McAfee SIEM

Przedstawiamy rozwiązanie klasy SIEM bazujące na produktach służących do monitorowania informacji bezpieczeństwa i ochrony danych firmy McAfee, będącej liderem rynku w obszarze bezpieczeństwa teleinformatycznego.

Oferowany przez nas system SIEM umożliwia zbieranie informacji ze wszystkich systemów – zarówno informatycznych (Solaris, Linux, HP-UX, Windows, Exchange, Lotus, Oracle, itp.), urządzeń sieciowych, baz danych, aplikacji, systemu DLP, systemów bezpieczeństwa oraz systemów fizycznego dostępu. Zebrane dane polegają analizie, a jej wyniki prezentowane są w jednej wspólnej konsoli.

Monitorowanie systemu fizycznego dostępu może polegać np. na wdrożeniu w SIEM korelacji pomiędzy systemami rejestracji wejść / wyjść (bramki elektroniczne na karty zbliżeniowe) i danymi o logowaniach użytkowników do systemu w celu wychwycenie anomalii polegających między innymi na połączeniach zdalnych (przez VPN) użytkowników, którzy jednocześnie według danych z systemu wejścia / wyjścia przebywają w budynku.

Proponowane rozwiązanie może znaleźć zastosowanie w systemach informatycznych klasy SMB i Enterprise, czyli od kilkuset do kilkudziesięciu tysięcy użytkowników.

Funkcje SIEM mogą być realizowane np. w oparciu o:

- centralne urządzenie analityczno-zarządzające **McAfee ESM 5700** oferujący obsługę 65 000 zdarzeń na sekundę i wydajność analityczną na poziomie poniżej 1 minuty dla danych zebranych w ciągu 30 dni oraz pojemność dyskową 32 TB + 800 GB SSD.
- moduł archiwizujący **ELM 4700** o maksymalnej wydajności 55 000 zdarzeń na sekundę i dyskach 5,6 TB SSD, o ile zachowanie logów w oryginalnej postaci będzie konieczne.
- jeden lub więcej modułów zbierających np. **ERC 2650** o wydajności do 14 000 zdarzeń na sekundę.

W/w urządzenia zawierają utwardzony system operacyjny i wbudowaną bazę danych **McAfee EDB**.

Do rozszerzenia pojemności bazy danych natychmiast dostępnych dla ESM można zastosować dedykowaną pamięć masową np. DAS50 (pojemność 50 TB).

ESM pełni rolę centralnego narzędzia zbierającego informacje z poszczególnych elementów rozwiązania oraz analityczno-raportowego udostępniającego dodatkowy kontekst do badanych zdarzeń.

ESM zapewnia centralne:

- zarządzanie systemem ESM, ERC i ELM przez jedną konsolę webową;
- zbieranie danych z innych źródeł;
- tworzenie i wdrażanie polis korelacyjnych;
- zarządzanie użytkownikami;
- tworzenie i dostosowywanie widoków i raportów.

ESM zapewnia korelację zdarzeń bezpieczeństwa dla wielu systemów IT w obrębie zintegrowanej i wbudowanej relacyjnej bazy danych, a ponadto umożliwia wybranemu personelowi monitorowanie bezpieczeństwa w czasie rzeczywistym polegające na możliwości:

- wykrywania anomalii na podstawie dynamicznie wyznaczanych linii bazowych,
- korelacji zdarzeń na podstawie reguł i ryzyk,
- prowadzeniu analizy behawioralnej, maszynowego uczenia się i analizy przepływów sieciowych.

ESM zbiera dane przy użyciu następujących metod: zbieranie logów pasywnych, zbieranie logów z autentykacją, CEF, OPSEC, SDEE, XML, ODBC.

ESM ma możliwość zbierania przepływów sieciowych w formacie Netflow, Sflow, Jflow i danych IPFIX oraz może je w pełni udostępnić na potrzeby analizy i korelacji.

ESM ma możliwość zbierania danych z bramek elektronicznych na karty zbliżeniowe i innych urządzeń bezpieczeństwa fizycznego oraz używania tych danych do budowania modelu działania systemu, wykrywania i interpretacji anomalii i naruszeń.

Rozwiązanie SIEM ma możliwość dołączenia dedykowanych dodatkowych urządzeń wspierających monitorowanie np. baz danych i aplikacji.

ESM poza zbieraniem, przechowywaniem i raportowaniem informacji dotyczących monitorowanych zdarzeń daje możliwość zwiększenia zakresu zbieranych informacji – również czasowego oraz wykorzystania ich w przygotowywanych analizach bezpieczeństwa i prowadzonych śledztwach, co umożliwia szybkie przygotowanie reakcji na incydent.

