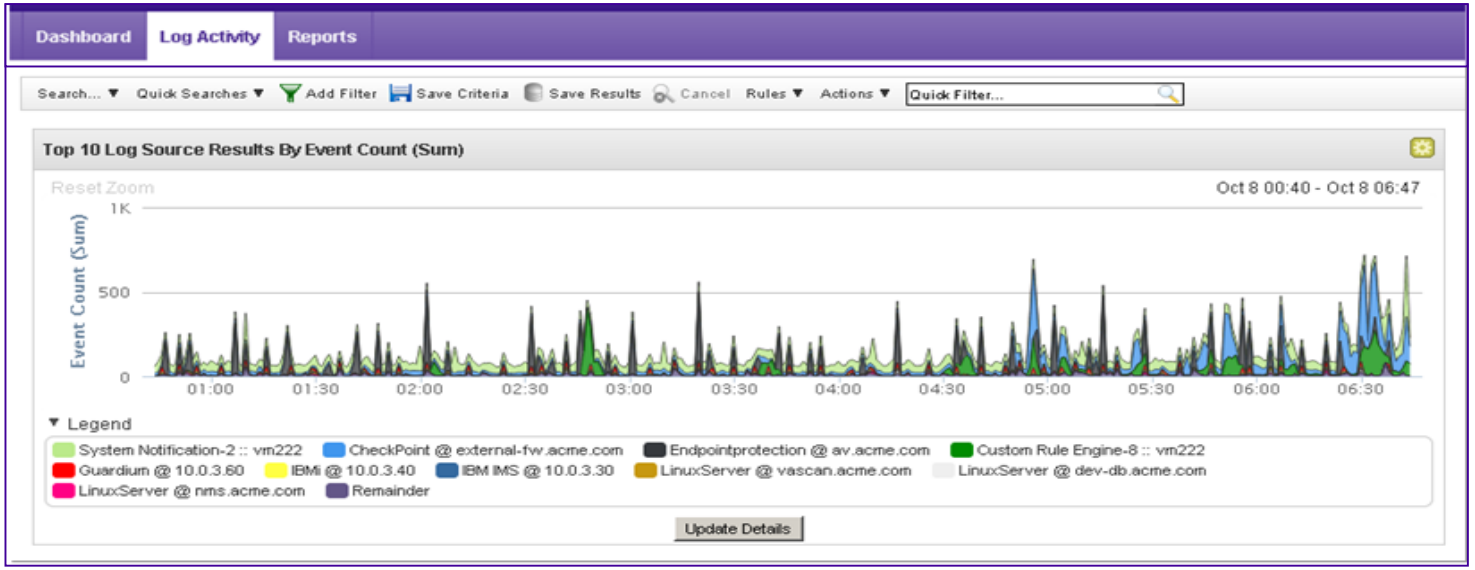
Extreme networks

NGE Polska

Zarządzanie logami

Podstawa systemów bezpieczeństwa

VERSIM
Dystrybutor IT



- Intuicyjny interfejs użytkownika dostępny z przeglądarki internetowej
- Możliwość tworzenia paneli sterowania (przestrzeni roboczych) dla każdego użytkownika
- Widoczność i raportowanie w czasie rzeczywistym i historycznie

- Łatwy w użyciu mechanizm reguł z wbudowanymi funkcjami bezpieczeństwa
- Zaawansowane przeszukiwanie i analizowanie danych
- Oparty na rolach dostęp do informacji i funkcji
- Skalowalność dla wsparcia największych na świecie wdrożeń – wbudowana baza danych i ujednolicona architektura danych

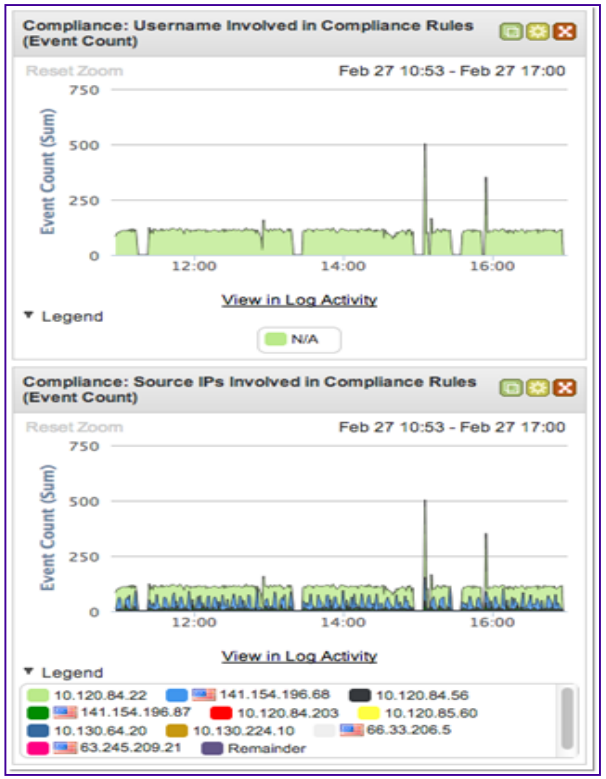
Extreme networks

NGE Polska

Realizacja wymagań zgodności

VERSIM
Dystrybutor IT

- Automatyczne wykrywanie źródeł logów – uproszczone wdrożenie i szybszy zwrot z inwestycji
- Rozproszone zbieranie logów, analizy, dane archiwalne, raportowanie i wyszukiwanie – dopasowane do rozmiarów każdej sieci
- Zaawansowane wyszukiwania (podobne do SQL) dla potrzeb dokładnych analiz
- Niezawodne i zapewniające integralność danych przechowywanie logów dla potrzeb analiz dochodzeniowych i procesu dowodowego
- Szablony raportów dla potrzeb audytowania i raportowania zgodności z przepisami
- Wspólna z SIEM architektura dla bezpieczeństwa aktualizacji



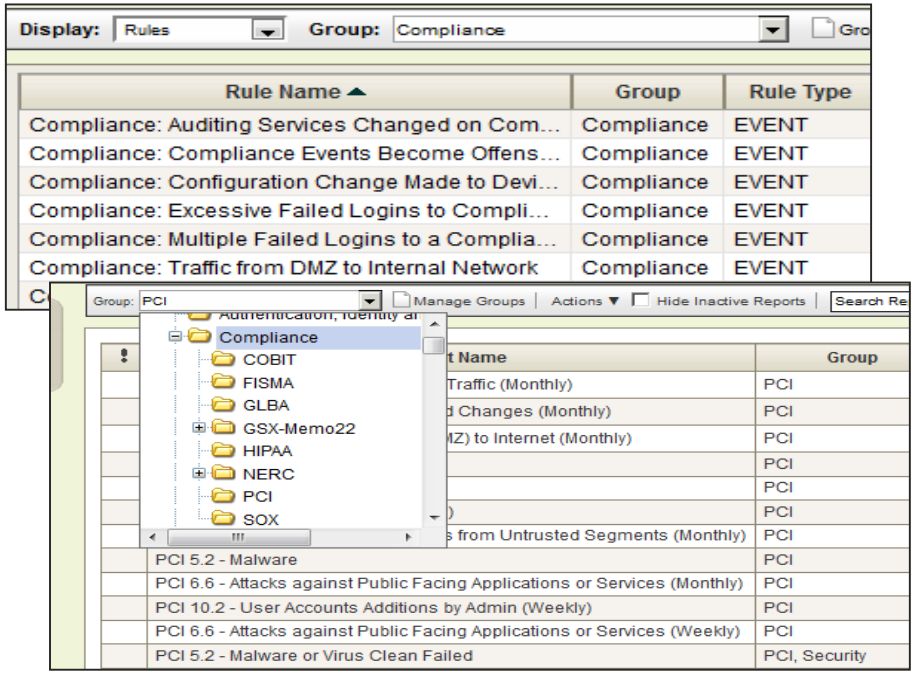
Extreme networks

NGE Polska

Reguły dotyczące zgodności i raportowanie – szybszy zwrot z inwestycji

VERSIM
Dystrybutor IT

- Wbudowane szablony raportów dla określonych regulacji:
  - COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, GPG13, UK GCSx, ISO 27001
- Możliwość łatwej modyfikacji dla uwzględnienia nowych definicji
- Możliwość rozbudowy – obsługa nowych regulacji i najlepszych praktyk
- Możliwość wykorzystania istniejących reguł korelacji



Extreme networks

NGE Polska

Zarządzanie logami
Wdrożenie ALL-IN-ONE

VERSIM
Dystrybutor IT

Korelacja logów zdarzeń pochodzących z infrastruktury sieciowej i bezpieczeństwa

Wdrożenie ALL-IN-ONE

- Jeden serwer zbiera dane o zdarzeniach z różnych urządzeń
- Realizacja korelacji danych, dopasowywanie reguł, raporty na temat zagrożeń/ powiadomień



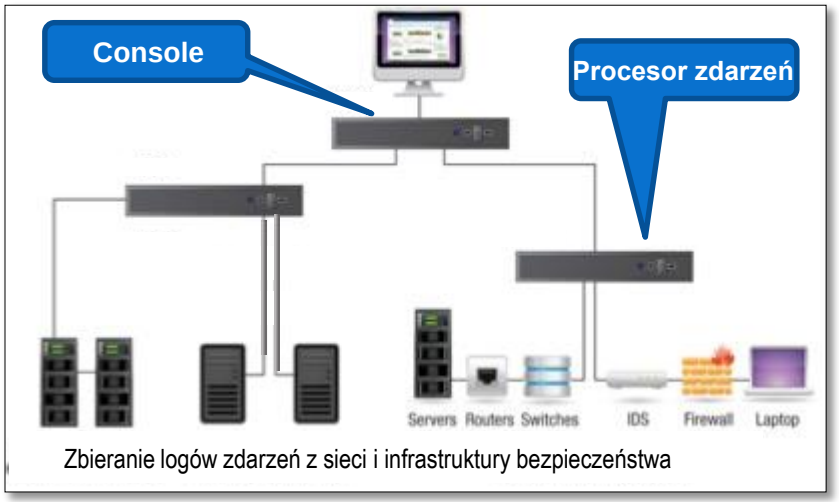

	VIRTUAL	STANDARD	ENTERPRISE	ENTERPRISE PLUS
Podst. EPS	100 EPS	500 EPS	1000 EPS	1000 EPS
Maks. EPS	5,000 EPS (możliwość zwiększania o 100 aż do 500, 1000, 2500, 5000)	1000 EPS (zwiększanie o 500)	5,000 EPS (zwiększanie o 2500)	15,000 EPS (zwiększanie o 2500)
Możliwości rozbudowy	✗ Rozbudowa do modelu DISTRIBUTED ✗ Rozbudowa do SIEM	✗ Rozbudowa do modelu DISTRIBUTED ✓ Rozbudowa do SIEM	✓ Rozbudowa do modelu DISTRIBUTED (Console) ✓ Rozbudowa do SIEM	✓ Rozbudowa do modelu DISTRIBUTED (Console) ✓ Rozbudowa do SIEM

