

Cyberoo: Built to Detect, Wired to Expand

ADD | Fair Value: €2.15 | Current Price: €1.28 | Upside: 68%

Initiation of Coverage

October 19th, 2026 – 7.00h

€mn	Dec '24	Mar '26	Mar '27E	Mar '28E	Mar '29E	Mar '30E
Sales Revenues	22.8	27.7	27.6	31.6	36.2	41.4
Total Revenues	25.0	31.2	31.8	36.3	41.5	47.2
EBITDA	9.7	8.6	10.8	13.1	15.8	18.9
margin	38.9%	27.4%	33.9%	36.1%	38.2%	40.1%
Net Income	4.4	2.6	2.9	3.9	5.5	7.2
Free Cash Flows	(3.8)	0.2	0.6	1.9	2.2	3.2
Net Debt (Net Cash)	(0.0)	(0.8)	(1.4)	(3.3)	(5.5)	(8.7)

Overview. Cyberoo is a cybersecurity company specialized in cyber risk management for the mid-market, an approach embodied in its ORBIS model, a 360-degree offering spanning Managed Detection & Response (MDR), external threat intelligence, and advisory services. Its proprietary platforms are powered by a 24/7 European I-SOC combining AI automation with 150+ specialists. Unlike asset-light peers reselling third-party software, Cyberoo controls the full value chain, from detection technology to SOC operations, incident response, and advisory. The Company retains technical and contractual governance while leveraging distributors' client relationships. Growth is driven by deeper market penetration, supported by NIS2, ORBIS-enabled cross-selling, and Keatrix, providing a low-friction route to international expansion.

Investment Thesis. Italian cybersecurity spending reached €2.8bn in 2025 (14% FY23-25 CAGR), while NIS2 is turning cybersecurity into a recurring mandatory expense, reinforced by a structural skills shortage making in-house security uneconomical for the mid-market. Multi-year contracts and low churn generate c.50% of divisional revenues annually from existing clients. Growth compounds through ORBIS, widening cross-sell across the full stack at no incremental acquisition cost, and Keatrix, launched in December 2025.

KT&P's Estimates. We estimate VoP of c.€31.8mn in FY26E (12-months ending March 2027), up against the FY25 15-months base of €31.2mn, and expected to grow at a 14% FY26-29E CAGR over the plan. Growth is led by the Cyber Security BU, which we model at c.€22.7mn in FY26E (rising at c.17% FY26-29E CAGR thereafter), comprising core MDR at c.€22.0mn, up 10% YoY, and Keatrix, with contract book billed rising from c.€2.0mn to c.€7.0mn by FY29E (spread over the multi-year life of the contracts). From FY26E the consolidation of Cyberoo Capital (lease-financing vehicle for multi-year contracts), adds a new stream of revenues we model at c.€2.0mn in FY26E, o/w c.80% flows to EBITDA, although entirely reabsorbed by D&A and interests, leaving null Net Income contribution. EBITDA is estimated at c.€10.8mn in FY26E, up +26% YoY, with margin on VoP expected at 33.9% (27.4% in FY25 15M). Net cash reaches c.€1.4mn in FY26E (€0.8mn FY25), strengthening thereafter as TWC normalizes to c.33% of VoP (c.50% historical average).

Valuation. We initiate coverage on Cyberoo with ADD rating. Our valuation, based on DCF (3.0% terminal growth rate; 9.0% WACC) and market multiples method (EV/EBITDA, EV/EBIT and P/E from 7 comparables, 25% size/liquidity discount), returns an average equity value of €86.8mn (€2.15ps), implying 8.0x FY26E EV/EBITDA.

Equity Research Team
connect@ktepartners.com

Michele FILIPPIG
 Head of Research
mfilippig@ktepartners.com
 +39 331 631 6783

Carlo Alberto MORLETTO
cmorletto@ktepartners.com
 +39 335 592 2660

Market Data

Mkt Cap (€ mn)	52.3
EV (€ mn)	51.4
Shares Out. (mn)	40.9
Free Float (%)	35.9%

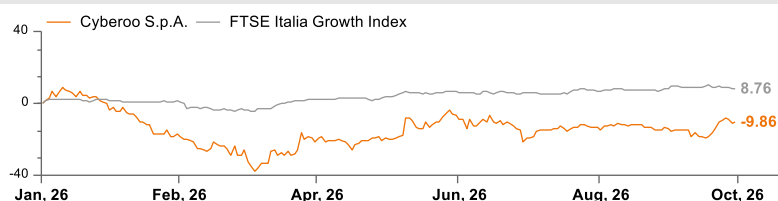
Market multiples

	2026E	2027E
EV/EBITDA		
CYB (KT&P Valuation)	8.0x	6.6x
CYB (Market Valuation)	4.7x	3.7x
Comps median	12.2x	10.7x
CYB vs CompsMedian	-61%	-65%
P/E		
CYB (KT&P Valuation)	30.3x	22.2x
CYB (Market Valuation)	18.2x	13.4x
Comps median	37.8x	31.7x
CYB vs CompsMedian	-52%	-58%

Stock Data

Avg. Daily Turnover 90d (€ k)	43.1
Price Change 1w (%)	4.1%
Price Change 1m (%)	5.8%
Price Change YTD (%)	-9.9%

Relative Performance Chart - YTD



Key Figures

Per Share Data	Dec '22	Dec '23	Dec '24	Mar '26 (15m)	Mar '27E	Mar '28E	Mar '29E	Mar '30E
Total shares outstanding (mn)	41.4	41.4	41.4	40.9	40.9	40.9	40.9	40.9
EPS	0.07	0.10	0.11	0.06	0.07	0.10	0.13	0.18
Profit and Loss (EUR million)								
Sales Revenues	15.6	20.0	22.8	27.7	27.6	31.6	36.2	41.4
Total Revenues (VoP)	17.6	22.0	25.0	31.2	31.8	36.3	41.5	47.2
growth (%)	68%	25%	14%	25%	2%	14%	14%	14%
EBITDA	6.7	9.3	9.7	8.6	10.8	13.1	15.8	18.9
EBITDA margin (%)	38.3%	42.2%	38.9%	27.4%	33.9%	36.1%	38.2%	40.1%
EBIT	4.3	6.1	6.5	4.3	4.8	6.3	8.5	11.0
EBIT margin (%)	24.7%	27.6%	25.9%	13.8%	15.2%	17.4%	20.6%	23.3%
Net Income	2.8	4.0	4.4	2.6	2.9	3.9	5.5	7.2
Net Profit margin (%)	15.9%	18.0%	17.5%	8.2%	9.0%	10.7%	13.1%	15.2%
Net Income attributable to the Group	2.8	4.0	4.4	2.6	2.9	3.9	5.5	7.2
Balance Sheet (EUR million)								
Total fixed assets	10.0	11.4	13.7	22.5	25.6	26.9	29.0	31.9
Net Working Capital (NWC)	3.5	5.8	11.9	4.7	3.8	4.6	5.8	6.9
Provisions	(0.0)	(0.1)	(0.1)	(0.1)	(0.1)	(0.2)	(0.2)	(0.2)
Total Net capital employed	13.2	16.7	24.9	26.2	28.5	30.5	33.7	37.8
Net financial position/(Cash)	(1.9)	(3.9)	(0.0)	(0.8)	(1.4)	(3.3)	(5.5)	(8.7)
Total Shareholder's Equity	15.0	20.5	24.9	27.0	29.9	33.8	39.3	46.4
Cash Flow (EUR million)								
Net operating cash flow	4.8	4.9	1.7	14.1	9.6	9.9	11.6	14.0
Change in NWC	(0.4)	(2.3)	(6.0)	7.3	0.8	(0.8)	(1.2)	(1.1)
Capital expenditure	(2.8)	(4.3)	(5.2)	(13.7)	(9.0)	(8.0)	(9.4)	(10.8)
Free cash flow	2.8	0.5	(3.8)	0.2	0.6	1.9	2.2	3.2
Enterprise Value (EUR million)								
Market Cap	86.98	124.67	87.80	58.01	52.29	52.29	52.29	52.29
Net financial position/(Cash)	(1.9)	(3.9)	(0.0)	(0.8)	(1.4)	(3.3)	(5.5)	(8.7)
Enterprise value	85.1	120.8	87.8	57.2	50.9	49.0	46.8	43.6
Ratios								
ROCE	33.0%	36.5%	26.0%	16.5%	17.0%	20.8%	25.3%	29.1%
ROE	18.5%	19.3%	17.6%	9.5%	9.6%	11.6%	13.9%	15.5%
Interest cover on EBIT	5.6%	6.5%	3.6%	11.5%	17.7%	14.3%	11.2%	9.1%
NFP/EBITDA	-0.3x	-0.4x	0.0x	-0.1x	-0.1x	-0.3x	-0.3x	-0.5x
Gearing - Debt/equity	-12.6%	-18.8%	-0.1%	-3.1%	-4.8%	-9.8%	-14.0%	-18.7%
TWC/Total Revenues	35.8%	46.6%	68.0%	36.0%	33.6%	33.9%	34.4%	33.5%
Free cash flow yield	5.0%	0.9%	-6.6%	0.4%	1.0%	3.3%	3.8%	5.6%
Multiples (x)								
EV/Sales	5.5x	6.0x	3.8x	2.1x	1.8x	1.6x	1.3x	1.1x
EV/EBITDA	12.6x	13.0x	9.0x	6.7x	4.7x	3.7x	3.0x	2.3x
P/E	31.2x	31.5x	20.1x	22.6x	18.2x	13.4x	9.6x	7.3x

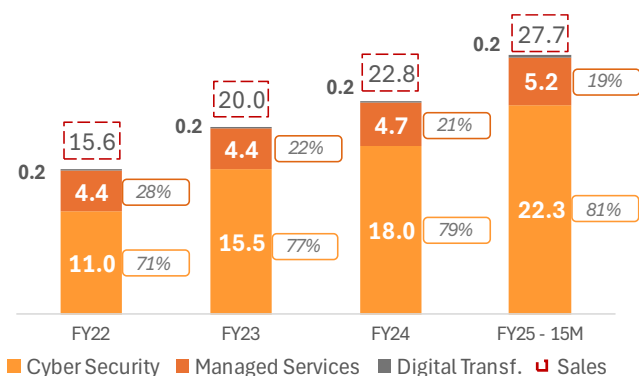
Source: Company Data (2022-2025 15M), KT&Partners' Forecasts (2026-2029E)

Contents

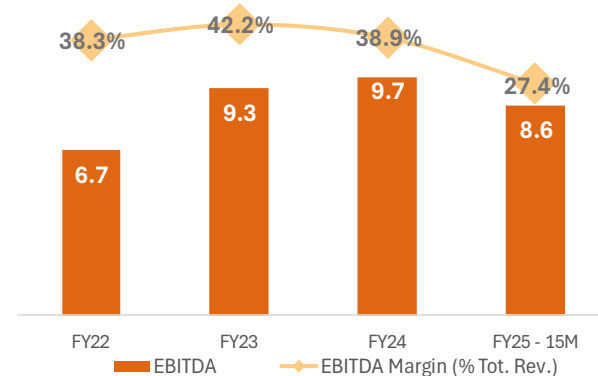
Key Figures	2
Key Charts	4
Investment Case	5
Statement of Risk	6
Company Overview	7
Company's History	8
Ownership	9
Group Structure	10
Management Team	11
Board of Directors	12
Business Model – ORBIS: Integrated Risk Model	13
The I-SOC: Cyberoo's Operational Core	14
Cyber Security Suite – Internal and External MDR Coverage	16
Cyber Security Advisory and Incident Response – Cyberoo Docetz	19
Titaan Neemesi – IT Governance & Compliance Suite	20
Keatrix – Cybersecurity Awareness	21
ORBIS – From Product Portfolio to Integrated Risk Governance	22
Go-to-Market	23
Stakeholders	25
Market Overview	28
Global Cybersecurity Market	28
NIS2 – A Catalyst	30
European Cybersecurity Market	31
The Italian Cybersecurity Industry	32
Competitive Arena	34
Historical Financials	35
Revenues Breakdown Analysis	35
Profitability Analysis	36
Capital Structure & Cash Flow Analysis	37
Deconstructing Forecasts	39
EBITDA: Margin Recovery First, Expansion Later	41
Structural De-Risking of Working Capital	42
Valuation	44
Market Multiples Valuation	47
DCF Valuation	48
DISCLAIMER	50

