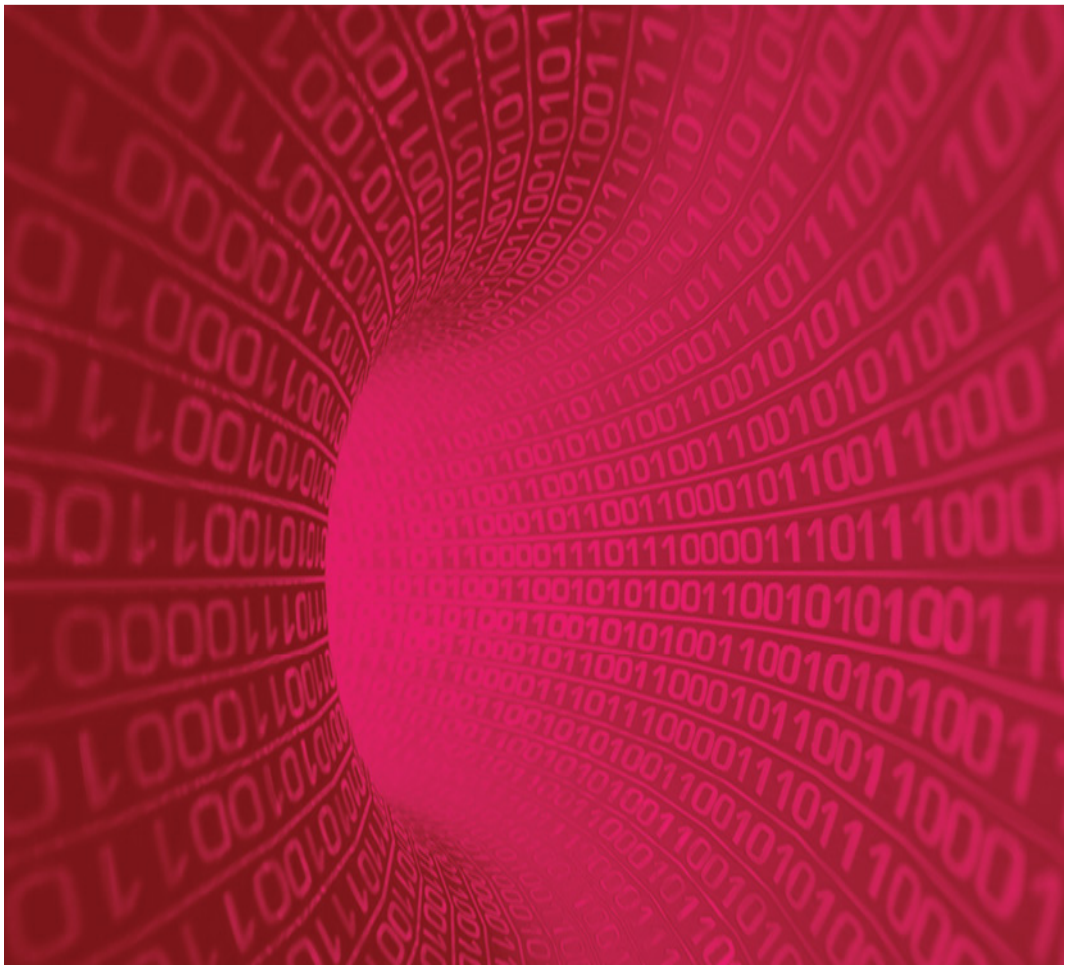
Intrusion Detection System



System Passus IDS jest rozwiązaniem, które monitoruje infrastrukturę IT przedsiębiorstwa wykrywając ataki oraz próby naruszenia zasad bezpieczeństwa. Wykryte incydenty mogą być zgłaszane bezpośrednio osobom odpowiedzialnym za bezpieczeństwo lub przekazywane do systemów klasy SIEM. Passus IDS wykorzystuje różne mechanizmy detekcji zagrożeń analizując ruch sieciowy na podstawie reguł. Do analiz wykorzystywane są zarówno wbudowane reguły jak i stale aktualizowane zewnętrzne zestawy reguł zgodnych z notacją SNORT. Zaawansowane mechanizmy tworzenia i edycji reguł pozwalają uniknąć nadmiernej ilości błędów false positive.