Extreme networks

NGE Polska

Zarządzanie logami
Wdrożenie DISTRIBUTED

VERSIM
Dystrybutor IT



Zbieranie logów zdarzeń z sieci i infrastruktury bezpieczeństwa

Wdrożenie DISTRIBUTED

- Wiele serwerów – CONSOLE & PROCESOR ZDARZEŃ (EVP)
- Proces zdarzeń (EVP) zbiera i przetwarza zdarzenia; wdrożenie N:1
- Console – korelacja danych i raportowanie



	VIRTUAL	ENTERPRISE	ENTERPRISE PLUS
Podst. EPS	Console – N/A EVP – 100 EPS	Console – N/A EVP – 2500 EPS	Console – N/A EVP – 2500 EPS
Maks. EPS	20,000 EPS (zwiększanie o 100 do 500, następnie 1000, 2500 i zwiększanie o 2500 EPS)	20,000 EPS (zwiększanie o 2500)	40,000 EPS (zwiększanie o 2500)
Możliwości rozbudowy	Rozbudowa do SIEM	Rozbudowa do SIEM	Rozbudowa do SIEM

Extreme networks

NGE Polska

Wolumetria zdarzeń

Zarządzalne

Incydenty i potencjalne incydenty

Niezarządzalne

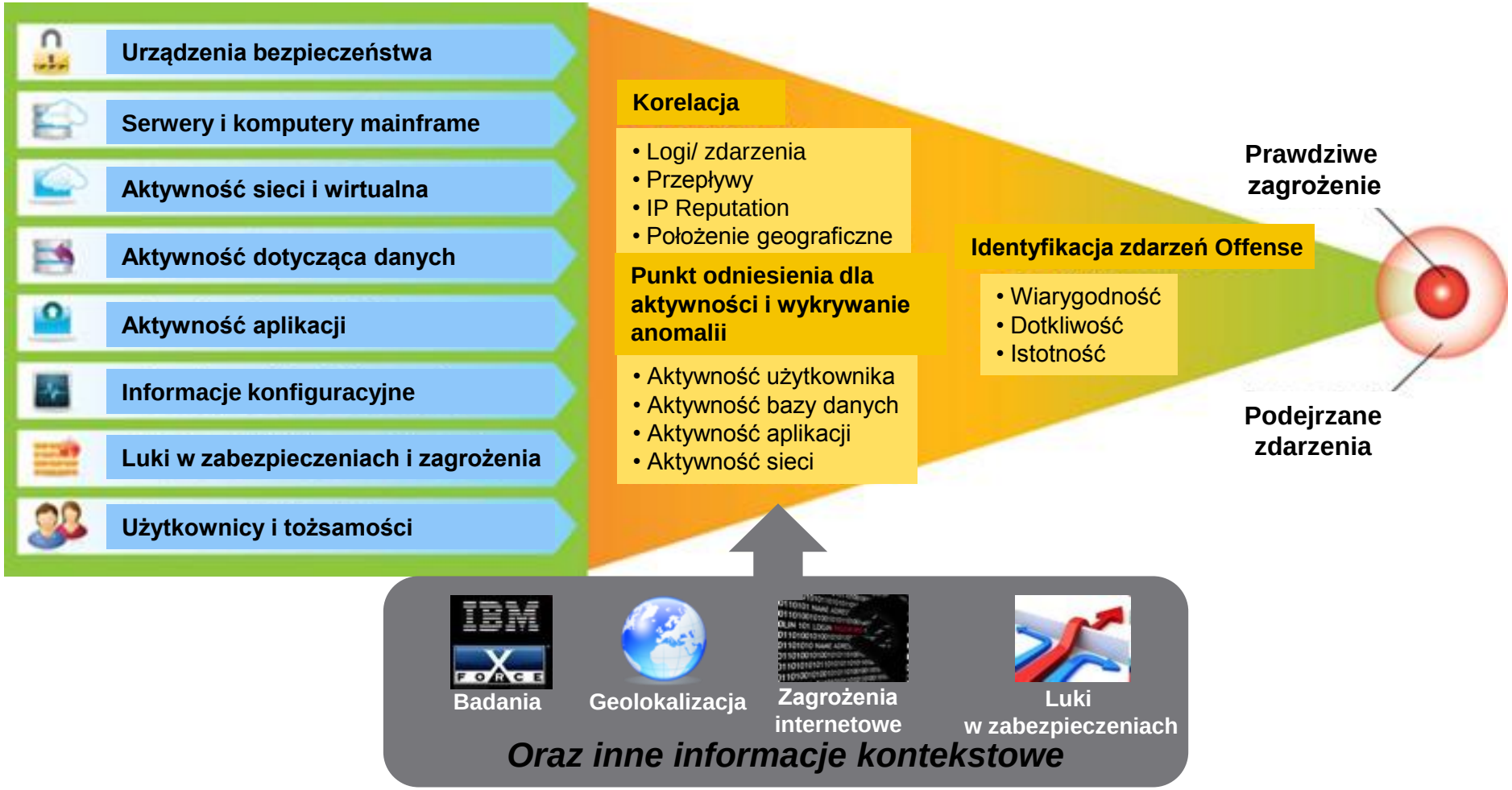
Wyniki działań mech. analitycznych

Niezarządzalne

Źródłowe zdarzenia z monitorowanych komponentów

SIEM
Zbieranie danych z wielu źródeł

VERSIM
Dystrybutor IT



Extreme networks

NGE Polska

SIEM

VERSIM
Dystrybutor IT

- ✓ Interesuje nas odpowiedź na pytanie „**kto**, **co robił i kiedy?**”
- ✓ Interesuje nas aby w przypadku wystąpienia rzeczywistego incydentu, system go wykrył i poinformował obsługę
- ✓ Interesuje nas aby nie każde podejrzane zdarzenie było incydentem obsługiwanym przez ludzi
- ✓ Chcemy mieć możliwość raportowania w obszarze bezpieczeństwa IT

Extreme networks

NGE Polska

Informacje o SIEM

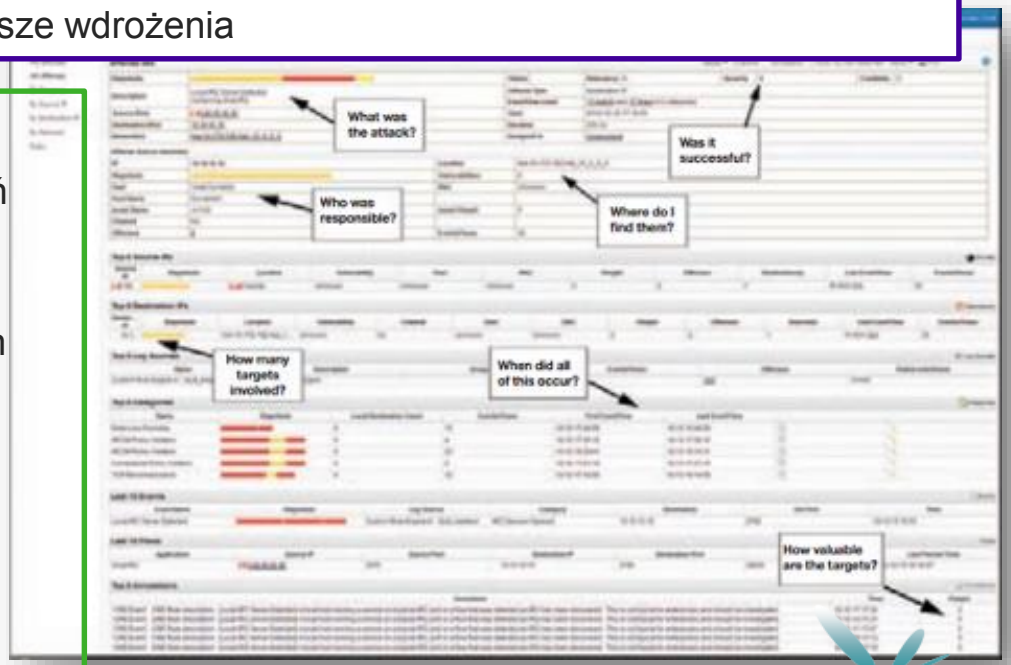
VERSIM
Dystrybutor IT

SIEM zapewnia pełną widoczność i użyteczne informacje dla ochrony sieci i zasobów IT przed szeroką gamą rozbudowanych zagrożeń – jednocześnie spełnia wymagania dotyczące zgodności

- Zaawansowana korelacja zdarzeń, przepływów, zasobów, topologii, luk w zabezpieczeniach i zewnętrznych danych w celu identyfikacji zagrożeń i nadawania im priorytetów
- Przechwytywanie i analiza przepływów sieciowych dla większej wiedzy o aplikacjach
- Zarządzanie przepływami pracy dla pełnego śledzenia zagrożeń i rozwiązywania problemów
- Skalowalna architektura obsługująca największe wdrożenia

Największe korzyści:

- Zmniejsza zagrożenie i dotkliwość naruszeń bezpieczeństwa
- Szybsze i bardziej dokładne korygowanie incydentów związanych z bezpieczeństwem
- Zapewnia zgodność z przepisami i wewnętrznymi zasadami postępowania
- Zmniejsza liczbę manualnych operacji związanych z bezpieczeństwem