Key Charts

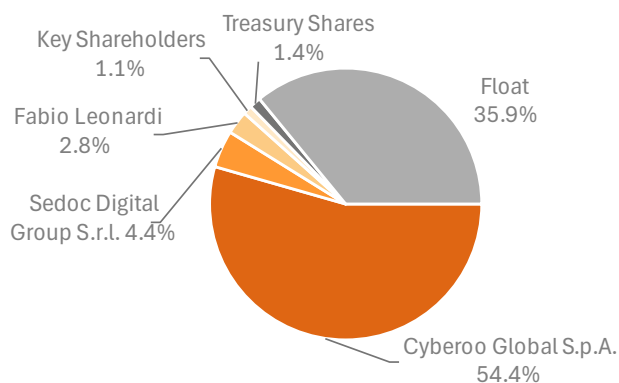
Revenues BD per Business Unit (€mn) - FY22-25 (15M)



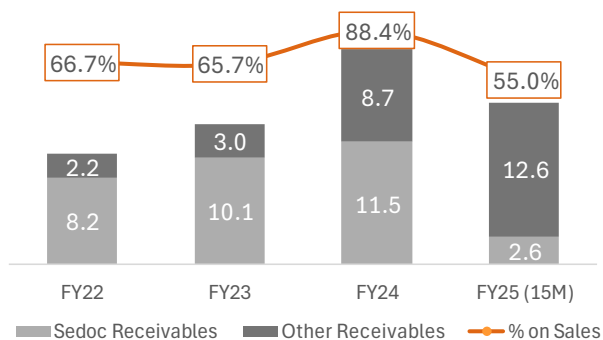
EBITDA and EBITDA margin (on VoP, %) – FY22-25 (15M)



Cyberoo's Shareholding Structure (% as of Oct '26)



Trade Receivables BD (% on Sales) - FY22-25 (15M)



Cyberoo at a Glance



Source: KT&Partners' Elaboration on Company Data (FY22-25)

Investment Case

Monetizing Cyber Inequity: A Regulatory Tailwind. Cyberoo is strategically positioned to capture a demand shift that is turning cybersecurity from a discretionary IT expense into a recurring, mandatory commitment. Italian cybersecurity spending reached €2.8bn in 2025 (14% FY23-25 CAGR), with Managed Security Services and Cloud the largest and fastest-growing segment at €969mn, and expected to grow at a +13% CAGR through 2028E¹. Additionally, NIS2 is progressively entering its enforcement phase, with operational, governance and incident-notification obligations becoming increasingly binding through 2026, extending mandatory detection, response, and governance requirements across a widening perimeter of Italian companies, while a structural skills shortage (4.8mn unfilled cybersecurity roles globally in late 2025, +19% YoY²) makes internal security operations economically unsustainable for SMEs. Cyberoo's outsourced MDR model converts this systemic weakness into a recurring, structurally under-served revenue stream.

High Topline Visibility and Low Churn. The revenue base is structurally sticky. Contracts typically span 1, 3, or 5 years with tacit renewal clauses, and roughly 50% of divisional revenues in any given year come from the existing client base. Because MDR embeds directly into a client's security operations, switching costs are high and retention strong, while the indirect channel leverages the pre-existing trust between partners and their end customers.

Service proximity at vendor margins. Most cybersecurity operators choose between two economics: sell a standardised platform and margin well, or deliver a hands-on service and grow with headcount. Cyberoo does both. It develops its detection platforms in-house and keeps the end client relationship, handling incident response itself rather than passing it on. ORBIS extends that proprietary base across four risk domains, so an existing client can be sold into the others without a matching increase in staff through up-/cross-selling. Over FY23-25 this produced an 18% revenue CAGR on a 25% average EBIT margin.

Land-and-Expand Through Keatrix and ORBIS. Cross-selling and up-selling sit at the core of the growth model. The ORBIS framework unifies the portfolio under a single risk-governance model, so that whichever product brings the client in, the relationship can then be widened across the full stack. Each engagement starts narrow and expands, lifting revenue per client at no incremental acquisition cost. Keatrix, launched in December 2025, extends this engine into a new addressable market: as a SaaS shelf product requiring no local delivery structure, it reaches large-scale distribution and offers a low-friction route to export the Cyberoo model abroad, opening accounts that ORBIS can subsequently expand across the international base. We estimate Keatrix contracts billed growing from c.€2.0mn in FY26E to c.€7.0mn in FY29E, a c.+57% CAGR.

¹ Osservatorio Cybersecurity & Data Protection, Politecnico di Milano, February 2026; Il Digitale in Italia 2025, Anitec-Assinform

² ISC2 Cybersecurity Workforce Study 2024, ISC2, October 2024

Statement of Risk

Working Capital and Payment Structure. End clients increasingly settle multi-year contracts in instalments while Cyberoo invoices most of the value at the kick-off, a mismatch that pushed trade receivables over €20mn in FY24. The Group has addressed this at source: the Sedoc exposure fell to €2.6mn from €11.5mn the year before, receivables to €15.2mn and net working capital to €4.7mn from €11.9mn. This while the new Cyberoo Capital moves credit management upstream and the new March year end sits after the Q4 billing peak and the Q1 collection cycle. The residual risk is one of transformation rather than elimination. Cyberoo Capital absorbs the instalment preference onto the Group's own balance sheet against a €15mn facility, so the exposure migrates from collection timing toward end client credit risk spread over one to five years and toward gross debt, which rose to €16.4mn at Mar-26 from €6.1mn in Dec-24. A deterioration in end-client credit quality could affect the collectability of lease-related receivables or require additional provisions, partially offsetting the working-capital benefits of the model.

Accounting Profile, D&A and Cash Conversion. Cyberoo's reported EBITDA reflects the accounting profile of a proprietary technology vendor, where part of the internal development effort is capitalised in line with investment in proprietary platforms. Capitalised internal work stepped up to c.€3.0mn in 15M FY25, and expensing it in full would have reduced EBITDA by the same amount, to c.€5.5mn, a gap that has widened since FY24. Cyberoo Capital adds a further layer: its operating-lease revenues largely reach EBITDA, while the cost of the acquired contract book is capitalised and surfaces below the operating line through D&A and financial expenses. Both mechanisms widen the distance between reported EBITDA and cash generation over the plan. For this reason, we complement EBITDA with EBIT and free cash flow analysis, which provide a more complete view of profitability and cash conversion.

Competitive Intensity and Technology Obsolescence. Cyberoo operates in a market where MDR has evolved from a differentiated service into a crowded category spanning managed EDR, SOC-as-a-Service, and managed XDR, contested at one end by well-capitalized global platform vendors (CrowdStrike, SentinelOne, WithSecure) and at the other by service-led operators embedded in larger groups. Sustaining differentiation requires continuous R&D on its proprietary platforms (c.€3.7mn capex over the past three years), with the pervasive and increasingly malicious use of AI raising the pace at which detection technology must evolve. Failure to keep pace could erode the technological moat central to the Company.

Democratization of Security. A recurring concern is that AI lowers the technical barrier to cybersecurity to the point where Cyberoo's clients bring the function in-house, compressing demand for outsourced MDR. We see this threat as limited, because what the Group sells is not technological capability, which AI does make more accessible, but governance: the ability to act on a confirmed threat and remediate it efficiently, and to run structured, continuous monitoring. These are competencies that AI accelerates but does not replace, and in the mid-to-upper market Cyberoo serves, clients lack the internal structure to operate security continuously. AI is therefore better read as a tool that makes Cyberoo's own delivery more efficient than as a force that disintermediates it.

Company Overview

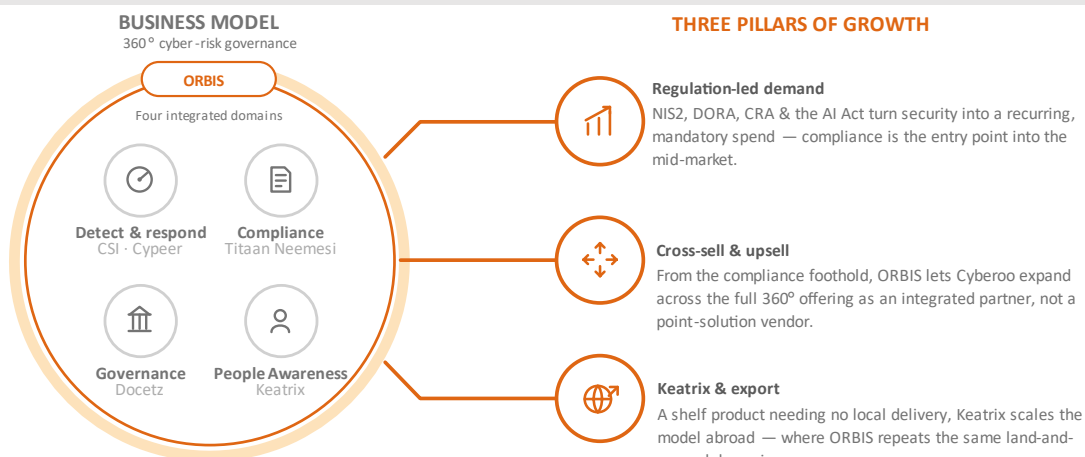
Cyberoo S.p.A. is a cybersecurity company specializing in cyber risk management for the mid-market, delivering fully integrated protection through its ORBIS model, a 360-degree offering that spans Managed Detection & Response (MDR), external threat intelligence, and advisory services. Its offering is built around a set of proprietary platforms (Cypeer, CSI, Titaan, Docetz, and Keatrix), all developed in-house and powered by a 24/7 European Intelligence Security Operations Center (I-SOC) that combines AI-driven automation with 150+ specialists.

Founded in 2008, Cyberoo progressively repositioned toward specialized cybersecurity, a shift that accelerated from 2016 with sustained investments. This effort culminated in 2019 with the launch of its first proprietary solutions and the listing on Euronext Growth Milan, making Cyberoo Italy's first publicly traded cybersecurity company (raising €7.2mn at a €20mn pre-money valuation). Fabio Leonardi, who acquired the Company through Sedoc Digital Group and reached full ownership in 2010, still leads it as CEO.

Unlike asset-light peers that resell third-party software, Cyberoo controls its full value chain, from proprietary detection technology to SOC operations, incident response, and advisory services. Delivery runs through a geographically diversified, multi-tier I-SOC architecture spanning Italy, Ukraine, Poland, and Albania, ensuring 24/7/365 monitoring alongside a data sovereignty model compliant with GDPR and NIS2. On the commercial side, Cyberoo operates through a Tier II indirect distribution model: it retains technical and contractual governance, while leveraging distributors and local partners' (system integrators, telcos, and consulting firms) already established relationship with the customer base. As of September 2026, the network counts five distributors across Italy, Poland, and Spain.

Cyberoo's growth strategy rests on three pillars. First, deeper penetration of the Italian mid-market, where NIS2 and the broader regulatory framework (DORA, the Cyber Resilience Act, the AI Act) are turning cybersecurity from a discretionary expense into a recurring, mandatory commitment, with compliance acting as the entry point into the client relationship. Second, the ORBIS ecosystem, which unifies the portfolio under a single risk-governance model: starting from compliance, Cyberoo can then cross-sell and upsell the full 360-degree cybersecurity offering, positioning itself as an integrated security partner rather than a point-solution vendor, a dynamic we see lifting Cyber Security & Device Security BU to grow from €22.7mn in FY26E to €36.0mn in FY29E, a +17% CAGR. Third, Keatrix, the innovative cybersecurity-awareness platform: as a shelf product requiring no local delivery structure, it reaches large-scale distribution and offers a low-friction route to export the Cyberoo model abroad, where ORBIS can in turn drive the same cross-selling and upselling dynamic across the international market. We expect Keatrix billings expanding from c.€2.0mn in FY26E to c.€7.0mn in FY29E (>50% CAGR), supporting an overall EBITDA margin expansion to c.40% by FY29E (from c.27% in FY25).

Cyberoo at a Glance: An Integrated Approach to Cyber Risk



Source: KT&Partners' Elaboration on Company Data

Company's History

Founded in 2008, Cyberoo initially operated as an IT hardware distributor. That same year, Sedoc Digital Group, an Italian IT player founded in 1973 and led by Fabio Leonardi (Cyberoo's Founder and CEO) since 1991, acquired a 51% stake, reaching full ownership by 2010.

