nomios

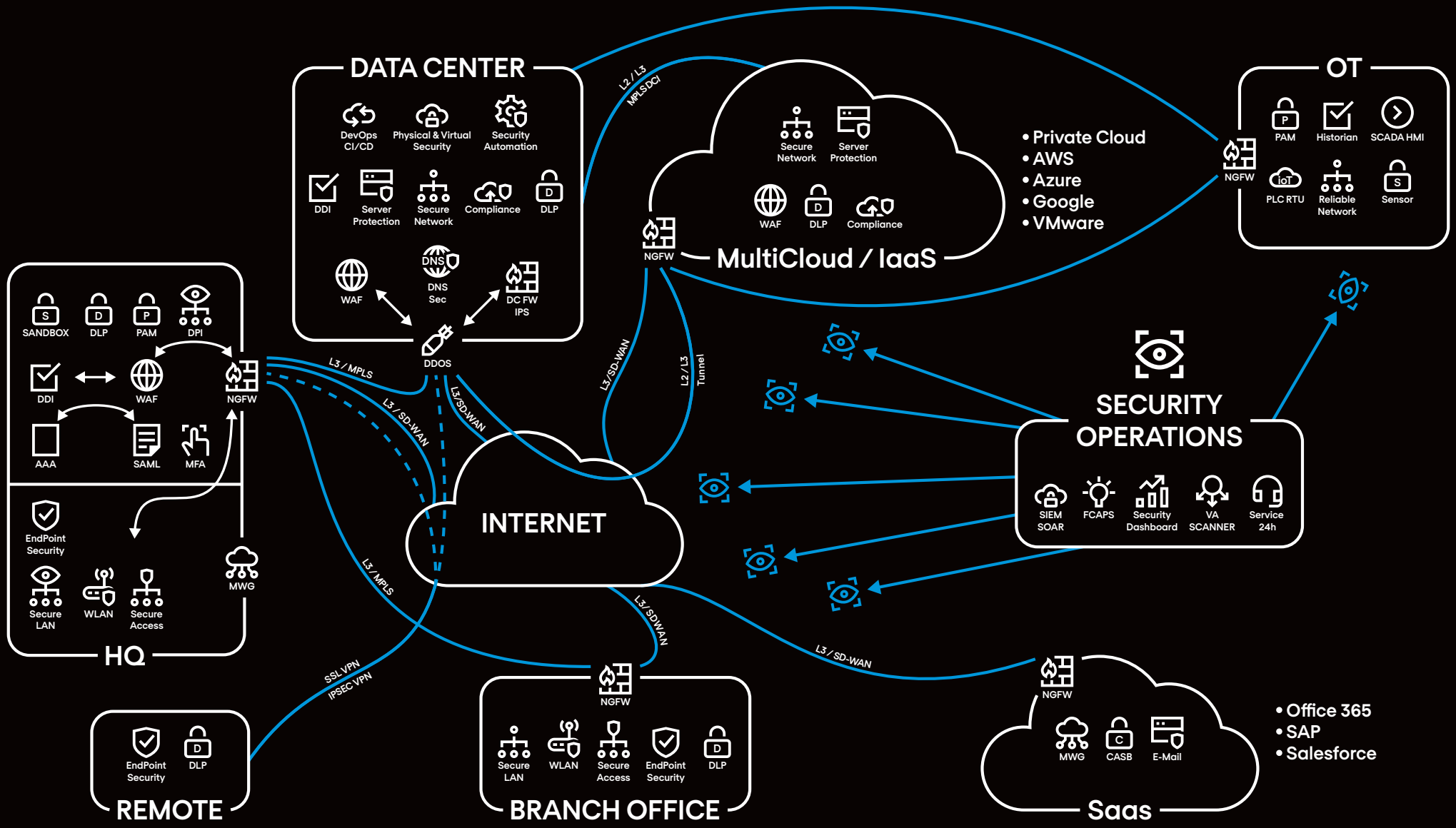
www.nomios.pl

systemy bezpieczeństwa cyfrowego

usługi zarządzane

sieci krytyczne dla biznesu

rozwiązania chmurowe


DATA CENTER
DevOps CI/CD
Physical & Virtual Security
Security Automation
DDI
Server Protection
Secure Network
Compliance
DLP
WAF
DNS Sec
DC FW IPS
DDOS
L2 / L3 MPLS DCI
NGFW
MultiCloud / IaaS
Secure Network
Server Protection
WAF
DLP
Compliance
• Private Cloud
• AWS
• Azure
• Google
• VMware
OT
PAM
Historian
SCADA HMI
PLC RTU
Reliable Network
Sensor
SANDBOX
DLP
PAM
DPI
DDI
WAF
NGFW
AAA
SAML
MFA
EndPoint Security
Secure LAN
WLAN
Secure Access
MWG
HQ
L3 / MPLS
L3 / SD-WAN
L3/SD-WAN
L3 / SD-WAN
L2 / L3 Tunnel
INTERNET
SECURITY OPERATIONS
SIEM SOAR
FCAPS
Security Dashboard
VA SCANNER
Service 24h
L3 / MPLS
L3/SDWAN
L3 / SD-WAN
SSL VPN
IPSEC VPN
EndPoint Security
DLP
REMOTE
NGFW
Secure LAN
WLAN
Secure Access
EndPoint Security
DLP
BRANCH OFFICE
NGFW
MWG
CASB
E-Mail
Saas
• Office 365
• SAP
• Salesforce