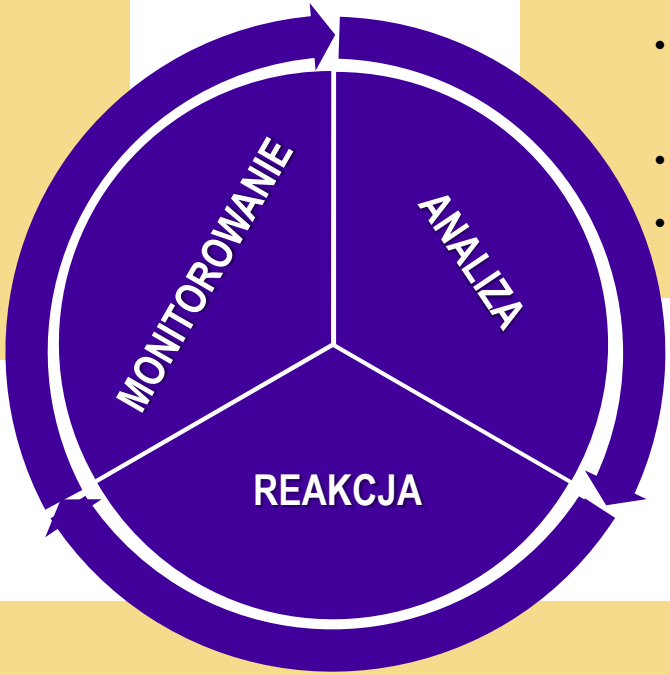
Extreme networks

NGE Polska

SIEM - Automatyzacja

VERSIM
Dystrybutor IT

- Automatyczne wykrywanie logów, aplikacji i zasobów
- Auto-grupowanie zasobów
- Scentralizowane zarządzanie logami
- Automatyczny audyt konfiguracji



- Priorytety oparte na zasobach
- Automatyczna aktualizacja zagrożeń
- Auto-odpowiedzi
- Ukierunkowana naprawa

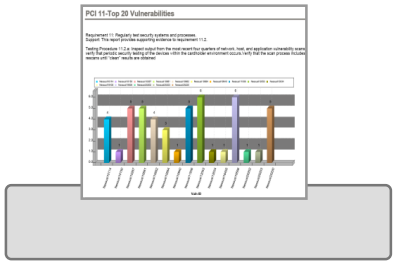
- Auto-tuning
- Automatyczne wykrywanie zagrożeń
- Tysiące predefiniowanych reguł i ról raportów w oparciu o łatwe w użyciu filtrowanie zdarzeń
- Zaawansowane zabezpieczenia analityczne

Extreme networks

NGE Polska

Modele użycia

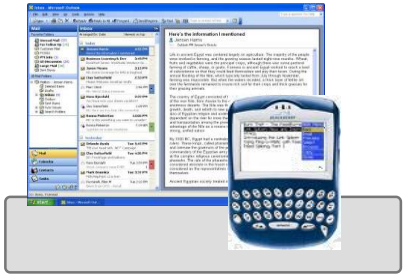
VERSIM
Dystrybutor IT



Raportowanie/analizy post factum

- Zbieranie logów
- Rozbudowane raportowanie
- Wydłużony czas odpowiedzi na incydent

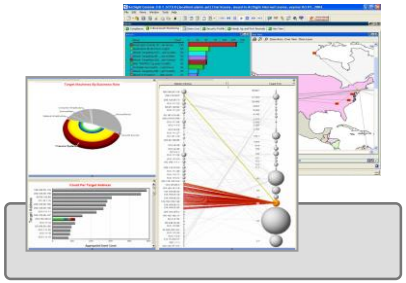
- Funkcjonalność SIEM nie jest wymagana!
- Skupienie na raportowaniu



Alertowanie

- Działanie w oparciu o powiadomienia
- Automatyzacja prostych incydentów
- Podstawowe analizy

- Ograniczone korelacje
- Skupienie na powiadomieniach



SOC

- System obsługi incydentów
- Dedykowany zespół ludzki
- Szybka odpowiedź na incydenty

- Zaawansowane korelacje
- Wiuzalizacje w czasie rzeczywistym

Extreme networks

NGE Polska

Zintegrowana konsola SIEM

VERSIM
Dystrybutor IT

- Jeden interfejs użytkownika dostępny z poziomu przeglądarki
- Oparty na rolach dostęp do informacji i funkcji
- Własne panele sterowania (przestrzenie robocze) dla każdego użytkownika

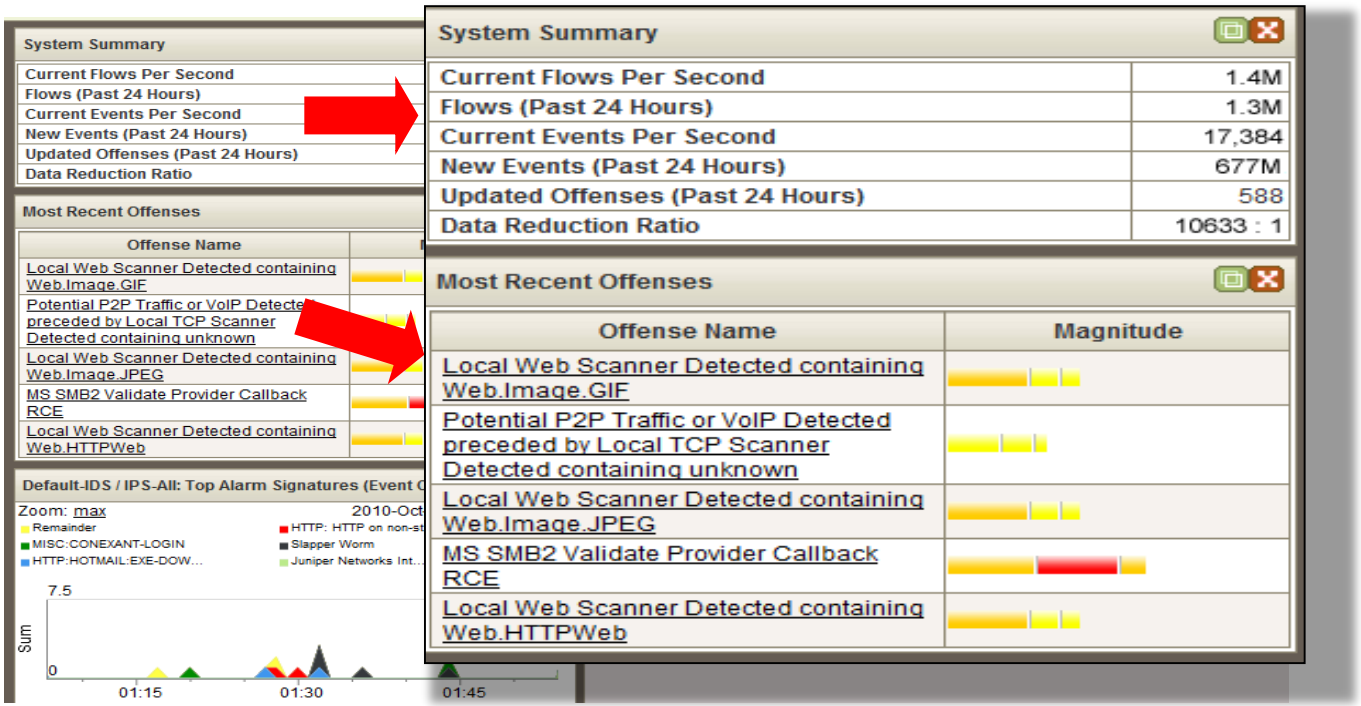
- Widoczność i raportowanie w czasie rzeczywistym i historycznie
- Zaawansowana analiza i przeszukiwanie danych
- Wbudowany mechanizm reguł z wbudowanymi funkcjami bezpieczeństwa

Extreme networks

NGE Polska

SIEM – wyodrębnianie danych i nadawanie priorytetów

VERSIM
Dystrybutor IT



24h okres aktywności sieci i bezpieczeństwa

↓

Korelacja i analiza danych generuje zdarzenia Offense

↓

Zdarzenia Offense zawierają pełną historię zagrożenia lub obejmują pełny kontekst sieciowy, zasobów i tożsamości użytkownika

↓

Zdarzeniom Offense są następnie nadawane priorytety z uwagi na ich wpływ na biznes

Extreme networks

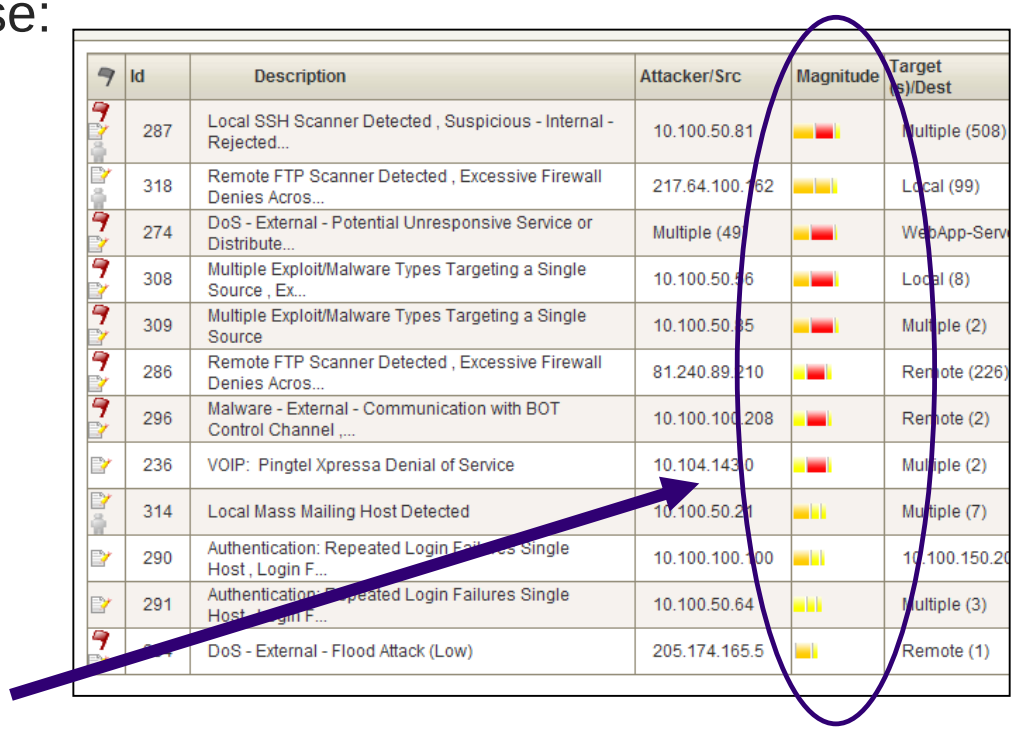
NGE Polska

SIEM – Inteligentna ocena zdarzeń Offense

VERSIM
Dystrybutor IT

SIEM ocenia wpływ zdarzeń Offense:

