GET INSIGHT INTO APPLICATION,
NETWORK AND IT SECURITY

Producent i integrator rozwiązań IT

Dostarczamy specjalistyczne produkty i świadczymy usługi, które zapewniają ochronę przed cyberatakami oraz umożliwiają przeciwdziałanie kradzieży poufnych danych, upraszczają diagnozowanie oraz eliminację czynników, wpływających niekorzystnie na wydajność i dostępność sieci i aplikacji. Oferujemy też rozwiązania, które ułatwiają planowanie rozwoju infrastruktury IT oraz umożliwiają monitorowanie jej pracy. Nasza oferta obejmuje zarówno produkty własne jak i czołowych, światowych dostawców oraz specjalistyczne usługi umożliwiające w szczególności:

- zarządzanie wydajnością sieci i aplikacji krytycznych, diagnozowanie i rozwiązywanie problemów z wydajnością baz danych, serwerów oraz urządzeń sieciowych,
- zabezpieczanie przed zaawansowanymi zagrożeniami zewnętrznymi (np. malware, ransomware, atakami 0-day i APT) oraz nadużyciami wewnętrznymi,
- weryfikację podatności sieci, aplikacji na cyberataki,
- zabezpieczenie poufnych i wartościowych danych przed wyciekiem lub kradzieżą (ang. DLP),
- wyodrębnianie i transformację w czasie rzeczywistym informacji ze zdefiniowanych przez użytkownika strumieni danych (np. z ruchu sieciowego), logów i baz danych,
- wdrożenie rozwiązań cloud w oparciu o chmurę obliczeniową Amazon Web Services.

Passus SA | ul. Goraszewska 19, 02-910 Warszawa | tel. +48 695 444 803 | e-mail: passus@passus.com | www.passus.com

Wydajność aplikacji i infrastruktury IT

Oferujemy kompleksowe rozwiązania do monitoringu i optymalizacji wydajności sieci IT (LAN, WLAN, SD-WAN) oraz krytycznych aplikacji w dużych organizacjach. Ich zastosowanie pozwala zidentyfikować i wyeliminować przyczyny problemu bez względu na to, czy leżą one po stronie aplikacji, serwerów, sieci lub urządzeń końcowych. Główne obszary zastosowań tej grupy rozwiązań to:

- monitorowanie działania poszczególnych komponentów infrastruktury IT oraz informowanie o aktualnych parametrach jej pracy,
- identyfikacja źródeł problemów z wydajnością lub dostępnością aplikacji – precyzyjne wskazanie czy przyczyny problemu leżą po stronie serwerów, usług sieciowych, aplikacji, urządzeń końcowych,
- analiza działania aplikacji, poszczególnych komponentów serwera, weryfikacja jakości kodu aplikacji bez konieczności ingerencji w środowisko produkcyjne,
- monitorowanie i wykrywanie problemów z wydajnością aplikacji na urządzeniach końcowych poszczególnych użytkowników,
- alarmowanie o odstępstwach od przyjętych warunków SLA,
- prowadzenie audytów i dokumentacja sieci, automatyzacja procesu tworzenia diagramów sieciowych zawierających szczegółowe informacje o fizycznych i logicznych połączeniach między urządzeniami wraz z ich konfiguracją.

Realizując projekty z zakresu wydajności infrastruktury IT korzystamy z rozwiązań wiodących światowych producentów m.in. takich firm jak:

sycope riverbed NETSCOUT

cisco Partner splunk>

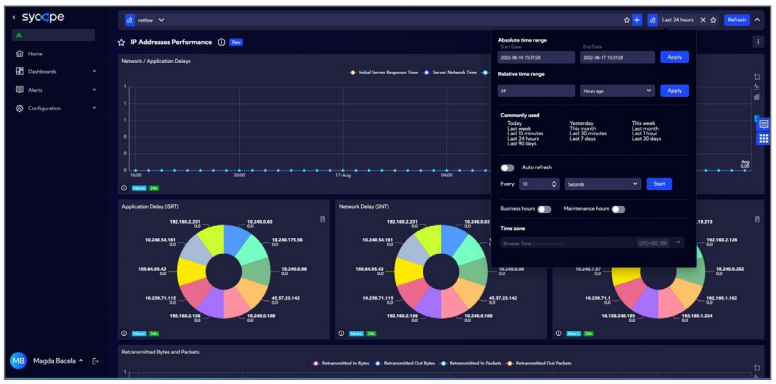
Passus SA | ul. Goraszewska 19, 02-910 Warszawa | tel. +48 695 444 803 | e-mail: passus@passus.com | www.passus.com

Wybrane projekty

Instytucja finansowa
System do monitoringu wydajności pracy aplikacji wykorzystywanych w Banku.