Dodatkowe funkcjonalności ESM:

- zdolność do wykrywania urządzeń i budowanie topologii sieci;
- możliwość geolokacji zdarzeń (baza adresów IP zarówno dla logów/zdarzeń jak i przepływów sieciowych z dokładnością do poziomu kodu pocztowego);
- integracja z systemem autentykacji Microsoft Active Directory (AD) i mapowanie grup użytkowników wraz z ich uprawnieniami;
- możliwość tworzenia stref adresów IP pozwalających na obsługę możliwego w środowisku IT nakładania się adresów IP, polegające na użyciu tych samych zakresów adresowych w różnych podsieciach;
- komunikacja z urządzeniami sieciowymi (np. przełącznikami LAN) w zakresie np. niedostępności portów lub zmiany przypisanego VLAN, bezpośrednio ze swojej konsoli zarządzającej, za pomocą protokołu SNMP lub profilu CLI (SSH, telnet);
- możliwość synchronizacji czasu przy użyciu protokołu NTP;
- możliwość grupowej dystrybucji agentów za pomocą zewnętrznych narzędzi np. MS SCCM, GPO, Altiris;
- możliwość budowania wewnętrznej bazy zasobów organizacji;
- automatyczna klasyfikacja logów, czyli możliwość wykrywania nowych źródeł danych poprzez analizę ruchu TCP;
- możliwość przeglądania logów w postaci niezaprzeczalnej za pomocą wyszukiwarki pełnotekstowej;
- powiązanie z polityką bezpieczeństwa – możliwość, w oparciu o reguły korelacyjne, zestawiania logów, przepływów sieciowych i informacji ze skanerów podatności z polityką bezpieczeństwa informacji;
- zbieranie informacji o zasobach – możliwość zbierania informacji o zasobach sieciowych poprzez import danych ze skanerów podatności;
- monitorowanie konfiguracji urządzeń sieciowych – umożliwia monitorowanie stanu urządzeń sieciowych i zmian w ich konfiguracjach oraz prowadzenie dziennika tych zmian. Badanie stanu konfiguracji odbywa się przez definiowalny profil CLI z użyciem protokołów SSH, Telnet.

ESM jest elementem zarządzającym i jednocześnie integrującym w jedną całość wszystkie elementy systemu monitorowania, które są podłączone pośrednio lub bezpośrednio do ESM. Udostępniana przez ESM jednolita, graficzna konsola systemu pozwala na wygodne zarządzanie wszystkimi zebranymi w jednej bazie danych informacjami.

ESM zawiera zarówno typowe szablony widoków (pomocne do prowadzenia śledztw) oraz tradycyjnych raportów – przygotowane przez producenta. Ma również gotowe szablony raportów do monitorowania aplikacji, baz danych, raporty dla kierownictwa, raporty incydentów, raporty anomalii, raporty przepływów sieciowych.

ESM posiada graficzny edytor raportów i widoków, co oznacza możliwość tworzenia własnych raportów dla wszystkich zebranych danych.

ESM generuje raporty (również w trybie ad-hoc) w czasie poniżej 5 minut za okres 30 dni bez względu na ilość zgromadzonych w tym okresie. Generowanie raportów nie wpływa na zdolność zbierania nowych zdarzeń.

ESM na możliwość przeszukiwania, sortowania i filtrowania dużej ilości zdarzeń w czasie rzeczywistym.

ESM pozwala na przeglądanie zdarzeń na podstawie bardzo wielu kryteriów np. adres MAC, adres IP, adres IPv6, port, identyfikator interfejsu, geolokacja, protokół sieciowy, użytkownik, podjęta akcja, identyfikator sygnatury, typ urządzenia, kategoria i identyfikator reguł normalizacyjnych, aplikacja, host, domena, komenda, obiekt, czas i data.

ESM z poziomu widoku udostępnia wszystkie zarejestrowane szczegóły zdarzenia.

ESM umożliwia szybki, zbliżony do rzeczywistego, dostęp do zebranych danych.

ESM ma możliwość eksportu raportów do plików w formacie PDF, CSV.

ESM umożliwia tworzenie grup użytkowników i przypisywanie im uprawnień do poszczególnych raportów.

ESM umożliwia tworzenie raportów i przeglądanie wszystkich logów powiązanych z określonym adresem IP, portem lub urządzeniem. ESM indeksuje dane o zdarzeniu, według szeregu kryteriów, oraz wyświetla raporty na podstawie tych danych.

Partner McAfee:
Orion Instruments Polska

05-082 Latchorzew, ul. Warszawska 164

tel. 22 638 31 45, fax 22 350 55 99, e-mail orion@orion.pl

więcej informacji: www.orion.pl/siem