- *Wiarygodność:*
  Fałszywy alarm czy prawdziwy?
- *Dotkliwość:*
  Poziom alarmu zależny od zaatakowanego zasobu
- *Stosowność:*
  Priorytet zależny od zasobu lub wpływu na sieć



Id	Description	Attacker/Src	Magnitude	Target (s)/Dest
287	Local SSH Scanner Detected , Suspicious - Internal - Rejected...	10.100.50.81		Multiple (508)
318	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	217.64.100.162		Local (99)
274	DoS - External - Potential Unresponsive Service or Distribute...	Multiple (49		WebApp-Serv
308	Multiple Exploit/Malware Types Targeting a Single Source , Ex...	10.100.50.96		Local (8)
309	Multiple Exploit/Malware Types Targeting a Single Source	10.100.50.85		Multiple (2)
286	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	81.240.89.210		Remote (226)
296	Malware - External - Communication with BOT Control Channel ,...	10.100.100.208		Remote (2)
236	VOIP: Pingtel Xpressa Denial of Service	10.104.143.0		Multiple (2)
314	Local Mass Mailing Host Detected	10.100.50.21		Multiple (7)
290	Authentication: Repeated Login Failures Single Host , Login F...	10.100.100.100		10.100.150.20
291	Authentication: Repeated Login Failures Single Host , Login F...	10.100.50.64		Multiple (3)
	DoS - External - Flood Attack (Low)	205.174.165.5		Remote (1)

Priorytety mogą być zmieniane w czasie zależnie od sytuacji

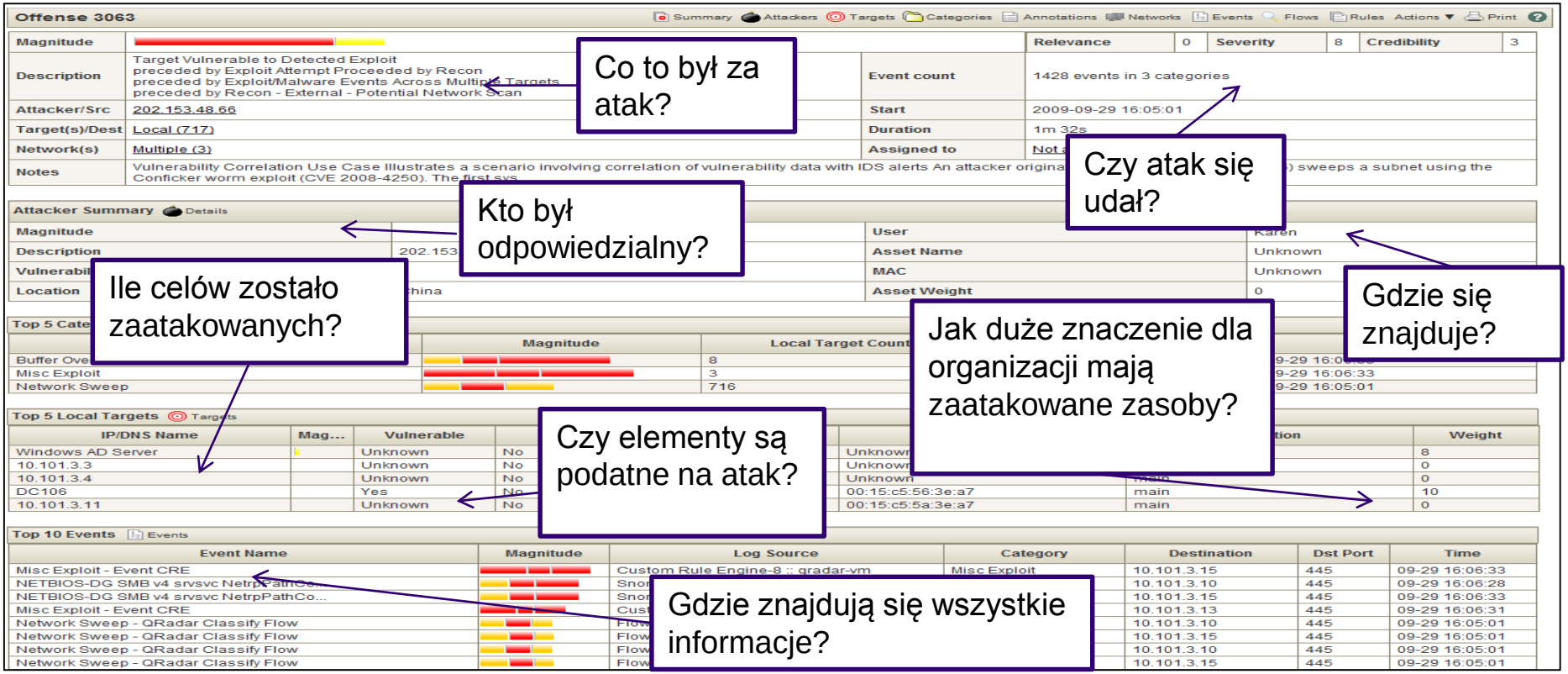
Extreme networks

NGE Polska

SIEM – zarządzanie zdarzeniami Offense

VERSIM
Dystrybutor IT

Jasne, zwięzłe i kompleksowe dostarczanie właściwych informacji



Extreme networks

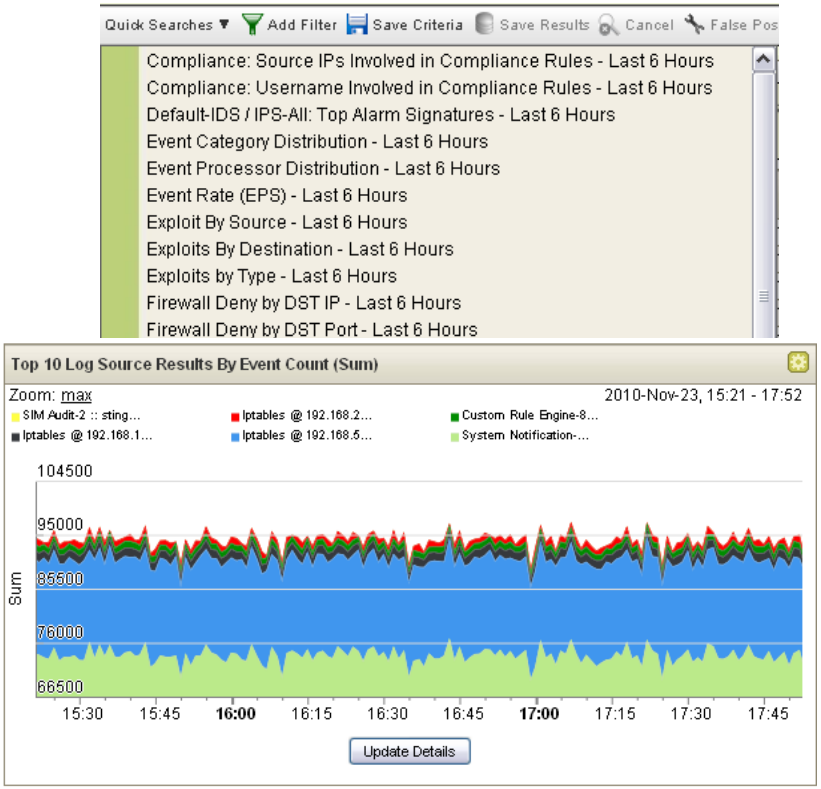
NGE Polska

SIEM – wbudowane reguły i filtry wyszukiwania

VERSIM
Dystrybutor IT

- Tysiące zasad korelacji i analiz w czasie rzeczywistym
- Setki wbudowanych wyszukiwań i widoków aktywności sieci oraz logów
- Szybki dostęp do krytycznych informacji
- Własne pola w zbieranych logach
  - Elastyczne wyodrębnianie danych o logach dla potrzeb wyszukiwania, raportowania i paneli sterowania. Produkt posiada dziesiątki predefiniowanych pól dla popularnych urządzeń.

