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?

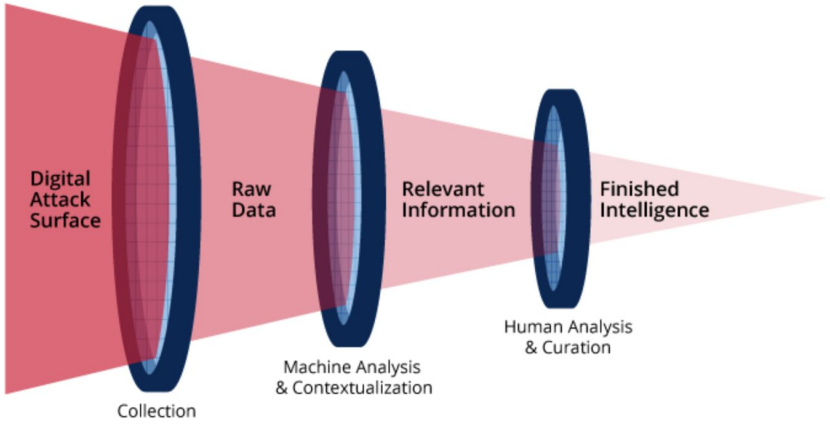
Two big benefits

1 - Lower Risks

for Known Attacks

2 - Improve efficiency

of your security team



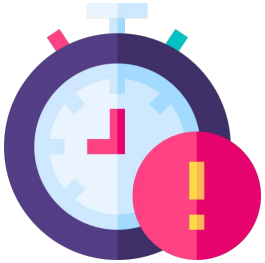
Frequent Problems

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.

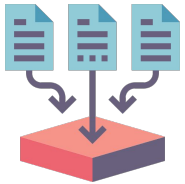
After Automation

IoC Expiration

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

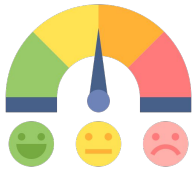
Maltiverse

Solution - Actionable Threat Intelligence



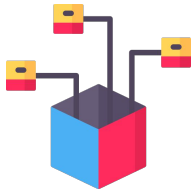
100+ Intelligence Sources

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



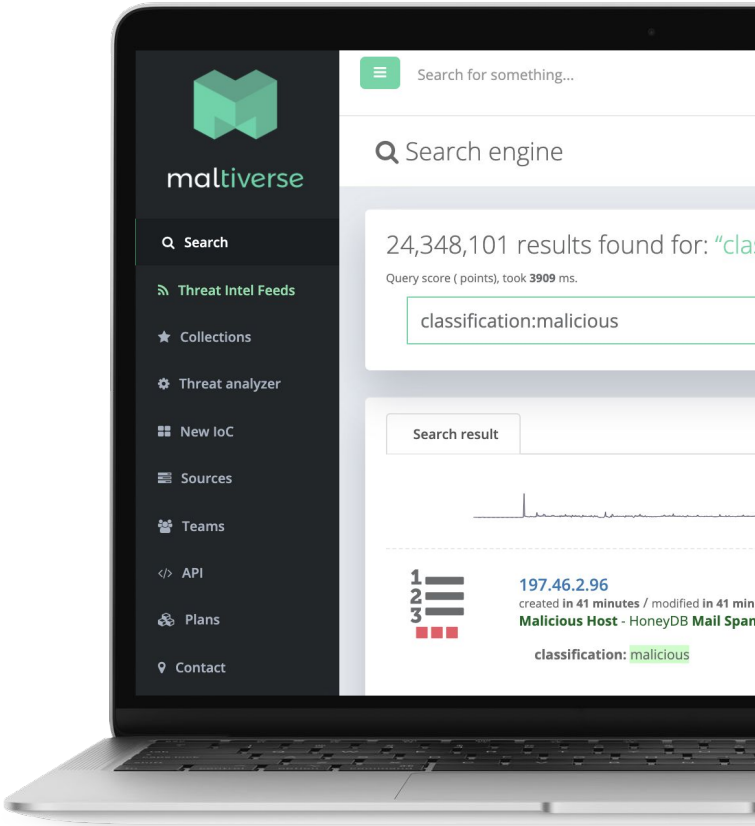
IoC Scoring Algorithm

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

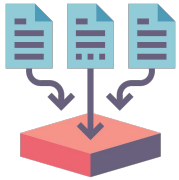
We provide integration to the most relevant commercial security devices. Integrations are completed in a matter of minutes.



