maltiverse

Praktyczna wiedza o cyberzagrożeniach

Zespół Maltiverse

Eksperci ds. cyberbezpieczeństwa

50 lat doświadczenia w branży cyberochrony

Dekady doświadczenia na stanowiskach menedżerskich w działach SOC, w obsłudze incydentów oraz w polowaniu na zagrożenia.

Automatyzacja jest niezbędna

Specjaliści ds. cyberbezpieczeństwa na co dzień mierzą się z powtarzającymi się zadaniami. Automatyzacja pozwala skupić się na tym, co najważniejsze.

Misja Maltiverse: pomoc we wdrożeniu praktycznej wiedzy o cyberzagrożeniach

Misją Maltiverse jest pomaganie firmom w rozpoczęciu korzystania z wiedzy o zagrożeniach przy minimalnym wysiłku i ingerencji w infrastrukturę.

Powody wdrożenia

Do czego przydaje się wiedza o cyberzagrożeniach?

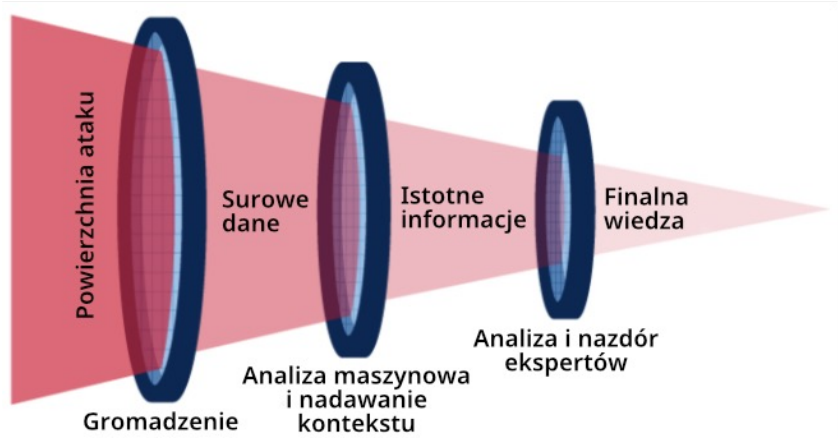
Dwie olbrzymie korzyści

1 – Mniejsze ryzyko

powodzenia znanych ataków

2 – Większa efektywność

zespołu bezpieczeństwa



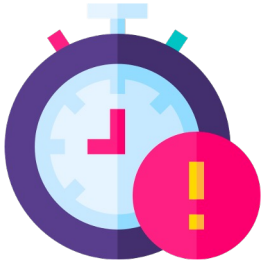
Częste problemy

Wiedza o cyberzagrożeniach – typowe problemy

Bez automatyzacji

Znużenie analityków

Ilość danych rośnie wykładniczo i uzyskanie odpowiedniej jakości wiedzy o zagrożeniach jedynie w oparciu o pracę ludzi jest niemożliwe.



Bez automatyzacji

Opóźnienia

Niezautomatyzowane dostarczanie wiedzy o zagrożeniach może prowadzić do opóźnień w wykrywaniu nowych zagrożeń.

Z automatyzacją

Fałszywe alarmy

Niektóre źródła wskaźników włamań (IoC) dostarczają nieprecyzyjne dane, co może prowadzić do blokowania niezainfekowanych zasobów lub marnowania czasu analityków na odsiewanie fałszywych alarmów.

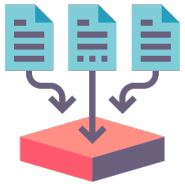
Z automatyzacją

Utrata ważności wskaź-ników ataków (IoC)

Szkodliwe obiekty nie muszą być niebezpieczne na zawsze. Zespół zajmujący się dostarczaniem wiedzy o zagrożeniach musi usuwać przestarzałe wskaźniki ataków, by unikać fałszywych alarmów.

