MAIN Partner Community

GREYCORTEX | MAIN

Producent oprogramowania klasy NDR

GREYCORTEX – producent oprogramowania klasy NDR (Network Detection and Response). Rozwiązania cyberbezpieczeństwa dla wykrywania i reagowania na nieprawidłowości w sieci, związane zarówno z bezpieczeństwem, wydajnością jak i codzienną administracją siecią.

Wśród klientów GREYCORTEX są instytucje rządowe i samorządowe, średnie firmy, duże przedsiębiorstwa, służba zdrowia, transport, energetyka i przemysł 4.0. Nieograniczona skalowalność GREYCORTEX oferuje użytkownikom elastyczność w monitorowaniu wszystkiego, od małej sieci składającej się z zaledwie 100 urządzeń, aż do kilkuset tysięcy urządzeń w wielu rozproszonych geograficznie lokalizacjach.

Branże

Finansowa, centralne instytucje i organizacje państwowe, logistyczna, software development, e-commerce, motoryzacyjna, produkcyjna, dystrybucyjna, handel i usługi, marketingowa.

Produkty i usługi

GREYCORTEX MENDEL

Greycortex Mendel zapewnia głęboką widoczność sieci. Wykorzystując najbardziej zaawansowane techniki detekcji, Mendel chroni Cię przed wszelkimi znanymi i nieznanymi zagrożeniami cyberbezpieczeństwa, na które narażona jest Twoja sieć. Wykrywając zagrożenia i luki w sieci w momencie ich wystąpienia, wykorzystując AI i uczenie maszynowe, Mendel szybko powstrzymuje ataki, oszczędzając czas i pieniądze oraz pomagając wykryć i uniknąć potencjalnych problemów z siecią. Mendel, narzędzie do wykrywania i reagowania w sieci, wypełnia również luki pozostawione przez starsze i nowoczesne rozwiązania IDS/IPS w sieciach informatycznych i przemysłowych.

Greycortex Mendel to narzędzie do wykrywania i reagowania w sieci, które wizualizuje komunikację sieciową we wszystkich podłączonych urządzeniach. Analizuje ruch sieciowy i wykrywa złośliwe działania oraz zaawansowane zagrożenia. Umożliwia analitykom systemowym zbadanie zdarzeń operacyjnych i bezpieczeństwa, znalezienie ich przyczyn źródłowych oraz szybkie i skuteczne reagowanie i łagodzenie ich skutków.

Dane kontaktowe GREYCORTEX:
WWW: www.greycortex.com
Telefon:
(PL) +48 501 678 008
(CZ) +420 511 205 216
Mail: info@greycortex.com

O firmie MAIN:
Firma MAIN to certyfikowane Data Center położone w centrum Warszawy.

Budujemy środowiska IT, które zapewniają ciągłość działania biznesu. Specjalizujemy się w rozwiązaniach Private i Hybrid/Multi-Cloud i świadczymy wszystkie poziomy administracji środowiskami fizycznymi i wirtualnymi. Nasze usługi oparte są na dwóch certyfikowanych, w pełni redundantnych ośrodkach Data Center w Warszawie.

Wspieramy firmy w pokonywaniu barier, na które natrafiają w związku z przetwarzaniem danych, takie jak niska wydajność czy wysokie koszty infrastruktury.

Produkty i usługi:
- Dedicated Private Cloud
- Virtual Private Cloud
- Hybrid Cloud
- Administracja Chmurą
- Disaster Recovery
- Metal as a Service
- Relokacja
- Kolokacja

WWW: www.main.pl
Telefon: (+48 22) 339 18 98
Mail: ask@main.pl

Wyzwania z którymi mierzą się nasi klienci

Nasi klienci polegają na GREYCORTEX, aby zapewnić bezpieczeństwo ich sieci, które ma krytyczne znaczenie. Zdobywamy i utrzymujemy ich zaufanie, dostarczając im najbardziej zaawansowane technologicznie i niezawodne narzędzie bezpieczeństwa oraz oferując indywidualne podejście, niezależnie od branży czy wielkości firmy. Chronimy tradycyjne sieci IT oraz infrastrukturę krytyczną i systemy sterowania OT/Industrial Control Systems w wielkoskalowych centrach danych.

Nieznane zagrożenia

Zaawansowane nieznane zagrożenia, takie jak złośliwe oprogramowanie, RAT i ransomware; jeśli nie zostaną wykryte na czas, prowadzą do:
- utraty wrażliwych danych,
- ataków na organizacje,
- szkody biznesowej,
- utraty reputacji.

Brak widoczności

Brak widoczności sieci sprawia, że są trudności w identyfikacji podejrzanych urządzeń i użytkowników, jak również:
- opóźnienia krytyczne,
- tajemnicze urządzenia,
- stracony czas,
- zmarnowane pieniądze.