Maltiverse

100+ Intelligence Sources - All in One

500 new IoC per hour!



Private

Research
Deception Honeynets
Mining Techniques

CYBER THREAT ALLIANCE
paloalto NETWORKS
RAPID7
CISCO
SOPHOS
McAfee
Symantec. A Division of Broadcom
CHECK POINT
vmware

Public

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

Community

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

Maltiverse

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***

198.136.61.196

blamed to be distributing malware by URLHaus Abuse.ch

Enrichment

AS33182
HostDime com Inc

61
Resolved Hostnames

60 whitelisted domains

1 blacklisted domain

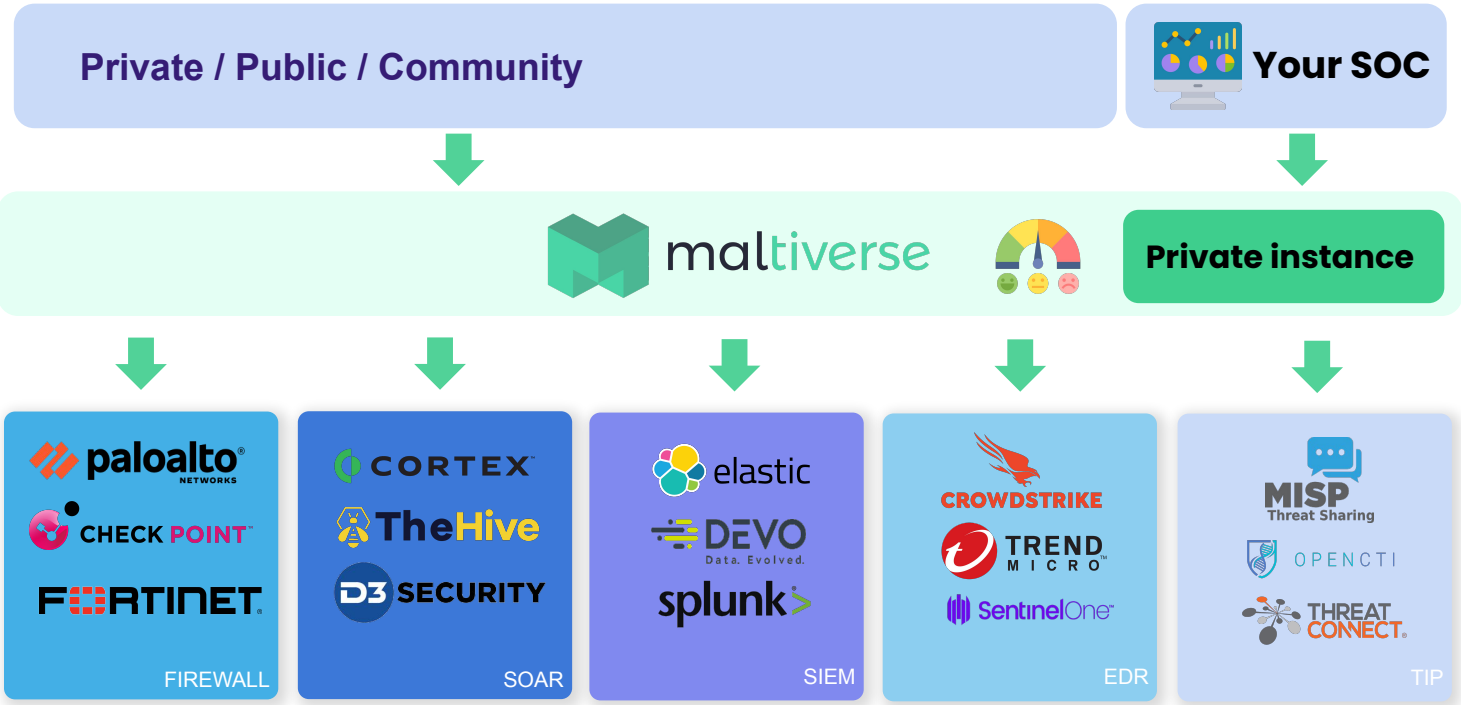
- is a known scanner?
- is storing phishing?
- is distributing malware?
- is a tor Node?
- is an IoT threat?
- is a Hosting?
- is a CnC Server?
- is providing anonymization?
- is a Known Attacker?
- Is a mining Pool?