Maltiverse

Rozwiązanie – praktyczna wiedza o cyberzagrożeniach

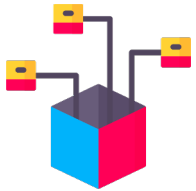


Ponad 100 źródeł wiedzy

Maltiverse łączy dane z ponad 100 różnych źródeł wiedzy o zagrożeniach. Są to źródła publiczne, prywatne i tworzone przez społeczność zaangażowaną w walkę z cyberprzestępczością.

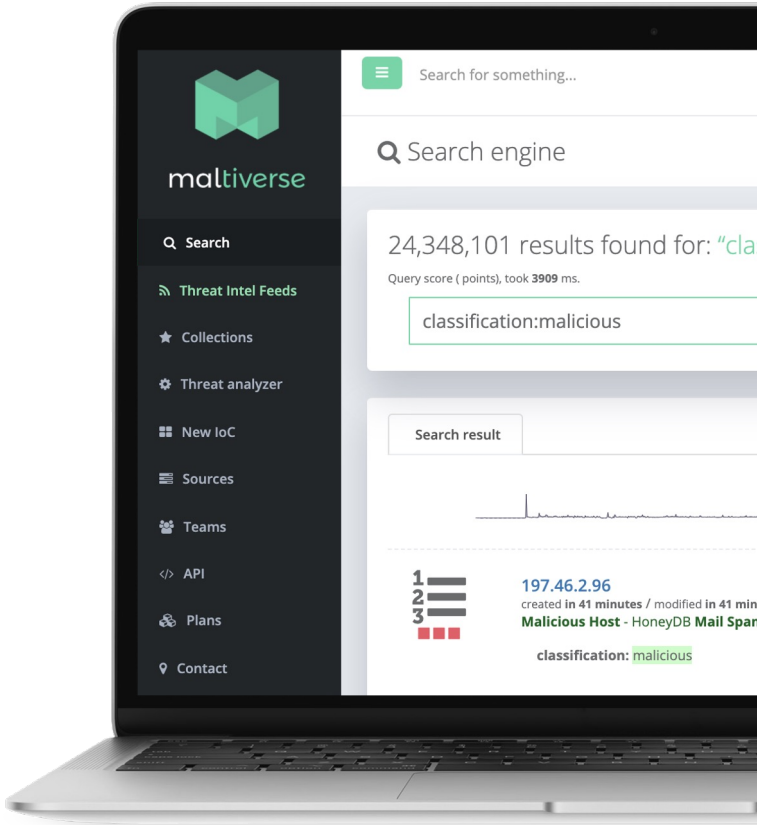
Algorytm oceny IoC

Maltiverse stosuje autorski algorytm oceny wskaźników ataków, który uwzględnia setki warunków. W rezultacie powstaje precyzyjna i przejrzysta dla analityków, uaktualniana w czasie rzeczywistym klasyfikacja.



Dostarczanie do urządzeń bezpieczeństwa

Maltiverse oferuje możliwość integracji z większością popularnych urządzeń bezpieczeństwa. Wykonanie integracji zwykle zajmuje zaledwie kilka minut.



Maltiverse

Ponad 100 źródeł wiedzy – wszystko w pakiecie

500 nowych wskaźników ataków co godzinę!

Prywatne

- Prace badawcze
- Honeypoty (pułapki)
- Techniki pozyskiwania

CYBER THREAT ALLIANCE

paloalto NETWORKS · RAPID7 · CISCO · SOPHOS · McAfee · Symantec. A Division of Broadcom · CHECK POINT · vmware