In 2009, Cyberoo pivoted toward IT services, partnering with HP to provide Device and Print Management monitoring. By 2015, the Company had evolved into a Managed Service Provider (MSP), overseeing clients' entire IT infrastructures. To support this expansion, in 2016 Cyberoo opened its first international hub in Ukraine, leveraging the country's deep pool of IT talent, marking the start of cybersecurity R&D initiatives.

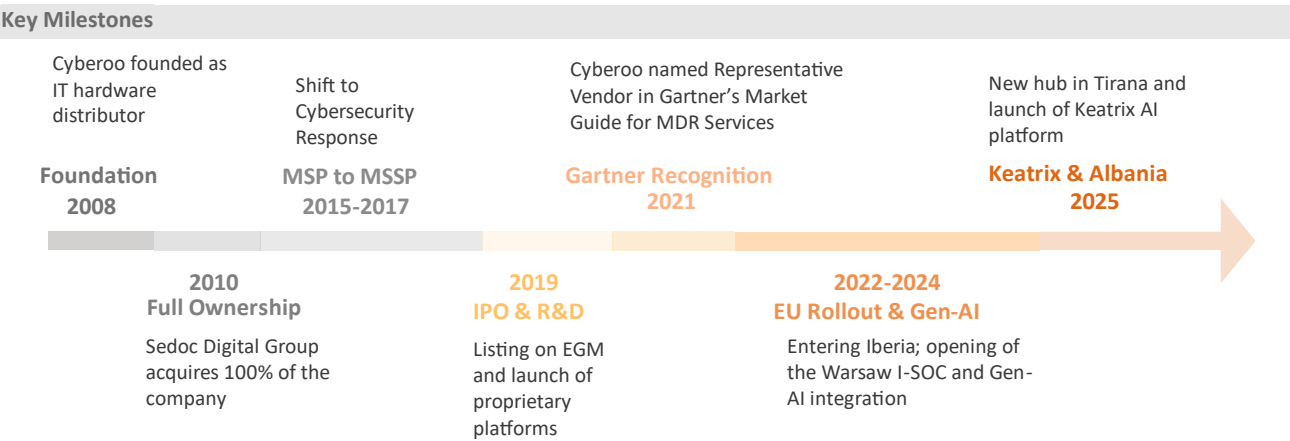
Starting in 2016, with increasingly complex and sophisticated cyberattacks on the rise, the Company invested more and more in research and development activities, repositioning itself as a Managed Security Service Provider (MSSP) focused on specialized cybersecurity monitoring, detection, and incident response.

After years of R&D investments, in 2019 the Company launched its first proprietary solutions: Cypeer (MDR platform for detection, analysis, and remediation), Cyber Security Intelligence (deep and dark web threat monitoring), and Titaan (compliance management). That same year, Cyberoo listed on Euronext Growth Milan, becoming Italy's first publicly traded cybersecurity company, raising €7.2mn at a €20.0mn pre-money valuation.

In 2021, Cyberoo expanded its service portfolio with an Incident Response Team (IRT) for active IT security incidents and vCISO services (providing virtual Chief Information Security Officer advisory). Thanks to its integrated Cybersecurity Suite, that year Cyberoo was named Representative Vendor in Gartner's Market Guide for MDR Services, becoming the first and only Italian company to receive this recognition, which it has retained every year since, and was recognized by Gartner among the top 50 global MDR players.

In 2023, Cyberoo launched its international expansion with the opening of a new office in Warsaw (Poland), establishing both an I-SOC team and a commercial team to enable 24/7 MDR operations and support its European rollout strategy. In 2H24, Cyberoo expanded its distribution network into Spain and Portugal, further building out its European footprint alongside Poland.

Between 2023 and 2025, Cyberoo progressively enhanced its technological platform and solution portfolio. In 2023, the launch of Cyberoo Docetz strengthened the Group's consulting and advisory capabilities. In 2024, Cyberoo introduced a new generation of integrated solutions, embedding generative AI across operations. In 2025, the Company enhanced its operational infrastructure and software development capabilities by expanding in Tirana, Albania. By year-end, the ecosystem expanded with Keatrix, an adaptive AI-based cybersecurity training platform, extending the value proposition from threat protection to prevention and awareness.

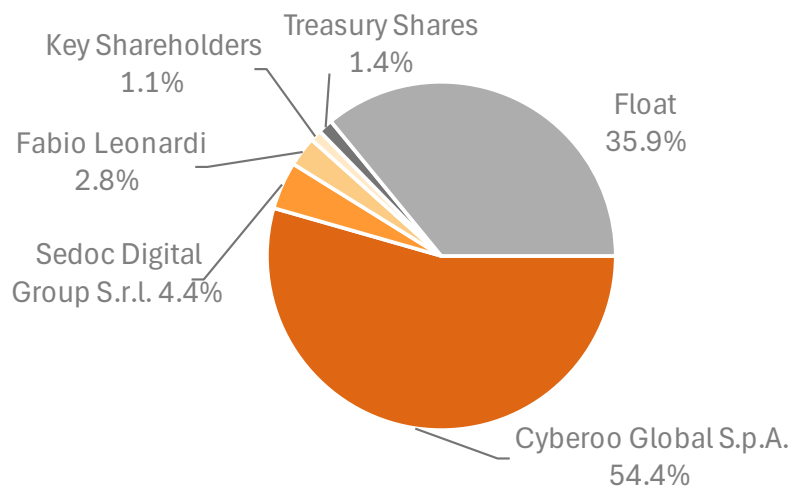


Source: KT&Partners' Elaboration on Company Data

Ownership

Cyberoo S.p.A. is controlled by Cyberoo Global, which holds 54.4% of the share capital. The remaining ownership is split between 35.9% free float, 3.9% held by Fabio Leonardi (CEO, 2.78%), Davide Cignatta (Director, 0.61%), Massimo Bonifati (Non-Executive President, 0.35%), and Veronica Leonardi (CMO and IR, 0.12%). A residual 4.42% stake is held by Sedoc Digital Group, which wholly owns Cyberoo Global, while 1.4% is held as treasury shares. Sedoc is in turn controlled by Fabio Leonardi (65.0%), Davide Cignatta (20.0%), and Massimo Bonifati (15.0%).

Cyberoo’s Shareholding Structure (% , as of October 2026)



Source: KT&Partners’ Elaboration on Company Presentation

Group Structure

Cyberoo S.p.A. holds 100% of three consolidated entities (Cyberoo 51, Cyberoo Docetz, Cyberoo Capital) and four non-consolidated foreign subsidiaries (Cyberoo PL, Cyberoo UA, Cyberoo Keatrix UA, Cyberoo AL), excluded from the consolidation perimeter as they are considered exclusively cost centers.

Cyberoo 51 S.r.l. (established in 2014) operates in Digital Transformation, Data Protection, and R&D in artificial intelligence. In turn, it holds 100% of Cyberoo UA LLC (Ukraine, Ternopil-based), which provides SOC operations and management services.

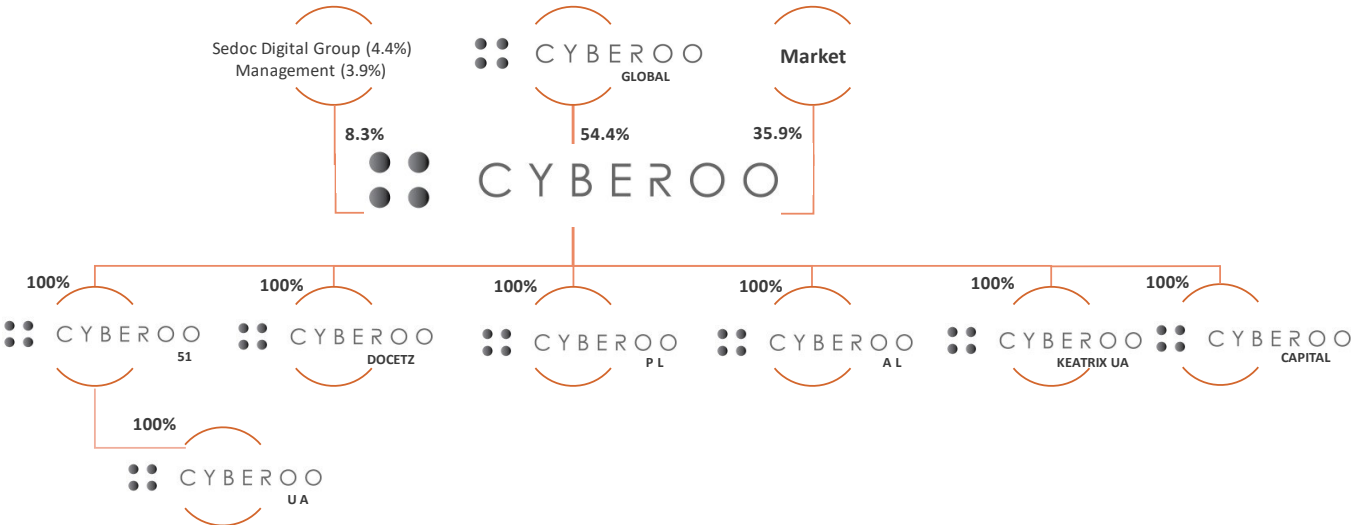
Cyberoo Docetz S.r.l. (acquired in two tranches: 51% in 2021 for €150k, remaining 49% in 2023 rebranded from Cyber Division S.r.l.) operates as the Group's consulting division, providing advisory services (vCISO, risk assessment, compliance, penetration testing) and incident response capabilities, complementary to its MDR unit.

Cyberoo PL Sp z.o.o (Warsaw-based, established in 2022) operates in the Cybersecurity Services business line as Polish hub for commercial activities and I-SOC Tier-2 operations. Manages 15+ cybersecurity specialists providing technical support to Tier-1 analysts, alongside a dedicated commercial team.

Cyberoo Keatrix UA I.l.c. (Kyiv-based) and **Cyberoo AL sh.p.k.** (Tirana-based), both transferred in 2025 from Cyberoo Global, operate in the Cybersecurity Suite BU. Cyberoo Keatrix UA focuses on the development of the Keatrix platform. Cyberoo AL specializes in VNOC (Virtual Network Operations Center for remote monitoring and management) services and houses the Cypeer Keera operational team.

Cyberoo Capital S.r.l. (established in 2025) is a wholly-owned subsidiary that acts as a commercial and financial facilitator for multi-year cybersecurity contracts, supporting resellers and partners when sales negotiations face financial constraints or upfront investment barriers. The vehicle purchases eligible multi-year rights, licenses or bundles from third-party suppliers, resellers or market counterparties, making them available to final customers through operating-lease structures. In doing so, it addresses the structural WC pressure created by the growing customer preference for deferred payments, including the elevated trade receivables toward Sedoc, Cyberoo's main shareholder, moving that exposure off trade receivables.

Group Structure (as of September 2026)



Source: KT&Partners' Elaboration on Company Presentation

Management Team



Fabio Leonardi – CEO – Chief Executive Officer of Cyberoo since its foundation, he is also Chairman of Sedoc Digital Group S.r.l., a role he has held since 1991. His entrepreneurial career began within Sedoc, where he joined the Board of Directors and progressively contributed to the Group's strategic development, taking on over time the roles of Commercial Director, General Manager and Chief Executive Officer. Previously, he served as Head of the Reggio Emilia branch of Decision System International, a multinational company specializing in IT systems and corporate digital solutions within the Olivetti Group.



Davide Cignatta – CCO – is also a partner and director of Sedoc Digital Group S.r.l., as well as Brand Ambassador of the relevant group. He began his entrepreneurial activity in 2001, when he joined the capital of Oversystem Computer Service, where he held the role of Director and Sales Manager. In 2005, following the acquisition of Oversystem by Sedoc Digital Group S.r.l. and the subsequent integration with Gamma Servizi, he gradually took on increasingly important roles until becoming Commercial Director of Sedoc Digital Group S.r.l. Continuing his professional development in the IT sector, he built his background in the services area, where he gained specific expertise in designing and implementing network infrastructures.