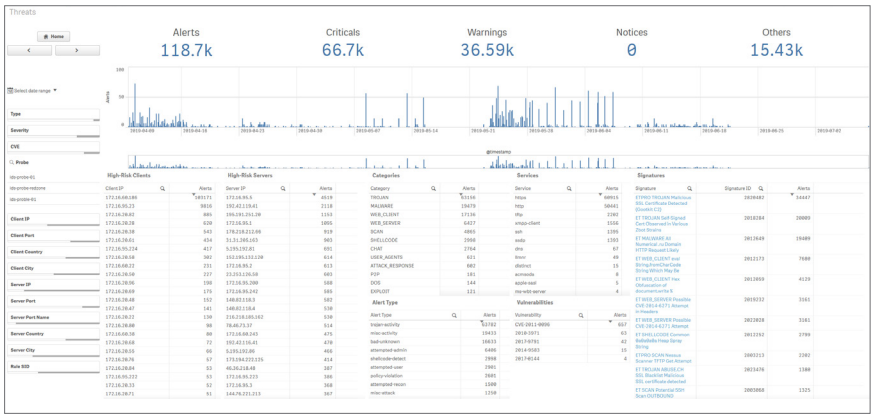
Kluczowe cechy rozwiązania

- Wykrywanie zagrożeń w oparciu o analizę ruchu sieciowego oraz zachowania systemu i urządzeń
- Predefiniowane widoki i zestawienia wykrytych incydentów
- Ponad 45 tysięcy reguł podzielonych na 40 kategorii
- Wbudowany kolektor zdarzeń, z pełnotekstowym mechanizmem wyszukiwania
- Integracja z systemami SIEM
- Intuicyjny mechanizm centralnego zarządzanie sondami
- Skalowalny, wieloprocesowy i wielowątkowy silnik przetwarzania reguł

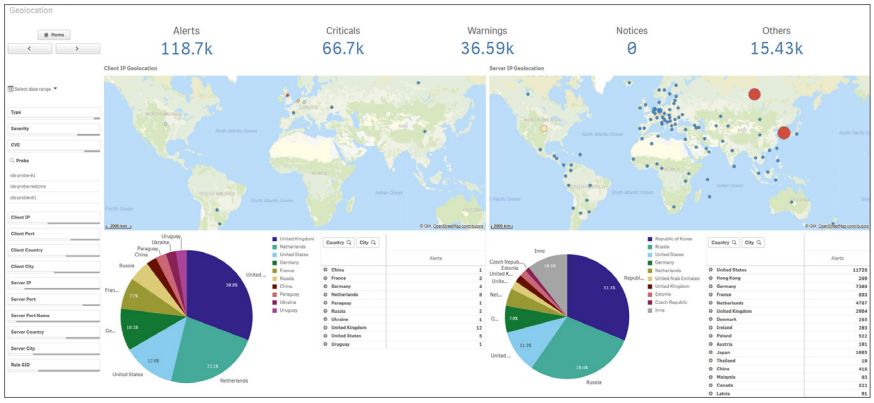
Passus SA | ul. Goraszewska 19, 02-910 Warszawa | telefon (+48) 695 444 804 | e-mail: passus@passus.com | www.passus.com

PASSUS IDS

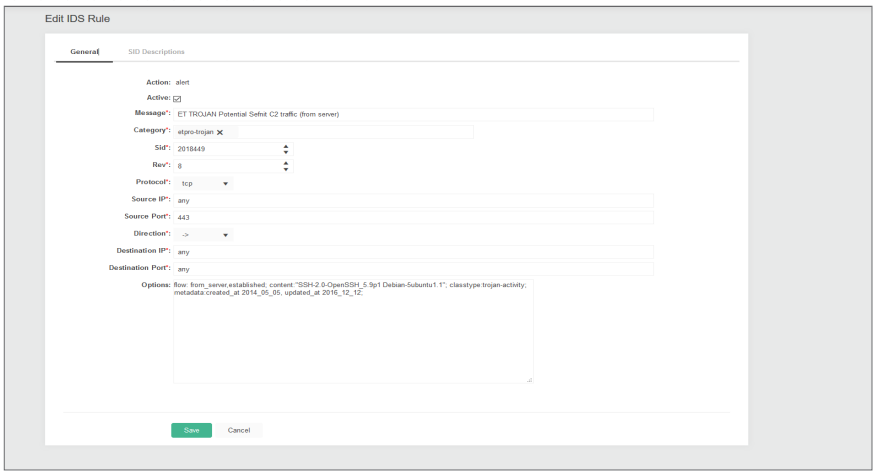
Passus IDS jest systemem klasy Enterprise wyposażonym w centralną konsolę do zarządzania sondami, mechanizmy kopii zapasowych, auditlog, funkcję importu i eksportu ustawień, możliwość wykorzystania reguł komercyjnych. Doskonale sprawdza się zarówno na styku z internetem (za systemem firewall, jak i do monitorowania ruchu wewnętrznego.



