



maltiverse

Actionable Threat Intelligence

Our Team

# Security Operations Experts



## 50 Years in Cyberdefense

Decades of experience working as SOC Managers, Incident Handlers and Threat Hunters.



## We believe in Automation

We are against repetitive tasks. Work smart and put your attention on what is important.



## Our mission: Help to adopt Threat Intelligence

Our mission is to help organizations to adopt Threat Intelligence with minimum friction.



Reasons to adopt

# Why Threat Intelligence?

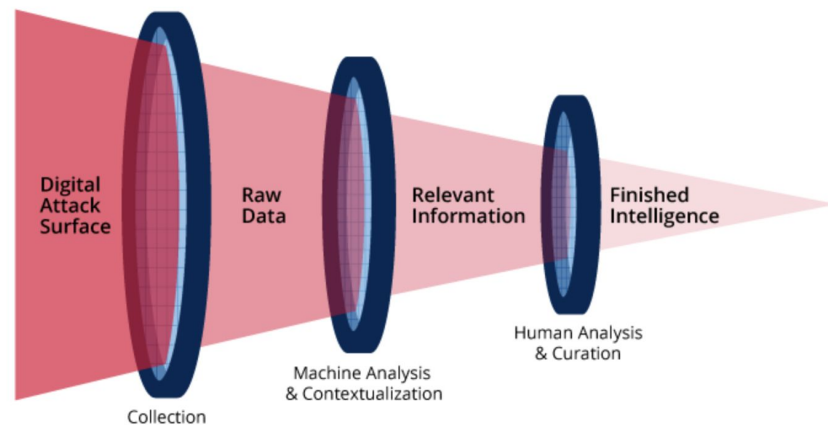
## Two big benefits

### 1 – Lower Risks

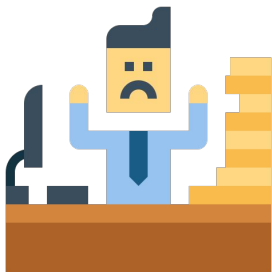
for Known Attacks

### 2 – Improve efficiency

of your security team



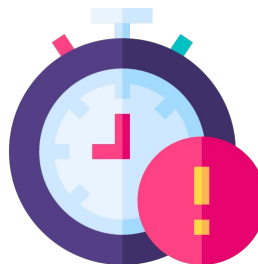
# Threat Intelligence - Common problems



Before Automation

## Analyst Fatigue

Data volume grows exponentially and it is not possible to succeed relying on human workload to maintain a valuable Threat Intelligence dataset.



Before Automation

## Being Late

Non-Automated upload of Threat Intelligence entails a clear risk. Sometimes there are bureaucratic change management processes involved.



After Automation

## False positives

Some IoC sources are providing unreliable data and you can end up blocking legitimate resources or wasting analysts time with noisy alerts.



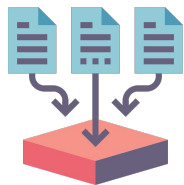
After Automation

## IoC Expiration

Malicious IoCs not always are malicious forever. It is needed for a Threat Intel team to expire old indicators to avoid noise.

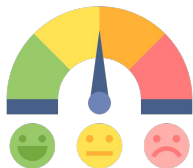
Maltiverse

# Solution - Actionable Threat Intelligence



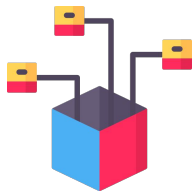
## 100+ Intelligence Sources

Maltiverse aggregates data from more than 100 different Threat Intelligence sources. Public, Private and Community feeds are merged to provide a powerful aggregation.