nomios secure and connected

Grupa Nomios to międzynarodowy, niezależny dostawca nowoczesnych systemów cyberbezpieczeństwa, sieci krytycznych dla biznesu, rozwiązań chmurowych i usług zarządzanych. Wspieramy naszych klientów we wdrażaniu innowacji, dostarczając im najlepszych w swojej klasie technologii. W Nomios budujemy fundamenty pod bezpieczeństwo i rozwój gospodarki cyfrowej i społeczeństwa cyfrowego.

Łącząc technologie, procesy i fachową wiedzę tworzymy rozwiązania i usługi następnej generacji. Przez naszych klientów jesteśmy cenieni za wysokiej jakości usługi i doskonałość operacyjną. Nasi partnerzy strategiczni należą do wiodących dostawców technologii na świecie. Dzięki temu nasi klienci mają dostęp do najbardziej zaawansowanych rozwiązań sprzętowych i programowych dostępnych na rynku, które pomagają im poprawiać bezpieczeństwo i niezawodność sieci.

Legitymujemy się najwyższym statusem partnerskim u producentów większości oferowanych systemów. Nasi inżynierowie mogą pochwalić się nie tylko najwyższymi certyfikatami producenckimi, ale także szerokim doświadczeniem w zakresie tworzenia kompleksowych architektur.

Wspieramy również naszych klientów w zakresie zarządzania ich infrastrukturą sieciową i cyberbezpieczeństwa realizując usługi typu SOC i NOC.

GRUPA NOMIOS W LICZBACH

Wielokrotnie nagradzana firma
Nagrody branżowe i akredytacje

400+ certyfikowanych inżynierów
Nasi specjaliści robią wielką różnicę

24/7 obsługa klienta na całym świecie
Wskaźnik satysfakcji klienta na poziomie 8,9

Doświadczenie, któremu możesz zaufać
Od 2004 roku wspieramy naszych klientów we wdrażaniu najbardziej zaawansowanych rozwiązań IT

20 biur w całej Europie
Obsługujemy klientów w ponad 50 krajach na świecie

40+ partnerów technologicznych
Strategiczne partnerstwa z czołowymi producentami

SOC24

nomios group

www.soc24.pl

Dbamy o bezpieczeństwo Twoich danych

Wykwalifikowana kadra SOC24 oraz wsparcie inżynierskie Grupy Nomios, która działa na rynku bezpieczeństwa od 2012 roku, gwarantuje rzetelną realizację obsługi operacyjnej. Dzięki temu powiązaniu SOC24 jest wiarygodnym i doświadczonym partnerem biznesowym dla wielu instytucji, które maja zapotrzebowanie na obsługę i analizę incydentów w różnych wariantach, często po godzinach funkcjonowania swojego przedsiębiorstwa czy działu SOC.

Co nas wyróżnia?

- międzynarodowe doświadczenie i międzynarodowi klienci
- wcześniejsza reakcja na nowe zagrożenia
- ponad 400 certyfikowanych inżynierów
- spełniamy wymagania KRI
- spełniamy wymagania D KNF i jej odpowiedniki dla funduszy ubezpieczeniowych
- zgodność z RODO

Korzyści z usługi SOC24

- Współpraca z doświadczoną i kompetentną kadrą inżynierów SOC24
- Niższa cena w porównaniu z kosztem budowy pierwszej linii własnymi zasobami
- Szybkie uruchomienie usługi
- Zmniejszenie kosztów utrzymania infrastruktury informatycznej
- SLA wynikające z umowy
- Podniesienie bezpieczeństwa danych i systemów
- Możliwość zbudowania SOC funkcjonującego w trybie ciągłym bez wykorzystania własnych zasobów
- Zmniejszenie liczby zadań własnego zespołu - możliwość relokacji kompetencji
- Gwarantowana ciągłość oraz wysoka jakość świadczonej usługi

Modele współpracy SOC24

W zależności od potrzeb Twojej organizacji:

- 8/5 - w godzinach roboczych
- 6/5 + 24/2- poza godzinami roboczymi i w dni wolne
- 24/7/365 - monitorowanie w trybie ciągłym przez wszystkie dni w roku

Dostępne pakiety rozwiązań

W zależności od potrzeb Twojej organizacji dopasujemy dla Ciebie odpowiednie rozwiązanie. Poza dostępnymi pakietami jest możliwość skorzystania z III linii SOC.