Veronica Leonardi – CMO and IR – Chief Marketing Officer (CMO) and Investor Relations Manager of Cyberoo since December 2018, Veronica Leonardi leads the company's entire communication and marketing area, also serving as spokesperson. She has coordinated Cyberoo's rebranding project and is responsible for the company's positioning strategy and international expansion. Previously, she worked as a Web Marketing Consultant at LYB and, in 2016, in Marketing at Henkel, Beauty Care division, where in 2018 she followed the launch plans for the division's main new products. She holds a degree in Management Engineering from Politecnico di Milano and completed her education with a master's in Marketing and Communication at SDA Bocconi.

Samuele Puggioninu – CFO – Appointed in 2019, he built his career as an administrative manager before specializing as a Project Manager at AFC. He subsequently founded and led Four Consulting S.r.l., providing consulting services to national and international clients on business and management consulting projects, drawing on his background in economics (University of Verona) and his managerial training at SDA Bocconi.



Matteo Ghiotto – CTO and R&D Director – was appointed in October 2024 after previously serving as AI Developer Director at Cyberoo since 2019. As CTO, he oversees the transformation of the SOC, Incident Response, and R&D teams, embedding AI at the core of the Company's innovation strategy. He brings 10+ years of experience in AI and machine learning, previously at multinational companies such as Honda.

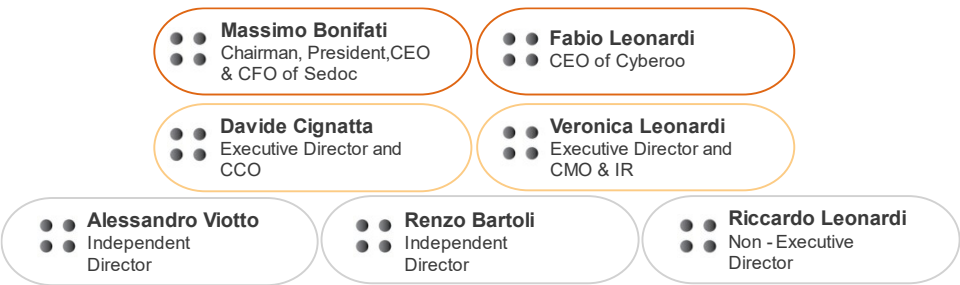
Board of Directors

As of 2025, Cyberoo’s Board of Directors is composed of seven members. The Board is chaired by Massimo Bonifati (President; CEO & CFO of Sedoc Digital Group) and includes Fabio Leonardi (CEO), Davide Cignatta (Executive Director and Chief Commercial Officer), and Veronica Leonardi (Executive Director and Chief Marketing Officer & IR). Additional members are Riccardo Leonardi (Non-Executive Director), alongside Independent Directors Renzo Bartoli and Alessandro Viotto.



Massimo Bonifati – President – with over 10 years of experience as a Project Manager in IT systems within Administration, Finance & Control, he joined Sedoc Digital Group in 2005, where he currently serves as CEO and CFO. He has played a key role in coordinating the Group’s extraordinary corporate operations, supporting major expansion transactions.

Cyberoo’s Board of Directors



Source: KT&Partners’ Elaboration on Company Presentation

Business Model – ORBIS: Integrated Risk Model

Cyberoo is a cybersecurity technology vendor specializing in Managed Detection & Response (MDR), external threat intelligence, and advisory services, delivering fully integrated protection targeted to SMEs. With a portfolio built around proprietary platforms (Cypeer, CSI, Titaan, Docetz, and Keatrix), the Company is powered by its 24/7 European Intelligence Security Operations Center (I-SOC). In the fifteen-month FY25 Cyberoo posted €27.7mn in sales revenues, of which c.81% from Cyber Security & Device Security (MDR contracts accounted for c.65% of FY24 sales), serving a base of +700 clients primarily located in Italy (c.85% of turnover) but diversified across Poland, Spain, and Portugal.

The Company controls its full value chain, from proprietary AI-driven detection technology to SOC operations, incident response, advisory services, and commercial support. Service delivery is executed through a multi-tier architecture combining automated data monitoring with 150+ specialists across Ukraine, Poland, Albania and Italy, ensuring continuous 24/7/365 monitoring. This architecture supports the Company’s core MDR suite: Cypeer for internal threat detection and CSI for external threat intelligence across the deep and dark web, which together generated €14.7mn in FY24 (c.65% of FY24 Sales). Cypeer is monetized via fixed-fee endpoint-based licensing across 1-, 3-, or 5-year contracts, with deal sizes ranging from c.€22k to €700k for deployments up to 5,000 endpoints, while CSI adds external intelligence layers.

Cyberoo complements its MDR offering with Docetz, the advisory and compliance unit (€3.2mn in FY24; c.14% of FY24 Sales) which serves as a key upselling channel. The portfolio also includes Titaan (SaaS), Cyberoo’s in-house observability and governance suite for network monitoring, AD auditing, and file-integrity controls. In Dec 2025 Cyberoo added Keatrix, a proprietary cybersecurity-awareness SaaS platform expanding its reach into employee cyber-risk training. These offerings are unified under Orbis, Cyberoo’s mid-market risk governance model, reducing fragmentation and embedding cybersecurity as scalable governance.

The commercial model is built on an indirect distribution structure comprising Cyberoo, national distributors, and a network of partners, including system integrators, telcos (telecommunications operators), and consulting firms. Cyberoo retains ownership of service delivery and signs agreements directly with end clients, while distributors (5 active as of September 2026) manage partner onboarding and financial flows, and partners negotiate commercial terms with customers. Cyberoo invoices distributors according to the contractual structure agreed for each solution, while distributors manage billing and payment flows with partners, with commission structures of 20-25% for partners and 5-7% for distributors. To manage deferred-payment schemes, Cyberoo combines non-recourse factoring with structured leasing solutions through the subsidiary Cyberoo Capital, mitigating NWC pressure in a model characterized by pronounced Q4 seasonality (c.50% of annual billings).

Cyberoo targets companies with up to 5,000 devices and no internal SOC, where outsourced MDR offers the most attractive cost-benefit profile. Client concentration risk is minimal, with no customer above 5% of revenues and a client base spanning virtually all sectors of the economy, from manufacturing to financial services.

Cyberoo at a glance

 1st Cybersecurity Vendor listed on Borsa Italiana	 200+ highly qualified internal resources	 700+ Mid-Size Enterprise Clients	 5 Strategic Hubs in the EMEA Region
 Gartner Market Guide for MDR Services	 Cyberoo is CERT	 Proprietary & Certified Technologies	 Fully GDPR Compliant

Source: KT&Partners’ Elaboration on Company Data

The I-SOC: Cyberoo's Operational Core

The technological and operational core of Cyberoo's value proposition revolves around its Intelligence Security Operations Center (I-SOC). Its architecture is built on a multi-tier model that integrates intelligent automation with the expertise of more than 150 specialists (analysts, ethical hackers, and an incident response team), to ensure continuous 24/7/365 monitoring, detection, and response across five distinct levels.

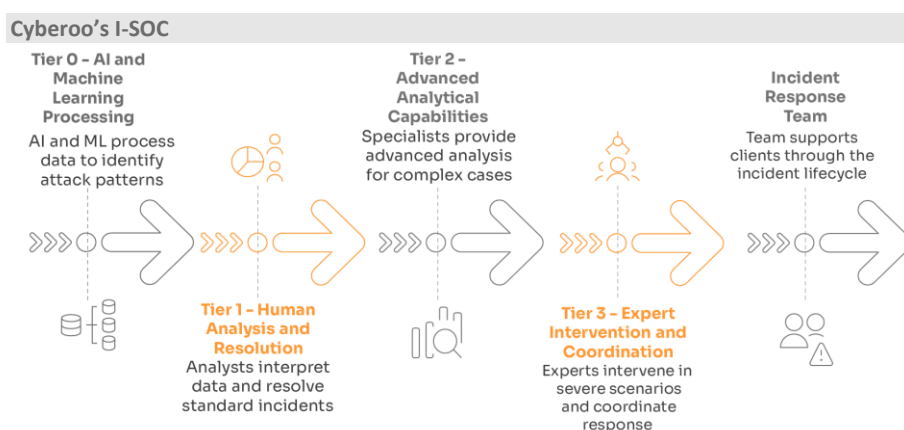
Every security alert begins at Tier 0, where AI and machine learning autonomously process vast data volumes. This automated layer correlates multiple data streams from customer systems to identify genuine attack patterns, drastically reducing false positives before human intervention. Only real alarms signal progress beyond this initial filter.

Alerts requiring human analysis escalate to Tier 1 (i-SOC). Based in Ternopil, Ukraine, this level represents the first line of human intervention, with 50+ Cyber Security Analysts operating 24/7 to interpret data processed by Tier 0 and determine necessary actions. These specialists resolve approximately 80% of incidents through real-time monitoring and structured playbooks, addressing threats such as unauthorized access attempts and suspicious activity. Resolution occurs directly at this level for most standard security events.

Cases demanding deeper investigation move to Tier 2 (h-SOC) in Warsaw, Poland, where 15+ Cyber Security Specialists provide advanced analytical capabilities. These experts support Tier 1 analysts in cases requiring vertical deep-dives into complex situations that exceed standard management, handling c.15% of incidents. Combined, Tier 1 and 2 resolve c.95% of all cases.

Critical incidents and high-risk threats (the remaining 5% of cases) escalate to Tier 3 (α-SOC), where 50+ Expert Cyber Security Specialists operate from Cyberoo's Italian HQ in Reggio Emilia. These experts intervene in the most severe scenarios, conducting in-depth forensic investigations and coordinating emergency response when breaches risk becoming systemic. In addition, the α-SOC team also performs scheduled pre-incident simulations and stress tests approximately 5–6 times per year, aimed at evaluating system resilience.

The Incident Response team completes the architecture supporting clients through the entire incident lifecycle including remediation and pre-incident activities.



Source: KT&Partners' Elaboration on Company Presentation

Geographic Distribution and Data Sovereignty

Cyberoo's operational structure is built on a strategic geographic distribution that follows the security by design principle. By operating across four European countries, the company ensures service continuity even in the event of disruptions affecting one or more sites.

This geographically diversified model is complemented by an infrastructure architecture that ensures the same level of security at the data layer. All Italian customer data and logs are processed and stored exclusively within national territory in one of the highest-reliability type of data center tier³ with all communication flows confined entirely to and from Italy. This approach reinforces security across the overall system and ensures compliance with GDPR restrictions on extra-EU data transfers and aligns with NIS2 requirements.

Cyberoo applies the same data sovereignty model in the international markets where it operates, deploying local data centers to ensure data remains within national borders and complies with local regulations.

Cyberoo's Hubs Geographic Distribution



Source: KT&Partners' Elaboration on Company Presentation

R&D

Since 2016, Cyberoo has focused on strengthening its core technological capabilities in AI, machine learning, deep learning, and big data to support advanced behavior and data analysis. In 2017, the Company established Cyberoo Lab, its internal R&D function, encompassing all its operational hubs. While the main development center is located in Ternopil, Ukraine—where personnel grew to 64 as of June 2025 (from 40 in 2023)—the R&D department includes the same analysts, engineers, and cybersecurity professionals that also staff the I-SOC network.

Cyberoo's R&D focus is attested by c.€3.8mn in capex over the past three years (FY23-26) and garnered the Company certifications and recognitions that attest its advanced technical capabilities. In particular, the company was included by Gartner as a Representative Vendor in the Market Guide for Managed Detection and Response Services in 2021, 2023, and 2024—a recognition awarded to a limited number of qualified international providers with validated capabilities in this domain. Additionally, Cyberoo was named Sample Vendor in the Behavioral Detection Analytics and Response category in the Gartner Hype Cycle for Security Operations, confirming the company's positioning at the forefront of next-generation detection technologies based on behavioral intelligence.

³ Based on the Uptime Institute's Tier Standard Classification, Tier 4 facilities guarantee 99.995% availability (i.e., basically an always on system) and full fault tolerance (i.e., with a backup system which prevents any service interruption), maintaining operations even in the event of component failures through fully duplicated power, cooling, and network systems.