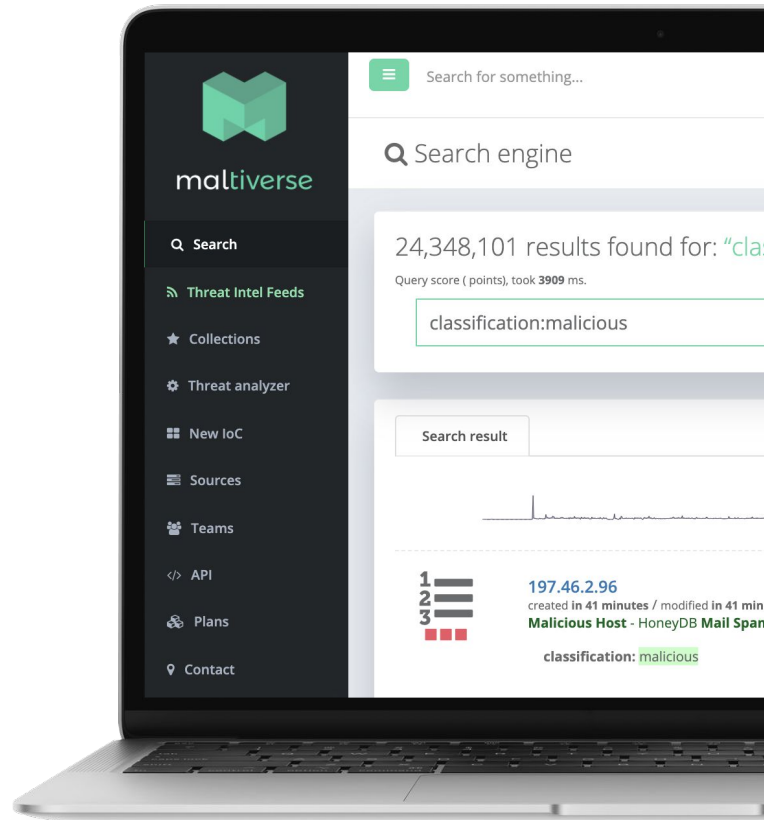
## IoC Scoring Algorithm

Maltiverse applies Scoring Algorithm taking into account hundreds of different conditions. The result is an accurate human readable classification that gets updated real time.



## Delivery to Security Devices

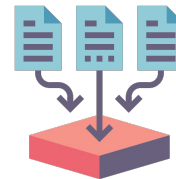
We provide integration to the most relevant commercial security devices. Integrations are completed in a matter of minutes.



Maltiverse

# 100+ Intelligence Sources - All in One

## 500 new IoC per hour!



### Private



Research  
Deception Honeynets  
Mining Techniques



### Public

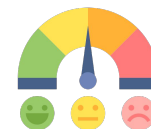
<b>Zeustracker</b>	<b>Google Safebrowsing</b>	<b>Talos Intelligence</b>
<b>Alexa</b>	<b>Sblam</b>	<b>Ransomware Tracker</b>
<b>Cyber Threat Coalition</b>	<b>DomainTools</b>	<b>Microsoft</b>
<b>Blocklist.de</b>	<b>RWTH</b>	<b>Public-dns.info</b>
<b>StopForumSpam.com</b>	<b>Myip.ms</b>	<b>Malwaremustdie.org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

