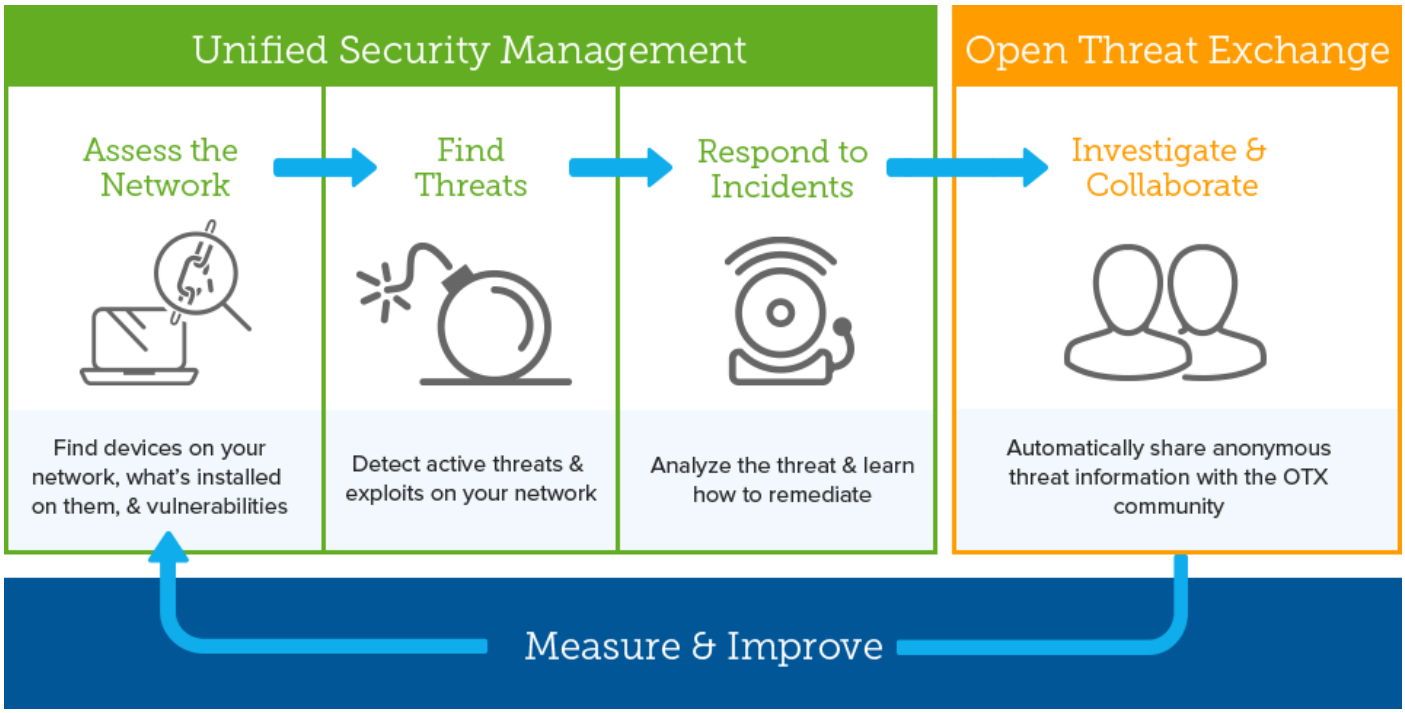
AlienVault USM

AlienVault Unified Security Management™ (USM) jest platformą typu all-in-one
Została ona zaprojektowana i jest pozycjonowana tak, aby małe i średnie organizacje mogły skutecznie bronić się przed występującymi dziś zaawansowanymi zagrożeniami.

W przeciwieństwie do tradycyjnych systemów SIEM i punktowych produktów bezpieczeństwa AlienVault USM zapewnia:

- ujednolicone i skoordynowane monitorowanie stanu bezpieczeństwa;
- proste zarządzanie i raportowanie zdarzeń bezpieczeństwa;
- działającą w sposób ciągły wiedzę o zagrożeniach – Threat Intelligence;
- szybkie i bezproblemowe wdrożenie;
- dostęp do wielu funkcji bezpieczeństwa bez konieczności korzystania z licznych konsol.