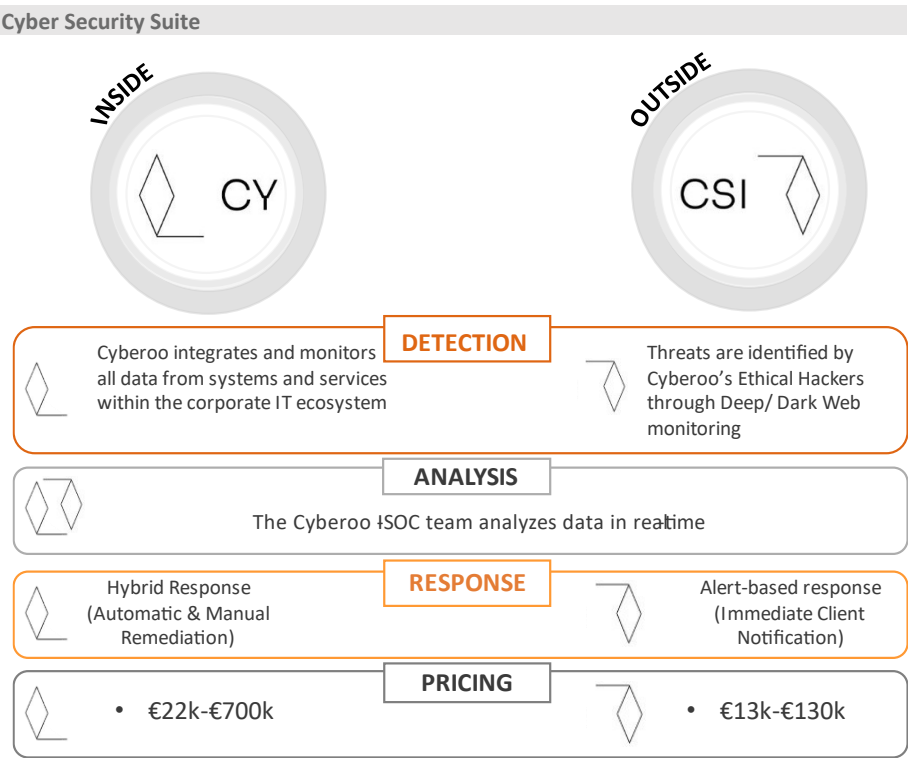
Cyber Security Suite – Internal and External MDR Coverage

The Cyber Security Suite represents one of Cyberoo’s core business units and delivers an end-to-end MDR proposition built on proprietary technology and its own 24/7 I-SOC. In 2024, the Suite generated €14.7mn, approximately 65% of the Group’s Revenues.

The Suite integrates the Company’s two complementary modules: Cypeer (CY), which safeguards the internal IT environment through continuous monitoring of infrastructures, endpoints, and network traffic; and Cyber Security Intelligence (CSI), which extends visibility beyond the corporate perimeter by scanning the deep/dark web for emerging external threats.

The Suite is commercialized through a fixed-fee, endpoint-based licensing model, with standard pricing systems across both Cypeer and CSI, typically spanning 1, 3 or 5 years (standard: 3 years). Fees scale with the number of protected endpoints (and in the case of Cypeer, level of tier) with an additional one-time upfront setup fee (c.10% of year-one contract value). Cypeer contracts range from c.€22k to €700k for deployments up to 5,000 endpoints, while CSI ranges from €13k to €130k.

By combining internal detection, external threat intelligence, and real-time incident response, the Cyber Security Suite provides a fully managed MDR framework.



Source: KT&Partners’ Elaboration on Company Presentation

Cypeer — MDR Suite for Internal Threat Management

Average revenue per client spans €20k to €50k annually across the Cypeer portfolio, offering four progressively advanced service tiers (Dek, Sonic, Keera, Keera+) tailored to different operational needs and levels of response automation. All versions share the same next-generation detection engine (I-SOC) and multi-channel contact points (email, phone, portal),

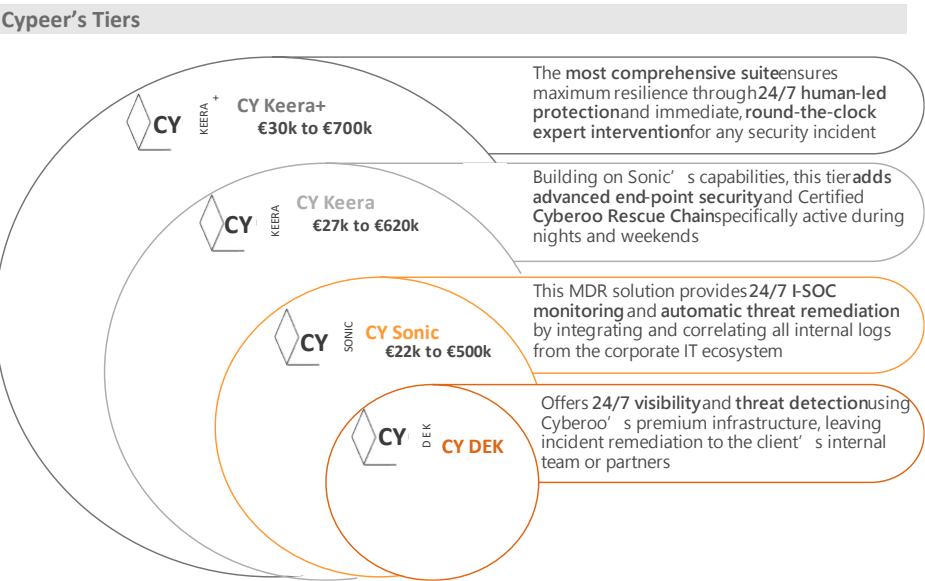
but differ critically in response automation and threat handling protocols, ranging from client-managed containment to full Cyberoo-led remediation (*Cyberoo Rescue Chain*).

CY Dek is Cyberoo’s entry-level solution, providing full system visibility and real-time threat detection across all I-SOC tiers. It uses the same detection and analysis infrastructure as higher-tier services, but remediation is entirely managed by the client or its partner, without Cyberoo-certified support (*Cyberoo Rescue Chain*). This configuration is suited to organizations that have internal resources for incident response but rely on Cyberoo for 24/7 monitoring, which would be too costly to maintain in-house.

CY Sonic builds on Dek by adding automated remediation algorithms driven by its operational arm, Cypeer Agent X. Once a threat is detected, it autonomously executes predefined containment actions to cut response times, although human intervention remains necessary for final resolution. However, since *Cyberoo Rescue Chain* is not included, final incident resolution still requires client or partner involvement during business hours. Sonic is the current volume leader, representing 60% of the product mix, with average three-year contracts ranging from c.€22k to c.€500k depending on clients’ size and endpoints. This tier is targeted at mid-market clients that need automated defense but prefer to retain internal control over incident handling.

CY Keera, launched in May 2024, expands on Sonic-level intervention by clients and partners during business hours, by adding Cyberoo Rescue Chain during nights and weekends. It targets companies that lack internal coverage outside daytime operations and require a professional rescue chain when IT teams are unavailable. It currently represents 5% of the product mix, with three-year contracts ranging from c.€27k to c.€620k for up to 5,000 endpoints, equivalent to almost a 25% premium over Sonic. The tier serves mid-market clients seeking extended protection windows without adopting full 24/7 support.

CY Keera+ delivers the most comprehensive Cypeer configuration, providing 24/7/365 certified rescue chain support alongside full automation and deep I-SOC integration. Designed for enterprises requiring always-on protection, Keera+ ensures end-to-end incident lifecycle management with minimal client involvement. Pricing spans from c.€30k to €700k for three-year contracts (40% premium to Sonic baseline), reflecting the complete transfer of security operations to Cyberoo's certified teams.



Source: KT&Partners’ Elaboration on Company Presentation

Cyber Security Intelligence

Cyber Security Intelligence (CSI) complements Cypeer by extending Cyberoo's protection beyond the corporate network and into the open, deep, and dark web. While Cypeer focuses on detecting and responding to threats inside the IT environment, CSI provides proactive external threat anticipation, combining OSINT (Open-Source Intelligence, from publicly available online data), proprietary tools, and a team of ethical hackers who operate undercover to spot early signs of compromise before they become security incidents.

CSI continuously monitors a broad spectrum of internet sources (social networks, public repositories, illicit marketplaces, and encrypted dark-web forums) to identify data breaches (stolen company data), credential exposures (leaked usernames/passwords), and data-leakage events (unintended disclosure of sensitive files). The service also includes brand monitoring (detecting fake or cloned domains), VIP monitoring (protecting high-risk executives), digital-footprint and shadow-IT analysis (mapping all exposed corporate assets), and continuous scanning (real-time checks for new vulnerabilities).

The value proposition of CSI is its ability to turn external intelligence into preventive action. When leaked credentials, confidential documents, or targeted reconnaissance attempts appear online, clients receive immediate alerts and practical remediation steps, such as enforcing password resets or isolating exposed systems, reducing both the likelihood and the impact of potential breaches.

Integrated with Cypeer, CSI creates a closed-loop security system: CSI provides external context to enrich Cypeer's internal monitoring, while Cypeer validates CSI findings against live network activity, strengthening overall detection accuracy. Together, they form a powerful Next-Gen defense shield which easily blocks advanced modern attacks that slip right past older, traditional security systems.

Cyber Security Advisory and Incident Response – Cyberoo Docetz

Cyberoo Docetz is Cyberoo's advisory and consulting division, designed both to enhance clients' cyber-resilience and to act as a strategic entry point for the Group's MDR offering. Cyberoo Docetz services represented 18% of Cybersecurity Services Revenues in FY24 (€3.2mn). The unit allows Cyberoo to enter organizations that lack the budget or maturity for a full MDR deployment, while also enabling cross-selling opportunities for customers already adopting the Cyber Security Suite. Cyberoo Docetz's services range from:

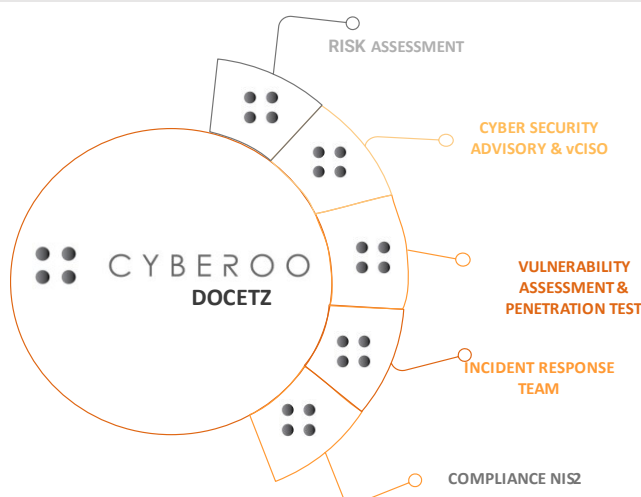
- Risk Assessment (evaluation of infrastructure, network, and processes to identify risk areas)
- Cyber Security Advisory & vCISO (Virtual Chief Information Security Officer) offering strategic guidance, governance, and tailored security programs)
- Vulnerability Assessment & Penetration Testing (technical scanning and real-attack simulations to uncover weaknesses)
- NIS2 Compliance Consulting (support for meeting EU cybersecurity obligations under the NIS2 Directive)

Cyberoo Docetz also includes the Incident Response Team, which manages critical attacks such as data breaches (unauthorized exposure of sensitive data) or ransomware (malware that encrypts data for extortion). The team oversees the entire response cycle, from incident identification (detecting and classifying the event), Incident scoping (mapping threat, attack vector, impact, and compromised assets), to define a Response Plan Definition (containment and mitigation actions) and Execution & Eradication (isolation of attackers, removal of the threat, restoration of operations).

From a strategic standpoint, Cyberoo Docetz strengthens Cyberoo's commercial reach: advisory engagements often precede the adoption of MDR solutions, with the Incident Response Team historically achieving a very high MDR conversion rate when intervening in organizations not yet clients. Additionally, NIS2 compliance services became a significant demand driver in 1H25, expanding Cyberoo Docetz's pipeline and accelerating cross-selling toward Cypeer and CSI as companies formalize their cybersecurity posture to meet regulatory requirements.

Overall, Cyberoo Docetz enhances Cyberoo's positioning as a full-fledged cybersecurity partner, enabling both immediate revenue generation and long-term MDR upselling.