### Community

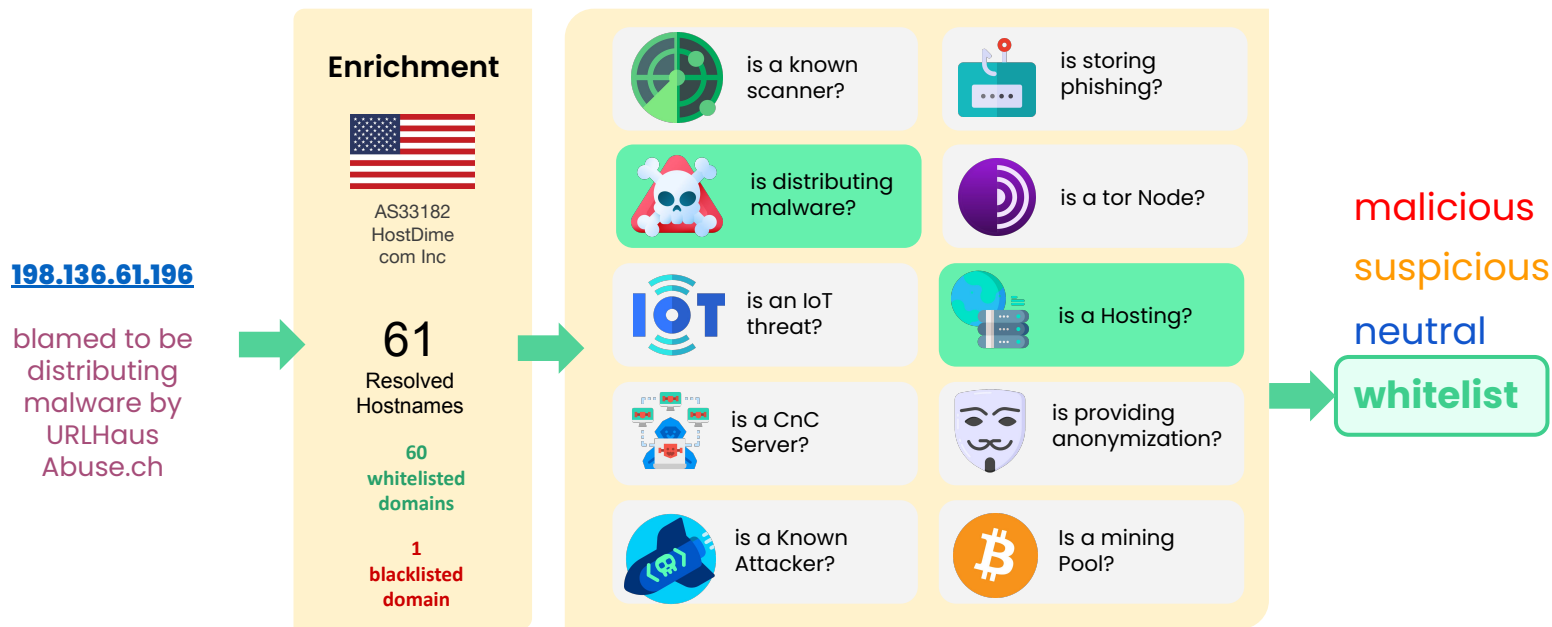
- 5M web requests
- +90 Active Research Teams
- 1M new monthly IoCs

# Scoring Algorithm

## Real time classification



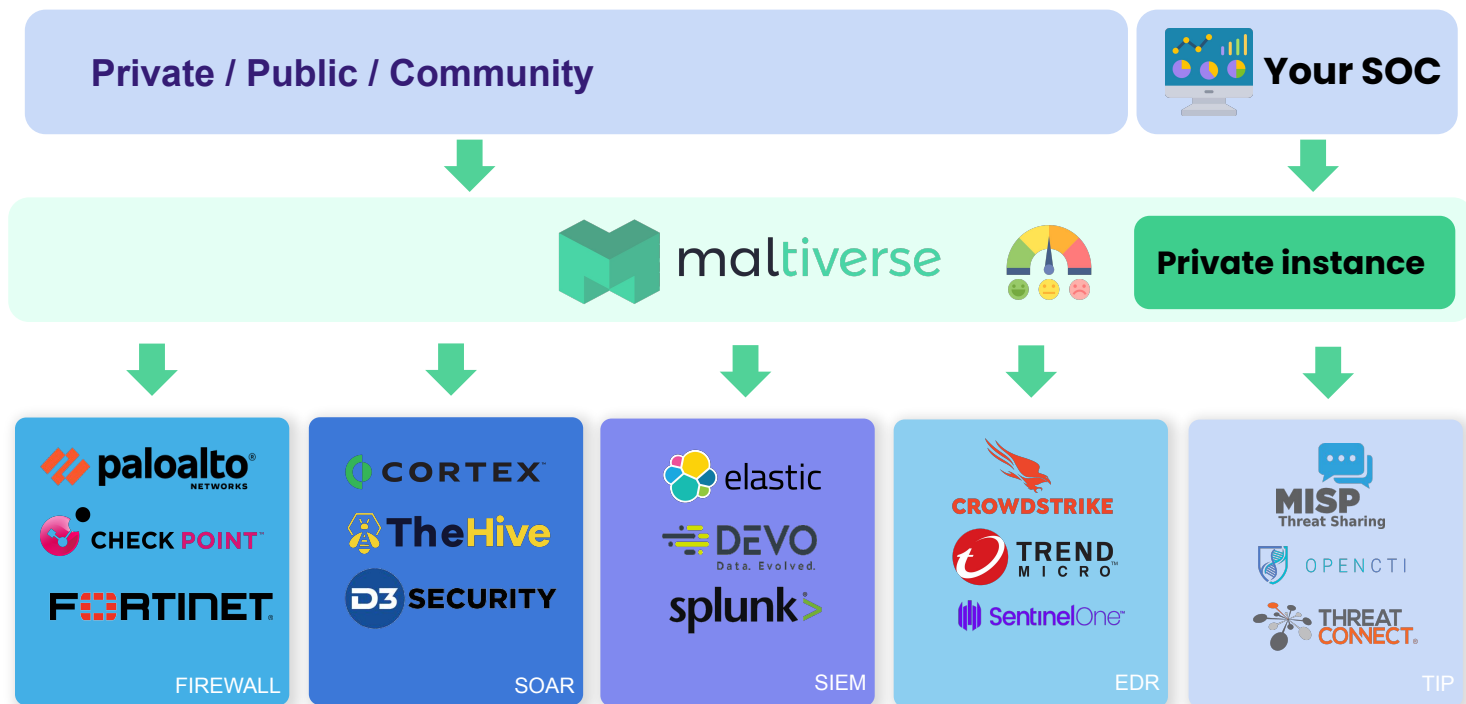
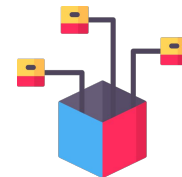
*False positive prevention: An incoming IP sighted distributing malware, nevertheless it allocates 60 legit domains behind, so it is considered as a Hosting and therefore classified as **whitelisted***



