„Co tam słychać mój drogi Watsonie”

wykorzystanie systemów samouczących się do optymalizacji działań w obszarze bezpieczeństwa.

Hubert Ortyl
Business Development Manager
Security Solutions
kom. +48 607 628 862
e-mail: hortyl@advatech.pl

Daniel Wysocki
Security Specialist
kom. +48 539 526 218
e-mail: dwysocki@advatech.pl

Przeciętnie, klient korzysta z 85 narzędzi od 45 vendorów – Big Data ?

Security analytics

Privileged user management

Access management

User behavior analytics

Data access control

Incident response

Data protection

Endpoint patching and management

Identity governance and administration

Network visibility and segmentation

Fraud protection

Mainframe security

Network forensics and threat management

Application scanning

Vulnerability management

Malware protection

IDaaS

Device management

Threat sharing

IoCs

Endpoint detection and response

Criminal detection

Content security

Transaction protection

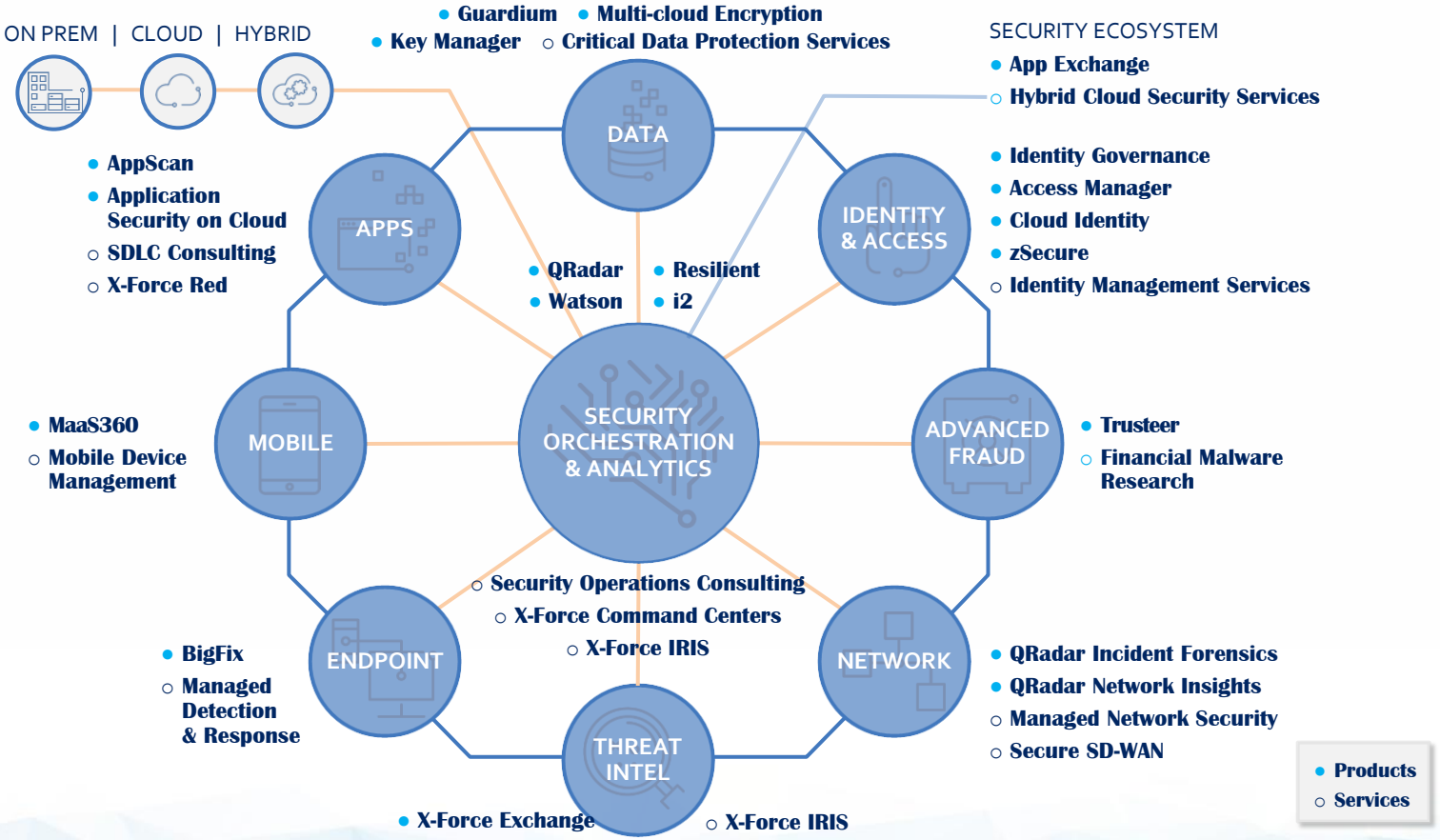
Firewalls and intrusion prevention

Threat and anomaly detection

Application security management

Threat hunting and investigation

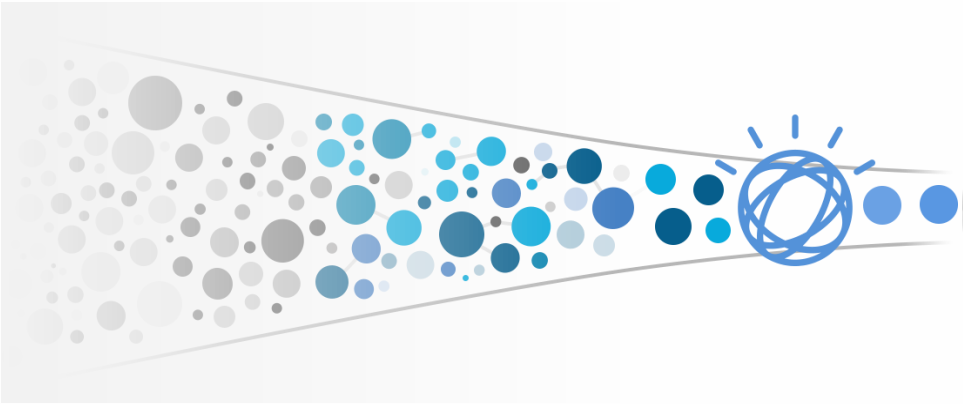