malicious
suspicious
neutral
whitelist

Maltiverse

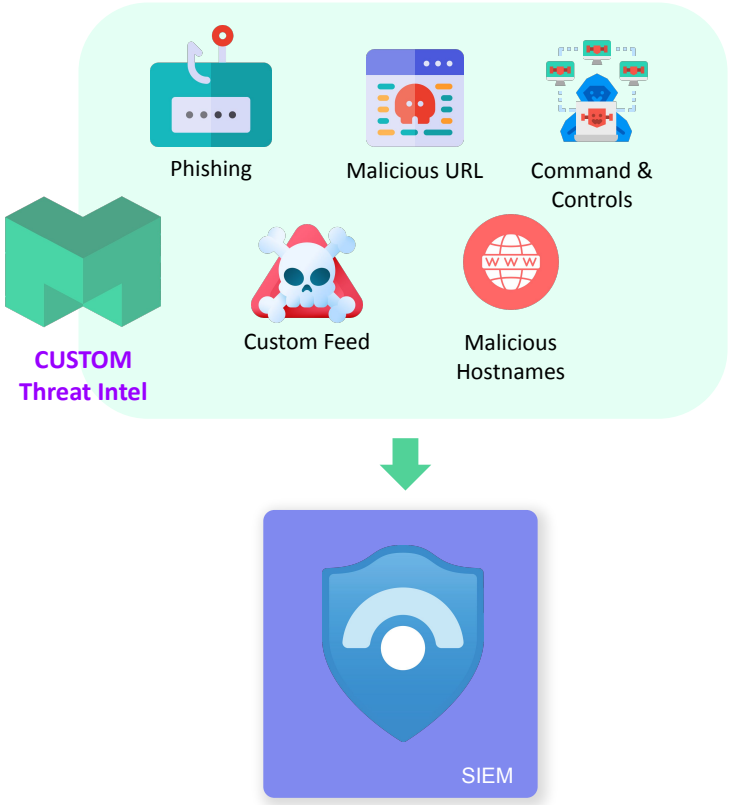
Delivery to Security Devices

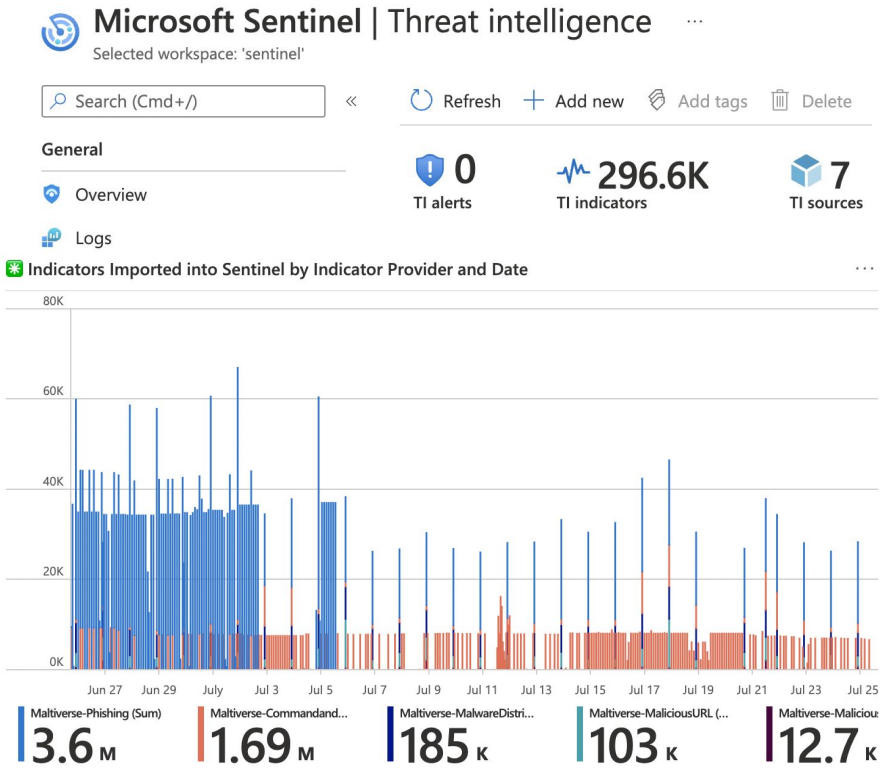
Integration with your security stack



Case Study

Detection & Prevention on a SIEM

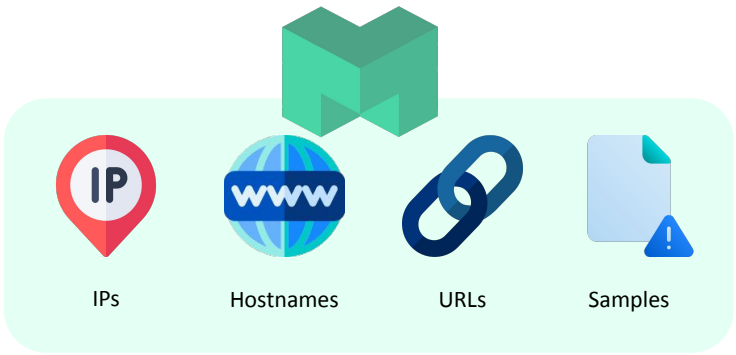


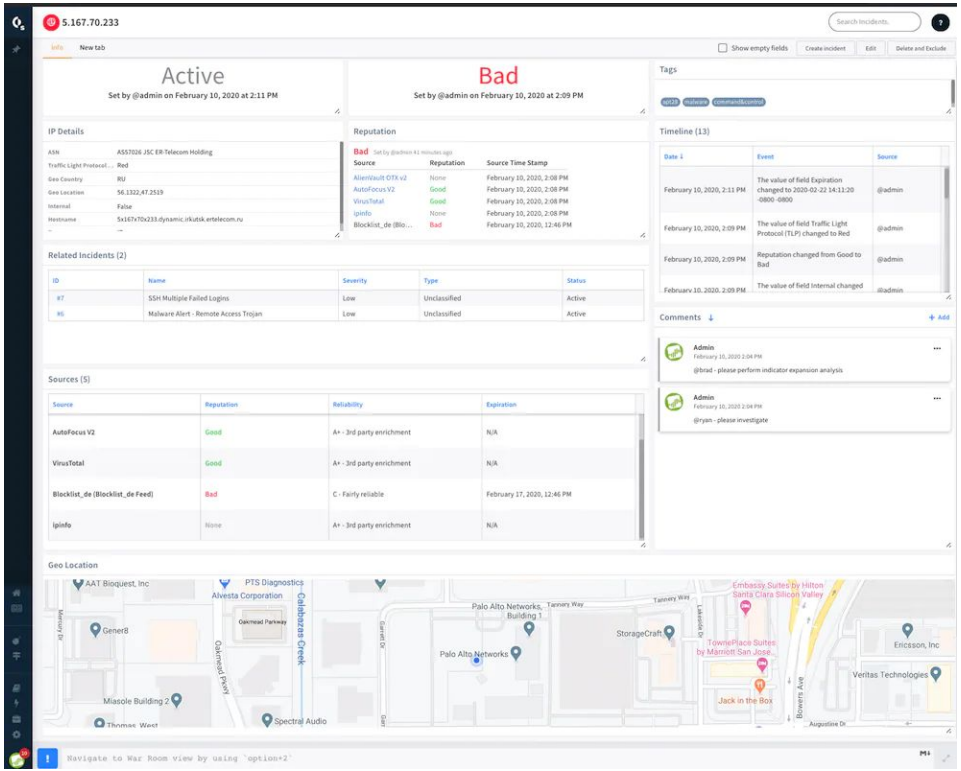