Riverbed, jeden z liderów rynku rozwiązań APM/NPM, oferuje kompleksową platformę do zarządzania wydajnością infrastruktury IT.

Firma konsultingowa
Rozwiązanie do optymalizacji wydajności infrastruktury IT w środowisku rozproszonym.



Sycope zapewnia szybki wgląd w działanie sieci IT, dzięki czemu menedżerowie IT mogą podejmować decyzje, pozwalające na uniknięcie nieplanowanych przestojów związanymi z awariami infrastruktury IT

Administracja publiczna (opieka zdrowotna)
Rozwiązanie do diagnozowania przyczyn problemów z połączeniami sieciowymi na podstawie danych z protokołu netflow.

Rozwiązania Splunk z obszaru tzw. „observability" umożliwiają monitoring m.in. środowisk Kubernetes czy usług opartych na mikroserwisach.

Bezpieczeństwo IT

Oferowane przez nas usługi i produkty pomagają zabezpieczyć dane oraz aplikacje (w tym aplikacje webowe) przed cyberatakami (m.in. 0-day, APT, ransomware, DDoS) oraz zagrożeniami wewnętrznymi, m.in. wyciekiem danych, nadużyciami lub nieświadomymi błędami użytkowników. Rozwiązania z tej kategorii, umożliwiają m.in.:

- weryfikację odporności środowiska informatycznego na próby przełamania zabezpieczeń wraz z oceną ryzyka i konsekwencji biznesowych wynikających z określonych luk lub podatności,
- monitorowanie ruchu sieciowego (w tym także ruchu szyfrowanego) oraz zachowania aplikacji w celu identyfikacji anomalii świadczących o ataku lub naruszeniu procedur bezpieczeństwa,
- wykrywanie skompromitowanych lub zapomnianych urządzeń,
- aktywne blokowanie zaawansowanych ataków (0-day, APT, ransomware) oraz zapobieganie wyciekom danych oraz dokumentów,
- prowadzenie działań z zakresu informatyki śledczej - odtworzenie przebiegu ataku lub procesu, który doprowadził do wycieku danych,
- szyfrowanie i zabezpieczanie poufnych danych przed ich utratą lub kradzieżą, bez względu na to, gdzie są przechowywane lub w jaki sposób są przekazywane,
- monitorowanie sesji zdalnych oraz aktywności firm świadczących usługi w formie outsourcingu,
- podnoszenie świadomości pracowników.

Rozwiązania z zakresu bezpieczeństwa IT tworzymy w oparciu o własne produkty i usługi, jak i z wykorzystaniem narzędzi wiodących producentów:

splunk> BROADCOM tenable Fidelis Cybersecurity

sycope cybereason MANDIANT Trellix

CORE SECURITY mira SECURITY ManageEngine

Wybrane projekty

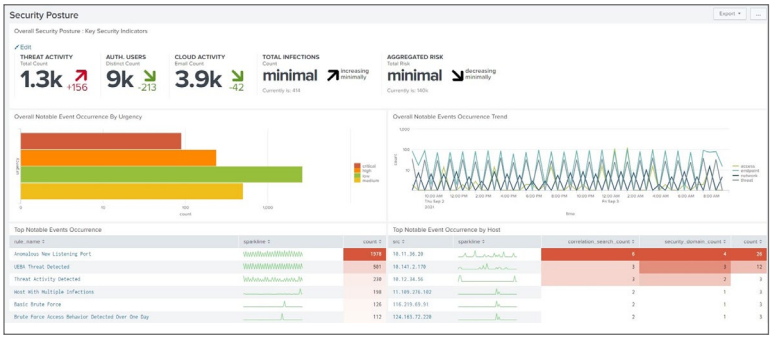
Operator sieci przesyłowej
Sprzedaż licencji, zaprojektowanie i wykonanie rozwiązania zapobiegającego wypływom informacji

