Bloor InBrief

Robin Bloor – Founder

Bloor MUTABLE AWARD 2025 GOLD

orange Cyberdefense

www.orangecyberdefense.com

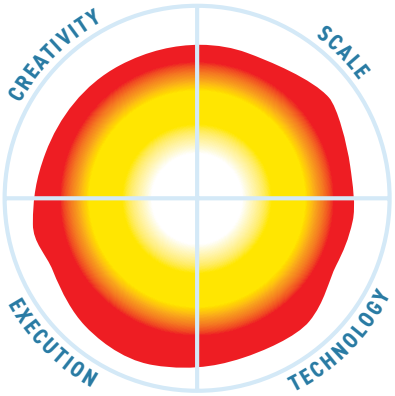
54 Place d'Ellipse, 92983, Paris, La Défense, France
Tel: +33 (0)1 46 53 53 53 Email: info@orangecyberdefense.com

Orange Cyberdefense

The company

Orange Cyberdefense, the cybersecurity division of the multinational telecommunications giant Orange Group, has carved out a significant niche in the Managed Detection and Response (MDR) market since its inception in 2016, a mere 8 years ago. Combining the resources of a telecom leader with specialized cybersecurity expertise, the company targets enterprise clients with complex security needs, offering a blend of global threat intelligence, regulatory compliance support, and integrated network-level defenses.

This **Mutable Quadrant** is derived from 13 high level metrics, the more the image covers a section the better. **Execution** metrics relate to the company, **Technology** to the product, **Creativity** to both technical and business innovation and **Scale** covers the potential business and market impact.



What is it?

As an MDR vendor, its primary differentiation is its ability to leverage the Orange Group's vast telecom infrastructure, including a network of 15 Security Operations Centers (SOCs) across Europe, Africa, Asia, and the Americas. This global footprint ensures 24/7 monitoring and rapid incident response tailored to regional threats and compliance requirements. For multinational corporations, this is a major advantage: localized SOCs enable compliance with regulations like GDPR in Europe, POPIA in South Africa, or APPI in Japan, reducing legal risks. Additionally, the company's threat intelligence is bolstered by SOC ART, its Security Operations Center Analysis and Research Team, which publishes regular reports on emerging threats, ransomware trends, and geopolitical cyber risks. This research-driven approach provides clients with actionable insights, such as proactive blocking of Indicators of Compromise (IoCs) linked to state-sponsored actors or cybercrime syndicates.

What does it do?

Orange Cyberdefense offers a comprehensive suite of services, including:

- Risk assessments and penetration testing.
- Incident response with guaranteed SLAs (e.g., 15-minute response times for critical threats).
- Vulnerability management and patch prioritization.
- Compliance advisory services for GDPR, NIS Directive, and sector-specific frameworks.

This breadth makes the company a possible "one-stop shop" for enterprises seeking to consolidate cybersecurity partnerships. For example, a financial institution could use its MDR services alongside compliance audits and employee phishing simulations, reducing the need to coordinate with multiple vendors.

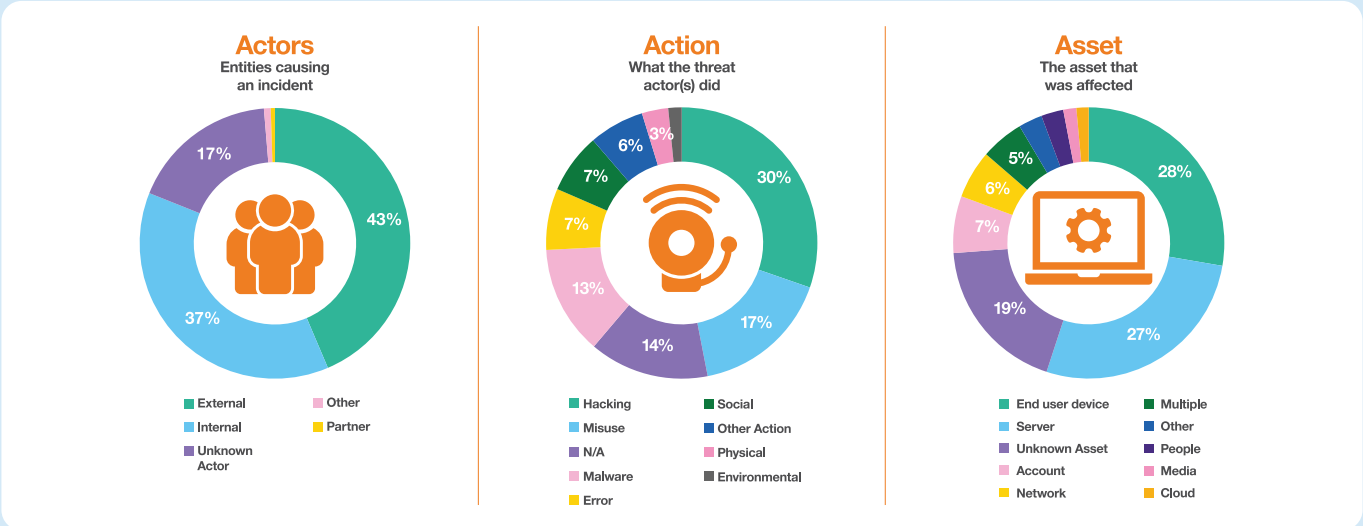


Figure 1 – Actors, Actions and Assets

> "I consider Orange Cyberdefense an extension of my team. In case of any problems or when I need a new requirement or solution, we always know who to call."
>
> Amol Gangras, Global Hybrid Datacenter Services Manager at Barry Callebaut

