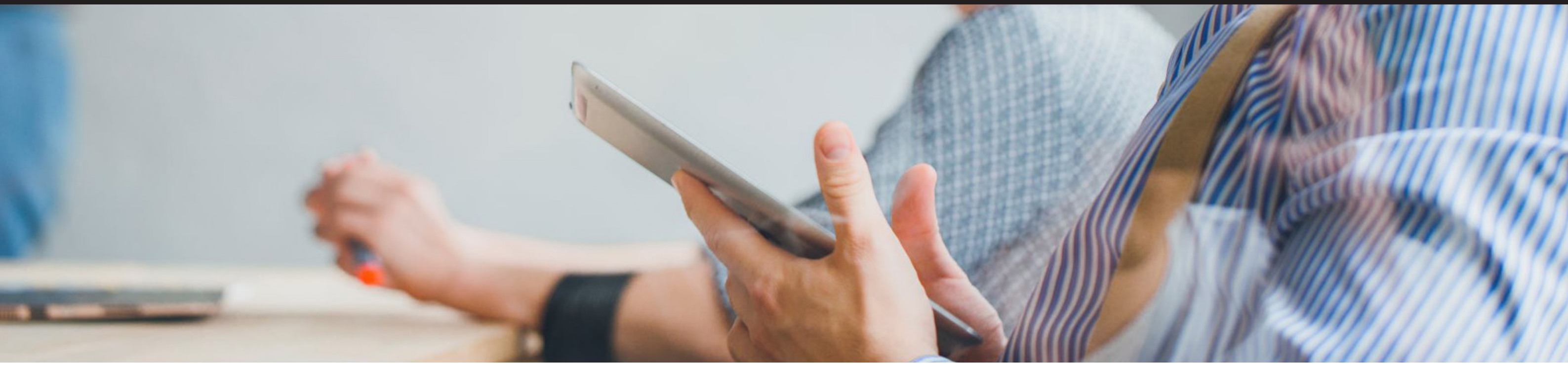
Orange
Cyberdefense



Service overview

Threat Advisory Services

Key benefits

Intelligence collection and analysis
Analysts collect, triage and review multiple sources to determine relevance to specific business envionments.

Regular security intelligence signals
Relevant and significant short–form alerts called 'Signals' are published to the portal as soon as they have been verified, analysed and appropriately categorised.

Occassional long-form analysis
Occasional long-form analysis papers are produced where the issue is considered significant enough or coverage from conventional sources (e.g. popular media) is lacking.

Occassional customer advisories
Where Signals can be directly linked to specific customers then an Advisory is generated and pushed directly to the predefined recipients.

Additional support
Additional UK Business Hours support is available via email or the portal to assist with clarification or elaboration of specific Signals.

Monthly report
Detailed monthly reports including an executive summary of developments for that month and long-term trends.

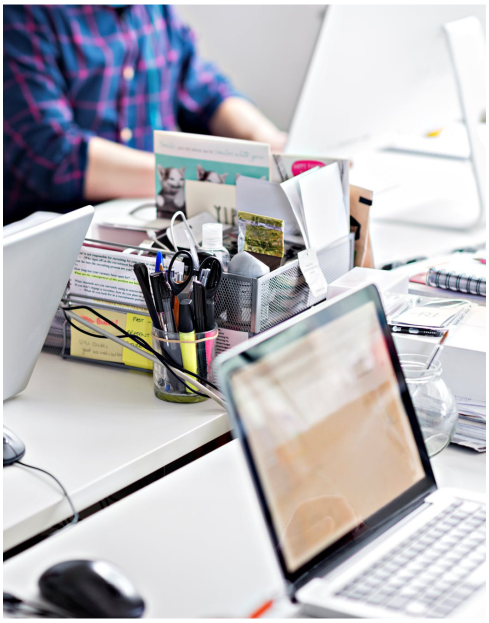
Service description

Modern Cyber Security operations involve ingesting and processing a huge amount of information from diverse sources. These various data points are used to by security teams to make minute-by-minute decisions on how to spend scarce time and resources. The wrong decision leaves the organisation exposed whilst precious time, money and energy are wasted.

With the landscape constantly changing and the adversary constantly evolving, a wrong decision, or a delayed decision can have devastating consequences. Businesses need sound intelligence with which to make sound decisions. Not too much, but not too little. Not too soon, but not too late. For Threat Intelligence to be actionable it must be accurate, relevant, clear and timely. This is the basis of every elective modern security operation.

Orange Cyberdefense's Threat Advisory Service works on behalf of the customer to collect, analyse, prioritise, contextualise and summarise global, geographical and vertical threat and vulnerability intelligence to provide actionable security intelligence relevant to the business, it's infrastructure, processes and applications.

The service takes in a continuous stream of data from a variety of open, commercial and proprietary data sources. The streams are manually triaged and distributed to provide the essential threat and vulnerability data our customers need to make good decisions, whilst filtering out the "F.U.D" and other hyperbole that can distract and disorient security operations teams.



Why Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Key service components

Threat and vulnerability information

- Based on disclosed information, Orange Cyberdefense's own research, open-source information, threat feeds, partner and proprietary threat intelligence feeds

Correlation of new intelligence

- This is against an organisation's assets via pre-defined tags where appropriate

Advisory triage and analysis to determine

- Accuracy
- Significance
- Relevance
- Urgency

Succinct advisories in the following categories

- Significant, relevant new vulnerabilities,
- New Threats
- Significant Data Breaches
- Developing situations
- Cautions
- Targetted Advisories specific to individual customers (where appropriate)
- Updates to exisiting advisories
- Detailed long-form analysis of selected significant intelligence.

Standard advisories including the following fields

- Category
- Urgency
- What you will hear
- What it means
- Tags
- Read More
- Indicators of Compromise

A monthly executive summary report

This summarises key events for the month and captures significant long-term trends, including:

- Analyst commentary on the month
- Summary of Signals for the month by Type, Urgency and Tag
- Monthly summary of Signals per day by urgency
- Summary of Analyses for the month
- Trackers for key themes, e.g. Malware / Ransomware
- Breach and incident histories
- Additional commentary piece to guide planning for the month ahead