Spółka Skarbu Państwa
Zaawansowana platforma do monitoringu i ochrony sieci przedsiębiorstwa wraz z wdrożeniem, usługami wsparcia technicznego i asysty w okresie 36 miesięcy

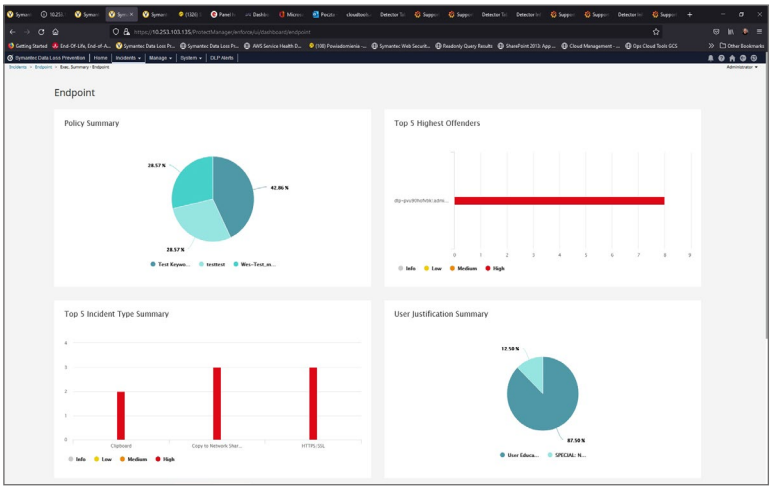
Branża motoryzacyjna
System ochrony poczty elektronicznej wraz z wdrożeniem integracją, opracowanie procedur operatora

Ministerstwo
Wdrożenie systemu zarządzania informacją i zdarzeniami bezpieczeństwa SIEM/SOAR wraz z wdrożeniem i wsparciem technicznym

Instytucja finansowa
Wdrożenie rozwiązania klasy SIEM umożliwiającego agregowanie i korelowanie w jednym miejscu danych, pochodzące z wielu systemów bezpieczeństwa.



Splunk Enterprise Security (ES) jest nowoczesnym rozwiązaniem do zarządzania informacjami i incydentami bezpieczeństwa (SIEM).



Rozwiązanie DLP firmy Broadcom znajduje się w gronie liderów w raporcie Forrester: Unstructured Data Security Platforms, Q2 2021.

Mandiant Security Validation umożliwia weryfikację infrastruktury odpowiadającej za bezpieczeństwo IT, pozwala edukować zespół i ustalać priorytety rozwoju SOC.

Sycope wykrywa i analizuje anomalie i zagrożenia bezpieczeństwa w oparciu o ruch sieciowy (protokół NetFlow) oraz porządkuje je zgodnie z metodologią MITRE ATT&CK.

Infrastruktura – budowa, wdrożenie i zarządzanie

Oferujemy rozwiązania do zarządzania operacjami IT związanymi ze środowiskiem sieciowym, serwerami, aplikacjami w tym usługami wsparcia technicznego (service-desk), obsługą środowiska Active Directory, urządzeń końcowych. Umożliwiają one:

- zarządzanie, z jednego centralnego miejsca serwerami, stacjami roboczymi i urządzeniami mobilnymi, zapewniając tym samym pełną kontrolę nad zasobami IT oraz oprogramowaniem,
- kompleksowe zarządzanie środowiskiem Active Directory w tym monitorowanie i raportowanie wszelkich wprowadzonych zmian,
- automatyzację działań związanych z obsługą zgłoszeń serwisowych (service-desk),
- zarządzanie środowiskiem Office365, w tym grupowe zarządzanie użytkownikami oraz delegacja uprawnień.

Dostarczamy i wdrażamy specjalistyczne urządzenia sieciowe w tym m.in.:

- brokery pakietów pozwalające na agregację przepływu pakietów, replikację, równoważenie obciążenia sieci oraz filtrowanie ruchu,
- specjalistyczne routery umożliwiające bezpieczną komunikację w sieciach bankomatowych, automatach loteryjnych, w autobusach, pociągach itp.
- rozwiązania i usługi do akceleracji sieci.