Oferujemy aż pięć unikalnych pakietów, z których możesz wybrać ten, który jest najbardziej odpowiedni dla Ciebie - nasi specjaliści chętnie pomogą Ci wybrać rozwiązanie na miarę Twoich indywidualnych potrzeb:

OCHRONA BRĄZOWA

- I linia SOC
- 8/5
- Service Delivery Manager

OCHRONA BRĄZOWA +

- I linia SOC
- poza godzinami pracy
- Service Delivery Manager

OCHRONA SREBRNA

- I linia SOC
- 24/7
- Service Delivery Manager

OCHRONA ZŁOTA

- I linia SOC 24/7
- II linia SOC 8/5
- Service Delivery Manager

OCHRONA PLATYNOWA

- I linia SOC 24/7
- II linia SOC 24/7
- Service Delivery Manager

I linia SOC24

Monitorowanie
Obsługa incydentów
Wychwytywanie zagrożeń
Raportowanie

II linia SOC24

Zarządzanie incydentami
Analiza logów i scenariuszy
Konsultacje i raportowanie
Threat hunting

III linia SOC24

Analiza forensic
Analiza malware
Konsultacje ekspertów
Nomios i SOC24

Systemy świadczone w modelu usługowym

Poniżej kilka przykładów systemów, którymi możemy wzbogacić usługę SOC24 dobierając je umiejętnie do specyfiki, wielkości i realnych potrzeb w Państwa organizacji.

- Rozwiązania klasy SIEM
- Rozwiązania klasy EDR/XDR
- Rozwiązania klasy SOAR
- Rozwiązania klasy vulnerability management

Dostępne modele usług zarządzanych

Jeśli nie posiadasz własnych systemów, możemy rozszerzyć nasze usługi o MSSP

Model lokalny

System bezpieczeństwa
jest zainstalowany
w lokalizacji klienta

Model centralny

System bezpieczeństwa
jest zainstalowany
na serwerach SOC24
i współdzielony pomiędzy klientami

Model chmurowy

System bezpieczeństwa
jest udostępniony
w chmurze producentów
danego oprogramowania

Potrzebujesz innego modelu wsparcia i ochrony swojego przedsiębiorstwa?
Skontaktuj się z nami i z pewnością znajdziemy odpowiednia usługę!

t. +48 22 46 00 785 biuro@soc24.pl www.soc24.pl

Posiadamy status
zespołu akredytowanego
w Trusted Introducer

22301:2012

Posiadamy
Certyfikat ISO
22301:2012

27001:2013

Posiadamy
Certyfikat ISO
27001:2013

Juniper Networks

Nowoczesne rozwiązania sieciowe

Produkty firmy Juniper Networks adresują potrzeby klientów z zakresu budowy nowoczesnej infrastruktury sieciowej, zarówno przedsiębiorstw, jak i operatorów telekomunikacyjnych oraz dostawców usług. Szeroka rodzina przełączników serii EX i QFX pozwala na dobór optymalnych rozwiązań, od poziomu sieci oddziałowej, przez kampus, aż do Centrum Przetwarzania Danych (CPD). W przypadku CPD, rozwiązania typu fabric wspierane technologią EVPN/VXLAN, zapewniają sieć podkładową dla wirtualizacji i automatyzacji. W kwestii obszaru sieci oddziałowej i kampusowej doskonałym i nieodzownym uzupełnieniem jest rozwiązanie WiFi MIST.

Firma Juniper Networks zapewnia również produkty do budowy nowoczesnych sieci międzyoddziałowych, tzw. Software Defined WAN (SD-WAN). Pozwalają one na łatwe i elastyczne łączenie oddziałów firm, z wykorzystaniem różnych dostępnych łączy (Internet, MPLS VPN, itp.) przy zachowaniu najwyższej jakości i bezpieczeństwa.

Juniper Networks jest również liderem w obszarze rutingu, z uznawanymi przez wielu klientów i specjalistów za najlepsze w klasie routerami serii MX, (zastosowanie: styk BGP, WAN/ MPLS/VXLAN/ EVPN/SD-WAN, CGNAT), oraz oddziałowymi ruterami z serii SRX. W zakresie bezpieczeństwa, firma oferuje kompleksowe rozwiązania do ochrony ruchu na styku sieci fi rmowych i Internetu oraz w CPD. Platformy z rodziny SRX to systemy klasy NG Firewall, cenione za ich wysoką wydajność i szerokość zastosowań. Całości dopełniają rozwiązania Sky ATP (sandbox chmurowy) i JATP (sandbox lokalny).

Trellix

Kompleksowa ochrona stacji, serwerów, sieci oraz monitorowanie bezpieczeństwa

Kluczowym elementem rozwiązań firmy jest serwer zarządzający ePolicy Orchestrator (ePO), zapewniający spójne zarządzanie końcówkami, siecią i bezpieczeństwem danych. Dzięki przejrzystości i rozbudowanej automatyzacji, które redukują czas odpowiedzi na incydenty, Trellix ePO w znaczący sposób wzmacnia mechanizmy bezpieczeństwa oraz obniża koszty i złożoność zarządzania ryzykiem.