Publiczne

Zeustracker	Google Safebrowsing	Talos Intelligence
Alexa	Sblam	Ransomware Tracker
Cyber Threat Coalition	DomainTools	Microsoft
Blocklist.de	RWTH	Public-dns.info
StopForumSpam.com	Myip.ms	Malwaremustdie.org
Rapid7 Open Data	Darklist	CCN-CERT
ClArmy	GreenSnow	CruzIT
Alienvault	Nothink.org	IP Blacklist Cloud
Blocklist.net.ua	BadIPs	malwaredomainlist.com
Hybrid-Analysis	SANS	Cyberprotect
Abuse.ch	Mr.Looquer	ThreatCrowd
Cleantalk.org	OpenPhish	Malware Domains
Phishtank	Greynoise	Spamhaus
HoneyDB	Zone-H	VxVault
Emerging Threats	Cybercrime-tracker.net	Feodotracker
Abuseat.org	Botscout	APT Notes
Barracuda	Bambernek	Dyndns.org
.BEware	TorProject.org	Politie.nl

Tworzone przez społeczność

- Ponad 90 aktywnych zespołów badawczych
- Milion nowych wskaźników ataków co miesiąc

Maltiverse

Algorytm oceny

Klasyfikacja w czasie rzeczywistym

*Przykład zapobiegania fałszywym trafieniom: wykryto szkodliwe oprogramowanie w danych przychodzących z określonego adresu IP, jednak adres ten alokuje także 60 legalnych domen, zatem może zostać uznany za hosting, a tym samym dodany do **białej listy**.*

198.136.61.196

adres podejrzany o dystrybucję szkodliwego oprogramowania

Wzbogacenie

AS33182
HostDime com Inc

61
rozwiązanych nazw hostów

60 domen na białej liście

1 domena na czarnej liście

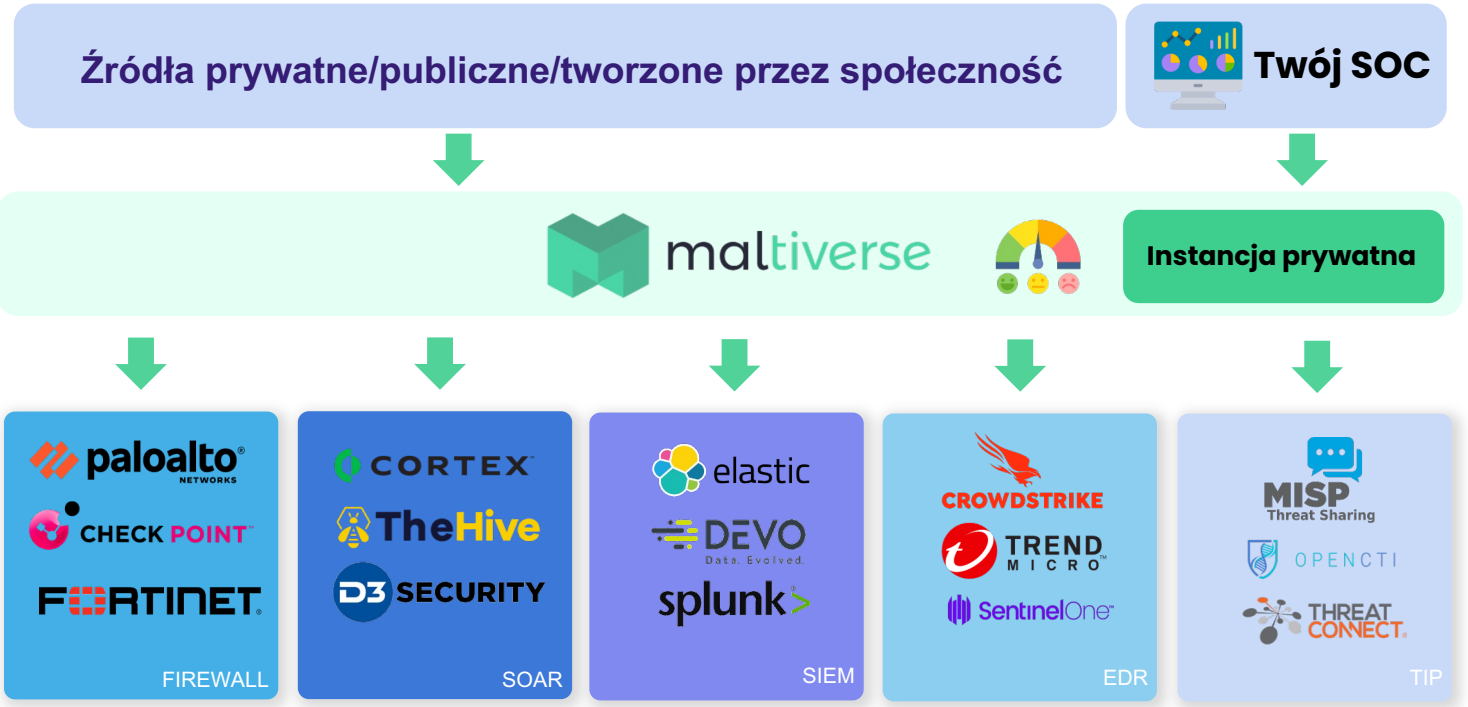
- Czy jest znanym skanerem?
- Czy przechowuje phishing?
- Czy dystrybuuje szkodliwe programy?
- Czy jest węzłem sieci Tor?
- Czy jest zagrożeniem dla IoT?
- Czy jest hostingiem?
- Czy jest serwerem przestępczym?
- Czy oferuje anonimizację?
- Czy jest znanym atakującym?
- Czy jest powiązany z kopaniem kryptowalut?