Widok zagrożeń prezentuje stacje i serwery, których dotyczą alarmy oraz klasyfikacja zagrożeń wg. kategorii, typów, usług, CVE i sygnatur.



Wizualizacja atakujących i atakowych obiektów na mapach.



Okno edycji reguły pozwala zdefiniować wszystkie parametry.

Szybki dostęp do kluczowych informacji

- Zarejestrowane w systemie zdarzenia są prezentowane w formie czytelnych tabel i wykresów zawierających m.in.:
  - ✓ liczbę wykrytych incydentów z uwzględnieniem priorytetów np. krytyczny lub informacyjny,
  - ✓ źródła powstania incydentów z uwzględnieniem adresów IP i geolokalizacji,
  - ✓ zdarzenia w formacie surowym tzw. „RAW" na potrzeby zaawansowanych analiz porównawczych,
  - ✓ wyniki analizy zdarzeń w odniesieniu do znanych podatności systemów opisywanych w CVE.
- Każdy widok umożliwia filtrowanie danych z uwzględnieniem przedziałów czasu i słów kluczowych.
- Użytkownik ma możliwość edycji istniejących widoków lub tworzenia nowych.
- Skalowalny i wydajny silnik indeksuje dane bezpośrednio w kolektorze dając możliwość pełnotekstowego przeszukiwania.

Mechanizm centralnego zarządzania sondami

System został wyposażony w mechanizm centralnego zarządzania, który w oparciu o interfejs graficzny umożliwia mi.in:

- zdefiniowanie i implementację parametrów pracy dla wszystkich lub wybranych sond,
- monitorowanie pracy sond i stały dostęp do informacji o jej statusie i aktualnej konfiguracji,
- definiowanie podsieci lokalnych i zdalnych, oraz adresów serwerów http w postaci zmiennej do wykorzystania w regułach,
- zarządzanie cyklem aktualizacji reguł wykrywania określonych wzorców ruchu,

- włączanie, wyłączanie reguł, a także ich edycję,
- wyszukiwanie i filtrowanie reguł wg różnych kryteriów (np. priorytetu zdarzenia, klasyfikacji zdarzenia, odniesienia do bazy CVE).

Zestaw reguł ProofPoint

Domyślnie wraz z licencją na system IDS dostarczana jest 12 - miesięczna subskrypcja na reguły ET Pro Ruleset firmy ProofPoint, która:

- zawiera ponad 45 tys. najnowszych reguł podzielonych na przeszło 40 kategorii,
- posiada rozbudowane opisy sygnatur, odnośniki i dokumentację,
- wykazuje wyjątkowo niski poziom false positive,
- jest stale aktualizowana – codziennie pojawia się kilkadziesiąt nowych reguł.

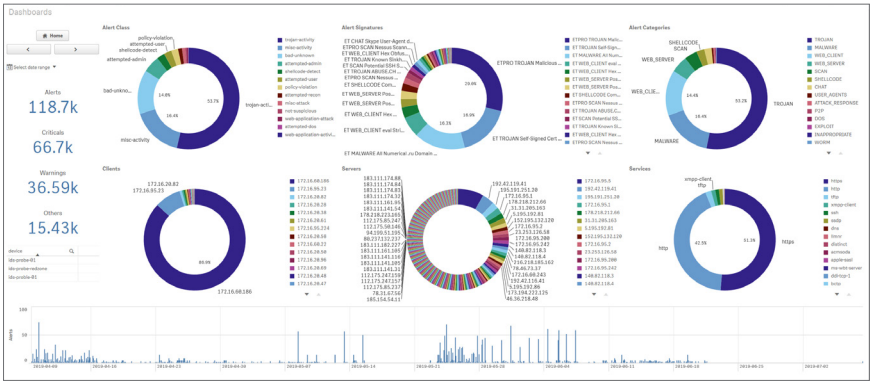
Możliwość dostosowania systemu do potrzeb klienta.

Passus oferuje szereg usług obejmujących m.in.:

- import zestawu reguł klienta,
- podłączenie dowolnego komercyjnego źródła reguł,
- stworzenie reguł dla nietypowych protokołów czy np. sieci przemysłowych,
- wsparcie inżynierów Passus podczas analizy incydentów,
- integrację rozwiązania z systemem SIEM lub innym rozwiązaniem umożliwiającym blokowanie nieporządanego ruchu.