Firma Trellix udostępnia bardzo szerokie portfolio rozwiązań bezpieczeństwa, w związku z czym – dla łatwiejszego ich przedstawienia – dobrze jest je pogrupować ze względu na obszar zastosowania oraz funkcjonalność. Produkty wchodzące w skład Trellix Data Protection chronią krytyczne dane i pomagają zapewnić zgodność z regulacjami. W ich skład wchodzą między innymi systemy szyfrujące oraz zapobiegające wyciekom danych (DLP), zapewniające wielowarstwowe bezpieczeństwo danych bez względu na to, gdzie się znajdują – w zasobach lokalnych, czy sieciowych.

Systemy wchodzące w skład Trellix Endpoint Security oferują ciągłe, zaktualizowane i silne zabezpieczenia przeciwko całemu spektrum zagrożeń. Trellix dostarcza ochronę dla wszystkich końcówek, w tym dla urządzeń mobilnych i środowisk wirtualnych, gwarantując bezpieczny, bezproblemowy dostęp do aplikacji biznesowych i danych korporacyjnych. Rozwiązanie to można także zintegrować z systemem klasy sandbox, zapewniającym analizę oraz wykrywanie nieznanych zagrożeń w danych przesyłanych siecią. Rozwiązania klasy SIEM (Security Information and Event Management) pozwalają łączyć logi dotyczące zdarzeń, zagrożeń i ryzyka oferując błyskawiczne reakcje na incydenty, bezproblemowe zarządzanie logami i zaawansowane mechanizmy raportowania. Umożliwiają konsolidowanie, korelowanie, ocenę i priorytetyzację zdarzeń dotyczących bezpieczeństwa pochodzących zarówno z systemów Trellix, jak i produktów firm trzecich. Firma Trellix wychodząc naprzeciw potrzebom zapewnienia bezpieczeństwa, działającym systemom w oparciu o platformy chmurowe. Udostępnia także stale rozszerzany katalog rozwiązań dostosowanych do specyfiki takich środowisk. Systemy te chronią przed zaawansowanymi zagrożeniami, wyciekiem danych oraz pozwalają na monitorowanie wykorzystywania aplikacji chmurowych przez użytkowników.

Istotnym elementem ekosystemu bezpieczeństwa Trellix jest także szyna danych (Data Exchange Layer/DXL) zapewniająca wymianę informacji pomiędzy poszczególnymi komponentami ochrony firmy Trellix oraz – co szczególnie istotne – także innych producentów.

F5 Networks

Programowalne rozwiązania o wysokiej dostępności dla bezpieczeństwa aplikacji

F5 Networks jest liderem rynku w klasie rozwiązań ADC (Application Delivery Controller). Produkty F5 zapewniają mechanizmy inteligentnego kierowania ruchem danych w sieci, lokalnie (LTM), oraz pomiędzy rozproszonymi Centrami Przetwarzania Danych (GSLB). Zapewniają również ochronę, zarówno w warstwie sieciowej (AFM), jak i aplikacyjnej (AWAF), oraz mechanizmy kontroli dostępu (APM). Dodatkowo, dzięki zastosowanemu wsparciu sprzętowemu, pozwalają na wysokowydajną inspekcję ruchu szyfrowanego (SSL Orchestrator, TLS/SSL Offl oad) oraz łagodzenie skutków ataków DDoS, zarówno wolumetrycznych (AFM), jak i aplikacyjnych (ASM). O wyjątkowej elastyczności platformy decydują ogromne możliwości programowania i wręcz dowolnej modyfikacji ruchu przechodzącego przez urządzenia. Programowalność dotyczy zarówno warstwy danych, jak i warstwy kontrolnej. Dzięki temu F5

staje się wyjątkową platformą dla tworzenia własnych, dostosowanych do potrzeb, mechanizmów optymalizacji i automatyzacji usług aplikacyjnych (BIG-IQ, AS3, iRule).

ProofPoint

Ochrona poczty elektronicznej

Rozwiązania dostępne w ramach platformy ProofPoint Enterprise Protection Suite, takie jak Targeted Attack Protection zapewniają kompleksową ochronę przed zagrożeniami poczty elektronicznej, włączając w to ochronę przed złośliwym oprogramowaniem (malware), wyłudzaniem informacji (phishing) oraz innymi formami niepożądanych lub niebezpiecznych treści.

Dodatkowo w ramach ProofPoint Enterprise Privacy Suite dostępne są funkcjonalności zapewniające ochronę informacji wrażliwych oraz prywatnych, zapobiegające wyciekom informacji poufnych wysyłanych z wykorzystaniem poczty elektronicznej (DLP) oraz zapewniające zgodność z powszechnie stosowanymi międzynarodowymi i branżowymi regulacjami w zakresie ochrony danych. Całość dopełnia moduł ProofPoint Encryption, automatycznie szyfrujący wskazane polityką wiadomości email, zmniejszając ryzyko powiązane z naruszeniami przepisów, utratą danych i złamaniem polityki korporacyjnej. Wiadomości mogą być szyfrowane z wykorzystaniem technologii S/MIME, PGP lub mogą być publikowane w bezpiecznym portalu, zapewniającym szyfrowany dostęp do informacji.