Cyberoo's Docetz



Source: KT&Partners' Elaboration on Company Presentation

Titaan Neemesi – IT Governance & Compliance Suite

Titaan Neemesi is the solution dedicated to maintaining regulatory compliance and data security within the corporate IT infrastructure. Developed internally since the Company's 2019 rebranding, the platform extends Cyberoo's addressable perimeter beyond pure cybersecurity, into IT governance, infrastructure observability, and regulatory compliance, providing unified monitoring, diagnostics, and auditing capabilities across the IT environment, though revenues remain negligible to date.

The platform supports compliance with EU Regulation 2016/679 (GDPR) by collecting and retaining administrator activity logs for the minimum period required under Italian privacy regulations (Garante per la Protezione dei Dati Personali). The system acts as a log aggregator and management interface, organizing information across three macro-areas: Active Directory, Extra Active Directory, and Services. Within Active Directory, it performs audits of domains, roles, and configurations, identifies deviations from Microsoft best practices, and generates complete reports for troubleshooting purposes.

Titaan Neemesi also integrates functionality supporting compliance with the NIS2 Directive (Legislative Decree 138/2024), which requires organizations to adopt adequate security measures to protect critical networks and information systems. These requirements are addressed through advanced monitoring tools, threat detection, and incident response capabilities.

The platform further enhances data visibility and file-system auditing through a File Integrity Monitoring (FIM) module, which detects real-time access to critical files, highlighting unauthorized access and helping safeguard corporate know-how. Leveraging machine learning, the module builds dynamic behavioral models to identify anomalies in file access patterns.

Collectively, Titaan Neemesi enables clients to monitor, govern, and secure their IT infrastructure through a single platform. By notarizing all logs on the blockchain, the suite ensures complete data immutability and tamper-proof integrity, legally compliant log retention, and a high level of traceability and security across the IT environment.

Managed Services

Cyberoo's Managed Services (MS) division represents the company's pre-2018 heritage as a traditional Managed Service Provider, predating the pivot toward pure-play cybersecurity. The division encompasses three standardized platform operations: Data Center Management (continuous monitoring and operations of physical/virtual servers, network devices, and storage infrastructure); Cloud Management (IaaS optimization covering resource provisioning, performance monitoring, cost control, and compliance); and Device Management (endpoint administration and lifecycle management).

In the fifteen-month FY25, MS generated €5.2mn in revenues (€4.7mn in FY24), representing 18.7% of group sales: a declining share from 20.6% in FY24, 21.8% in FY23 and 28.0% in FY22. This progressive dilution reflects Cyberoo's focus on fuelling growth through higher-margins cybersecurity services.

Keatrix – Cybersecurity Awareness

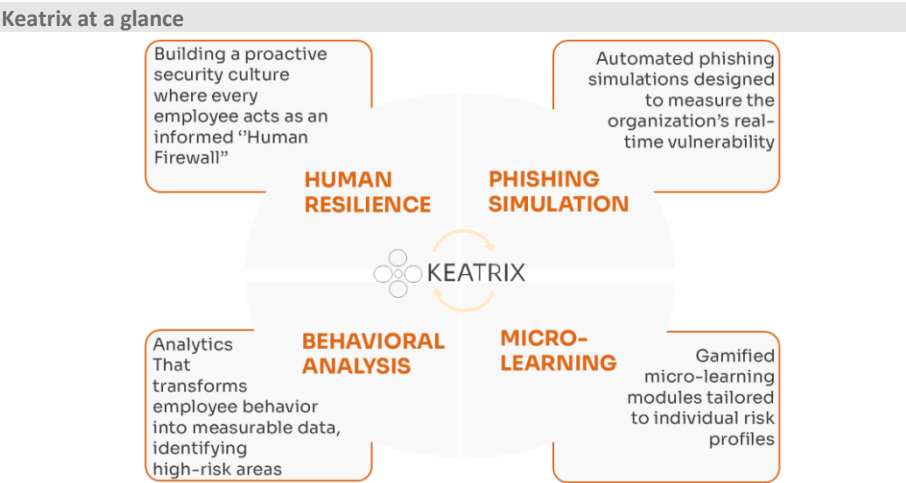
Keatrix is Cyberoo’s proprietary SaaS platform for cybersecurity awareness training, designed to reduce human-driven cyber risk through AI-personalized micro-learning. Launched in December 2025 after a three-year R&D cycle, the platform represents Cyberoo’s innovative entry into the human-risk domain, a structural gap in its portfolio where most corporate breaches still originate.

Keatrix delivers training through high-engagement video content (on top of a 120-minute episodic series), gamification, and adaptive learning algorithms that tailor modules to each employee’s risk profile. The content architecture is built around 61 mapped cyber behaviors and 325 modular lessons, allowing organizations to highly customize training to their threat landscape. The platform applies spaced repetition and interleaving techniques (neuroscience-based learning methods) to reinforce long-term behavioural change beyond basic compliance.

From an economic standpoint, Keatrix exhibits software-like margin structure: content is pre-produced, variable costs are negligible, and delivery is entirely digital. The go-to-market model is based on three-year contracts, with pricing expected to range from €20k to €200k depending on user count (up to 5,000 employees). Average deal size is expected at €20–50k annually, with post-commission margins >40%, even after accounting for partner commissions (20–25%) and distributor fees (5–7%). This creates higher structural profitability than MDR services, which require recurring SOC staffing.

Strategically, Keatrix completes Cyberoo’s portfolio across technology (Cypeer), processes (Docetz), and people (Keatrix), enabling the Group to offer a holistic cybersecurity stack. It also expands Cyberoo’s addressable market: while MDR is optimized for companies with 200–2,000 employees, Keatrix scales efficiently also to mid-large enterprises and multinational groups, unlocking new segments with lower operational intensity. Furthermore, the platform provides Cyberoo with a low-friction access point to new geographies. Its SaaS nature allows rapid partner-led distribution, establishing a commercial presence that can be leveraged to introduce MDR and additional services over time, with substantially lower investment compared to traditional MDR-driven expansion, which would require an established localized SOC.

Commercially, domestic strategy focuses on cross-selling into Cyberoo’s 700-client MDR installed base, where adoption barriers are low and security awareness tools are often missing. Internationally, distribution will rely on independent partners capable of autonomous sales, reducing market-entry costs and supporting scalable expansion across Europe. An optional NIS2 compliance add-on enhances demand without diluting the platform’s behavioural-change positioning.



Source: KT&Partners’ Elaboration on Company Presentation

ORBIS – From Product Portfolio to Integrated Risk Governance

Each of Cyberoo's solutions is managed not as a standalone product but under ORBIS, the company's cyber risk governance framework, built around four domains addressing distinct categories of enterprise risk.

Threat Management, delivered through the Cyber Security Suite (Cypeer, CSI), sits at the core, covering active threats, malware, and anomalous access through continuous detection and response. The other three domains extend coverage to where risk propagates once a threat materializes: Docetz handles Process Governance, defining who validates and authorizes a response; Titaan covers Regulatory Compliance, ensuring events can be reported and defended under audit; Keatrix addresses People Security and Training, targeting the human driven risk (phishing, social engineering, credential exposure), behind most attack chains.

The rationale reflects a broader market shift. As MDR has evolved from a differentiated service into a crowded category spanning managed EDR, SOC as a Service, and managed XDR, differentiation on technology alone has become harder to sustain, and tool and vendor fragmentation has become a risk in itself. According to IBM Institute for Business Value, organizations manage on average 83 security tools from 29 vendors, with 52% of executives citing fragmentation as a constraint on threat response, while more integrated organizations identify incidents 72 days faster and contain them 84 days faster.

ORBIS therefore functions less as a new technology layer and more as the commercial architecture through which Cyberoo converts single service MDR relationships into broader, multi domain engagements, a shift reinforced by regulatory pressure from NIS2, DORA, the Cyber Resilience Act, and the AI Act, which increasingly require coordinated control across technology, process, and personnel.

ORBIS Risk Domains		
DOMAIN	FUNCTION	RISK COVERED
Threat Management	Detect, analyze and respond.	TECHNICAL COMPROMISE Active threats, malware, anomalous access.
Process Governance	Define roles, priorities and decision flows.	OPERATIONAL RISK Delays, unclear responsibilities, poor coordination.
Regulatory Compliance	Manage obligations, evidence and controls.	REGULATORY RISK Non-compliance, weak audits, incomplete documentation.
People Security & Training	Reduce risky behaviors.	HUMAN RISK Human error, phishing, social engineering, exposed credentials.

Source: KT&Partners' Elaboration on Company Presentation

Go-to-Market

Cyberoo's commercial strategy is built on a Tier II indirect distribution model, meaning the product reaches the end customer through two successive intermediaries: distributors per country (managing financial flows and partner onboarding) and a network of local partners, including system integrators, that own the end-customer relationship. This structure leverages the pre-existing trust between partners and their clients, allowing Cyberoo to accelerate market penetration and customer engagement.

Cyberoo retains technical and contractual governance and service delivery, while the model reduces direct commercial acquisition costs and mitigates part of the credit risk through distributors, factoring, and Cyberoo Capital. The model articulates into two distinct partner programs: Black Club, covering the Company's full product portfolio (ORBIS, with Cyber Security Suite, Cyberoo Docetz, Titaan, and Keatrix), and Black Academy, launched in May 2026 and dedicated specifically to Keatrix. The two programs share part of the distributor network but operate independently, with separate partner onboarding, incentive structures, and commercial positioning.

The Company sits at the top of the value chain, where it engages, trains, and retains partners according to each program's incentive structure, manages all after-sales technical activities, and maintains direct service delivery to final customers through contractual agreements (EULA signed directly with each end customer).

In a diversification effort, Cyberoo has moved in the past year from a single distributor per country to a multi-distributor non-exclusive model. The Company now counts five distributors total across the three geographies (3 in Italy, 1 in Poland and 1 in Spain) for the Black Club network. Black Academy at launch counts the same three distributors in Italy, with international expansion planned in a subsequent phase.

At the base of the pyramid, partners maintain direct commercial relationships with end customers, leveraging established trust relationships built over time. Partners negotiate contracts autonomously, including economic terms such as discounts and payment conditions, operating with significant commercial independence. Customer contracts typically span 1, 3, or 5 years with tacit renewal clauses, providing revenue visibility.

Cyberoo Tier II Model: From Distributor to Client

CYBEROO & PARTNER : TIER II MODEL				
	CYBEROO	DISTRIBUTOR	PARTNER*	CLIENT
	Technical and legal governance. In the case of "pro soluto", it does not assume direct financial risk.	Distributors per country, nonexclusive ITALY - ICOS, COMETA, V-VALLEY POLAND - ARROW SPAIN - ZALTOR	Mainly System Integrators, different per country ITALY - 101 POLAND - 15 SPAIN - 6	Contract of 1 / 3 / 5 years with tacit renewal.
Relationship flow	Engages, trains and retains partners through the Partner Program. Manages post-sale technical activities and end -client services under EULA terms.	•Scouting of new partners. •Manages invoicing to the partner and the transfer of financial flows between partner and Cyberoo.	Has a commercial relationship with the client, already grounded in consolidated trust with the reference partner.	Has a relationship with both the partner and Cyberoo in the pre-sale phase. Post-sale, it mainly interfaces with Cyberoo and, if involved, in the support chain, with the partner.
Invoicing flow	Invoices the distributor 100% of the contract: 80% for the upfront license and 20% for the service distributed per year of competence.	Invoices the partner under the same terms received from Cyberoo.	Stipulates the contract with the client, with autonomy in negotiating economic conditions and managing payment terms.	Receives the invoice from the partner under the agreed terms.
Payment flow	Receives the payment from the distributor.	The distributor pays Cyberoo and handles financial management toward the resellers.	The partner pays the distributor under the terms agreed with the client, or in some cases anticipating the payments.	The client pays the partner under the agreed terms.

* Partners can join different programsBlack Club, if the agreement covers the entire portfolio of solutions, oBlack Academy, if the agreement is limited exclusively to Keatrix.

Source: KT&Partners' Elaboration on Company Presentation

Italian Network

In Italy, Cyberoo operates through a nationwide network of 101 partners (as of July 2026) under the Black Club, ensuring full geographic coverage. The channel is anchored by three non-exclusive distributors: ICOS (€148mn FY25 revenues), Cometa (€179mn) and V-Valley (€460mn), the advanced solutions arm of Esprinet, Italy's largest ICT distributor with c.30,000 active resellers. All three distributors are also anchor partners of Black Academy.