Maltiverse

# Delivery to Security Devices

## Integration with your security stack





## Case Study

# Detection & Prevention on a SIEM



## Microsoft Sentinel | Threat intelligence

Selected workspace: 'sentinel'

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

### General

Overview

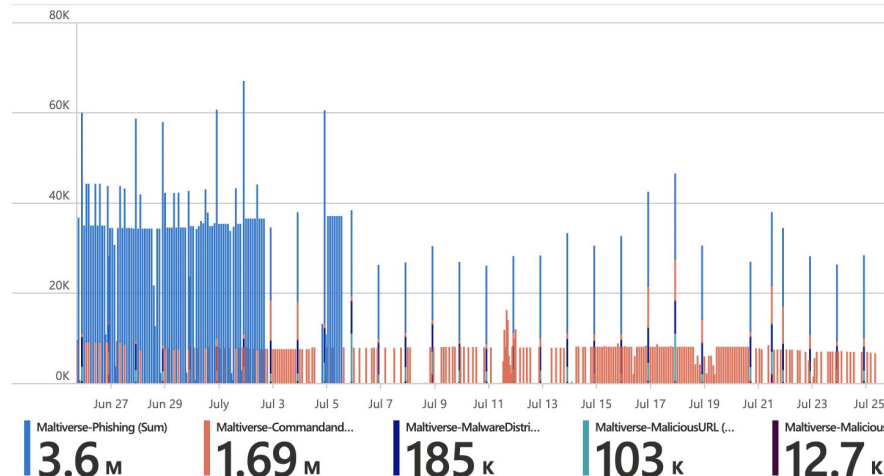
Logs

0  
TI alerts

296.6K  
TI indicators

7  
TI sources

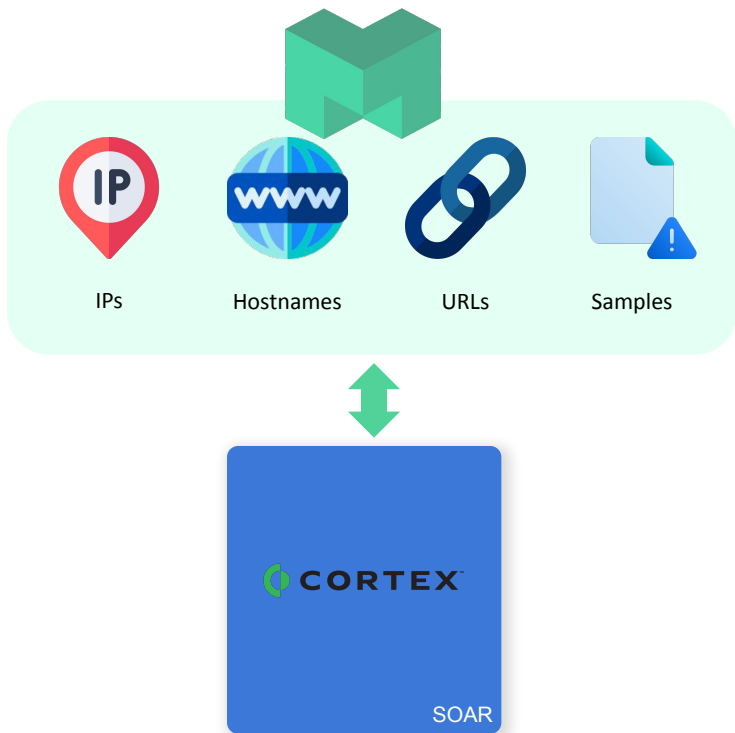