Case Study

SOAR Enrichment

Maltiverse provides classification and context to the SOAR alerts

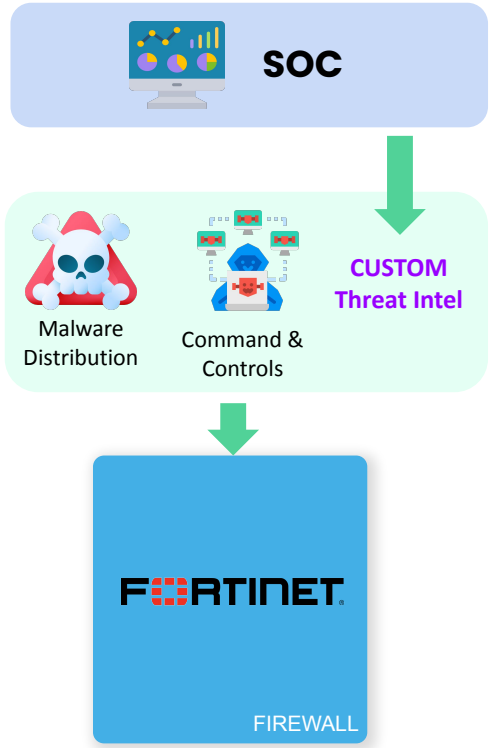


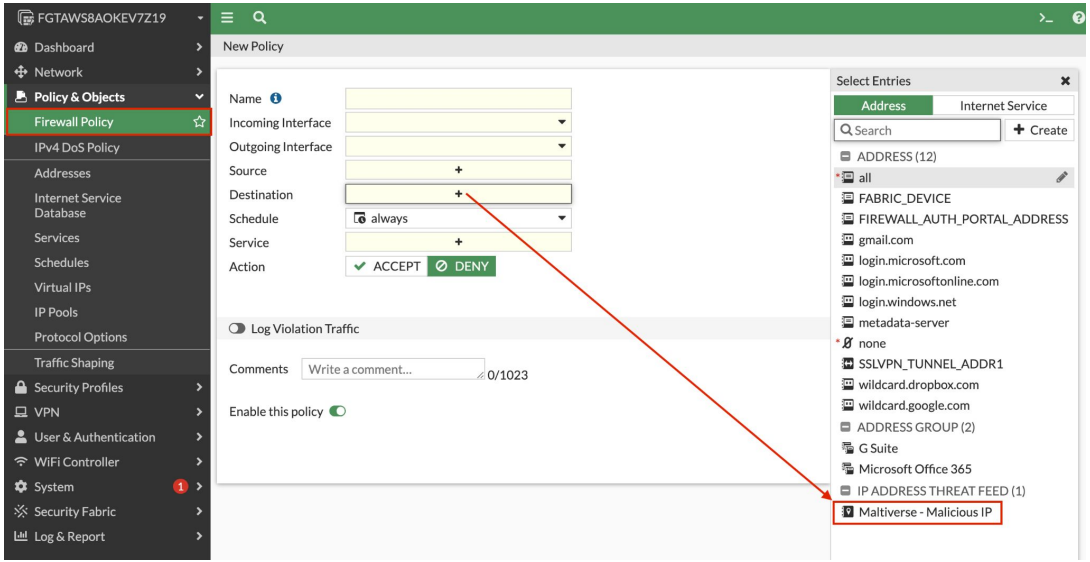


Case Study

Firewall Traffic Prevention

Change management overridden by uploading IoCs to Maltiverse





maltiverse

Case Study

Product enrichment - Firedome IoT