szkodliwy
podejrzany
neutralny
biała lista

Maltiverse

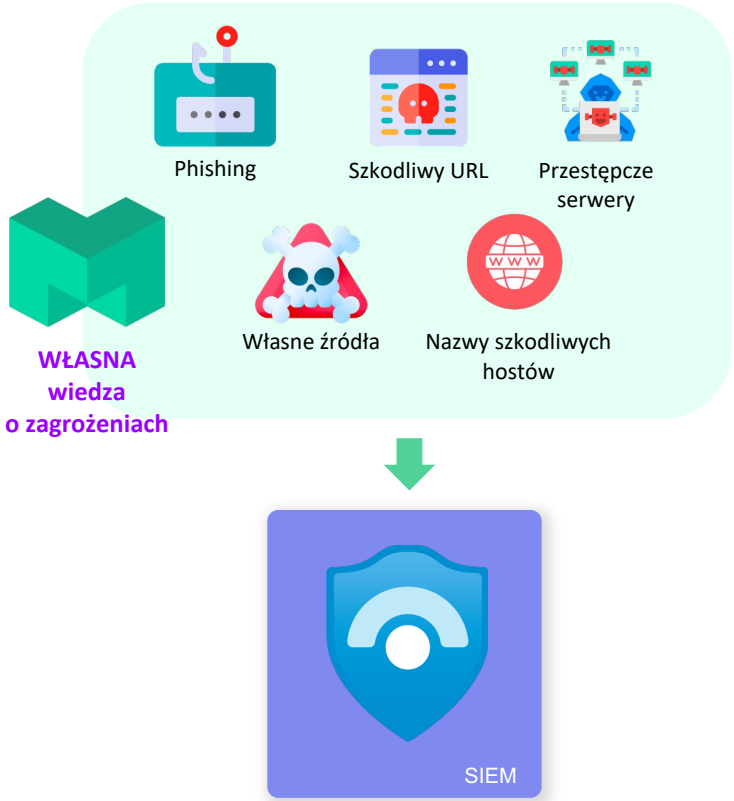
Dostarczanie do urządzeń bezpieczeństwa

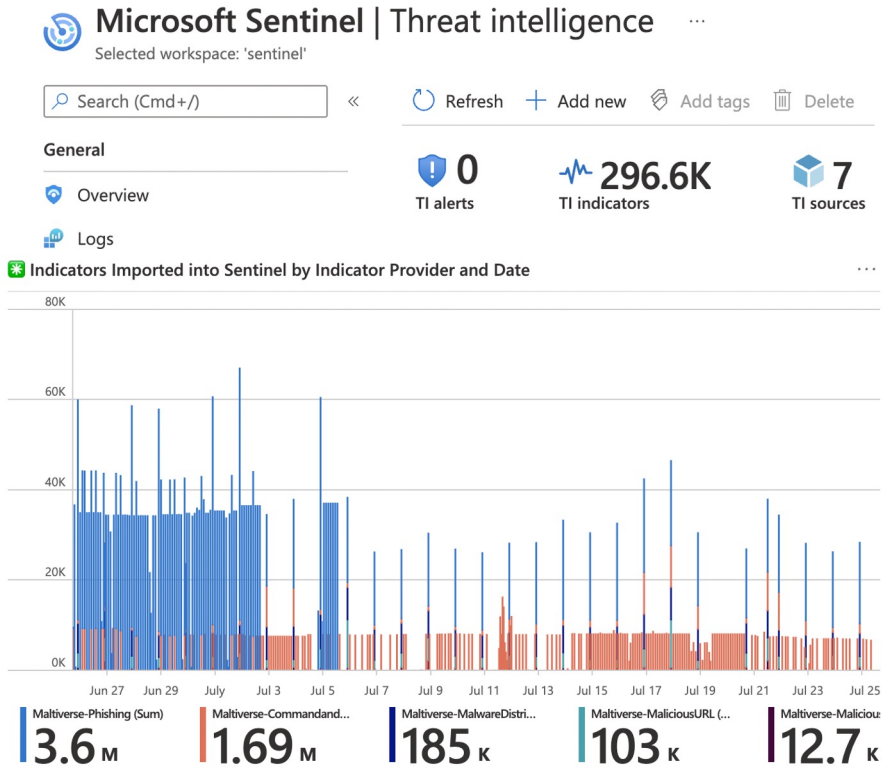
Integracja z istniejącą infrastrukturą



Przykład zastosowania

Wykrywanie i zapobieganie z użyciem rozwiązania SIEM

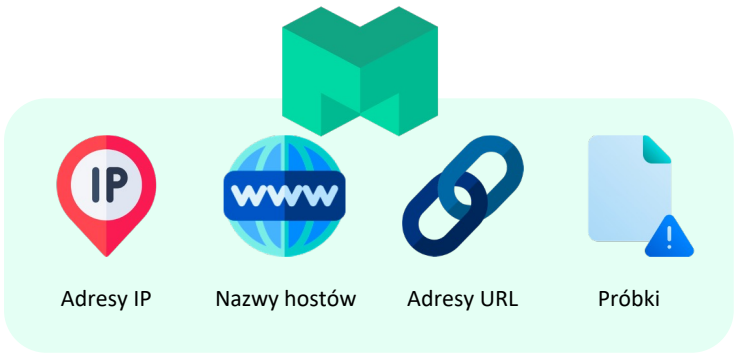


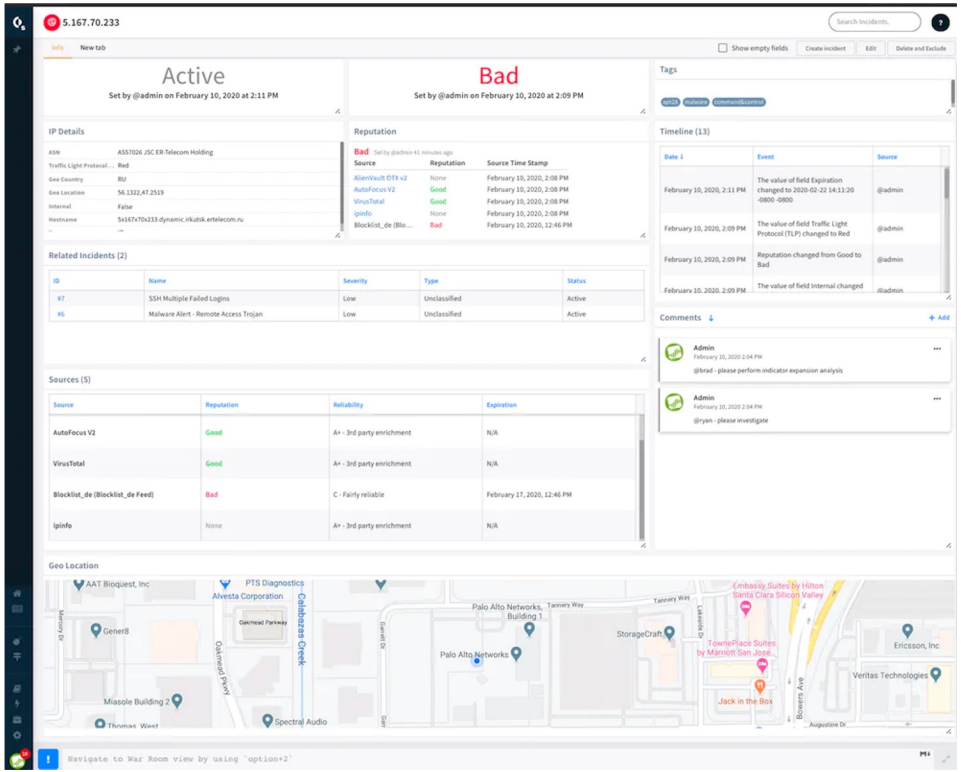


Przykład zastosowania

Wzbogacenie rozwiązania SOAR

Maltiverse dostarcza klasyfikację i kontekst dla alertów rozwiązania SOAR

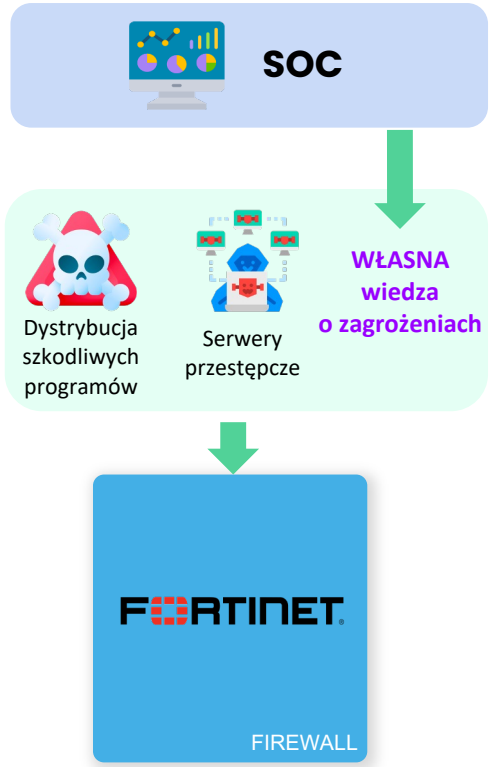


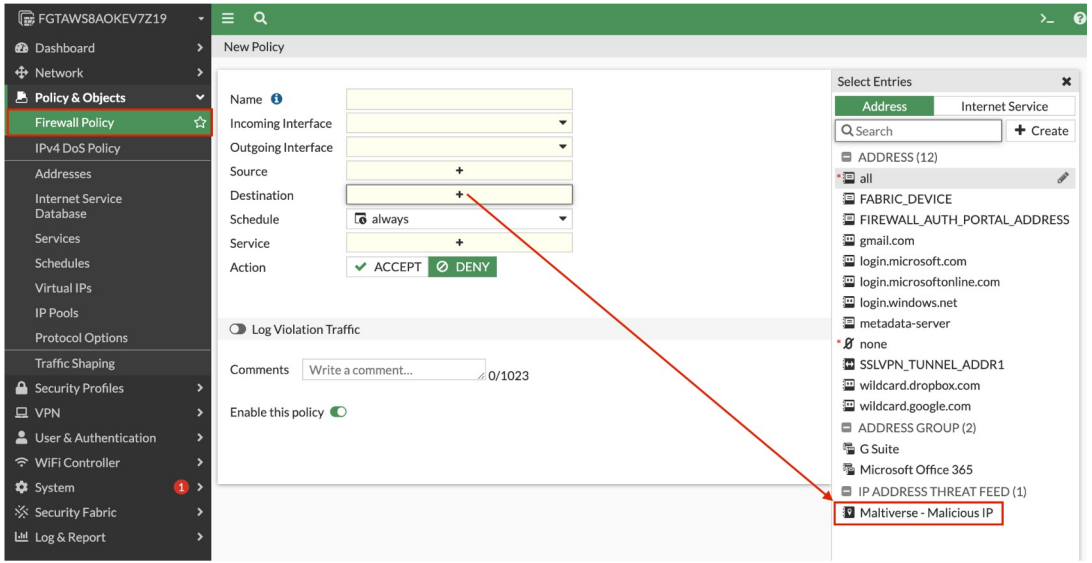


Przykład zastosowania

Usprawnienie wykrywania na zaporze sieciowej

Przesyłanie wskaźników włamań bezpośrednio do Maltiverse





Przykład zastosowania