Domyślne widoki/ zapytania dotyczące logów



Extreme networks

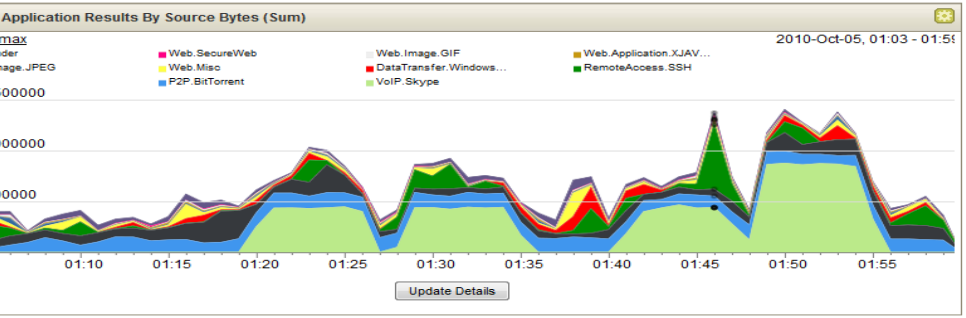
NGE Polska

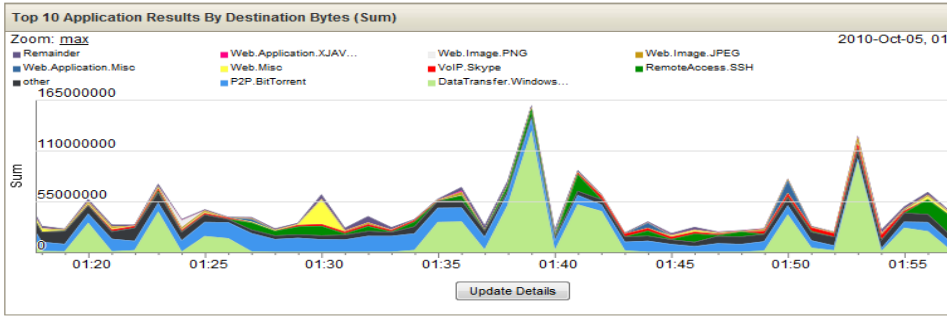
SIEM – Analiza przepływów dla zwiększenia inteligencji sieci

VERSIM
Dystrybutor IT

- Wykrywanie ataków typu zero-day bez określonych sygnatur
- Monitorowanie polityk oraz wykrywanie fałszywych serwerów
- Pełny obraz komunikacji atakującego

- Pasywne monitorowanie przepływów tworzy profile zasobów i automatycznie klasyfikuje hosty
- Widoczność sieci i rozwiązywanie problemów (nie tylko związanych z bezpieczeństwem)





(Hide Charts)

olication	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Coun
nsfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708	547 851 023	178 629	390 655	569 284	
Torrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654	235 838 522	127 854	161 966	289 820	
	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101	206 151 800	93 672	228 533	322 205	
ype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290	177 991 748	195 570	76 007	271 577	
Access.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020	149 113 136	101 404	261 727	363 131	
c	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741	31 361 821	33 634	23 904	57 538	
olication.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267	23 780 010	8 193	15 674	23 867	
age.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204	20 957 061	15 449	14 150	29 599	
b.Misc	Multiple (16)	Multiple (4)	Multiple (152)	80	other	256 544	9 127 264	9 383 808	4 184	6 830	11 014	

1 to 40 of 64 items (Elapsed time: 0:00:00.106)
Page: 1 Go

Extreme networks

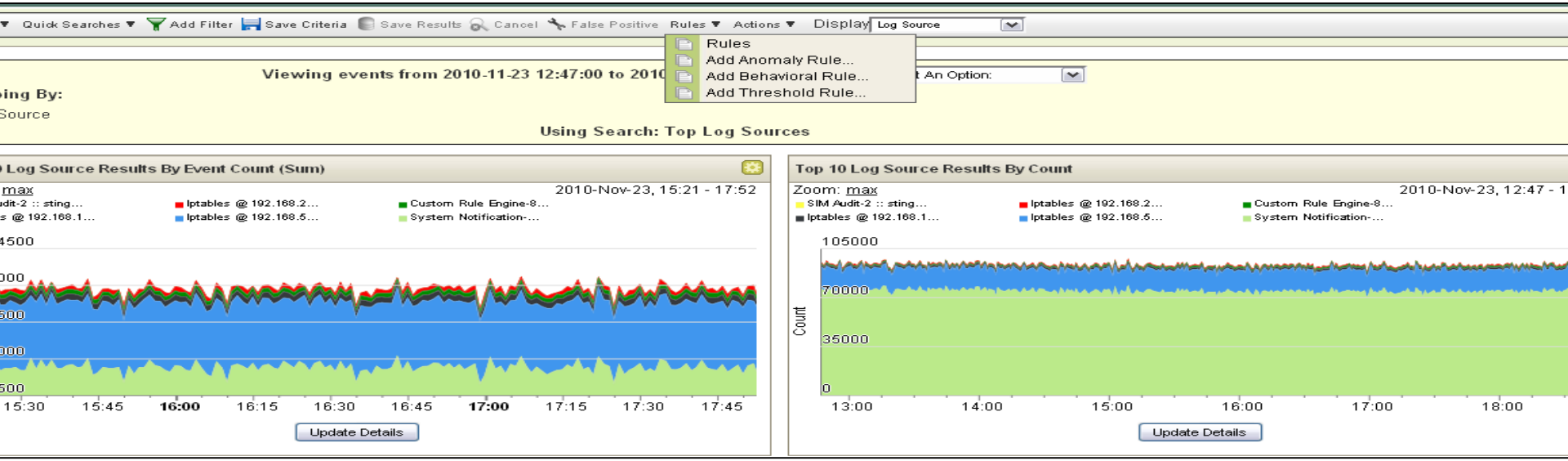
NGE Polska

SIEM – Analiza przepływów dla potrzeb widoczności aplikacji

VERSIM
Dystrybutor IT

- Zbieranie przepływów z natywnej infrastruktury
- Pełna korelacja, analiza i przeszukiwanie danych w źródłach przepływów dla zaawansowanego wykrywania zagrożeń i analiz dochodzeniowych

- Zbieranie i analiza danych z warstwy 7
- Widoczność i powiadamianie w oparciu o role/ polityki, wartości progowe, zachowanie lub nietypowe warunki dotyczące aktywności sieci lub logów

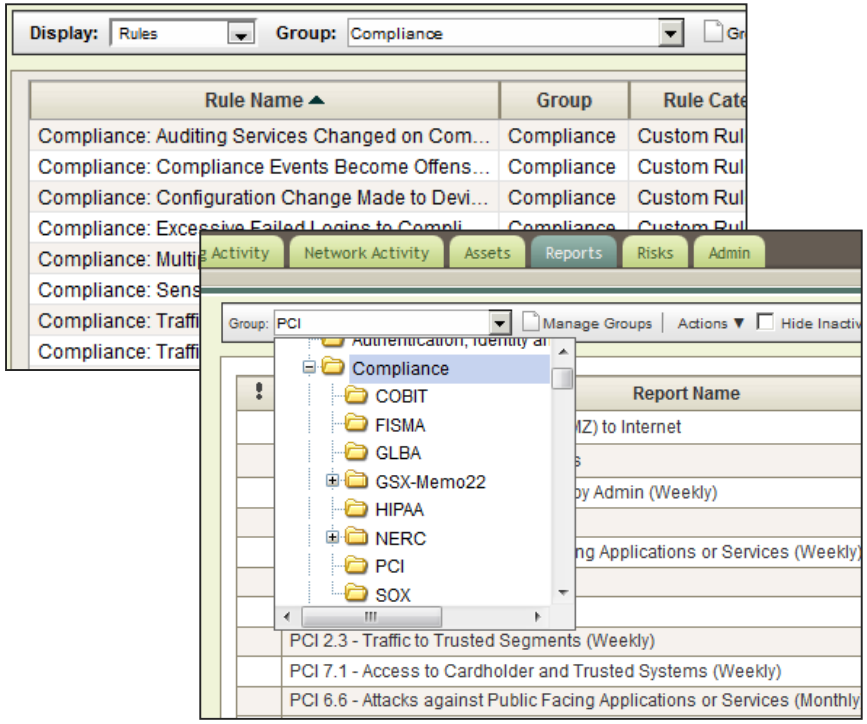


Extreme networks

NGE Polska

SIEM – Reguły zgodności i raportowanie

VERSIM
Dystrybutor IT



- Wbudowane szablony raportów dla różnych regulacji:
  - COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx
- Łatwe modyfikowanie w celu uwzględnienia nowych definicji
- Możliwość rozbudowy – obsługa nowych regulacji i najlepszych praktyk
- Możliwość wykorzystania istniejących reguł korelacji

Extreme networks

NGE Polska

Przykłady zastosowań

VERSIM
Dystrybutor IT

- **Obszar IT**
  - Nieudane logowania
  - Współdzielenie kont (równoległe logowania, niezgodność kont używanych w OS i aplikacji, logowanie w czasie nieobecności w pracy itp.)
  - Monitorowanie działań administracyjnych (ekstrakt operacji podwyższonego ryzyka, weryfikacja zgodności kont administracyjnych z osobami uprawnionymi itp.)
  - Monitorowanie zarządzania kontami (logowania na konta po resecie hasła, dodawanie/usuwanie użytkowników)
  - Obszar ochrony AV (nieusunięte infekcje, monitorowanie szczególnie groźnych malware itp.)
  - Monitorowanie prac podmiotów zewnętrznych (operacje wykonywane z kont podmiotów zewnętrznych, weryfikacja z uzgodnionym zakresem dostępu itp.)
- **Obszar sieciowy**
  - Skanowania portów
  - Ataki w warstwie sieciowej (logi z IPS, FW)
  - Monitorowanie wyników DLP sieciowego
  - Weryfikacja zgodności obserwowanego ruchu z założeniami polityki
  - Monitorowanie podejrzanego ruchu sieciowego (dynamiczne blacklisty/whitelisty)
  - Monitorowanie operacji wykonywanych na urządzeniach sieciowych
  - Dostęp zdalny – kontrola skąd dostęp i do jakich systemów

Przykłady zastosowań

VERSIM
Dystrybutor IT

- **Aplikacje:**
  - Niespójność między warstwą aplikacji a warstwami niższymi (logowanie do bazy danych bez logowania do aplikacji, wykonywanie zapytań bazodanowych na tabeli haseł bez logowania do aplikacji, aktualizacja tabeli uprawnień bez zdarzenia zmiany uprawnień w aplikacji itp.)
  - Nietypowe zachowania (np. wyszukiwań korzystających z tych samych, nietypowych kryteriów, wyszukiwanie klientów będących pracownikami, logowania się z oddziałów na wysoko uprzywilejowane konta, nieudane próby logowania na wysoko uprzywilejowane konta itp.)
  - Zaburzenia uprawnień (np. znalezienie użytkowników, których uprawnienia zostały ostatnio zmienione i były także zmieniane w ciągu ostatnich 30 dni, nadanie uprawnień użytkownikom, których stanowisko służbowe nie zezwala na posiadanie takowych, prowadzenia operacji nie wymagających wysokich uprawnień z konta wysoko uprzywilejowanego itp.)
  - Zaburzenia workflow (np. wykonanie czynności, w przypadku gdy użytkownik zatwierdzający czynność nie posiada już takich uprawnień, wykonywanie czynności, w przypadku gdy użytkownik udzielający zgody na wykonanie jest kontem technicznym itp.)

