Orange
Cyberdefense

Service overview

Managed Threat Detection
Managed Threat Hunting
Managed Advanced Threat Hunting

Key benefits

Enhanced security and visibility
Constant vigilence of security events rapidly identifies anomolous behaviour

Analyst led detection
Experienced, skilled human analysis reduces false positives and enables threat prioritisation focussing efforts on meaningful events (Threat Hunting Only

Reduced risk:24x7x365
Analysis of events with risk-based scoring using over 700 advanced indicators of attack and compromise

Minimised time-on-target
Earlier discovery reduces threat persistence and improves attack disruption

Ongoing detection enhancement
Tuning and retuning log collectors reduce false positives over time increasing ability to accurately detect anomalous events

Improved productivity
Cloud based and proactively managed market leading SIEM platform complemented with proprietary Orange CyberDefense technology reduces management overhead, complexity and costs

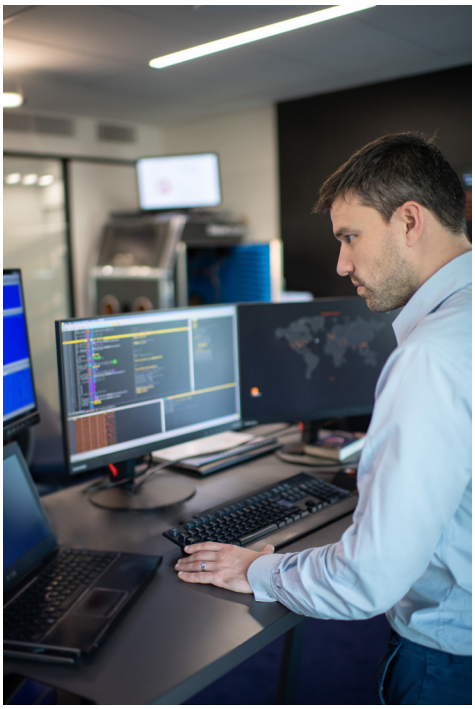
Service description

In response to the realisation that not all attacks can be prevented, organisations with mature risk assessment and mitigation policies are investing in methods of detecting and hunting the threats that have bypassed traditional defences and penetrated their networks.

Accurately detecting threats requires more than simply collecting device logs or reviewing SIEM entries. Multiple contributing factors need to be considered:

- Events and behaviours need to be correlated across an organisation's entire estate
- Vulnerability data and emerging threats need to be considered
- The broader threat environment needs to be factored in using targeted threat intelligence
- Behaviour analytics that do not rely on signatures to detect sophisticated attacks need to be applied
- Expert review determining whether suspicious events and behaviour represent an indicator of attack or compromise is required
- Threat hunting needs to be an ongoing exercise constantly assessing the behaviour of the network for anomalies

Using our proprietary Managed Threat Detection platform to apply context and substance to collected data through commercial technology, open-source and proprietary software and human resources, our service rapidly and accurately focusses in on the handful of indicators that reveal an attacker's presence.



Key benefits

Reduced costs
Fully-fledged SIEM functionality without the costs of purchasing and maintaining self-managed on premise or cloud devices

Improved compliance
Internal or regulatory compliance policies auditing requirements fulfilled thorough 365-day storage of logs

Holistic security approach
Event collection across the estate's devices ensures improved compliance reporting

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

- Log and event collection by Orange CyberDefense's Managed Threat Detection platform
- Log storage for 1 year with retrieval of historical log data as requested
- Log and event correlation and aggregation with automated advanced attack analytics
- Modification and customisation of standard log parsing rules. Custom log sources can be developed on request at additional cost
- Access to Orange CyberDefense's Threat Advisory Services and risk scored CVE vulnerability database
- Use of proprietary and commercial reputation lists to track communication with potentially malicious IP addresses
- Use of proprietary and commercial malware analysis databases to identify malware
- Use of proprietary and commercial compromise databases to identify compromised passwords, sites and devices (Threat Hunting Services only)
- Alarm triage by skilled SOC Security Analysts
- Investigation of alarms in context for potential attacks or compromises on an ongoing basis (Threat Hunting Services only)
- Retrieval and interpretation of historical log data as required (Threat Hunting Services Only)
- Ongoing access to designated security consultant (Advanced Threat Hunting Only)
- Access to the Orange CyberDefense portal with views of current alerts, alert/ incident trends and service performance
- Access to pre-defined reports
- Monthly annotated management reporting with information on alerts and incidents with commentary and trend information (Threat Hunting Services Only)
- Monthly review meeting with Security Consultant to examine and interpret alerts, attacks and compromises highlighting noteworthy trends (Advanced Threat Hunting Only)
- Compliance reporting against supported compliance frameworks
- Communication of:
  - details of compliance violations
  - triaged alert details
  - full details of potential attacks or compromises
- Alert classification by skilled SOC Security Analyst

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.