



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?

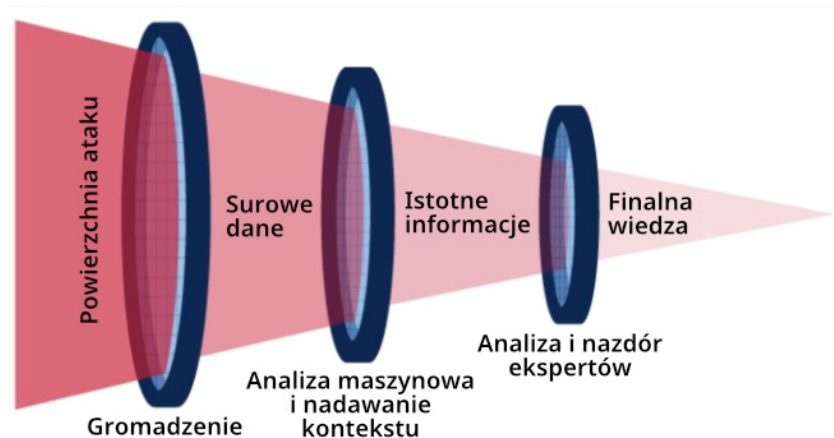
**Dwie olbrzymie korzyści**

## 1 – Mniejsze ryzyko

powodzenia znanych ataków

## 2 – Większa efektywność

zespołu bezpieczeństwa



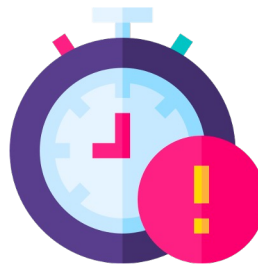
# Wiedza o cyberzagrożeniach – typowe problemy



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

Nieautomatyzowane 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.



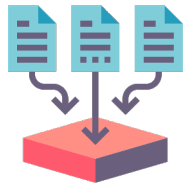
Z automatyzacją

## Utrata ważności wskaźników 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.

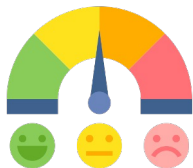
Maltiverse

# Rozwiązanie – praktyczna wiedza o cyberzagrożeniach



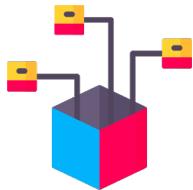
## Ponad 100 źródeł wiedzy

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.



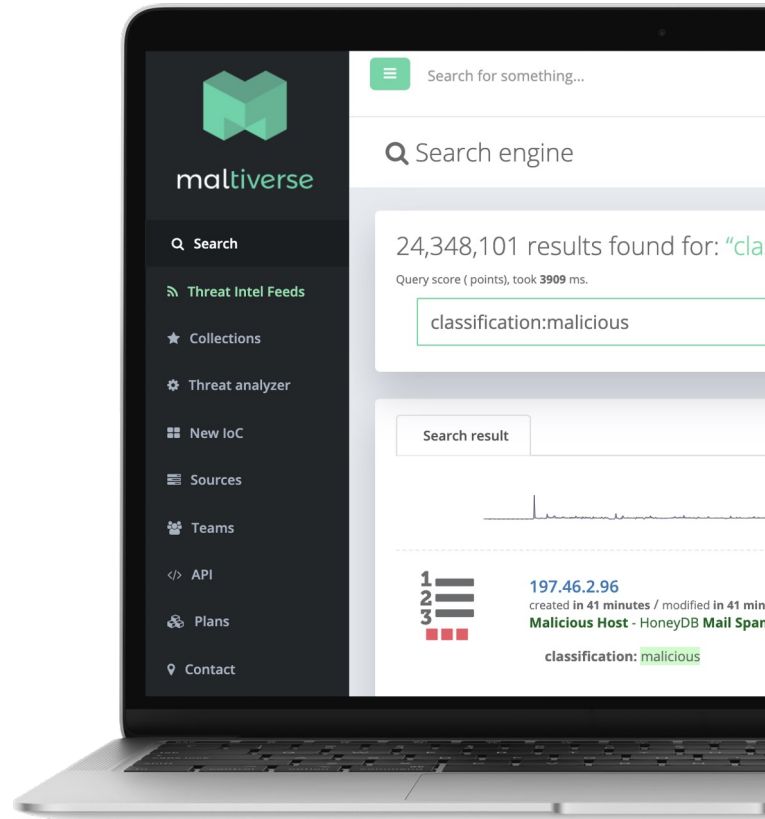
## Algorytm oceny IoC

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 urzędów bezpieczeństwa

Maltiverse oferuje możliwość integracji z większością popularnych urzędów 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



