

Managed Threat Intelligence [protect]

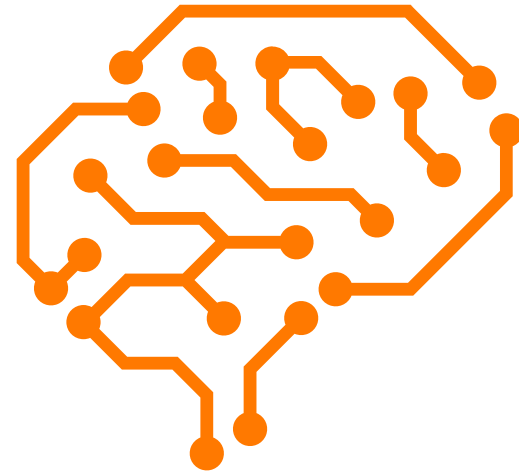
Empower your security & network teams with the right information at the right time

Being protected from emerging threats without disrupting the network

Security and network teams are sometimes facing conflicting challenges: they must be able to detect and block malicious emerging threats without disrupting the network.

Cyber Threat Intelligence (CTI) can help address this issue.

However, it can lead to an overwhelming number of false positives and even application disruption when applied as a blocking rule in a firewall.



Going beyond organizational & technology silos

Security and network teams work with different security technologies. They don't have the same process and their tools are not connected with each other

How to block threats across multiple, unconnected security systems?

Reinforce your security tools via actionable Threat Intelligence integration

Thanks to Managed Threat Intelligence [protect], you have access to:



Timely and accurate Intelligence without any false positive



Robust REST API: easy-to-integrate with your existing security tools



Insights updated in real-time to detect threats faster



Increase network security technology ROI

Adopt a proactive security posture based on Cyber Threat Intelligence

01 Actionable Threat Intelligence data embedded in all your network and endpoints security technologies.

XDR, EDR, Next-gen firewalls, IDS, proxies, Internet Access Gateway


02 Risk-based approach: instead of aiming to get Intelligence on everything with low accuracy, we are focused on major threats and take a proactive posture.

Gathering relevant information to focus on the most used tools by hackers


03 Intelligence-led approach: all our managed Services in Orange Cyberdefense feed our Threat Intelligence capability.

Leverage our unique Threat Intelligence to invest where it matters.

Leverage Threat Intelligence to prevent cyber-attacks



Block incoming propagation of malware in firewalls without blocking legitimate traffic



Block lateral movement of malware and ransomware in firewalls



Enhance EDR with Threat Intelligence data to secure devices

What you will get

We deliver qualified lists of malicious IP addresses, fully qualified domain names (FQDNs) with associated threat names and telemetry data.

IOC Type	IP address list	FQDN Domain list
Use case	Blocks CnC probing or hacking tools	Blocks hacking tools
Context provided	Name of the associated threat: Cobalt Strike, Covenant, DcRat, Deimos C2, Empire, Metasploit, PlugX, PoshC2, Pupy, Responder, Shadow, SilentTrinity, SliverC2	Name of the associated threat: Cobalt Strike, Covenant, DcRat, Deimos C2, Empire, Metasploit, PlugX, PoshC2, Pupy, Responder, Shadow, SilentTrinity, SliverC2
Statistics	First/last time seen, Count, confidence score	First/last time seen, Count, confidence score
Data Format	Csv, stix1.2, table, bind, snort, bindrpz, json, plainlist	Csv, stix1.2, table, bind, snort, bindrpz, json, plainlist
Sources	100% Internal	100% Internal

How we deliver

Simple and effective: our Cyber Threat Intelligence data is delivered as a self-service in our platform through a public and secured REST API.

Why Orange Cyberdefense ?

- Listed on the Gartner Market Guide for Cyber Threat Intelligence Services
- Insights unbiased and independent of specific vendors
- Proprietary CTI data enriched with Telecom Intelligence
- Data enhanced with key insights from our 18 CyberSOC's