Skyhigh Security

Ochrona Chmury i środowisk hybrydowych

Skyhigh Security jako jedni z pierwszych dostrzegli potencjał chmury. Widzieli, że ochrona danych osobowych w nowym hybrydowym świecie wymaga zupełnie nowego podejścia. W erę rozwiązań chmurowych weszli przygotowani na nowe wyzwania.

Dostępne rozwiązania to:

Secure Web Gateway integruje w sobie zabezpieczenia przed złośliwym oprogramowaniem, kontrolę treści oraz serwisy reputacyjne, chroniąc użytkowników, aplikacje, dane i sieci przed wszystkimi formami zagrożeń przenoszonych poprzez pocztę elektroniczną i Internet. Secure Web Gateway zapewnia kompleksową ochronę wszystkich aspektów ruchu sieciowego za pomocą jednej wysokowydajnej architektury oprogramowania.

Broker bezpieczeństwa dostępu do chmury CASB (ang. Cloud Access Security Broker) to oprogramowanie lub sprzęt w chmurze, które pośredniczy między użytkownikami a dostawcami usług w chmurze. Zdolność CASB do eliminowania luk w zabezpieczeniach rozciąga się na środowiska typu software-as-a-service (SaaS), platforma-as-a-service (PaaS) oraz infrastructure-as-a-service (IaaS).

Zero Trust Network Access (ZTNA) egzekwuje granularne, adaptacyjne i kontekstowe zasady zapewniające bezpieczny i bezproblemowy dostęp typu Zero Trust do prywatnych aplikacji działających w chmurach i korporacyjnych centrach danych z dowolnego urządzenia i lokalizacji. Tym kontekstem może być połączenie tożsamości użytkownika, lokalizacji użytkownika lub usługi, pory dnia, rodzaju usługi i stanu zabezpieczeń urządzenia.

Rozwiązanie Security Service Edge (SSE) to struktura bezpieczeństwa pomiędzy pracownikami a ich zasobami, które umożliwia szybki bezpośredni dostęp do Internetu poprzez wyeliminowanie konieczności kierowania ruchu przez centrum danych w celu zapewnienia bezpieczeństwa. Ochrona danych i zagrożeń są wykonywane w każdym punkcie kontroli w jednym przejściu, aby zmniejszyć koszt zabezpieczeń i uprościć zarządzanie.

Ivanti

Bezpieczny dostęp do sieci firmowej

Ivanti jest jednym z liderów dostarczających mechanizmy bezpiecznego dostępu do sieci firmowej: NAC oraz SSL VPN. Rozwiązanie Network Access Cotrol (NAC), współpracujące z większością dostawców infrastruktury sieciowej, zapewnia szczegółową wiedzę o tym, w jaki sposób oraz przez kogo sieć jest wykorzystywana, które urządzenia lub/i użytkownicy wykorzystują sieć w sposób zgodny z polityką firmy. Mając wgląd i widoczność w to jak funkcjonują urządzenia w sieci, możliwe jest wdrażanie właściwych reguł kontrolnych, zgodnych z polityką bezpieczeństwa firmy, dzięki temu tylko uwierzytelnieni oraz autoryzowani użytkownicy i urządzenia będą mieli dostęp do sieci firmy. Dzięki integracji systemu NAC z firewallami, możliwe staje się m.in. budowanie reguł filtrowania na bazie tożsamości konkretnego użytkownika lub grup użytkowników, np. Active Directory oraz szczegółowe śledzenie aktywności danej osoby w sieci tzw. user awareness.

Ivanti dostarcza także rozwiązania zdalnego dostępu do zasobów (Data Center, Cloud) z wykorzystaniem SSL VPN, wspierające wiele platform systemowych oraz przeglądarek internetowych.

Fudo Security

Monitorowanie, rejestracja, kontrola i audyt zdalnych sesji administracyjnych

Sztandarowym produktem firmy Fudo Security jest rozwiązanie FUDO, dedykowane do monitoringu, kontroli, rejestracji i audytu zdalnych sesji administracyjnych. Pozwala ono podsłuchiwać

i nagrywać sesje SSH, RDP, VNC, umożliwiając analizę zarówno sesji archiwalnych, jak i obecnie trwających, a także zakończenie, wstrzymanie lub włączenie się w prace zdalnych konsultantów czy pracowników.

InfoBlox

Ochrona ruchu DNS oraz zarządzanie siecią

Infoblox jest jednym z liderów w technologiach zarządzania DNS, DHCP i adresami IP (IPAM) oraz Secure DNS. Infoblox zapewnia blokowanie wycieków danych w zapytaniach DNS oraz komunikacji Command&Control over DNS oraz blokuje zapytania dotyczące domen powiązane z malware i ransomware. Umożliwia integrację z innymi narzędziami bezpieczeństwa (np. NAC, NGFW, End-Point Protection, skanery podatności), zapewniając ochronę publicznych serwerów DNS przed atakami DDoS, próbami amplifikacji, exploitami, czy DNS hijackingiem.