## Publiczne

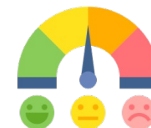
Zeustracker	Google Safebrowsing	Talos Intelligence
Alexa	Sblam	Ransomware Tracker
Cyber Threat Coalition	DomainTools	Microsoft
Blocklist.de	RWTH	Public-dns.info
StopForumSpam.com	Myip.ms	Malwaremustdie.org
Rapid7 Open Data	Darklist	CCN-CERT
CIArmy	GreenSnow	CruzIT
Alienvault	Nothink.org	IP Blacklist 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

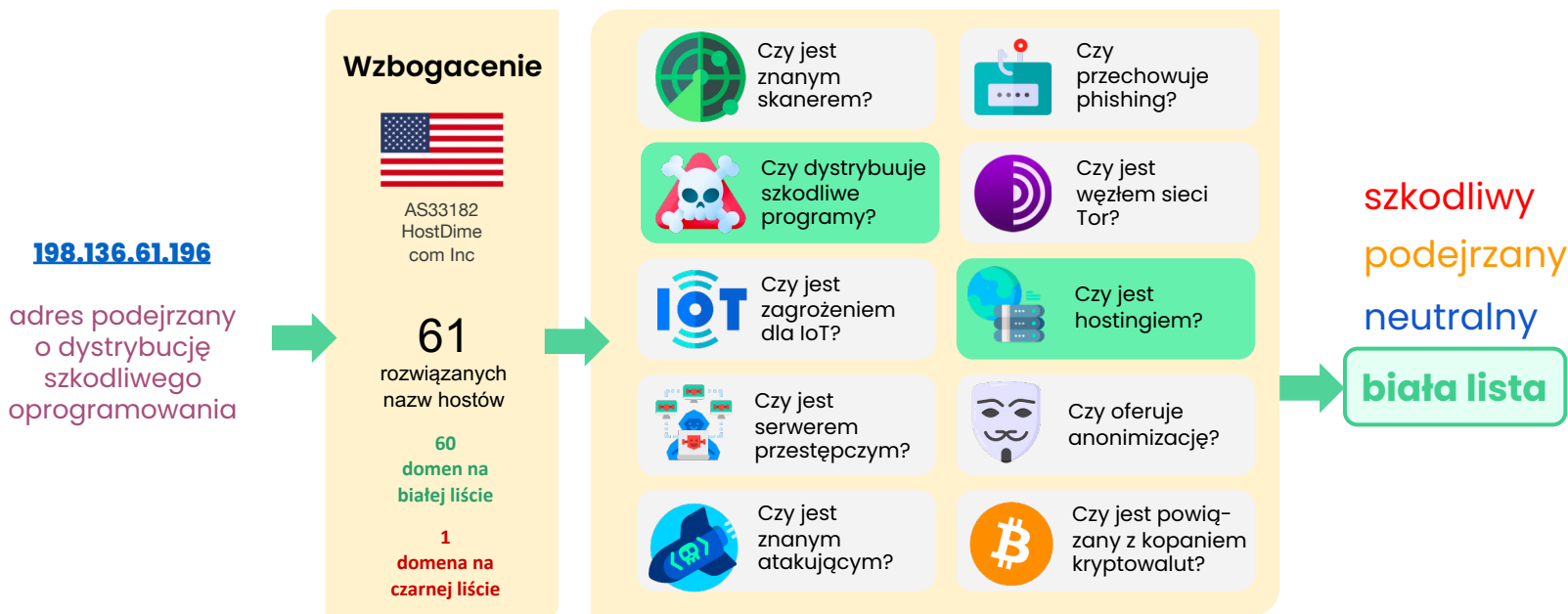
- Ponad 90 aktywnych zespołów badawczych
- Milion nowych wskaźników ataków co miesiąc

# Algorytm oceny

## Klasyfikacja w czasie rzeczywistym



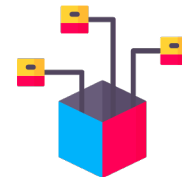
Przykład zapobiegania fałszywym trafieniom: wykryto szkodliwe oprogramowanie w danych przychodzących z określonego adresu IP, jednak adres ten alokuje także 60 legalnych domen, zatem może zostać uznany za hosting, a tym samym dodany do *białej listy*.