Przykłady zastosowań

VERSIM
Dystrybutor IT

- **Fizyczna kontrola dostępu:**
  - Wejścia bez wyjścia lub odwrotnie
  - Wejścia/wyjścia poza godzinami pracy
  - Jednoczesne lub zbyt szybkie pojawienie się karty dostępowej w dwóch miejscach fizycznych

- **Wskaźniki bezpieczeństwa:**
  - Zestandaryzowany poziom infekcji wirusowych
  - Współczynnik udane/nieudane logowania
  - Wskaźnik liczby odnowień DHCP
  - Parametry statystyczne ruchu sieciowego
  - Metryki obsługi incydentów bezpieczeństwa

Przykłady zastosowań

VERSIM
Dystrybutor IT

Major Electric Utility	wykrywanie zagrożeń	wykryto 500 hostów zawierających wirusa, których nie wykryły inne rozwiązania
Fortune 5 Energy Company	konsolidacja danych	2 miliardy zdarzeń z logów dziennie obniżono do 25 zdarzeń wysokiego ryzyka
Branded Apparel Maker	wykrywanie oszustwa dot. danych poufnych	wykryto przypadki kradzieży i niszczenia poufnych kluczowych danych
$100B Diversified Corporation	przewidywanie zagrożeń skierowanych przeciwko firmie	automatyzacja procesu monitorowania i oceny polityki na podstawie zmian konfiguracji w infrastrukturze
Industrial Distributor	adresowanie upoważnień regulacyjnych	monitorowanie aktywności sieci w czasie rzeczywistym

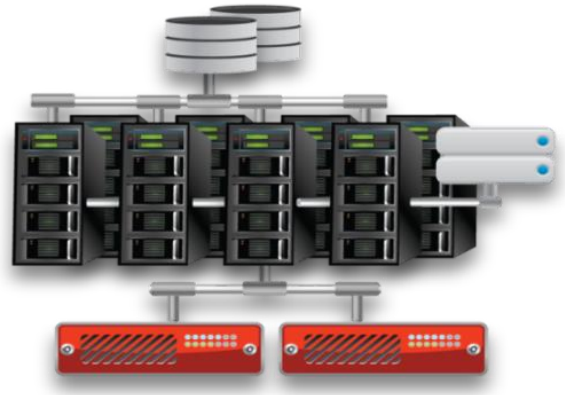
Extreme networks

NGE Polska

Integracja / jednolita skalowalna platforma

VERSIM
Dystrybutor IT

Wiele powiązanych rozwiązań



SKALA PROBLEMÓW
- nie zintegrowane raportowanie i wyszukiwanie
- lokalne decyzje
- administracja wieloma produktami
- duplikowanie repozytoriów logów
- wąskie gardła operacyjne

SIEM Extreme – zintegrowane rozwiązanie

WYSOCE SKALOWALNE
- wspólne raportowania i wyszukiwania
- pełna możliwość korelacji
- jednolita administracja
- logi przechowywane raz
- doskonała widoczność zidentyfikowanych problemów

Extreme networks

NGE Polska

Korzyści i oferowane wartości

VERSIM
Dystrybutor IT

Administrator sieci

- **Wiodąca na rynku technologia zabezpieczeń**
- **Ochrona przed przerwami w pracy sieci związanymi z bezpieczeństwem**
- **Wykrywanie wewnętrznych nadużyć**
- **Dostosowywanie się do szybko zmieniającego się krajobrazu zagrożeń**
- **Szybkie odróżnianie rzeczywistych zagrożeń od fałszywych alarmów**

Dyrektor IT

- **Wiodąca na rynku i zintegrowana technologia**
- **Mniejsze ryzyko przerw w pracy sieci**
- **Poprawiona efektywność operacyjna zespołów ds. bezpieczeństwa**
- **Przyszłościowe i skalowalne rozwiązania**
- **Aktualizacje oferowane przez dostawcę gwarantują bezpieczeństwo**

CIO

- **Ochrona przed utratą zysku na skutek przerw w działaniu sieci**
- **Stabilne IT**
- **Konsolidacja dostawców zabezpieczeń**
- **Zmniejszone koszty operacyjne**

Wizjonerski CIO

- **Ochrona marki przedsiębiorstwa**
- **Przewidywanie wpływu zagrożeń bezpieczeństwa na biznes**
- **SIEM to „Lider rynku" według rankingu MQ Gartnera; IPS to „Mistrz" według klasyfikacji Info-Tech Group**
- **Skalowalne i przyszłościowe rozwiązanie**

Chief Security Officer

- **Ochrona marki przedsiębiorstwa i wartości intelektualnej**
- **Zgodność z regulacjami takimi jak PCI, SOX, HIPAA**
- **Kompleksowe raportowanie dla potrzeb audytów bezpieczeństwa**
- **Skuteczne zarządzanie i korelowanie dużych ilości danych o bezpieczeństwie**

OD DECYZJI TECHNOLOGICZNYCH PO DECYZJE BIZNESOWE

Extreme networks

NGE Polska

SIEM – konkurencja na kwadracie Gartnera

VERSIM
Dystrybutor IT

Figure 1. Magic Quadrant for Security Information and Event Management

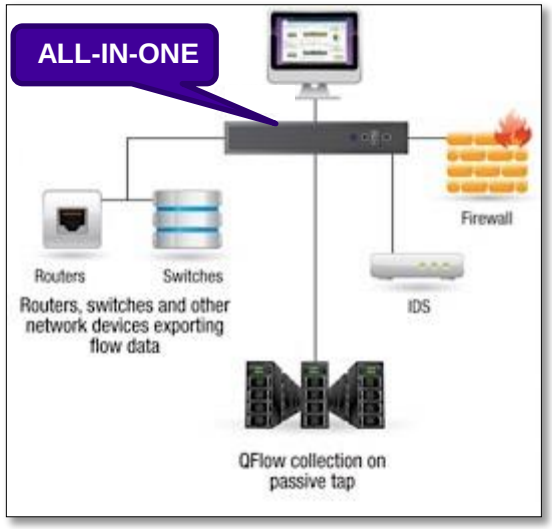
Source: Gartner (July 2015)

Extreme networks

NGE Polska

Wdrożenie SIEM ALL-IN-ONE

VERSIM
Dystrybutor IT



Wdrożenie ALL-IN-ONE

- Jeden serwer zbiera zdarzenia i dane o przepływie z różnych urządzeń
- Realizacja korelacji danych, dopasowywanie reguł, raporty dotyczące zagrożeń/ powiadomień



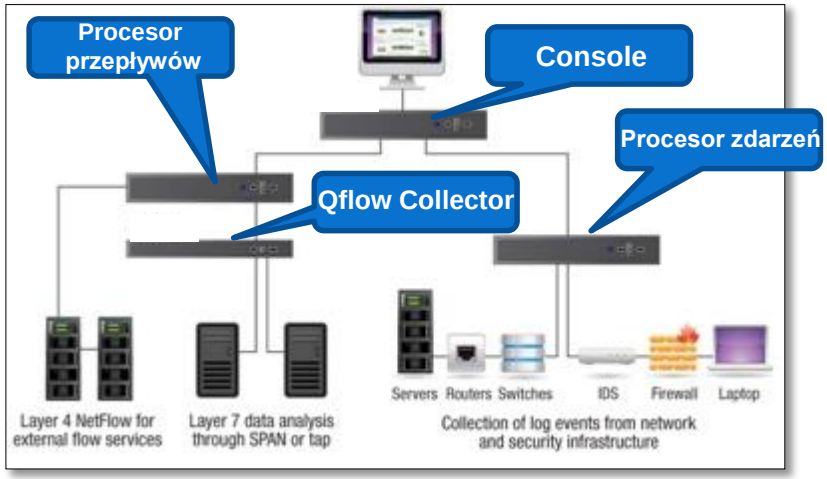

	VIRTUAL	STANDARD	ENTERPRISE	ENTERPRISE PLUS
Podst. EPS & FPM	100 EPS 15K FPM	1000 EPS 25K FPM	1000 EPS 25K FPM	1000 EPS 25K FPM
Maks. EPS & FPM	5,000 EPS 200K FPM	50K FPM	5,000 EPS 200K FPM	15,000 EPS 300K FPM
Możliwości rozbudowy	Rozbudowa do modelu DISTRIBUTED	Rozbudowa do modelu DISTRIBUTED	Rozbudowa do modelu DISTRIBUTED (CONSOLE)	Rozbudowa do modelu DISTRIBUTED (CONSOLE)

Extreme networks

NGE Polska

Wdrożenie SIEM DISTRIBUTED

VERSIM
Dystrybutor IT



Wdrożenie DISTRIBUTED

- Wiele serwerów – Console, Procesor zdarzeń (EVP), Procesor przepływów (FLP); wdrożenie N:1
- Procesor zdarzeń zbiera i przetwarza zdarzenia;
- Procesor przepływów zbiera i przetwarza przepływy;
- Q-Flow Collector zbiera dane z warstwy L7
- Console – korelacja danych i raportowanie



	VIRTUAL	ENTERPRISE	ENTERPRISE PLUS
Podst. EPS & FPM	Console – N/A EVP: 100 EPS FLP: 15K FPM	Console – N/A EVP: 2500 EPS FLP: 100K FPM CEF: 1000 EPS & 25K FPM	Console – N/A EVP: 2500 EPS FLP: 100K FPM CEF: 1000 EPS & 25K FPM
Maks. EPS & FPM	EVP: 20K EPS FLP: 600K FPM	EVP: 20K EPS FLP: 600K FPM CEF: 5000 EPS & 200K FPM	EVP: 40K EPS FLP: 1.2M FPM CEF: 15K EPS & 300K FPM

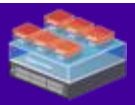
CEF: Combined Event & Flow Processor (połączenie procesora zdarzeń i przepływów)