### Indicators Imported into Sentinel by Indicator Provider and Date



## Case Study

# SOAR Enrichment

Maltiverse provides classification and context to the SOAR alerts



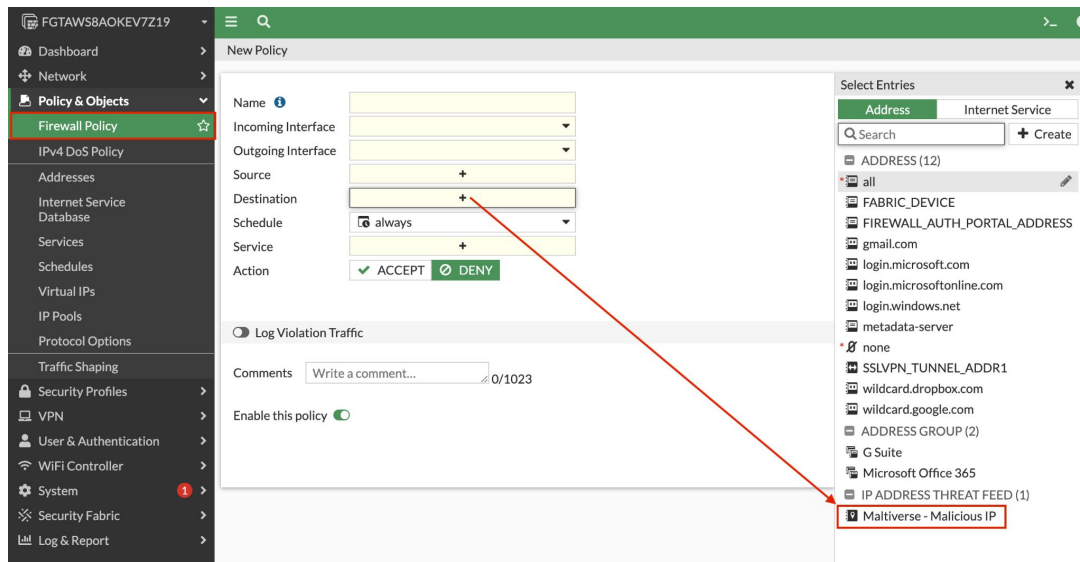
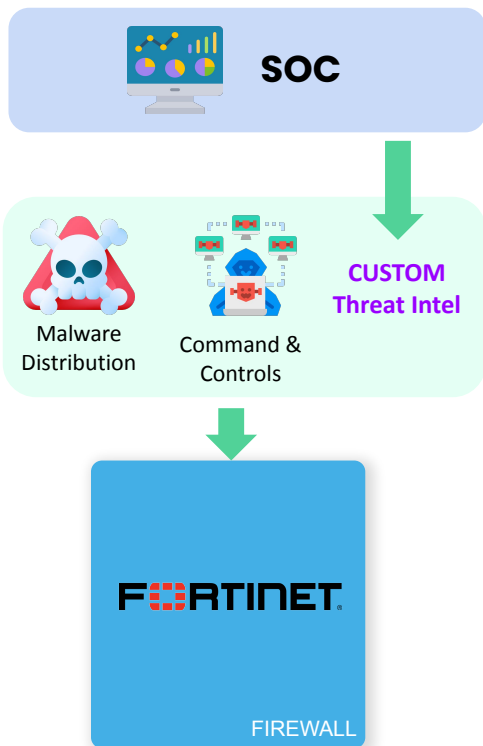
The screenshot shows a SOAR interface for an incident with ID 5.167.70.233. The incident is currently 'Active' but has a 'Bad' reputation. The interface is divided into several sections:

- IP Details:** AS57036 - JSC ER-Museum Holding, Traffic Light Protocol: Red, Geo Country: RU, Geo Location: 56.1322,47.2519, Internal: False, Hostname: 56.1322,47.2519.dynaminic.kutak.entelecom.ru
- Reputation:** A table showing source reputations: AlienVault OTX v2 (None), AutoFocus V2 (Good), VirusTotal (Good), IgiInfo (None), and Blocklist\_de (Bad).
- Related Incidents (2):** A table listing related incidents with IDs #7 and #6, both with Low severity and Unclassified type.
- Sources (5):** A table listing enrichment sources: AutoFocus V2 (Good), VirusTotal (Good), Blocklist\_de (Blocklist\_de Feed) (Bad), and IgiInfo (None).
- Timeline (13):** A list of events showing field changes and reputation updates.
- Comments:** Two comments from users Admin and @brad.
- Geo Location:** A map showing the location of Palo Alto Networks, Tenaro Way Building 1.

## Case Study

# Firewall Traffic Prevention

## Change management overridden by uploading IoCs to Maltiverse



## Case Study

# Product enrichment - Firedome IoT

Firedome is a fast growing IoT solution provider with global presence enabling growth of IoT adoption



## Problem

- IoT is a huge potential but also a high risk
- Our solution is security by default
- We need to ensure that our users and devices don't access malicious sites, IPs and domains
- We needed Threat Intelligence to embed to our solution
- We need to have IoT threats Indicators

## Solution

- We evaluated different sources of threat Intelligence IoCs and have chosen Maltiverse Pack Advanced with:
  - Malicious IPs
  - Malware Distribution
  - Command & Controls
  - Phishing
  - IoT
  - Malicious URLs



## Customer

# References

### 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 selected. The main content area includes a 'Maltiverse Ratings Overview' section with a 4.7 star rating and a '67% Would Recommend' gauge. A 'Rating Distribution' bar chart shows 67% for 5 stars and 33% for 4 stars. A 'Customer Experience' section lists scores for Evaluation & Contracting (5.0), Integration & Deployment (4.5), Service & Support (5.0), and Product Capabilities (4.3). Filter options for review weighting, time period, and email page are also present.

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%

Distribution based on 3 ratings ⓘ

### Customer Experience

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



# Threat Intelligence made simple **for everybody.**

The SecOps teams cannot invest such a big time and effort to onboard tens of Threat Intelligence sources, curate and maintain them. Maltiverse automates this hard job and provides a strongly effective and affordable Threat Intelligence service.



Sync multiple devices



Professional Grade  
Threat intelligence



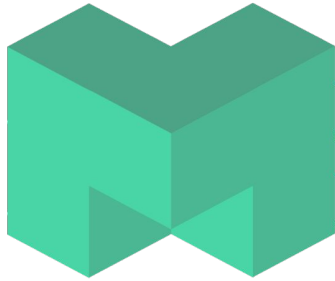
Best cost/benefit  
service



Quick Win in your  
organization



Thank You



maltiverse

Calle Goya 51 1º Izquierda,  
28001, Madrid, Spain.

**Email**

[root@maltiverse.com](mailto:root@maltiverse.com)