Radware

Ochrona przed atakami DDoS

Radware jest, obok firmy F5, globalnym liderem w zakresie rozwiązań bezpieczeństwa aplikacyjnego dla centrów danych w modelach wirtualnych i w chmurze. Rozwiązania Radware sprawdzają się m.in. w takich obszarach, jak: ochrona przed atakami DDoS, ataki wolumetryczne oraz ataki aplikacyjne. Ciekawym i bardzo dobrze ocenianym przez klientów mechanizmem jest behawioralna ochrona przed atakami DDoS (DefensePro), która jest jednym z elementów autorskiej referencyjnej architektury Nomios Poland, dotyczącej bezpiecznego brzegu w datacenter.

Logmanager

Zarządzanie logami, które wspiera wszystkie obszary IT

Logmanager to system zaprojektowany z myślą o zapełnieniu luki pomiędzy tradycyjnymi komercyjnymi rozwiązaniami do zarządzania logami, a open-source. Przeznaczony również dla małych i średnich organizacji, łatwy w używaniu, utrzymaniu i wdrożeniu. Wyposażony we wszystkie najważniejsze funkcjonalności i o dobrym stosunku cena/jakość, dzięki zintegrowanej platformie sprzętowej oraz braku licencji ograniczających użytkownika w podłączaniu źródeł logów.

Co istotne, rozwiązanie nie jest w żaden sposób licencjonowane – nie ma ograniczeń licencyjnych co do ilości źródeł zbieranych logów.

VMware

Platforma wirtualizacji oraz rozwiązania dla zarządzania i automatyzacji środowisk wirtualnych

Współczesna architektura Centrum Przetwarzania Danych (SDDC – Soft ware Defined Data Center) opiera się na wirtualizacji i automatyzacji wszystkich jej komponentów – zasobów obliczeniowych, dyskowych i sieci. Celem jest uzyskanie jak najbardziej elastycznych środowisk, w których warstwa sprzętowa nie jest już przedmiotem codziennej konfiguracji. VMware zapewnia narzędzia do wirtualizacji serwerów (VMware vSphere), macierzy dyskowych (VMware vSAN), oraz infrastruktury sieciowej (NSX V/T). Pozwala również na poprawę bezpieczeństwa w SDDC poprzez mechanizmy mikrosegmentacji (NSX V/T). Włącz wirtualną sieć w chmurze dzięki pełnej wirtualizacji sieci i zabezpieczeń. W nowoczesnych Centrach Przetwarzania Danych zaczynają wieść prym technologie kontenerowe, dla których warto zastanowić się nad spójnym zarządzaniem wszystkimi komponentami, także w środowiskach MultiCloud (NSX-T, PKS, PKS Essentials, VMware Cloud AWS). Zastosowanie automatyzacji sprawia, że istotnym staje się zapewnienie odpowiedniej widoczności, narzędzi do planowania i optymalizacji procesów, co dostarczają produkty z rodziny vRealize.

Fortinet

Rozwiązania do budowy i ochrony sieci

Firma Fortinet jest dostawcą wysokowydajnych informatycznych rozwiązań zabezpieczających, które umożliwiają klientom ochronę i kontrolę używanej infrastruktury informatycznej. Jej specjalnie opracowane, zintegrowane technologie zabezpieczeń wraz z badającymi zagrożenia usługami FortiGuard, zapewniają klientom niezwykle skuteczną ochronę treści, dotrzymującą kroku nieustannie rozwijającym się zagrożeniom. Fortinet dostarcza szerokie portfolio produktów bezpieczeństwa sieci i organizacji, zawierające między innymi rozwiązania typu Firewall NGFW (SSL/ IPSec VPN, SD-WAN), systemy uwierzytelniania wieloskładnikowego (MFA), komponenty sieci bezprzewodowych, Web Application Firewall, sandbox oraz ochronę stacji końcowych (FortiEDR). Ponadto Fortinet dostarcza rozwiązania do analizowania i korelacji zdarzeń klasy SIEM (FortiSIEM) oraz narzędzie SOAR do automatyzacji i orkiestracji procesów związanych z cyberbezpieczeństwem (FortiSOAR). FortiSOAR to platforma do zarządzania i automatyzacji odpowiedzi na incydenty związane z cyberbezpieczeństwem, która integruje różne narzędzia bezpieczeństwa oraz źródła informacji w celu usprawnienia procesów reagowania na zagrożenia. FortiSOAR umożliwia wczesne wykrywanie, kategoryzowanie i analizowanie incydentów, a także automatyzuje powtarzalne zadania, usprawniając procesy pracy

zespołów bezpieczeństwa. Platforma oferuje także funkcje raportowania i analizy wydajności SOC, co umożliwia ciągłe doskonalenie procesów reagowania na zagrożenia.

Progress Flowmon

Monitorowanie ruchu sieciowego

Flowmon dostarcza narzędzia do monitorowania oraz analizowania ruchu sieciowego w czasie rzeczywistym. Umożliwia to administratorom sieci szybki wgląd w bieżący stan sieci, komunikację urządzeń, identyfikację hostów, aplikacji i użytkowników oraz szybkie eliminowanie usterek i optymalizację sieci. Dodatkowe moduły zapewniają wykrywanie anomalii sieciowych (mechanizm wykorzystujący machine learning), analizę wydajności usług, zbieranie statystyk z ruchu sieciowego w celu wykrywania anomalii i zainicjowania automatycznych działań obronnych oraz nagrywanie ruchu sieciowego do późniejszej analizy.

