WDROŻENIE RSA NETWITNESS SUITE W BRANŻY E-COMMERCE

AKTYWNE MONITOROWANIE DO 60K EPS ORAZ DO 20 GBPS RUCHU SIECIOWEGO

Oczekiwania Klienta

Założeniem projektu było wdrożenie takiego systemu klasy SIEM, który będzie również platformą threat huntingową pozwalającą na aktywne monitorowanie w czasie rzeczywistym do **60k EPS oraz do 20 Gbps ruchu sieciowego**.

Wybór partnera technologicznego, który zrealizuje wdrożenie i zaprojektuje architekturę bezpieczeństwa IT był poprzedzony analizą rozwiązań SIEM oraz projektami POC mającymi sprawdzić kompetencje dostawców. Ostatecznie do realizacji projektu wybrano **specjalistów Mediarecovery**, którzy na podstawie swojego doświadczenia i wiedzy zaproponowali wdrożenie platformy **RSA NetWitness** oraz dostosowali architekturę IT Security, aby zapewniała wyższy poziom bezpieczeństwa.

Licencje

Zgodnie z założeniami, elementy systemu RSA dostarczone zostały z licencją wieczystą (perpetual license) wraz ze wsparciem producenta.

Komponenty do monitorowania części biurowej dostarczono w opcji wirtualnej. W wariancie wirtualnym system rozliczany jest w zależności od ilości danych przetwarzanych przez system w jednostce czasu (przepustowość GB/day). Natomiast

komponenty monitorowania Data Center dostarczono w opcji sprzętowej, w której ilość danych analizowanych przez system ograniczona jest jedynie wydajnością zastosowanego sprzętu. W ten sposób osiągnięto jednocześnie bardzo wysoką wydajność i skalowalność dostarczonego rozwiązania.

Zaimplementowane rozwiązania

Platforma RSA NetWitness Suite wychodzi poza standardową funkcjonalność SIEM, pozwalając na wykrywanie zaawansowanych ataków w czasie rzeczywistym, odpowiednie zarządzanie incydentem oraz rekonstrukcję ataku. Dzięki przechwytywaniu ruchu sieciowego, zbieraniu zdarzeń z endpointów (EDR) oraz korelacji zdarzeń z każdej płaszczyzny monitorowania, system RSA NetWitness podnosi efektywność i skuteczność wykrywania zagrożeń minimalizując czas bezczynności.

Kluczowe elementy:

Silnik korelacyjny (Event Strem Analysis):

- Koreluje zdarzenia, logi, przepływy sieciowe, istotne informacje z przechwyconego ruchu sieciowego oraz dane z endpointów. Pojedyńcza instancja jest w stanie przeanalizować nawet do 100k EPS

Silnik Reagowania (Reposne Engine):

- Pozwala zrozumieć scenariusz działania atakującego, dzięki pełnej rekonstrukcji ataku, analizie całego procesu oraz podejrzanych zdarzeń, zachowań i incydentów

Silnik raportowy (Reporting Engine):

- Umożliwia budowanie reguł opartych nie tylko o logi, ale również o ruch sieciowy

Moduł Live:

- Posiada dostęp do platformy RSA udostępniającej gotowe parsery, reguły apliakcyjne oraz sieciowe, feedy, listy aktywne, gotowe raporty itp.

Architektura

W skład zaprojektowanej przez specjalistów Mediarecovery architektury wchodzą poniższe komponenty:

- NW Server (SA) - stanowi konsolę zarządzania systemem, zdarzeniami i incydentami oraz prowadzenia dochodzeń.
- Event Stream Analysis (ESA) - zapewnia mechanizm procesowania i korelacji zdarzeń.
- Dekoder pakietów - umożliwia gromadzenie, filtrowanie i analizę pakietów ruchu sieciowego w czasie rzeczywistym.
- Dekoder logów - zapewnia gromadzenie, filtrowanie i analizę logów systemowych w czasie rzeczywistym.
- Concentrator - agreguje metadane w celu zapewnienia dostępności i skalowalności. Jego zadaniem jest indeksacja metadanych pozyskanych z sieci lub logów i udostępnienie ich na potrzeby zapytań i analiz w czasie rzeczywistym, jak również wsparcia procesu raportowania i systemu alarmowego.
- Remote Log Collector (VLC) - umożliwia odbieranie logów w zdalnych lokalizacjach oraz ich przesłanie za pomocą

szyfrowanego połączenia. Dodatkowo wspiera konfigurację wysokiej dostępności (wysokiej niezawodności).

- Archiver - składuje logi oraz metadane w długim terminie, umożliwia eksport danych na zewnętrzne zasoby dyskowe w celu wykonania kopii zapasowych.
- Broker - umożliwia przeglądanie metadanych znajdujących się na urządzeniu Archiver. Wymagany jest w przypadku wykorzystania opcji logowania pełnych pakietów.

Na co warto zwrócić uwagę w tym projekcie?

Krótki czas trwania projektu
Projekt wdrożeniowy trwał tylko 54 dni! Dogłębne zrozumienie potrzeb Klienta, ścisła współpraca między Klientem a zespołem Mediarecovery oraz zastosowanie metodyki Agile przy realizacji projektu to elementy, które spowodowały, iż projekt wdrożeniowy (bez fazy planowania i Proof of Concept) zakończył się pełnym sukcesem w niespełna 3 miesiące.

Największe wdrożenie tego typu
Wdrożone rozwiązanie ma dokonywać ciągłej analizy 60k EPS oraz do 20 Gbps ruchu sieciowego.

Zastosowanie hybrydowego podejścia
Architektura rozproszona z wykorzystaniem komponentów idealnie dopasowanych do wymagań:

- komponenty sprzętowe - do monitorowania dużej ilości danych w Data Center.
- komponenty wirtualne - do monitorowania rozproszonego środowiska biurowego.

Najważniejsze korzyści powdrożeniowe dla Klienta

- Zabezpieczenie stabilności krytycznych procesów biznesowych, których naruszenie mogłoby spowodować straty związane z utratą wizerunku.
- Możliwość szybkiego wykrycia ewentualnych objaw ataku oraz podjęcia szybkich działań w przypadku jego wystąpienia, dzięki zbieraniu informacji w czasie rzeczywistym z ruchu sieciowego.
- Zapewnienie wysokiego poziomu bezpieczeństwa aktualnych transakcji oraz użytkowników platformy e-commerce.
- RSA NetWitness, jako jedyne rozwiązanie, pozwala na generowanie raportu zwierającego pełen zrzut PCAP, ekstrakcję plików, rekonstrukcję wiadomości mailowych, strony internetowe - protokoły aplikacyjne np. HTTP/HTTPS. Dzięki tej funkcji w 72h, zgodnie z Rozporządzeniem o Ochronie Danych Osobowych, spółka jest w stanie dostarczyć Organowi Nadzorczemu kompleksowe informacje dot. incydentu.

Kontakt

Media Sp. z o.o.
ul. Piotrowicka 61, 40-723 Katowice
tel: +48 32 782 95 95
e-mail: biuro@mediarecovery.pl