Italy is the company's most mature market, supported by its largest and most structured sales organization. Since the December 2025 launch, Keatrix has already closed its first multi-year contracts through the Black Academy network, with activations concentrated in Northern Italy and a growing presence in Central Italy, across both existing MDR accounts and net-new logos in industrials, food and agri, pharma, healthcare, and business services.

International Network

Cyberoo began building its Poland presence in 2023 and strengthened it with a distribution agreement with Arrow Electronics, a global technology distributor with FY25 revenues of c.\$31bn. The region now counts 15 active partners supported by a lean commercial team focused on technical pre-sales and early market enablement. The model has already delivered at scale: in July 2025 Cyberoo secured a three-year contract with a major international Real Estate & Construction group, demonstrating the scalability of the indirect go-to-market approach in enterprise environments.

The Iberian expansion began in late 2024 with a strategic distribution agreement in Spain and Portugal, and gathered pace through 2025 with the onboarding of local partners and the first end customer contracts signed in November of that same year, across companies in the energy, hospitality and financial holding sectors. The current network includes six partners supported by a commercial team primarily dedicated to partner enablement and ecosystem expansion. Given Cyberoo's limited brand visibility in the region, the strategy prioritizes rapid partner onboarding to accelerate market access. Both Poland and Iberia currently distribute the Cyber Security Suite exclusively.

Keatrix international expansion is expected to leverage the same international distributors as a near-term entry point, with broader European rollout to follow.

Stakeholders

Clients

Cyberoo targets the mid-market to lower-enterprise segment, where cybersecurity needs, budget availability, and outsourcing propensity converge. The core addressable market comprises companies with up to 5,000 devices and, most importantly, no internal cybersecurity team, making MDR outsourcing the most cost-effective solution. Within this range, management identifies a profitability sweet spot in organizations with 200–2,000 employees, where service adoption, ticket size, and retention rates are highest.

Below roughly 7,000 employees, outsourcing remains economically rational; beyond that threshold, large enterprises tend to build internal SOC capabilities for cost-efficiency and control. In these cases, Cyberoo's role shifts from MDR provider to specialized advisory, with CSI used to cover specific gaps rather than full-stack protection.

This segmentation aligns with Cyberoo's installed base of 700+ mid-sized enterprises (as of 1H25) across Italy and international markets, including companies with revenues between €200mn and €2bn spanning virtually all sectors of the economy, from manufacturing to healthcare.

Geographically, the business is still concentrated in Italy, historically accounting for c.85% of revenues, but international expansion is underway following the opening of a local I-SOC hub in Poland and the establishment of new partnerships in Spain and Portugal. These initiatives, together with targeted agreements with multinational distributors, as well as with the launch of Keatrix, are expected to progressively reduce domestic dependency while broadening Cyberoo's exposure to the European cybersecurity market.

Client diversification is further reinforced by a multi-sector footprint, spanning manufacturing, retail, professional services, and healthcare. Historically, no single customer represents more than 5% of total revenues, significantly mitigating concentration risk.

Distributors & Partners

Cyberoo invoices distributors which in turn invoice partners, who in turn invoice end customers, according to agreed terms, in some cases advancing payments to accelerate cash flow. The typical commission structure allocates 20-25% margins of the contract value to partners and 5-7% to distributors. The relationship flow sees customers engaging with partners initially, then interfacing with Cyberoo during pre-sales phases and primarily with Cyberoo during post-sales service delivery, reducing dependency on the partner layer and reinforcing Cyberoo's direct relationship with the end customer, although partners may remain involved in the support chain.

The financial mechanics reflect adaptations to a macroeconomic environment where customers increasingly prefer deferred payments aligned with amortization schedules. Cyberoo employs two distinct practices to manage this dynamic: (i) under the pro-soluto model, Cyberoo leverages non-recourse factoring. The Company invoices distributors according to the contractual structure agreed for each solution, then discounts invoices pro soluto through factoring partners, eliminating credit risk as distributors assume it entirely; (ii) under the deferred model, distributors pay Cyberoo following cash collections from partners over 36 to 60 months, creating temporary mismatches between invoiced revenues and cash receipts.

Credit dynamics are amplified by pronounced seasonality, with approximately 50% of annual revenues concentrating in Q4 and invoice maturities clustering in Q1, causing receivables to

peak in the first half of the year before normalizing as deferred collections are received in H2. Third-party trade receivables (c.20% of overall trade receivables at FY23, rising to 42% at FY24 and c.82% at FY25) grew from €8.3mn at FY24 to €11.6mn at FY25, reflecting business expansion, structural collection cycle lengthening and the €5.3mn portfolio of third-party receivables acquired from Sedoc in March 2026.

To structurally address this dynamic, in December 2025 Cyberoo established Cyberoo Capital, a wholly owned subsidiary with a dedicated facility of up to €15mn, designed to enable partners to offer Cyberoo solutions under operating lease arrangements. The mechanism works as follows: the end customer accesses the solution through periodic payments rather than an upfront commitment, lowering adoption barriers; the partner proposes Cyberoo solutions in OPEX format; and Cyberoo Capital acts as the financial vehicle backing the lease structure. From a balance sheet standpoint, the operation removes receivables from the trade credit perimeter and replaces them with structured lease obligations accounted below EBITDA, improving the quality of working capital while preserving EBITDA margins. The model also extends Cyberoo's traditional positioning from a pure technology vendor to an operator that controls the financing layer of its own distribution chain, a structural advantage in a market where deferred payment is becoming the norm.

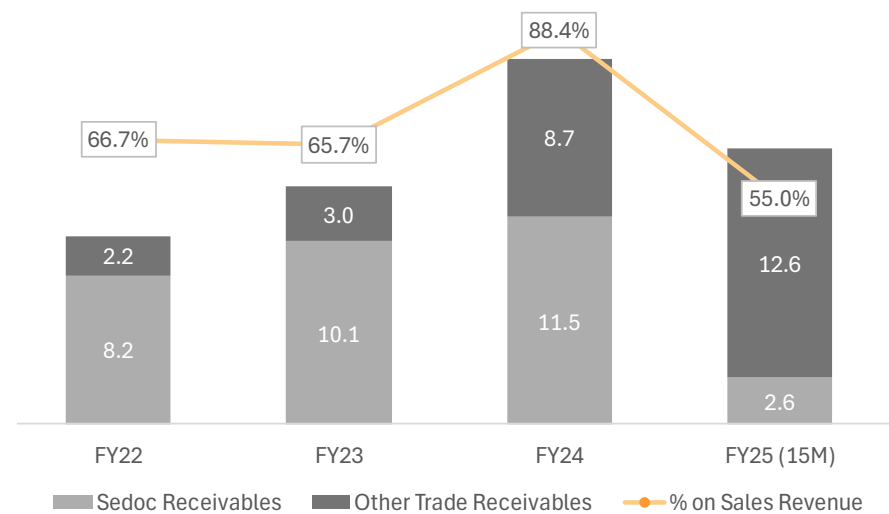
Sedoc receivables: a concentrated exposure in progressive reduction

A second feature of Cyberoo's balance sheet is the historical receivable exposure to Sedoc Digital Group, the controlling shareholder, of predominantly commercial nature. At FY24, Sedoc receivables stood at €11.5mn, exceeding the €8.3mn of third-party trade receivables and accounting for over half of the Group's total receivable exposure in current assets. The concentration of credit risk in a single related party, outside the ordinary business perimeter, represented a structural weakness in balance sheet quality that the market had repeatedly flagged.

The exposure has been managed through a series of repayment plans agreed since 2022, carrying interest between 3.0% and 3.5% over durations ranging from 21 to 48 months, all instalments honoured on schedule. The deleveraging was already visible by 1H25, when Sedoc receivables declined to €11.3mn while third-party trade receivables grew to €10.6mn: the two components, which at FY24 stood in a roughly 40/60 ratio in favour of Sedoc, had reached near-parity, with the trajectory pointing toward a progressive inversion as commercial volumes grow and the Sedoc exposure continues to amortize.

The rebalancing then accelerated in March 2026 through a portfolio operation. Cyberoo acquired from Sedoc a portfolio of receivables that Sedoc in turn held toward its own end clients, for €5.29mn against a nominal value of €5.7mn. Rather than being paid in cash, the purchase was settled by offsetting it against the amounts Sedoc already owed to Cyberoo: in effect, Cyberoo collected part of its related-party credit not in cash but in the form of a portfolio of third-party receivables of equivalent value. The transaction does not change the size of the exposure so much as its nature, replacing a single, concentrated claim on a related party with a granular set of credits toward independent end clients, thereby improving the diversification of counterparty risk and the visibility of prospective collections.

Trade Receivables Breakdown (FY22-25 15M): Focus on Sedoc & Incidence on Sales



Source: KT&Partners' Elaboration on Company Data (FY22-25).

The combined effect is visible in the FY25 accounts, where the Sedoc balance fell to €2.56mn at 31 March 2026, down roughly 78% from €11.5mn at FY24 and ahead of the agreed repayment trajectory, while third-party trade receivables rose to €15.2mn: the related-party exposure, which at FY24 represented more than half of total receivables, has thus been reduced to a residual share of the book.

In our estimates, we expect the Sedoc balance to continue declining over the plan without modelling its full extinction, since Sedoc remains a commercial client of the Group and a physiological residual exposure is likely to persist even as the legacy overdue position is cleared. More importantly, we do not expect trade receivables to inflate as they did in the past despite continued top-line growth, because the structural payment mismatch that drove the historical build-up is now addressed at source: the shift of clients toward instalment-based payments increasingly absorbed by Cyberoo Capital, the vehicle that makes eligible multi-year rights, licenses or bundles available to final customers through operating-lease structures, moving the associated exposure off trade receivables and into the leased-asset book, while the migration toward distributors that better align end-client collections with partner payment terms works in the same direction.

Market Overview

Cyber risk is becoming a systemic issue for companies, as digital threats intensify in scale and complexity, fueled by the malicious adoption of AI and growing geopolitical instability. At the same time, most organizations, particularly SMEs, face structural constraints in building adequate in-house security capabilities, due to a persistent shortage of qualified professionals and rising regulatory requirements. The entry into force of the NIS2 Directive raises the bar further, progressively turning cybersecurity from a discretionary IT expense into a mandatory, ongoing operational commitment, alongside emerging frameworks such as DORA, the Cyber Resilience Act, and the AI Act. In this environment, demand is increasingly converging toward managed and integrated security models, capable of connecting threat detection with governance, compliance, and the human factor, as fragmented, siloed approaches struggle to keep pace with the complexity of the risk.

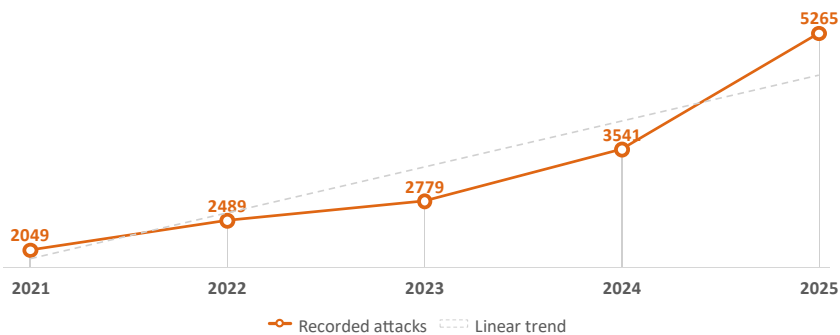
Global Cybersecurity Market

Cybersecurity has become a structural component of global IT spending, driven by the increasing frequency, sophistication, and economic impact of cyber threats. According to Gartner (a leading global research and advisory IT firm), global information security spending has reached USD215.6bn in 2025, up from USD193.4bn in 2024 (11.5% YoY growth)⁴, supported by rising investments in security software and managed services. The growth is expected to steadily continue in the near future, reaching USD472bn in 2031, growing at 12.3% CAGR over 2026-2031⁵.