Zintegrowany system immunologiczny



System wspierany przez setki rozwiązań firm trzecich

Zidentyfikowanie incydentu bezpieczeństwa, to dopiero początek….

Zdarzenia
Aktywności sieciowa
Transfer danych
Zachowanie użytkowników
Threat intelligence
Konfiguracja urządzeń
Podatności
Aplikacje
Platformy chmurowe



Zagrożenia wewnętrzne
Zagrożenia zewnętrzne
Incydent
Ryzyko
Wyciek danych

Jak łatwo pominąć istotne dane w analizie bezpieczeństwa?

- Zdarzenia i alerty bezpieczeństwa
- Logi i dane konfiguracyjne
- Aktywność użytkowników
- Listy zagrożeń i podatności

Co pomijamy?

Analitycy wykorzystują tylko ok 8% niezbędnych danych do skutecznej analizy incydentów bezpieczeństwa

Przykłady:

- Dokumentacja
- Publikacje branżowe
- Informacje śledcze
- Threat intelligence
- Prezentacje
- Raporty analityczne
- Strony www
- Wiki
- Blogi
- Media
- Newslettery
- Tweety

Typowe czynności wykonywane przez analityków bezpieczeństwa IT

Przeglądanie listy incydentów w SIEM

Analiza danych - zdarzenia/flows

Modyfikacja zapytań aby uzyskać dodatkowy kontekst

Dokonanie priorytetyzacji

Analiza malware'u w oparciu o dedykowane narzędzia np. VirusTotal, IBM X-Force, Cisco Talos