Unified Security Management™ (USM): kompletny, prosty i w przystępnej cenie.

Produkty z rodziny Unified Security Management™ (USM) firmy AlienVault pozwalają organizacjom z ograniczonym personelem i budżetem zarządzać zagrożeniami bezpieczeństwa i skutecznie kontrolować zgodność z wymaganymi regulacjami.

Doskonały bieżący obraz stanu zabezpieczeń uzyskać można dzięki wbudowanym wskaźnikom bezpieczeństwa oraz ciągłej aktualizacji wiedzy o zagrożeniach otrzymywanych z AlienVault Labs.

Badanie zagrożeń kluczowe dla dzisiejszego krajobrazu zagrożeń cybernetycznych.

Środowisko zagrożeń rozwija się i zmienia na tyle dynamicznie, że przeciążone zespoły bezpieczeństwa nie mają ani czasu ani środków, aby we własnym zakresie analizować bieżące zagrożenia, dlatego tak ważne jest korzystanie z wyników prac organizacji badawczych takich jak AlienVault Labs.

W przeciwieństwie do rozwiązań, które skupiają się na jednym rodzaju zagrożeń i na jednym tylko wskaźniku bezpieczeństwa, AlienVault Labs Threat Intelligence dostarcza osiem skoordynowanych zestawów reguł zasilanych w sposób ciągły dzięki działaniom społeczności skupionej wokół Open Threat Exchange™.

AlienVault Labs Threat Intelligence zasila USM danymi na temat identyfikacji najnowszych zagrożeń, co pozwala uzyskać najszersze pole widzenia technik ataków i zastosować najskuteczniejsze metody obrony.

Threat Intelligence firmy AlienVault maksymalizuje efektywność programu monitorowania bezpieczeństwa, dostarczając bezpośrednio do instalacji AlienVault Unified Security Management (USM) następujące funkcje:

→ sygnatury sieciowe IDS do wykrywania nowych zagrożeń w sieci;
→ sygnatury hostowe IDS do wykrywania najnowszych zagrożeń w systemach;
→ sygnatury wykrywania aktywów do identyfikacji najnowszych systemów operacyjnych, aplikacji i urządzeń;
→ sygnatury do oceny podatności pozwalające wykryć najnowsze luki w systemach;
→ reguły korelacji pozwalające dotrzeć do zdarzeń źródłowych (raw logs), które mogą stanowić podstawę prawną zaskarżenia;
→ moduły raportowania dostarczające nowe sposoby wyświetlania danych o środowisku;
→ dynamiczne szablony odpowiedzi na incydenty pozwalające na zastosowanie optymalnej reakcji na dany alarm;
→ wtyczki do nowo obsługiwanych źródeł danych rozszerzające zakres monitorowania.

Wiedza o zagrożeniach. Wykrywanie zagrożeń. Kluczowe korzyści.

Platforma USM™, zasilana w informacje dzięki Threat Intelligence, pozwala z łatwością wykrywać najnowsze zagrożenia i priorytetyzować odpowiedzi.

W szczególności, możliwe jest rozszerzenie programu ochrony poprzez:

→ wykrywanie botnetów w czasie rzeczywistym – identyfikacja zakażenia i niewłaściwego wykorzystania aktywów korporacyjnych;
→ wykrywanie eksfiltracji danych – zapobieganie wyciekom informacji wrażliwych lub zastrzeżonych;
→ identyfikację ruchu Command-and-Control (C&C) – identyfikacja skompromitowanych systemów komunikujących się ze złośliwymi podmiotami;
→ dane o reputacji IP, URL i domen – priorytetyzacja prób reakcji poprzez identyfikację rozpoznanych źródeł zagrożeń i zainfekowanych stron;
→ wykrywanie APT (Advanced Persistent Threat) – wykrywanie ukierunkowanych ataków często pomijanych przez inne punkty ochrony;
→ dynamiczne reagowanie na incydenty i wytyczne dla śledztw – zapewnienie zindywidualizowanych instrukcji w jaki sposób reagować i badać każdy alarm.