Orange Cyberdefense has a particular focus in some heavily regulated industries like healthcare, finance, and energy. Its team includes legal and compliance specialists who guide clients through complex frameworks, such as the EU's Digital Operational Resilience Act (DORA) for financial entities or HIPAA for healthcare data. The company also holds certifications like ISO 27001 and PCI DSS, which reassures clients undergoing audits. This focus on compliance is particularly valuable in Europe, where data privacy laws are complex, stringent and evolving rapidly.

A unique differentiator is Orange Cyberdefense's ability to integrate MDR with the Orange Group's telecom infrastructure. For clients using Orange's network services, this enables deeper visibility into traffic patterns and quicker mitigation of network-layer attacks (e.g., DDoS attempts). The company also offers Secure Access Service Edge (SASE) solutions, combining SD-WAN with cloud security, which aligns with modern hybrid-work infrastructure needs.

The company prioritizes large organizations, offering tailored SLAs that guarantee response times, escalation paths, and post-incident reviews. For example, its "Platinum" service tier includes dedicated threat hunters and a CISO advisory board. Scalability is another strength: Orange Cyberdefense supports hybrid and multi-cloud environments (AWS, Azure, Google Cloud) and can adapt to organizations with thousands of endpoints.

> "We are empowering our customers with industry-leading networking and security that is simple to deploy, easy to scale and manage, and delivers the best performance in the industry."
>
> Helmut Reisinger, CEO EMEA and LATAM, Palo Alto Networks

In common with other major MDR vendors Orange Cyberdetense has a Strategic Partnership with Microsoft. It is a Solutions Partner with specializations in Security and Azure, reflecting strong integration with Microsoft's security ecosystem. This partnership enables joint solutions and co-selling opportunities.

It includes technology integration Orange Cyberdefense integrates Microsoft's security tools (e.g., Azure Sentinel, Microsoft 365 Defender) into its MDR services. This allows clients to leverage Microsoft's SIEM/XDR platforms with Orange's 24/7 SOC monitoring and threat hunting.

In respect of Azure Security, Orange provides managed security services for Azure environments, including cloud workload protection and compliance management.

It also includes threat intelligence sharing, including occasional joint research reports and advisories. There are some co-developed solutions: Orange Cyberdefense combines Microsoft Defender data with third-party telemetry (e.g., firewalls, endpoints) to deliver unified XDR solutions.

Additionally, there is joint training programs for clients on Microsoft security products, joint focus area on cloud security and compliance.

Why should you care?

Orange Cyberdefense has a clear enterprise focus and pricing that reflects this and is less suited to smaller organizations. Its MDR services can require multi-year contracts with six-figure annual commitments, putting them out of reach for SMBs. Even mid-sized companies may find simpler, cheaper alternatives (e.g., Sophos MDR or Arctic Wolf) more practical. While the company offers "Essentials" tiers, these lack advanced features like threat hunting, limiting their value.

As part of a large telecom corporation, Orange Cyberdefense sometimes struggles with agility. Clients report that onboarding processes can be slow, and custom requests (e.g., integrating niche third-party tools) may require lengthy approvals. By contrast, smaller MDR vendors often provide more flexible, personalized service. Additionally, the sheer breadth of Orange's portfolio – spanning MDR, risk consulting, and managed SIEM – can overwhelm clients seeking a straightforward solution.

While very strong in Europe (particularly France, its home market), Orange Cyberdefense has a smaller presence in North America and Asia-Pacific. Clients in these regions occasionally note slower response times or less familiarity with local threat landscapes.

Despite supporting multi-cloud environments, Orange Cyberdefense's tools sometimes face compatibility issues with non-Orange infrastructure. Clients using competing firewalls (e.g., Fortinet or Check Point) or niche SaaS platforms report needing extra configuration work. While the company provides APIs for integration, the process is less seamless than with cloud-native MDR providers like CrowdStrike or SentinelOne.

Despite its telecom pedigree, Orange Cyberdefense lacks the cybersecurity brand recognition of some of its pure-play rivals.

The bottom line

Orange Cyberdefense is best suited for large, compliance-driven organizations – particularly those in Europe or industries like finance and healthcare – that value global threat intelligence, regulatory expertise, and integration with telecom infrastructure. Its ability to bundle MDR with risk management and incident response makes it a good strategic partner for enterprises with complex needs.

Ultimately, Orange Cyberdefense's telecom-backed MDR model offers unique advantages for the right client profile, but its premium positioning and regional biases necessitate careful evaluation against organizational priorities.