Maltiverse

# Dostarczanie do urzędów bezpieczeństwa

## Integracja z istniejącą infrastrukturą



Źródła prywatne/publiczne/tworzone przez społeczność



Twój SOC



maltiverse



Instancja prywatna

**paloalto**  
NETWORKS

**CHECK POINT**

**FORTINET**

FIREWALL

**CORTEX**

**TheHive**

**D3 SECURITY**

SOAR

**elastic**

**DEVO**  
Data. Evolved.

**splunk**

SIEM

**CROWDSTRIKE**

**TREND MICRO**

**SentinelOne**

EDR

**MISP**  
Threat Sharing

**OPENCTI**

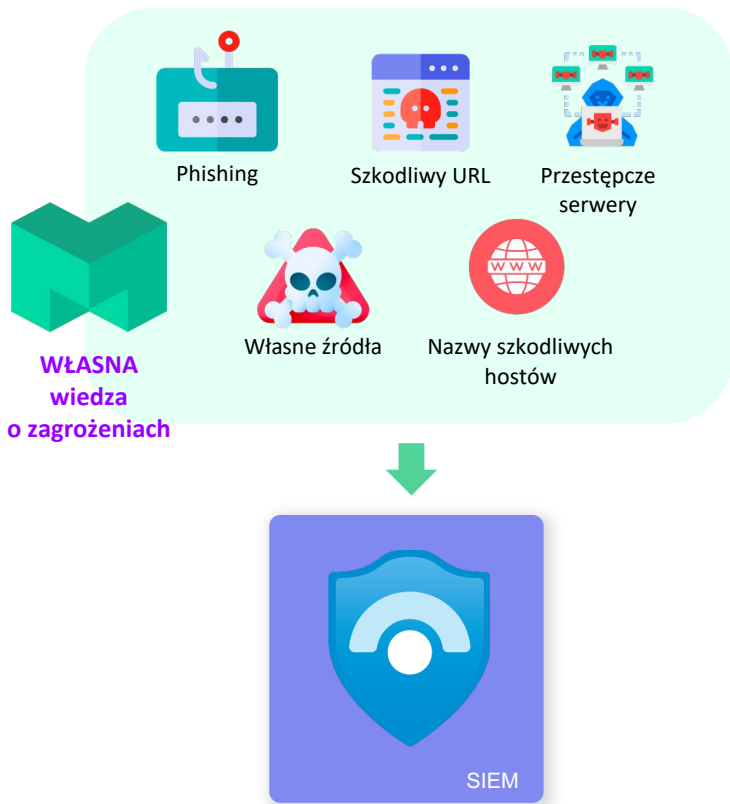
**THREAT CONNECT**

TIP



Przykład zastosowania

# Wykrywanie i zapobieganie z użyciem rozwiązania SIEM



## Microsoft Sentinel | Threat intelligence

Selected workspace: 'sentinel'