Rozwiązania do budowy i zarządzania infrastrukturą tworzymy w oparciu o produkty i usługi wiodących światowych producentów:

ManageEngine Gigamon DIGI NETSCOUT Cisco Partner

Passus SA | ul. Goraszewska 19, 02-910 Warszawa | tel. +48 695 444 803 | e-mail: passus@passus.com | www.passus.com

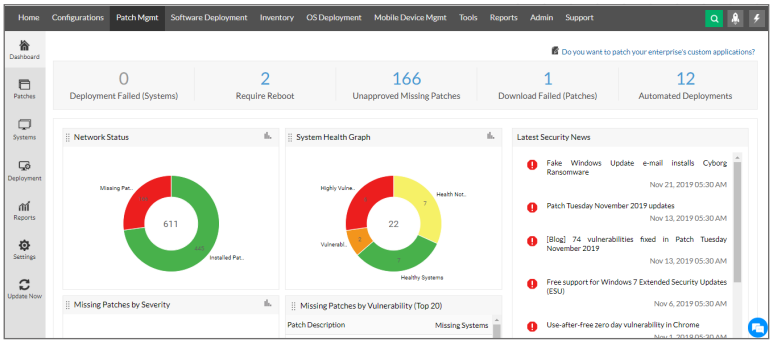
Wybrane projekty

Ministerstwo

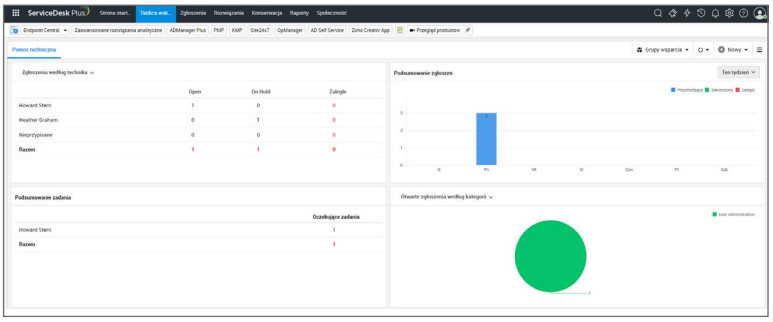
dostarczenie i wdrożenie rozwiązania do zarządzania urządzeniami końcowymi (stacjami roboczymi, serwerami, urządzeniami mobilnymi)

Sieć restauracji

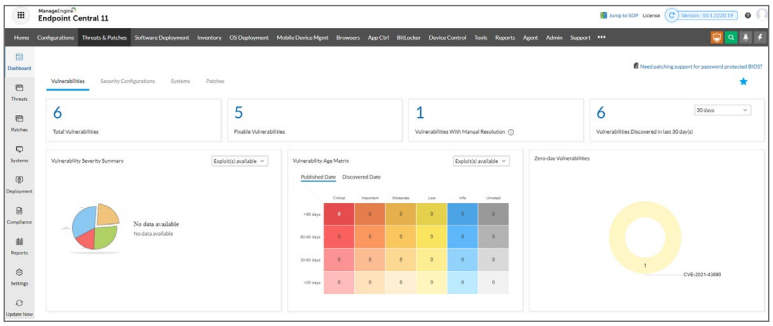
Wykorzystanie routerów Digi w restauracjach jako rozwiązanie awaryjne dla istniejącej kablowej infrastruktury łączności (kasy fiskalne, terminale).



Czytelny dashboard Manage Engine PatchManager z najważniejszymi informacjami na temat procesu instalacji patchy.



Service Desk Plus to kompleksowy system umożliwiający centralne zarządzanie m.in. incydentami, zgłoszeniami, zmianami, projektami, zasobami oraz SLA.



Manage Engine Endpoint Central wyposażono w mechanizmy zarządzania bezpieczeństwem punktów końcowych, związane m.in. z wykrywaniem i niwelowanime podatności, bezpieczeństwem przeglądarki, kontrolą aplikacji.

Passus S.A.