Extreme networks

NGE Polska

Urządzenia do analityki zabezpieczeń

VERSIM
Dystrybutor IT

	 Virtual	 Standard	 Enterprise	 Enterprise Plus
Obudowa	-	1 RU	2 RU	2 RU
Pamięć	-	32GB	64GB	128GB
Dysk		1.5TB (użyteczne)	6.2TB (użyteczne)	40TB (użyteczne)
Maks. EPS	5K EPS (All-in-One) 20K (Distributed)	1K EPS(All-in-One)	5K EPS(All-in-One) 20K EPS (Distributed)	15K EPS(All-in-One) 40K EPS (Distributed)
Maks. FPM	200K FPM (All-in-One) 600K (Distributed)	50K FPM (All-in-One)	200K FPM (All-in-One) 600K EPS (Distributed)	300K FPM (All-in-One) 1.2M FPM (Distributed)

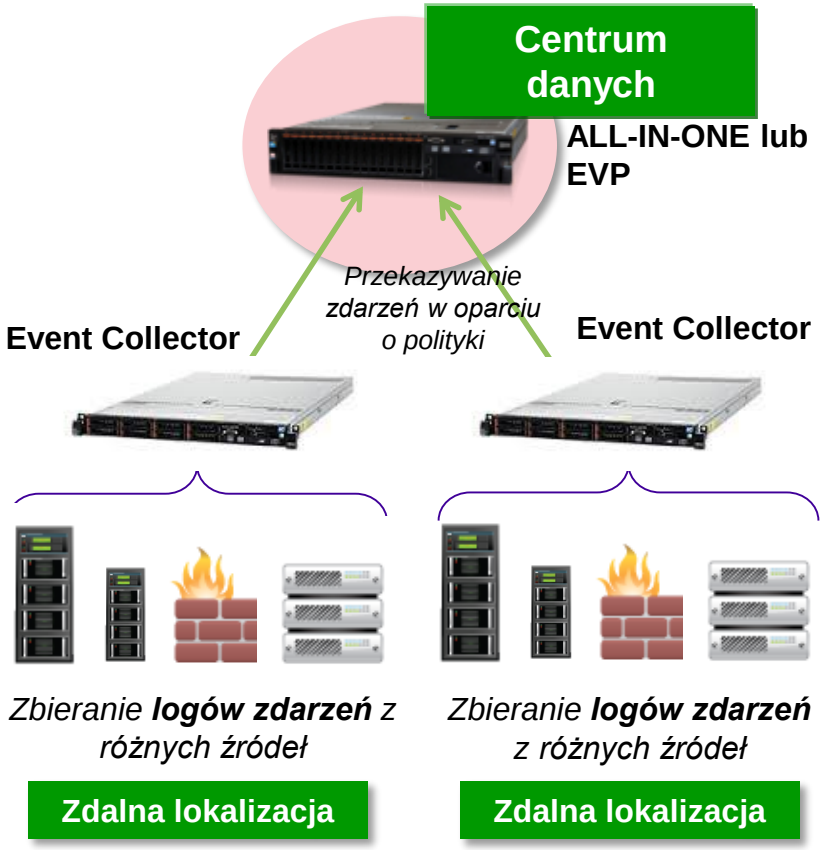
Extreme networks

NGE Polska

SIEM Event Collector

VERSIM
Dystrybutor IT

- Zbieranie i analizowanie zdarzeń w zdalnych lokalizacjach (oddział banku, sieć sklepów, itp.), które mają ograniczenia co do pasma lub niezbyt stabilne połączenia
- Tymczasowe przechowywanie zdarzeń i przekazywanie ich (w oparciu o politykę) do procesora zdarzeń (upstream)
- Wdrożenie - N [liczba Event Collector]:1 [Procesor zdarzeń]
- Brak konieczności stosowania licencji dla zbierania zdarzeń; tylko polityka Right-to-Use
- Dostępny jako urządzenie fizyczne lub maszyna wirtualna



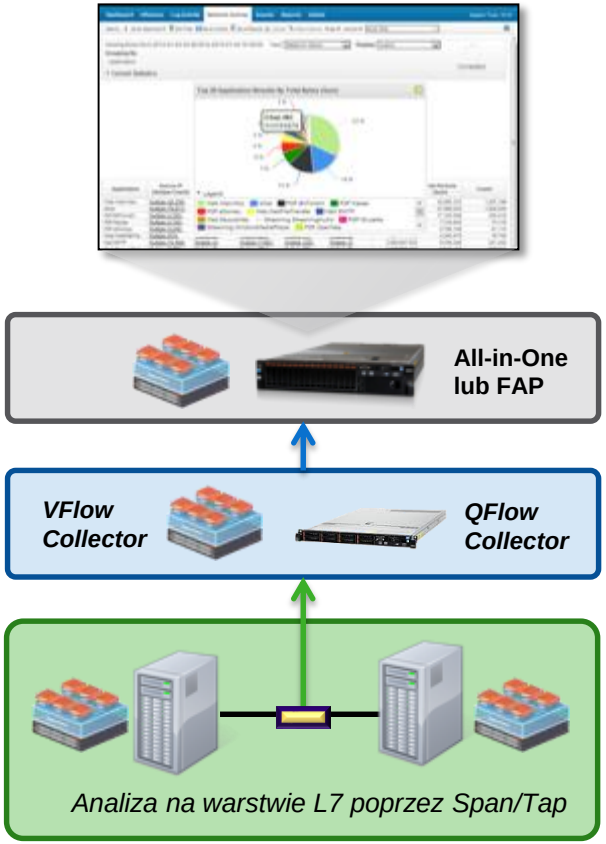
Extreme networks

NGE Polska

SIEM Flow Collector (QFlow & VFlow)

VERSIM
Dystrybutor IT

- Zaawansowane przechwytywanie i analizowanie przepływów dla realizacji widoczności warstwy L7 w sieciach fizycznych i wirtualnych
  - Szczegółowa kontrola pakietów oraz klasyfikacja aplikacji typu stateful
- Zaawansowana analiza incydentów poprzez korelację danych o przepływach z logami
  - Zgodność z regulacjami dzięki szczegółowym analizom danych aplikacji i protokołów
- Ciągłe profilowanie zasobów
  - Monitorowanie sieci, aplikacji oraz aktywności użytkowników
- Wdrożenie N [Liczba Flow Collector]:1 [Procesor przepływu]
- Brak konieczności stosowania licencji dla zbierania przepływów; tylko polityka Right-to-Use
- Wiele prędkości interfejsów (1G, 10G) i konfiguracji (TX, SX, SR, LR)



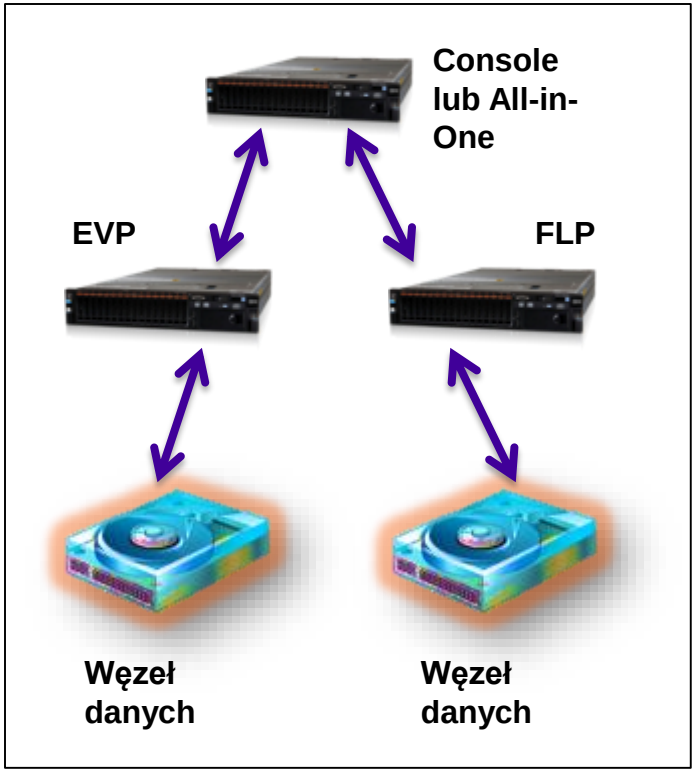
Extreme networks

NGE Polska

SIEM – węzeł danych (Data Node)

VERSIM
Dystrybutor IT

- Skalowalne wdrożenia SIEM przechowujące peta bajty informacji
- Poprawa wydajności zapytań i wyszukiwania
- Dystrybucja danych dla optymalizacji wykorzystania zasobów
- Olbrzymi wzrost wydajności procesów obliczeniowych takich jak prezentowanie zagregowanych widoków danych
- Rozbudowa On-demand dzięki klastrowaniu
- Wdrożenie N [Węzłów danych]:1 [EVP/FLP/All-in-one]
- Brak konieczności stosowania licencji dla węzłów danych
- Dostępny jako urządzenie fizyczne (Enterprise lub Enterprise Plus) lub maszyna wirtualna