Tukan IT

System do klasyfikacji plików i poczty elektronicznej w przedsiębiorstwach

Systemy do klasyfikacji dokumentów podnoszą poziom bezpieczeństwa, pozytywnie wpływając na zwiększenie świadomości pracowników i współpracowników organizacji w zakresie ochrony danych oraz ich przetwarzania. Proces klasyfikacji nie tylko ułatwia wyszukiwanie i odzyskiwanie danych, ale ma także szczególne znaczenie w zarządzaniu: ryzykiem, zgodnością z regulacjami i normami oraz bezpieczeństwem. Dzięki temu firmy mogą świadomie wykorzystywać skategoryzowane dokumenty i zapewniać im adekwatną ochronę. Systemy klasyfikacji są doskonałym uzupełnieniem systemów DLP.

Firma Tukan IT jest twórcą autorskiego dedykowanego rozwiązania GREENmod – systemu do klasyfikacji plików i poczty elektronicznej w przedsiębiorstwach.

Tenable

Zarządzanie podatnościami

Zarządzanie podatnościami (ang. Vulnerability Management) jest kluczowym elementem systemu bezpieczeństwa każdej firmy, której działalność biznesowa jest wspomagana przez systemy informatyczne. W infrastrukturze IT, w której brakuje dobrej jakości narzędzi do identyfikacji podatności, szybko dochodzi do naruszeń bezpieczeństwa, a komputery i inne urządzenia dostają się w ręce przestępców. Tenable Nessus, Tenable.sc, Tenable.io zapewniają identyfikację podatności oraz ocenę implikowanego przez nie ryzyka dla wszystkich elementów systemu informatycznego firmy. Dostępne w narzędziach Tenable.sc czy .io rozbudowane narzędzia raportowania pozwalają na prezentowanie informacji w sposób zrozumiały dla osób decyzyjnych oraz sprawne planowanie działań naprawczych.

Tenable.io WebAppScanner wykrywa podatności aplikacji internetowych (web), ułatwiając szybkie minimalizowanie ryzyka związanego z wypływem danych lub niedostępnością serwisów biznesowych. Opcjonalnie system ten można zintegrować z rozwiązaniami klasy WAF (Web Application Firewall), uniemożliwiając wykorzystanie podatności do czasu wprowadzenia stosownych poprawek. Tenable Lumin umożliwia zaawansowane zarządzanie całym procesem wykrywania i usuwania podatności w systemach IT. Tenable.AD jest rozwiązaniem dedykowanym do monitorowania i wykrywania podatności (np. błędnych konfiguracji, nadmiarowych uprawnień czy tzw. „martwych kont") w firmowym Active Directory, które jest sercem każdej organizacji.

Nozomi Networks

Rozwiązanie wspierające utrzymanie bezpieczeństwa sieci i systemów OT, ICS i IoT

Nozomi Networks Guardian™ minimalizuje ryzyko wystąpienia zagrożeń dla infrastruktury krytycznej największych firm z sektora energetycznego, produkcyjnego, wydobywczego, transportu, automatyki budowlanej na całym świecie. Przyspiesza wprowadzanie zmian w systemach bezpieczeństwa i transformacji cyfrowej, dostarczając natychmiastowy i bieżący wgląd do świata infrastruktury OT, IoT i IT. Dostarczany jako urządzenie fizyczne lub rozwiązanie wirtualne pasywnie monitoruje komunikację sieciową i zachowania urządzeń. Daje natychmiastowy wgląd w stan sieci OT/ICS/IoT i występujące w niej wzorce zachowań. Obserwując najpoważniejsze podatności, zagrożenia i nietypowe zachowania, pozwala reagować szybciej zapewniając wyższą niezawodność i bezpieczeństwo.

Cybereason

Nowa generacja ochrony urządzeń końcowych (EDR)

Cybereason jest liderem w dziedzinie ochrony urządzeń końcowych nowej generacji. Cybereason zrewolucjonizował ochronę urządzeń końcowych, będąc pierwszą firmą, która ujednoliciła antywirusa nowej generacji, wykrywanie i reagowanie na zdarzenia (Endpoint Detection and Response - EDR) oraz zaoferowała zarządzaną przez całą dobę usługę aktywnego wykrywania zagrożeń

(Threat Hunting) — wszystko dostarczane za pośrednictwem jednego lekkiego agenta.

Cybereason wskazuje złośliwe operacje (MalOps) od źródła do każdego dotkniętego punktu końcowego i użytkownika, wyświetlając w czasie rzeczywistym wielostopniowe szczegóły ataku, co daje analitykom możliwość natychmiastowego zrozumienia, wskazania i zakończenia ataków jednym kliknięciem. Dzięki Cybereason nie tylko powstrzymasz naruszenie, ale zakończysz je zanim się rozpocznie.