Identyfikacja malware'u

Analiza zewnętrznych raportów

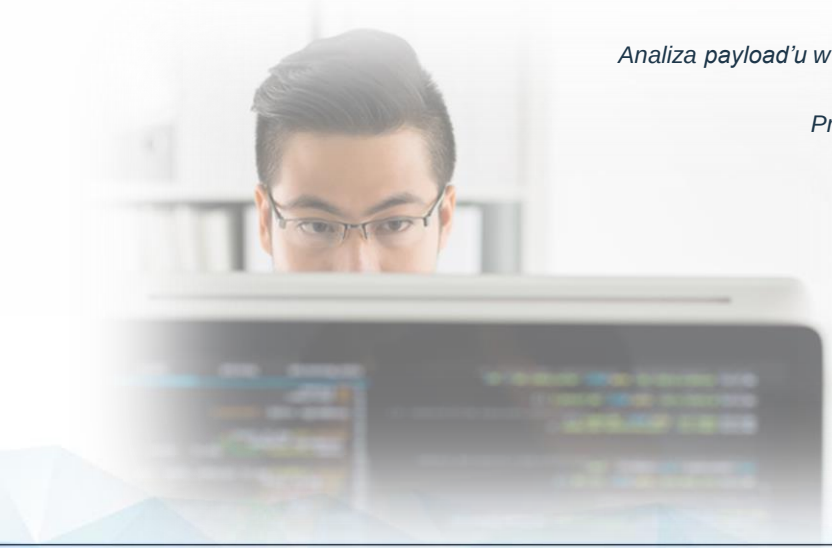
Identyfikacja innych elementów infrastruktury podatnych na atak

Porównanie analizy uzyskanej z zewnętrznych źródeł z elementami incydentu

Analiza payload'u w poszukiwaniu przydatnych informacji np.. Domain, MD5

Przeszukiwanie zgromadzonych danych w kontekście podejrzanych plików, URL, komunikacji

Rozpocznij ponownie analizę dla każdego odkrytego IP



Musi istnieć lepszy sposób!

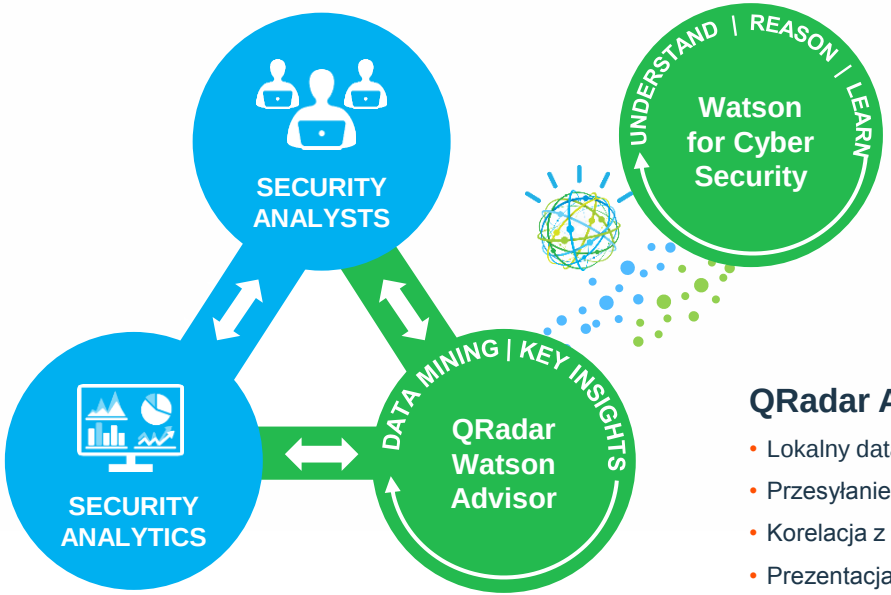
QRadar Advisor with Watson wraz Watson for Cyber Security