Zaawansowana wiedza firmy AlienVault w walce z zagrożeniami.

Poniżej niektóre ze stosowanych przez AllienVault technik zbierania i analizy danych:

→ Analiza złośliwego oprogramowania. Do kwarantanny próbek malware wykorzystywane są zaawansowane techniki typu sandbox. AlienVault przeprowadza analizy statyczne i dynamiczne, analizując dziennie ponad 500 000 unikalnych próbek złośliwego oprogramowania. Badania te mają kluczowe znaczenie dla poznawania najnowszych narzędzi i technik ataków.
→ Analiza i wdrażanie honeypotów. Globalne honeypoty firmy AlienVault stanowią „wirtualną pułapkę" przeznaczoną do wykrywania, przechwytywania i analizowania najnowszych narzędzi i technik ataków. Dzięki wykorzystaniu honeypotów umieszczonych w dużych sieciach komunikacyjnych subskrybenci firmy AlienVault wyposażeni są w najnowsze strategie obronne w postaci aktualizacji reguł korelacji zdarzeń, sygnatur podatności IDS itp.
→ Analiza profilu napastnika. AlienVault stale monitoruje fora hakerskie i sieci podziemne w celu dogłębnego profilowania wspólnych cech cyberprzestępców. Informacje tego typu pozwalają na dogłębne zrozumienie „horyzontu ataku" i prowadzą do licznych odkryć w tym zakresie, takich jak ewolucja *Sykipot*, *Czerwony Październik* i innych epidemii złośliwego oprogramowania.
→ Otwarta współpraca z organami państwowymi, akademickimi i innymi firmami badawczymi w zakresie bezpieczeństwa. Producentowi, dzięki szerokiemu zasięgowi społeczności AlienVault w zakresie informacji o zagrożeniach, udało się nawiązać na całym świecie dobre stosunki z agencjami państwowymi, akademickimi ośrodkami badawczymi i dostawcami rozwiązań z dziedziny bezpieczeństwa. Relacje te umożliwiają firmie AlienVault dostęp do nie opublikowanych jeszcze luk i aktualizacji malware oraz weryfikację własnych badań. Poprzez gromadzenie wiedzy o zagrożeniach, pochodzącej od zróżnicowanej bazy różnej wielkości użytkowników z wielu różnorodnych branż i krajów, AlienVault jest w stanie ograniczać atakującym możliwość wyznaczania celów właściwych dla danego sektora lub wielkości organizacji.

Unified Security Management™ (USM) vs OSSIM

USM AlienVault jest rozwinięciem rozwiązania OSSIM (Open Source SIEM) i korzysta z jego najlepszych przymiotów oferując jednocześnie profesjonalne wsparcie oraz rozwinięcie kluczowych, z punktu widzenia bezpieczeństwa IT oraz łatwości użytkowania, cech.

Podstawowe różnice:

OSSIM	AlienVault
Społeczna analiza zagrożeń	Cotygodniowe uaktualnienia realizowane przez AlienVault Labs
Ograniczone zbieranie logów, retencja logów tylko dla zdarzeń SIEM	Zaawansowany log management, możliwość wyszukiwania logów, długookresowa retencja logów
Tylko trzy szablony raportów	Ponad 150 edytowalnych szablonów do tworzenia raportów, w tym pozwalające tworzyć raporty zgodne z regulacjami
Możliwość wdrożenia tylko na jednym serwerze	Wielopoziomowa skalowalna architektura umożliwiająca obsługę wielu serwerów w różnych lokalizacjach, a także za pomocą jednego serwera i wielu sensorów zbierających zdarzenia
Jeden użytkownik	Możliwość stworzenia wielu użytkowników z opcją ustawienia indywidualnego poziomu uprawnień dla każdego z nich
Oddzielne zarządzanie każdym z komponentów	Konsola umożliwiająca centralną konfigurację i obsługę wszystkich elementów systemu.
Wsparcie i rozwój dzięki aktywności społeczności OSSIM	Profesjonalne wsparcie AlienVault

Partner AlienVault w Polsce – jedyny dysponujący ACSE (AlienVault Certified Security Engineer):

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