Passus S.A. jest notowanym na Giełdzie Papierów Wartościowych polskim producentem i integratorem wysokospecjalizowanych rozwiązań IT z zakresu: monitoringu oraz poprawy wydajności sieci i aplikacji, bezpieczeństwa IT, utrzymania ciągłości działania infrastruktury IT, dostaw, wdrożenia i utrzymania infrastruktury dostępowej.

Spółka jako jedno z niewielu przedsiębiorstw z branży IT w Polsce posiada świadectwo bezpieczeństwa przemysłowego, potwierdzające zdolność do ochrony informacji niejawnych o klauzuli „tajne", „NATO secret" i „NATO confidential" oraz klauzuli „EU secret" i „EU confidential". Potwierdza ono zdolność Spółki do zapewnienia ochrony informacji niejawnych i umożliwia realizację projektów informatycznych dla strategicznych z punktu widzenia państwa firm i instytucji.

Klientami Passus S.A. są przede wszystkim największe spółki i organizacje z listy TOP 500, w szczególności z sektorów telekomunikacyjnego, finansowego, energetyczno-paliwowego, administracji publicznej i rządowej.

Grupę Passus S.A. tworzą także:

Chaos Gears S.A.

Chaos Gears specjalizuje się w realizacji projektów informatycznych w chmurze publicznej dla dużych firm i instytucji, a także szybko rozwijających się start-upów. Spółka jest partnerem Amazon Web Services o statusie Advanced Consulting Partner. Oferuje szereg usług i narzędzi służących wsparciu innowacji w firmach. Realizuje projekty migracji ze środowiska on-premise do chmury, świadczy usługi w obszarze Cloud Manage Services (DevOps), zajmuje monitorowaniem usług i aplikacji oraz optymalizacji kosztów działania rozwiązań chmurowych. Chaos Gears projektuje też wysoko dostępne i odporne na awarie ośrodki obliczeniowe oraz aplikacje w modelu SaaS z wykorzystaniem technologii AWS, w szczególności Serverless.

Firma specjalizuje się również w rozwiązaniach Disaster Recovery dla środowisk aplikacyjnych z wykorzystaniem AWS. Pracownicy Spółki posiadają szereg certyfikatów potwierdzających kompetencje zespołu w budowaniu i zarządzaniu chmurą publiczną AWS: AWS Certified Solution Architect Professional, AWS Certified DevOps Professional, AWS Certified SysOps Administrator Associate oraz AWS Certified Advanced Networking Specialty, AWS Certified Security Specialty.

Sycope S.A.

Sycope S.A. odpowiada za wsparcie rozwoju produktów własnych. Obecnie w ofercie Spółki znajdują się trzy rozwiązania własne: system Sycope do monitorowania sieci i urządzeń sieciowych z wykorzystaniem protokołu NetFlow uzupełniony o moduł bezpieczeństwa, Ambience (system do ekstrakcji i transformacji danych z ruchu sieciowego w czasie zbliżonym do rzeczywistego oraz wykrywania zagrożeń wewnętrznych), nDiagram (system do wizualizacji połączeń i parametrów pracy urządzeń sieciowych). W ofercie Spółki znajdują się także system IDS (rozwiązanie do wykrywania zagrożeń i ataków w sieciach komputerowych) oraz system StressTester do prowadzania testów wydajnościowych i obciążeniowych aplikacji

Wisenet sp. z o.o.

Wisenet specjalizuje się w realizacji projektów informatycznych z bezpieczeństwa IT w szczególności SIEM, SOAR i DAM oraz świadczy usługi doradztwa oraz profesjonalnego wsparcia 24/7. Potwierdzeniem kompetencji zespołu Wisenet jest szereg certyfikatów indywidualnych w tym m.in IBM Certified Deployment Professional Security QRadar SIEM, IBM Certified Deployment Professional Security QRadar Vulnerability Manager, Certified Information Systems Security Professional, Certified Ethical Hacker, ArcSight Certified AS Data Platform Technical, Offensive Security Certified Professional (OSCP), Certified Incident Handling Engineer (CIHE), Certified Vulnerability Assessor (CVA), Certified Penetration Testing Engineer (CPTE), PRINCE2 Foundation.