Wzbogacenie produktu - Firedome IoT

Firedome to szybko rosnący, globalny dostawca rozwiązań IoT

Problem

- Urządzenia IoT mają ogromny potencjał, jednak jednocześnie generują duże ryzyko
- Firma stawia w swoim rozwiązaniu bezpieczeństwo na pierwszym planie
- Firma chce mieć pewność, że jej klienci i urządzenia nie uzyskują dostępu do szkodliwych stron, adresów IP oraz domen
- Firma chce, by wiedza o cyberzagrożeniach była wbudowana w rozwiązanie
- Firma wymaga dostępu do wskaźników zagrożeń powiązanych z urządzeniami IoT

Rozwiązanie

Firma oceniła różne źródła wiedzy o zagrożeniach i wybrała pakiet Advanced rozwiązania Maltiverse, łącznie z informacjami o:

- szkodliwych adresach IP
- dystrybucji szkodliwego oprogramowania
- serwerach kontrolowanych przez cyberprzestępców
- phishingu
- atakach na urządzenia IoT
- szkodliwych adresach URL

Maltiverse Trial

Wersja testowa Maltiverse – kroki

Cały proces trwa 30 dni

Wybór	Integracja	Dostosowanie i przegląd	Zakończenie
Decyzja dotycząca najlepszego podejścia do integracji oraz technologii, które mają zostać wzbogacone wiedzą o cyberzagrożeniach.	Integracja Maltiverse z uzgodnionymi technologiami. Wdrożenie następuje stopniowo, by uniknąć przerw w pracy.	Dostosowanie konfiguracji i okresowy przegląd pojawiających się alertów. Rozszerzenie lub zredukowanie liczby wybranych źródeł danych.	Przedstawienie ostatecznego raportu na spotkaniu podsumowującym. Jeżeli zostanie wybrany plan Enterprise, nie są wymagane dalsze działania.