Analitycy

- Pomysłowość
- Intuicja
- Przeczucie
- Doświadczenie
- Wiedza

Narzędzia

- Korelacja danych
- Identyfikacja wzorców
- Wykrywanie anomalii
- Priorytetyzacja
- Wizualizacja



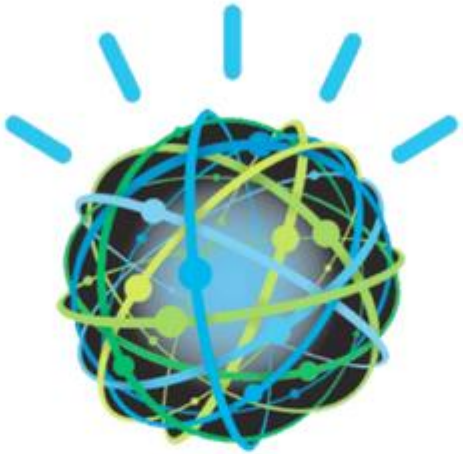
Watson for Cyber Security

- Klasyfikacja danych
- Stawianie tez i analiza
- Machine Learning
- Eliminacja zniekształceń
- Ciągłe udoskonalanie
- Analiza danych (strukturalnych i niestrukturalnych)

QRadar Advisor with Watson

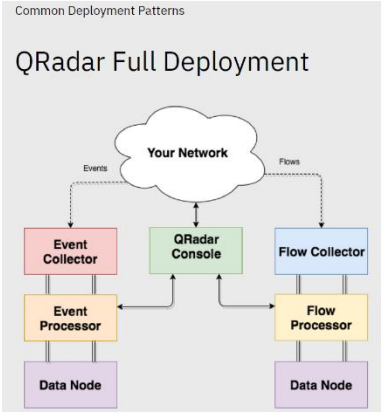
- Lokalny data mining
- Przesyłanie danych do Watson for Cyber Security
- Korelacja z Incydentami bezpieczeństwa
- Prezentacja rozwiązania

QRadar Advisor with Watson - w akcji



IBM WATSON

Architektura IBM Qradar

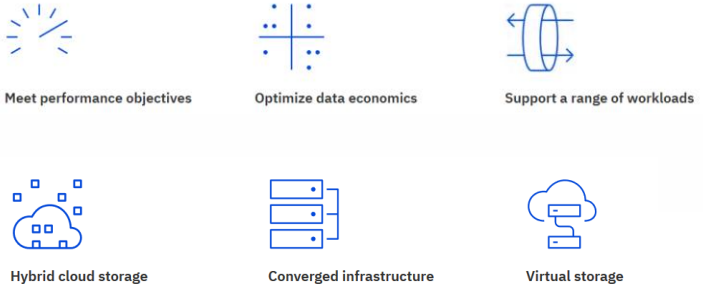


- AIO lub architektura rozproszona?
- HW Appliance, Software, Virtual Appliance?
- Storage -wydajność, retencja, elastyczność?

IBM Spectrum Storage

IBM Storage

- IBM FlashSystem 9100
- IBM Storwize V7000F
- IBM Storwize V5100F
- IBM Storwize V5100
- IBM Storwize V7000 with NVMe



Podsumowanie

Poprawiona wydajność analizy incydentów i reakcji na nie

- Analiza zajmuje kilka sekund lub minut
- Analityk bezpieczeństwa może zareagować na zagrożenie nawet 60x szybciej
- Szerszy kontekst incydentu ujawniający pełniejszy obraz objawów
- Lepsze podejmowanie decyzji w planowaniu odpowiedzi

Pewność oceny incydentów

- Spójność i niezawodność procesu dochodzeniowego
- 10x więcej przydatnych informacji, dla skutecznej aby odkryć nowe zagrożenia

Szersza wiedza na temat bezpieczeństwa

- Zagregowany widok wszystkich informacji związanych z incydentem - wiedza lokalna i zewnętrzna
- Umiejętność wykorzystania wiedzy historycznej, a także najnowszych odkryć

Nie bierze urlopu!