IBM

Monitorowanie i zarządzanie bezpieczeństwem

IBM QRadar SIEM stanowi kompleksowe rozwiązanie do analizy bezpieczeństwa informatycznego, zapewniające integrację z różnorodnymi źródłami zdarzeń i przepływów sieciowych oraz możliwość automatyzacji procesów obsługi incydentów. IBM QRadar SIEM pozwala widzieć to, co dzieje się w sieci, w centrum przetwarzania danych i w środowisku aplikacyjnym, a dzięki temu też lepiej chronić zasoby informatyczne i spełniać wymogi formalno-prawne. Uzupełnieniem systemu Qradar SIEM jest narzędzie IBM Resilient – rozwiązanie klasy SOAR (Security Orchestration, Automation and Response).

Zscaler

Zero Trust w praktyce

Zscaler to globalna usługa, która działa w pełni w chmurze i zapewnia kompleksowe rozwiązania z zakresu bezpieczeństwa. Dostarcza bezpieczne i szyfrowane połączenia z punktu użytkownika lub oddziału firmy, wykorzystując technologię typu SD-WAN, bezpośrednio do aplikacji w chmurze publicznej lub prywatnej. Dodatkowo, usługa monitoruje ruch sieciowy i aktywność użytkowników zapewniając ochronę przed wirusami, dostępem do stron internetowych zawierających szkodliwe oprogramowanie, atakami APT i wyciekiem poufnych danych.

Zscaler Internet Access zapewnia szybki i bezpieczny dostęp do Internetu oraz aplikacji SaaS, zapewniając bezpieczną transformację sieci. Poprzez ustawienie Zscaler Internet Access jako domyślnej trasy do Internetu, wszyscy użytkownicy - niezależnie od lokalizacji - otrzymują identyczną ochronę. Zscaler działa jako pośrednik między użytkownikami a Internetem, kontrolując ruch i stosując wiele różnych technik bezpieczeństwa w celu zapewnienia najwyższego poziomu ochrony.

Zscaler Private Access zapewnia szybki i bezpieczny dostęp do aplikacji wewnętrznych. Tradycyjne podejście do dostępu do aplikacji wymagało dostępu do sieci, co niosło ze sobą ryzyko wprowadzenia użytkowników do sieci. Zscaler wprowadził nowe podejście, łącząc określonego użytkownika z określoną aplikacją. Zscaler Private Access stanowi alternatywę dla rozwiązań VPN.

Rapid 7

Zarządzanie podatnościami

Rozwiązania firmy Rapid7 to kompleksowe narzędzia służące do zarządzania bezpieczeństwem IT oraz weryfikacji zabezpieczeń. Rapid7 to zintegrowana platforma, która umożliwia monitorowanie i zarządzanie podatnościami, która pozwala na wykrycie i zabezpieczenie przed najnowszymi zagrożeniami. Rozwiązania Rapid7 integrują się z innymi narzędziami i systemami cyberbezpieczeństwa, co usprawnia zarządzanie bezpieczeństwem i pozwala automatyzować zadania związane z bezpieczeństwem IT, co zwiększa efektywność pracy zespołów odpowiedzialnych za cybersecurity. Platforma InsightVM oferuje bogate możliwości analizy i raportowania, co ułatwia zarządzanie bezpieczeństwem i podejmowanie decyzji.

Platforma Rapid7 oferuje szeroki wachlarz narzędzi do zarządzania ryzykiem, testowania penetracyjnego, monitorowania zabezpieczeń, analizy logów oraz wykrywania i reagowania na incydenty.

SOC24

Wykrywanie i zapobieganie zdarzeniom związanych z bezpieczeństwem IT. 24 godziny na dobę, 7 dni w tygodniu.

SOC24 (Security Operations Center) to zespół analityków i inżynierów ds. bezpieczeństwa zajmujący się monitorowaniem i reagowaniem na incydenty związane z cyberbezpieczeństwem. Główne korzyści posiadania SOC to szybsze wykrywanie i reagowanie na zagrożenia, co przyczynia się do minimalizacji szkód wynikających z ataków. SOC pozwala na skuteczne zarządzanie incydentami, a także umożliwia ciągłe doskonalenie strategii bezpieczeństwa na podstawie analizy trendów i statystyk dotyczących incydentów. SOC24 pomaga także zapewnić zgodność z regulacjami np. KSC oraz zwiększyć świadomość w zakresie zagrożeń cybernetycznych w całej organizacji. Wykwalifikowana kadra SOC24 oraz wsparcie inżynierskie firmy Nomios, gwarantuje rzetelną realizację obsługi operacyjnej. Dzięki temu powiązaniu SOC24 jest wiarygodnym i doświadczonym partnerem biznesowym dla wielu instytucji, które mają zapotrzebowanie na obsługę i analizę incydentów w różnych wariantach, często po godzinach funkcjonowania swojego przedsiębiorstwa czy działu SOC.

nomios secure and connected

www.nomios.pl

Nomios Poland Sp. z o.o.
ul. Puławska 537
02-844 Warszawa
t. +48 22 567 17 40
info@nomios.pl