Search (Cmd+/) << Refresh + Add new Add tags Delete

### General

Overview

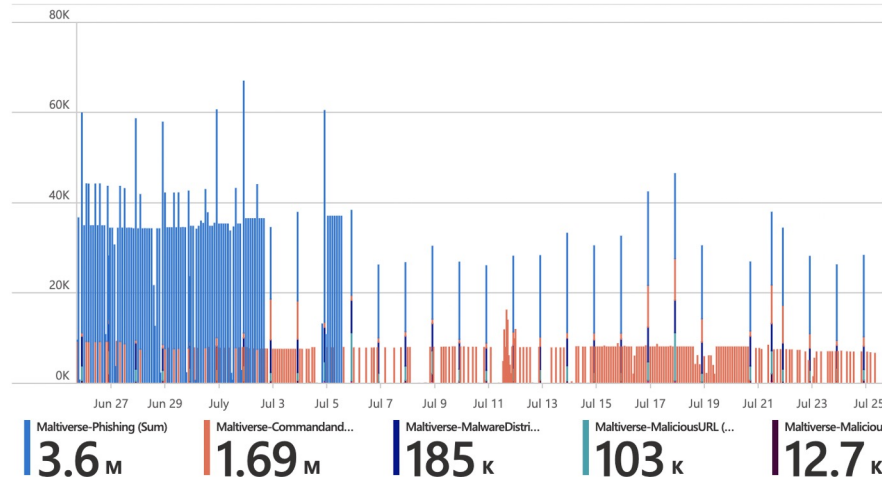
Logs

0  
TI alerts

296.6K  
TI indicators

7  
TI sources

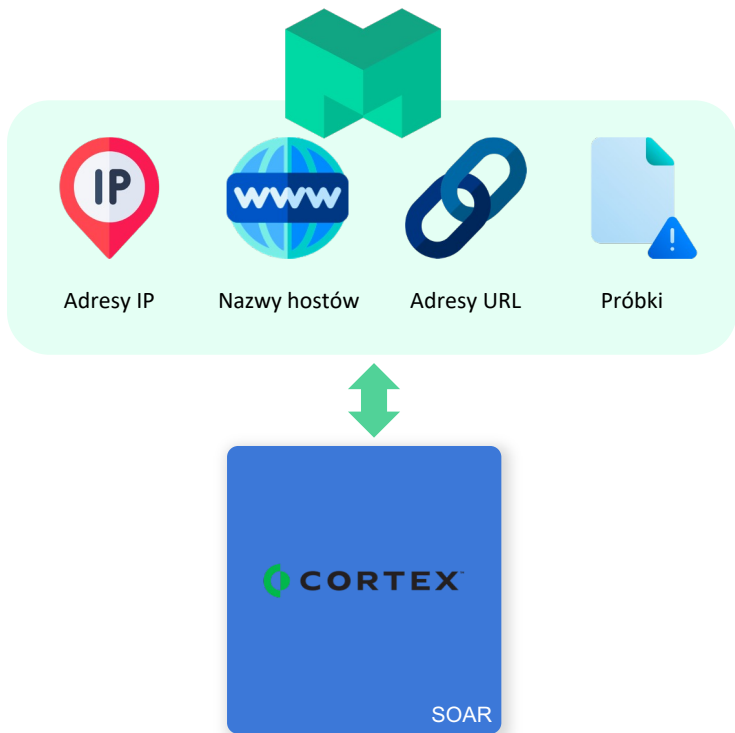
### Indicators Imported into Sentinel by Indicator Provider and Date



Przykład zastosowania

# Wzbogacenie rozwiązania SOAR

Maltiverse dostarcza klasyfikację i kontekst dla alertów rozwiązania SOAR



The screenshot shows a SOAR interface for an active incident with ID 5.167.70.233. The incident is classified as 'Bad' and was set by @admin on February 10, 2020, at 2:09 PM. The interface is divided into several sections:

- IP Details:** Shows AS57024 - JSC ER Telecom Holding, Traffic Light Protocol: Bad, Geo Country: RU, Geo Location: 56.1322,47.2519, Internal: False, and Hostname: 5616770x233.dynamic.rk.utok.ertelecom.ru.
- Reputation:** A table showing source reputations: AlertVault OTR v2 (Bad), Autofocus V2 (Good), VirusTotal (Good), Iginfo (None), and Blocklist\_de (Bad).
- Related Incidents (2):** A table listing related incidents: ID 97 (SSH Multiple Failed Logins, Low severity, Unclassified type, Active status) and ID 96 (Malware Alert - Remote Access Trojan, Low severity, Unclassified type, Active status).
- Sources (5):** A table listing sources: Autofocus V2 (Good reputation, A+ reliability), VirusTotal (Good reputation, A+ reliability), Blocklist\_de (Bad reputation, C reliability), and Iginfo (None reputation, A+ reliability).
- Geo Location:** A map showing the location of Palo Alto Networks, Tennen Hwy Building 1, and other nearby locations.
- Timeline (13):** A list of events showing the incident's history, including field expiration changes and reputation updates.
- Comments:** A section for user comments, including one from @brad asking for indicator expansion analysis.

Przykład zastosowania

# Usprawnienie wykrywania na zaporze sieciowej

Przesyłanie wskaźników włamań bezpośrednio do Maltiverse



The screenshot shows the Fortinet Firewall Policy configuration interface. The left sidebar lists various configuration areas, with 'Policy & Objects' and 'Firewall Policy' highlighted. The main area shows the 'New Policy' configuration form. The 'Destination' field is highlighted with a red box, and a red arrow points from it to the 'Select Entries' panel on the right. In the 'Select Entries' panel, the entry 'Maltiverse - Malicious IP' is highlighted with a red box.