Zaniedbania pracownicze

Naruszanie zasad przez pracowników i wykonawców, co powoduje:
- wyciek wrażliwych danych,
- ataki na inne organizacje,
- problemy z przestrzeganiem przepisów,
- naruszenia GDPR,
- naruszenia polityki bezpieczeństwa.

Problemy kadrowe

Brak wysoko wykwalifikowanej kadry w obszarze zarządzania sieciami i bezpieczeństwa IT. Rozwiązaniem jest wykorzystanie GREYCORTEX MENDEL, które wspomaga działania obecnego personelu w tym obszarze. Dostarcza w sposób przejrzysty, szybki i kompleksowy informacje o ruchu w sieci i zagrożeniach.

Głowne korzyści

Widoczność
GREYCORTEX Mendel zapewnia możliwość wizualizacji każdego urządzenia w sieci w czasie rzeczywistym, dzięki czemu można dokładnie zobaczyć, jakie urządzenia znajdują się w sieci - w tym z kim się komunikują, kiedy, ile danych wysyłają i odbierają, na jakim protokole, wraz z metadanymi, co oznacza, że dzięki naszemu rozwiązaniu zdarzenia związane z bezpieczeństwem i operacjami wreszcie mają pełny i szczegółowy kontekst, tożsamość użytkowników i wszelkie powiązane informacje o zagrożeniach.

Ale to nie koniec, ponieważ Mendel idzie o krok dalej w tej wizualizacji. Dzięki zaawansowanemu filtrowaniu, łączącemu ponad 25 parametrów, z wykorzystaniem operatorów logicznych, każde urządzenie może być nie tylko widoczne, ale również jego komunikacja w sieci może być dokładnie zbadana, co sprawia, że analiza przyczyn źródłowych, wyszukiwanie zagrożeń i rozwiązywanie problemów z siecią staje się proste.

Wykrywanie
GREYCORTEX Mendel wykorzystuje wykrywanie i reagowanie sieciowe do analizy i wykrywania zaawansowanych, nieznanych ataków (APT) infekujących inne urządzenia, pobierających Torrenty, skanujących w poszukiwaniu otwartych portów lub komunikujących się z serwerem dowodzenia i kontroli w całej sieci w czasie rzeczywistym. Działania te powodują powstawanie w sieci ruchu komunikacyjnego, który jest anomalny w stosunku do „normalnego" ruchu sieciowego.

Mendel składa się z kilku najnowocześniejszych technologii i silników detekcji:

- Intrusion Detection System (IDS)
- Głęboka inspekcja pakietów (DPI)
- Analiza zachowań sieciowych (NBA) oparta na sztucznej inteligencji
- Analiza ruchu szyfrowanego
- Monitorowanie wydajności sieci i aplikacji (NPM, APM)
- Korelacja zdarzeń (EC)
- Ocena ryzyka (RA)

Reakcja
Analiza ryzyka i korelacji łączy kilka wykrytych zdarzeń w jeden incydent i ocenia stopień ryzyka sieci, podsieci, hostów i usług. Funkcje zarządzania incydentami pozwalają kilku analitykom pracować nad problemem w tym samym czasie lub zrównoważyć obciążenie pracą w zespole.

Dla tych, którzy pracują z systemami SIEM, GREYCORTEX Mendel może eksportować dane o przepływach i zdarzeniach do SIEM w celu ich dalszego zbadania. Analitycy mogą również powrócić z SIEM do GREYCORTEX Mendel za pomocą jednego kliknięcia, aby uzyskać więcej szczegółów.

Mendel integruje się z narzędziami bezpieczeństwa, które są już w sieci, takimi jak firewalle, systemy kontroli dostępu i inne aktywne narzędzia bezpieczeństwa, dzięki czemu można reagować na ataki, prowadzić dochodzenia, zarządzać wszystkimi incydentami i blokować złośliwą komunikację z jednego interfejsu.

OT - SCADA/ICS
Nasze rozwiązanie uczy się wzorców typowego zachowania w sieci i dostosowuje swój model do aktualnej pory dnia i tygodnia, wykrywając kto, kiedy i z jaką częstotliwością komunikuje się z kim, uwzględniając również komendy, zmienne danych i ich wartości.

Tworząc modele zachowań dla wszystkich fizycznych i logicznych urządzeń i wyposażenia, w tym każdej stacji, usługi i kanału komunikacyjnego pomiędzy urządzeniami w sieci OT, Mendel może wykryć wszystkie anomalie. Jednocześnie łączy specyficzne sygnatury wykrywania znanych zagrożeń i nasze sygnatury wykrywania, aby zidentyfikować około 300 typów ataków przemysłowych i infrastruktury krytycznej na najczęściej używane protokoły OT.