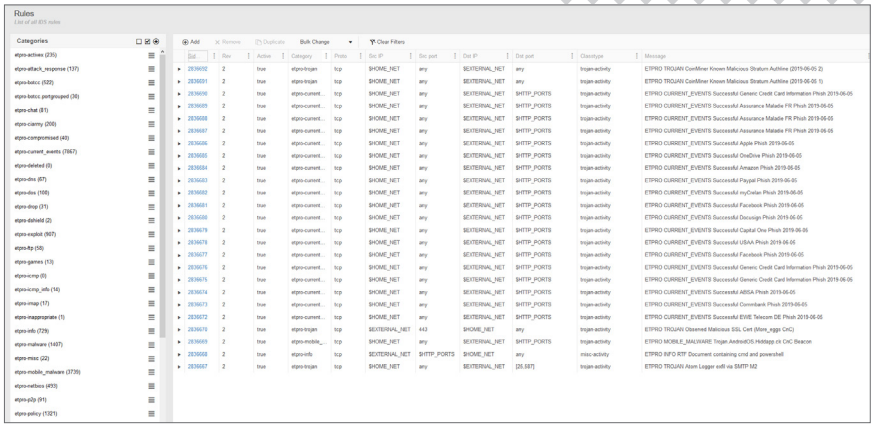
Passus IDS został wdrożony w jednej z wiodących firm z branży telekomunikacyjnej:

- wdrożenie objęło kilkanaście centralnie zarządzanych sond w różnych lokalizacjach,
- stale monitorowanych jest kilka tysięcy hostów,
- blisko 2Gb/s analizowanego ruchu,
- na życzenie klienta przygotowano szereg dostosowanych do jego potrzeb widoków i zestawień,
- dostosowano reguły i alerty do specyfiki środowiska informatycznego klienta.



Dashboard - agregacje - zestawienia podsumowujące najczęściej pojawiającej się typy ataków oraz najczęściej atakowane hosty i usługi.

Statystyki dot. pracy systemu w tym ilości analizowanego ruchu oraz liczby komponentów sprzętowych z uwzględnieniem poszczególnych sond.



Lista reguł umożliwia ich sortowanie, filtrowanie oraz grupową edycję typowych działań m.in. aktywacja,dezatywacja oraz zmiana kategorii.

Grupa Passus specjalizuje się w projektowaniu i wdrażaniu wysoko specjalizowanych rozwiązań informatycznych z zakresu monitorowania i poprawy wydajności sieci i aplikacji oraz bezpieczeństwa IT zarówno w architekturze on-premise jak i środowiskach hybrydowych, chmurze prywatnej i publicznej. W skład Grupy wchodzą firmy Passus S.A., Wisenet sp. z o.o. oraz Chaos Gears sp. z o.o.

Oferta Grupy obejmuje:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT w szczególności wykrywanie podatności, zabezpieczenie sieci, aplikacji oraz danych, systemy monitorowania i zarządzania incydentami bezpieczeństwa (SIEM/SOC);
- projektowanie rozwiązań chmurowych, migracja aplikacji i danych do chmury oraz wsparcie w zarządzaniu i optymalizacja środowiskiem cloud;

Nasi inżynierowie zrealizowali największe w Polsce projekty z zakresu Application and Network Performance Management oraz SIEM. **Ponad 20 lat współpracy z firmami oraz instytucjami z Polski i z zagranicy zaowocowało znajomością uwarunkowań biznesowych i technicznych tych organizacji.** Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Ikea, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Spółka zapewnia kompleksową obsługę, począwszy od analizy potrzeb, przez planowanie, usługi wdrożeniowe, rozwiązania na zamówienie, szkolenia pracowników, aż po opiekę serwisową oraz posprzedażną.

Grupa Passus jest partnerem firm Riverbed (Riverbed Premier Partner), Symantec (Gold Partner), IBM, Amazon Web Services, Fidelis Cybersecurity, Core Security, NetScout, New Relic, Cisco oraz Tenable. Passus posiada także własny zespół Research and Development. Na bazie zebranych doświadczeń zespół ten przygotował własne rozwiązania – zaawansowany sniffer sieciowy Passus Ambience oraz Passus FlowControl - system do monitorowania sieci w oparciu o protokół NetFlow.

Grupa zatrudnia blisko 60 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów. **Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.:** poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S, Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed NPM/APm Qualified Trainer, IBM Certified Deployment Professional Security QRadar SIEM, ArcSight Certificate AS Data Platform Technical, Certified Ethical Hacker, Offensive Security Certified Professional. W 2017 roku firma spełniła wymagania stawiane przez Agencję Bezpieczeństwa Wewnętrznego i uzyskała świadectwa bezpieczeństwa przemysłowego, które potwierdzają zdolność spółki do realizacji usług w instytucjach i gałęziach przemysłowych związanych z dostępem do informacji niejawnych - krajowych jak i NATO oraz Unii Europejskiej.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Od lipca 2018 roku spółka notowana jest na rynku NewConnect.