FGTAW58AOKEV7Z19

- Dashboard
- Network
- Policy & Objects
- Firewall Policy
- IPv4 DoS Policy
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles
- VPN
- User & Authentication
- WiFi Controller
- System
- Security Fabric
- Log & Report

New Policy

Name: [ ]

Incoming Interface: [ ]

Outgoing Interface: [ ]

Source: [ ]

Destination: [ ]

Schedule: [ always ]

Service: [ ]

Action: [ ACCEPT ] [ DENY ]

Log Violation Traffic: [ ]

Comments: [ Write a comment... ] 0/1023

Enable this policy: [ ]

Select Entries

Address Internet Service

Q Search + Create

- ADDRESS (12)
- all
- FABRIC\_DEVICE
- FIREWALL\_AUTH\_PORTAL\_ADDRESS
- gmail.com
- login.microsoft.com
- login.microsoftonline.com
- login.windows.net
- metadata-server
- none
- SSLVPN\_TUNNEL\_ADDR1
- wildcard.dropbox.com
- wildcard.google.com
- ADDRESS GROUP (2)
- G Suite
- Microsoft Office 365
- IP ADDRESS THREAT FEED (1)
- Maltiverse - Malicious IP

# 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

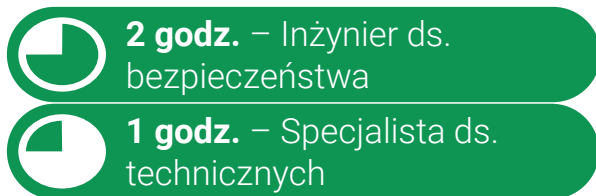


Decyzja dotycząca najlepszego podejścia do integracji oraz technologii, które mają zostać wzbogacone wiedzą o cyberzagrożeniach.

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.



# Referencje

## Overall experience with Maltiverse

● FAVORABLE REVIEW

5.0 ★★★★★ May 11, 2022

Time and cost savings in Threat Intelligence adoption

The solution has greatly simplified our internal workflows with IOC. We have saved a lot of work time by implementing this solution and being able to offer an answer to our customers needs from day 0

[Read Full Review](#)

## Likes and dislikes about Maltiverse

● LIKES

I would like to highlight the ease of deployment (2 hours) and the degree of customization of the service, but above all the quality of the data and the low rate of false positive

May 10, 2022

[Read Full Review](#)

The screenshot shows the G2 Crowd review page for Maltiverse in the 'Security Solutions - Others' category. The page features a dark blue header with the Maltiverse logo and a 4.7 star rating based on 3 ratings. Navigation tabs for 'Overview' and 'Reviews' are visible, with 'Reviews' being the active tab. The main content area is titled 'Maltiverse Ratings Overview' and includes a '67% Would Recommend' gauge. A 'Rating Distribution' section shows a bar chart where 67% of reviews are 5 stars and 33% are 4 stars. A 'Customer Experience' section lists scores for various categories: Evaluation & Contracting (5.0), Integration & Deployment (4.5), Service & Support (5.0), and Product Capabilities (4.3). The page also includes options to 'Write A Review' and 'Download PDF'.

Security Solutions - Others

**Maltiverse Reviews**  
by Maltiverse in Security Solutions - Others  
4.7 ★★★★★ 3 Ratings

[Write A Review](#) [Download PDF](#)

Overview **Reviews**

### Maltiverse Ratings Overview

Review weighting ⓘ  Reviewed in Last 12 Months [Email Page](#)

4.7 ★★★★★ 3 Ratings (All Time) 67% Would Recommend

Rating Distribution

5 Star	67%
4 Star	33%
3 Star	0%
2 Star	0%
1 Star	0%

Customer Experience

Evaluation & Contracting	5.0
Integration & Deployment	4.5
Service & Support	5.0
Product Capabilities	4.3

Distribution based on 3 ratings ⓘ

# 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  
urzędów



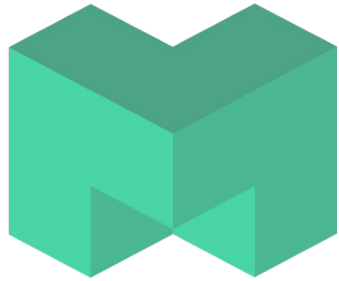
Profesjonalna wiedza  
o cyberzagrożeniach



Najlepszy współczynnik  
cena/korzyści



Zwiększenie  
bezpieczeństwa  
w firmie



maltiverse