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

firedome

Problem

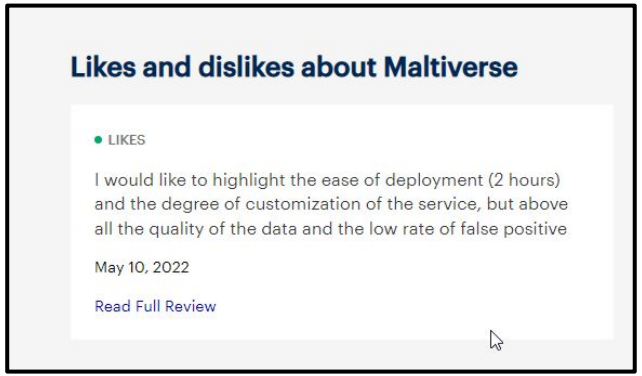
- IoT is a huge potential but also a high risk
- Our solution is security by default
- We need to ensure that our users and devices don't access malicious sites, IPs and domains
- We needed Threat Intelligence to embed to our solution
- We need to have IoT threats Indicators

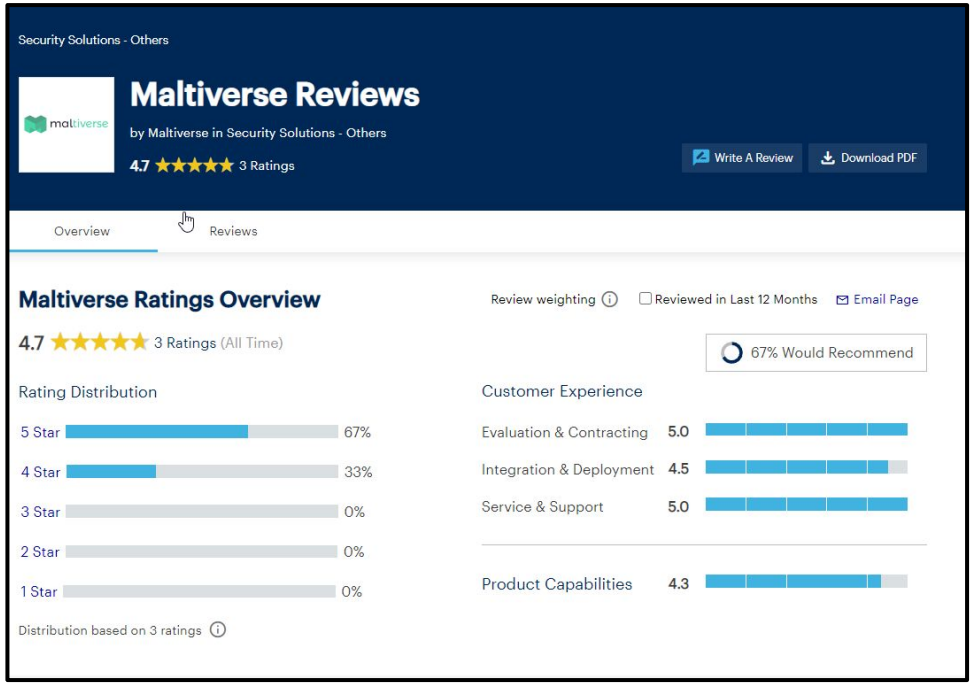
Solution

- 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





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.

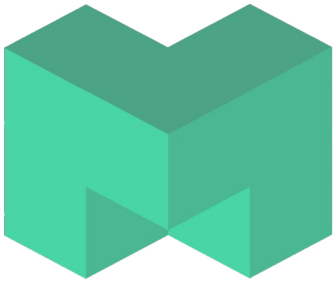
Sync multiple devices

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