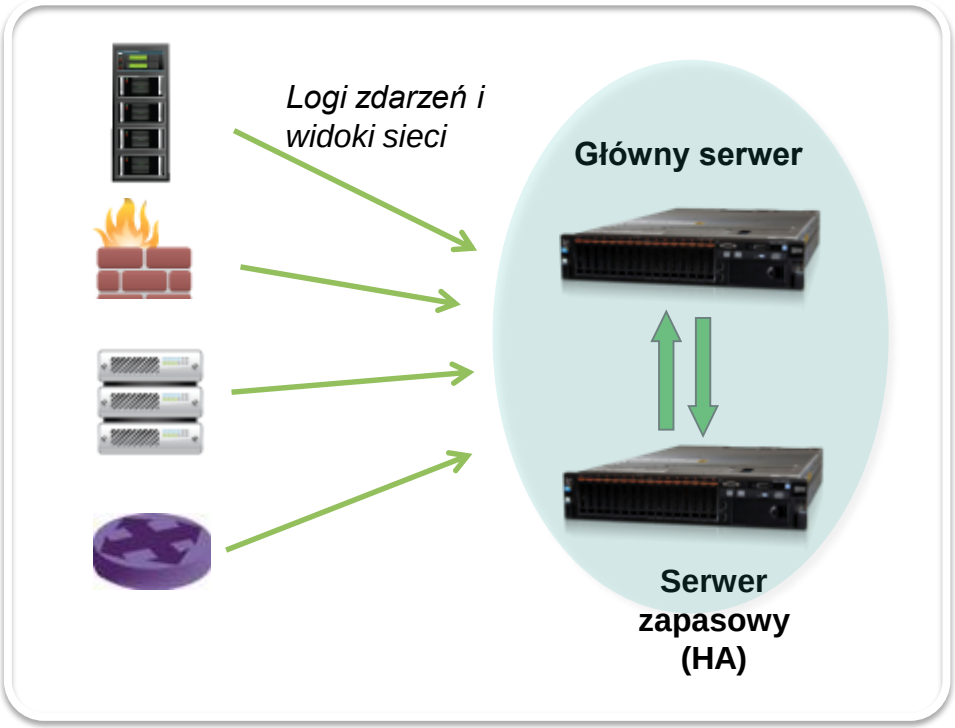
Extreme networks

NGE Polska

Wdrożenia w trybie wysokiej dostępności

VERSIM
Dystrybutor IT

- Dane i ustawienia konfiguracyjne głównego urządzenia są odtwarzane na urządzeniu zapasowym w czasie bliskim rzeczywistemu.
- Przełączanie (faiover) na urządzenie zapasowe, gdy główne urządzenie stanie się niedostępne.
- Urządzenie zapasowe dzieli licencje na wielkość EPS/Przepływów z głównym urządzeniem (nie ma potrzeby zakupu dodatkowych licencji)
- Wysoka dostępność tylko dla SIEM i LM
  - Brak opcji wysokiej dostępności dla Risk Manager i Vulnerability Manager

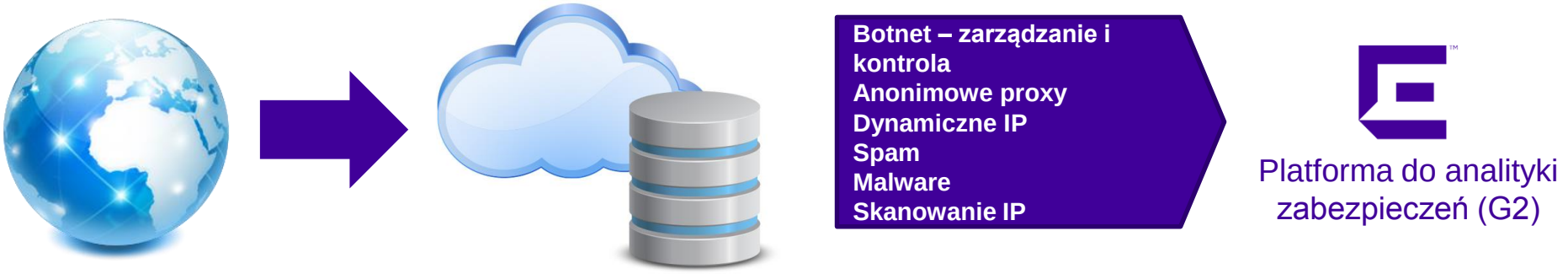


Extreme networks

NGE Polska

X-Force – Informacje o zagrożeniach

VERSIM
Dystrybutor IT



Zagrożenia internetowe

X-Force – baza danych z informacjami o zagrożeniach

Źródło informacji o zagrożeniach

- Poszerza możliwości korelacji SIEM
  - Zwiększa możliwości analityki zagrożeń SIEM przez automatyczne dostarczanie dynamicznych danych internetowych o zagrożeniach
- Ponad 50 mld stale monitorowanych i klasyfikowanych adresów URL
- Informacja o złośliwych adresach IP, hostach malware, źródłach spamu, dynamicznych IP, anonimowych proxy, itp.
- Usługa subskrypcji z IBM X-Force Cloud

Extreme networks

NGE Polska

Większa inteligencja oraz bezpieczeństwo poprzez integrację z SIEM

VERSIM
Dystrybutor IT

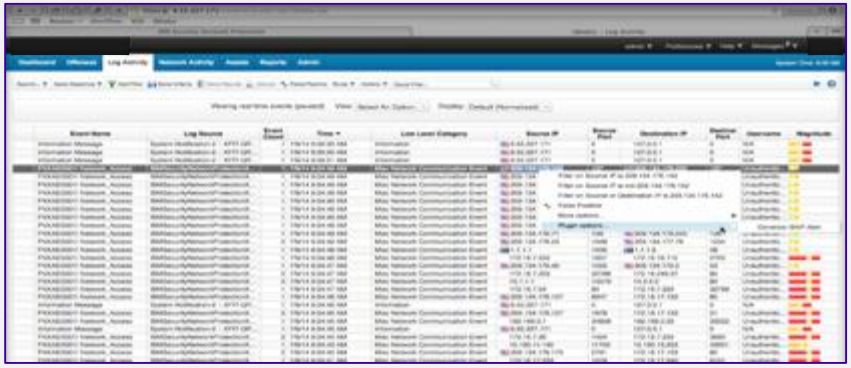
Dane o przepływach z warstwy L7 do SIEM

Wykrywanie anormalnych zachowań na podstawie danych o przepływach wygenerowanych z IPS

Identyfikacja niewłaściwego wykorzystywania aplikacji poprzez informacje o użytkownikach i aplikacjach

Oszczędności wynikające z braku konieczności stosowania oddzielnego urządzenia do obsługi przepływów

Blokowanie zdarzeń Offense z SIEM



Wykorzystywanie IPS do blokowania trwających ataków – w oparciu o informacje z SIEM

Zmniejszenie czasu reakcji dzięki inicjowaniu blokowania z poziomu konsoli SIEM – szybkie powstrzymywanie zagrożeń

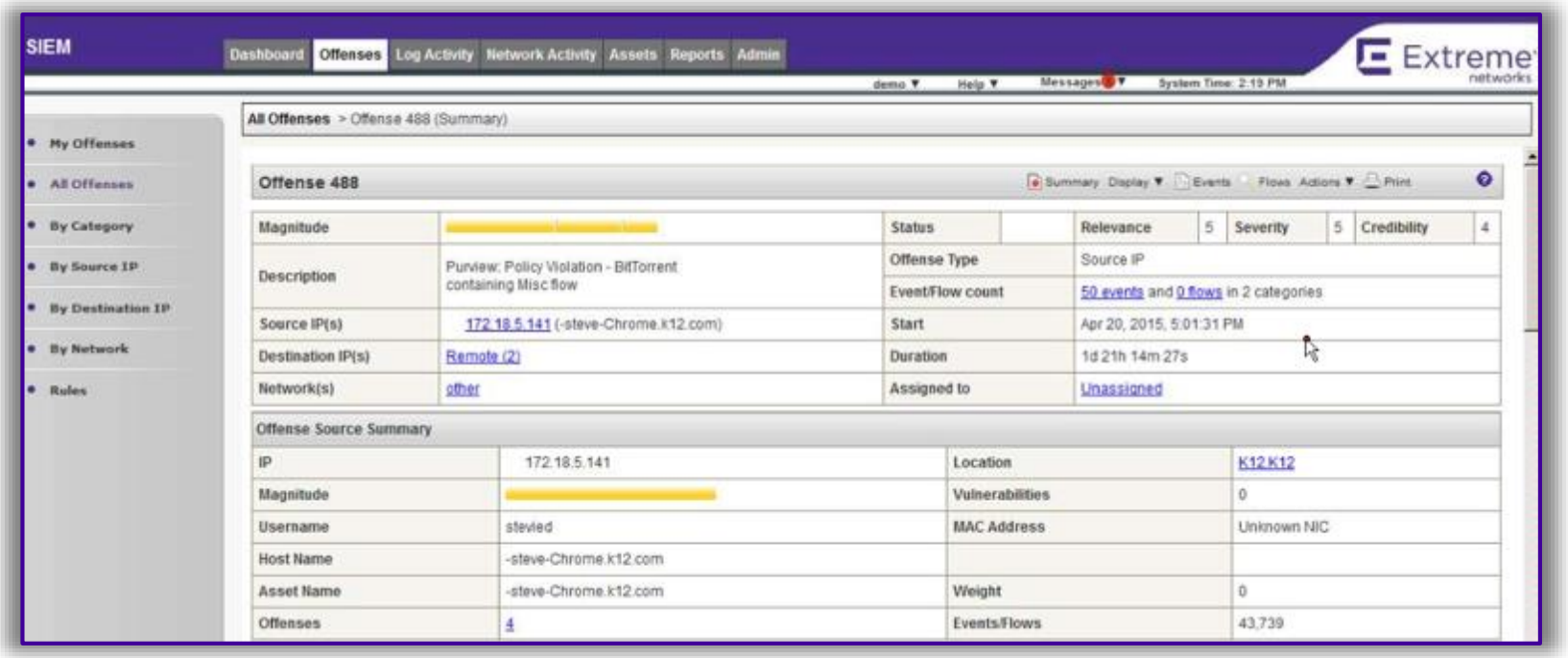
Wysyłanie przepływów danych oraz odbieranie poleceń dotyczących kwarantanny

Extreme networks

NGE Polska

Większa inteligencja oraz bezpieczeństwo poprzez integrację z SIEM

VERSIM
Dystrybutor IT



- Purview posiada opcję eksportu przepływów aplikacji, która pozwala na przesłanie poprzez Syslog wszystkich przepływów z Purview do SIEM w formacie LEEF (Log Event Extended Format)
- Wszystkie zdarzenia z Purview są indeksowane, przechowywane i natychmiastowo dostępne dla potrzeb bieżących zapytań lub raportów dotyczących trendów

Extreme networks

NGE Polska

VERSIM

Dystrybutor IT

Dziękuję za uwagę!

e-mail: tomasz.sroczynski@versim.pl
tel.: 61 8648 244
kom.: 799 158 547