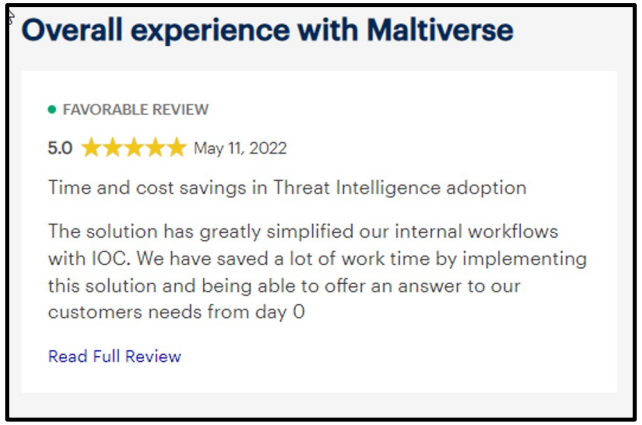
2 godz. – Inżynier ds. bezpieczeństwa

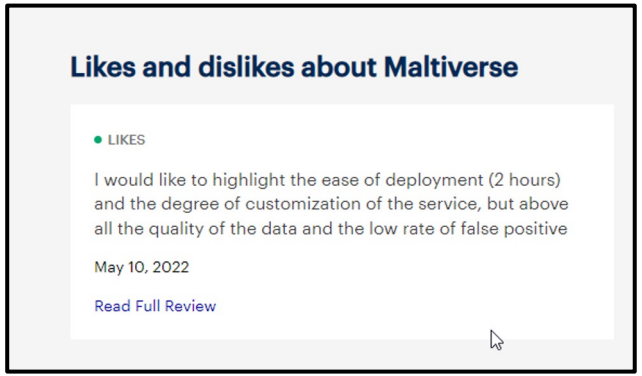
1 godz. – Specjalista ds. technicznych

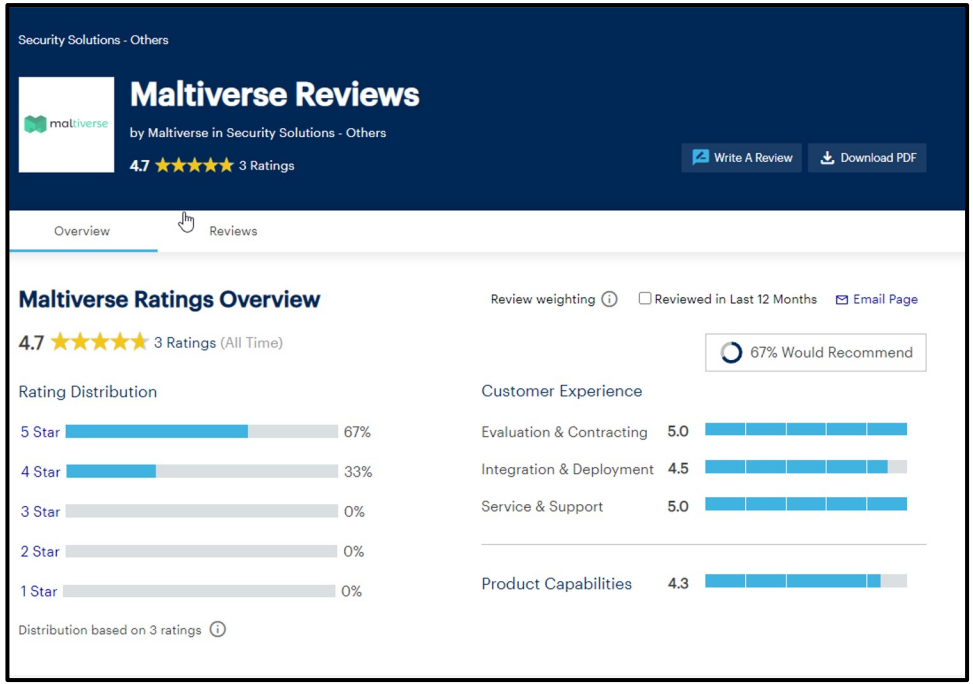
Łącznie: 3 godz.

Klienci

Referencje







Wiedza o cyberzagrożeniach - łatwo, szybko i dla wszystkich.

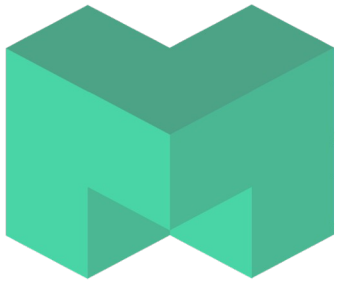
Zespoły zajmujące się bezpieczeństwem nie mogą inwestować odpowiednio dużo czasu w analizę, wdrażanie i konserwację dziesiątek źródeł wiedzy o zagrożeniach. Maltiverse automatyzuje ten żmudny proces i oferuje efektywny dostęp do źródeł danych dotyczących zagrożeń.

Synchronizacja wielu urządzeń

Profesjonalna wiedza o cyberzagrożeniach

Najlepszy współczynnik cena/korzyści

Zwiększenie bezpieczeństwa w firmie



maltiverse