This sustained market expansion mirrors the rapid escalation in both the scale and sophistication of cyber threats, whose economic impact continues to intensify globally. In 2025, a total of 5,265 significant cyber incidents were recorded worldwide, the highest number ever observed in a single year and a +48.7% increase compared to the previous year, with an average of 439 incidents per month.⁶

Over the 2021 to 2025 period, cumulative incidents reached 16,123 events. Recent figures point to a clear intensification in attack frequency, as the 5,265 incidents registered in 2025 alone account for roughly 32.6% of all cyber incidents recorded globally since 2021, indicating an accelerating pace of cyber threats. This trend is also evident on a run-rate basis: the average monthly number of cyber incidents reached 439 in 2025, representing a 156% increase compared to 2021 (171 incidents per month). Overall, the continued rise in both frequency and severity reflects the increasing systemic relevance of cybersecurity, driven by expanding digitalization, the pervasive use of Artificial Intelligence and heightened geopolitical tensions.

Number of Registered Cyber Incidents (2021 – 2025)



Source: Clusit - Rapporto 2026 sulla Cybersecurity – Update March 2026

⁴ Gartner. (2025, June 19). 2025 Cybersecurity and IT Risk Coverage Areas.

⁵ Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031), Mordor Intelligence, 2026

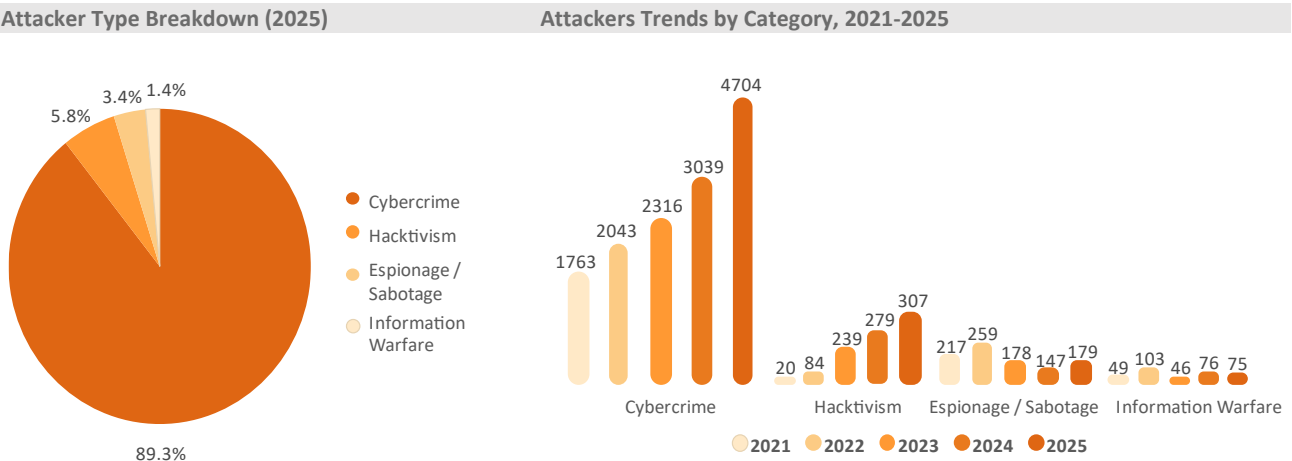
⁶ Rapporto Clusit sulla Cybersecurity in Italia e nel mondo – Update March 2026.

The Global Cybersecurity Outlook 2026⁷ highlights an increasingly complex threat environment, characterized by supply-chain vulnerabilities, geopolitically driven cyber-espionage, and the growing malicious use of AI. In this context, 94% of survey respondents identified AI as the most significant driver of change in cybersecurity in the year ahead, while 73% reported direct or indirect personal exposure to cyber enabled fraud over the course of 2025. Supply-chain security risks, that is vulnerabilities originating from third-party vendors and software providers integrated into an organization’s digital infrastructure, is now a top priority, with 65% of large organizations identifying it as a critical challenge to cyber resilience, while 64% of companies report having revised their cybersecurity strategies in response to geopolitical tensions.

Against this backdrop, organizations’ ability to scale internal cybersecurity capabilities is increasingly constrained by a structural shortage of skilled professionals. The global cybersecurity skills gap reached approximately 4.8mn unfilled roles in late 2025, marking a 19% YoY increase according to the ISC2 Cybersecurity Workforce Study. This imbalance is driven by the rapid evolution of attack techniques, the expanding breadth of security domains, and persistent challenges in hiring, retention, and skill obsolescence.

The talent shortage is also amplifying cyber inequity across organizations. Approximately 35%⁷ of small organizations now consider their cyber resilience inadequate, a proportion that has increased sevenfold since 2022, while the share of large organizations reporting insufficient cyber resilience has nearly halved over the same period. This evidence points to an accelerating cybersecurity gap between SMEs and large enterprises. Smaller and less-resourced entities are disproportionately exposed, lacking the scale and financial capacity required to sustain 24/7 internal security operations.

In this context, the widening gap between cybersecurity demand and available talent is structurally accelerating the shift toward managed security services, particularly Managed Detection and Response (MDR), as a scalable alternative to fully internalized security models. While managed services currently account for only c.30% of global cybersecurity revenues⁵, they are expanding at a faster pace, with demand increasingly favoring integrated, all-in-one platforms that combine cloud, identity, application, and network security, rather than fragmented point solutions.



Source: KT&Partners’ Elaboration on Clusit - Rapporto 2026 sulla Cybersecurity – Update March 2026

⁷ World Economic Forum Global Risk Report, 2025

NIS2 – A Catalyst

The NIS2 Directive (EU 2022/2555) represents a structural inflection point for the European cybersecurity market, as it formally enters its enforcement phase and materially expands the pool of regulated companies. Adopted to replace the original 2016 NIS framework, the directive aims to ensure a high common level of cybersecurity across the EU by strengthening the resilience of network and information systems not only within critical infrastructures, but across the entire digital value chain, explicitly including suppliers and service providers.

While NIS2 was adopted at EU level in 2022, its practical impact becomes tangible from 2024 onwards, as national transposition takes effect and enforcement mechanisms are activated. In Italy, implementation is overseen by the Agenzia per la Cybersicurezza Nazionale (ACN), with mandatory annual registration of in-scope entities starting in December 2024 and progressive enforcement of operational obligations. From 2026, incident notification and governance obligations are becoming increasingly binding, requiring companies to structure detection, response and continuity frameworks. As a result, cybersecurity spending is progressively shifting from optional or reactive to mandatory and recurring.

NIS2 significantly broadens applicability across sectors and company sizes, introducing stricter obligations on ICT risk management, continuous monitoring, incident detection and reporting, business continuity, governance accountability, and supply-chain security. Regulated organizations are classified as either essential or important entities, depending on sector criticality and systemic relevance. Essential entities include operators in highly sensitive domains (e.g., energy, transport, banking, healthcare), subject to the strictest supervisory regime and proactive enforcement. Important entities cover a broader set of sectors with lower systemic impact (e.g., manufacturing, food, chemicals), facing similar obligations but generally under a more reactive, ex-post enforcement approach.

The directive primarily targets medium-sized and large companies operating in high-impact sectors, although it indirectly captures a large number of SMEs embedded in regulated supply chains. Sanctions for non-compliance are material, reaching up to €10mn or 2% of global turnover for essential entities, reinforcing cybersecurity as a strategic priority at board level.

From a market perspective, NIS2 marks the beginning of a structurally larger addressable market for cybersecurity providers. As enforcement progresses from 2024 onward, a growing number of European and Italian companies are progressively required to adopt continuous monitoring, 24/7 incident response, and formalized security governance, capabilities that many mid-market firms lack internally. This shift is already visible at governance level: according to the Politecnico di Milano's Osservatorio Cybersecurity & Data Protection (2026), 57% of large Italian companies report increased board level attention to cybersecurity as a direct consequence of NIS2, while 56% are actively seeking synergies to manage regulatory complexity more efficiently. This dynamic is expected to drive sustained demand for outsourced and managed solutions, particularly managed detection and response (MDR), threat intelligence, and security operations services, creating a multi-year regulatory tailwind for specialized cybersecurity players such as Cyberoo, whose offerings are directly aligned with the directive's operational requirements, a dynamic reinforced by growing choice overload across the vendor landscape, with 95% of organizations reporting limited trust in cybersecurity providers and 79% struggling to assess new ones⁸.

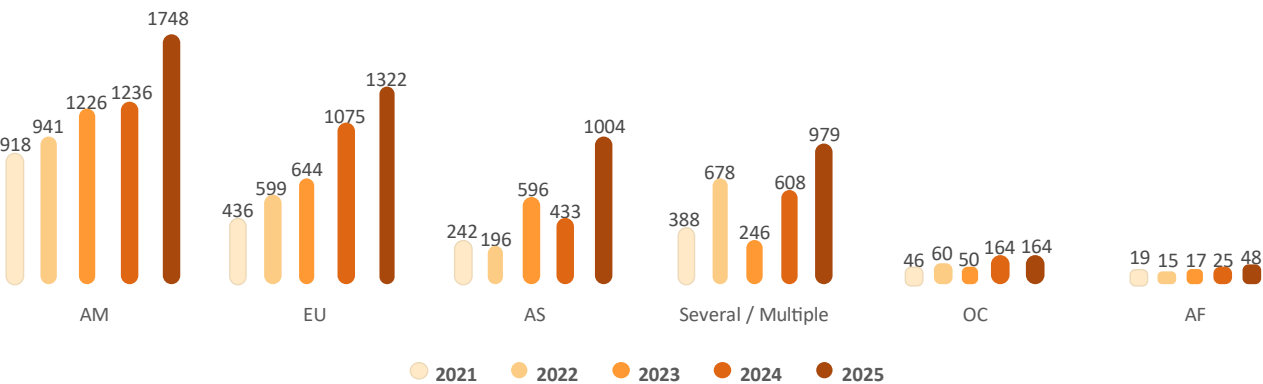
⁸ The Cybersecurity Trust Reality in 2026, Sophos, 31 March 2026.

European Cybersecurity Market

Europe represents one of the primary global targets of cyberattacks. In 2025, approximately one out of four cyber incidents worldwide involved European victims, with Europe accounting for 25% of total recorded attacks, down from 30% in 2024 (-5pp YoY). In absolute terms, the number of incidents targeting Europe reached a record high (1,322 out of 5,265), confirming a clear acceleration in threat exposure. This increase reflects both the progressive digitalization of European economies and the expansion of regulatory and institutional infrastructures, which have heightened the attractiveness of the region for cybercriminal activities, reinforcing its position as a structurally high-risk cyber environment.

Against this backdrop, the European cybersecurity market reached an estimated USD81.81bn in 2025 and is projected to grow to USD165.73bn by 2034, at an 8.16% CAGR over 2025-2034⁹. Within this broader market, the European Union Agency for Cybersecurity estimates that managed services specifically will grow at a faster 13.6% CAGR over the next 6-7 years, driven by the need to combine regulatory compliance, operational resilience, and cost efficiency within a single service framework. At the same time, market growth is increasingly supported by the mid-market: although large organizations accounted for 62% of revenues in 2025, SMEs are expected to grow at a faster 14.4% CAGR, following the expansion of the regulatory scope under NIS2 and the limited availability of internal cybersecurity resources, further accelerating adoption of MDR and outsourced security models. This trend is also reinforced by ENISA's subsequent work on the EU Managed Security Services certification scheme (EUMSS), which signals a shift from market assessment toward certification, standardization, and trust-building in the European MSS market.

Geographical Distribution of Cyberattack Victims, 2021-2025



Source: KT&Partners' Elaboration on Clusit - Rapporto 2026 sulla Cybersecurity – Update March 2026

However, the ability of European organizations to internalize these requirements is constrained by a persistent shortage of skilled professionals. The European cybersecurity skills gap is estimated at over 299k unfilled positions², 76% of employees in cybersecurity related roles lack formal qualifications or certified training, a dynamic further confirmed by the CLUSIT 2026 survey data which identifies staff shortages (42%) and lack of specific competencies (37%) among the primary obstacles to cybersecurity adoption globally⁶. This shortage is limiting implementation capacity and is further reinforcing demand for managed detection and response services as a substitute for internal teams.

⁹ IMARC Group (2026). Europe Cybersecurity Market Size, Share, Trends and Forecast by Component, Deployment Type, User Type, Industry Vertical, and Country, 2026-2034. IMARC Group.

The Italian Cybersecurity Industry

Italy stands out as one of the most exposed and structurally vulnerable cybersecurity markets in Europe, due to a combination of high threat intensity, broad regulatory exposure, and limited defensive capabilities, and recent data confirms a structurally elevated and accelerating exposure.

In 2025 alone, 507 cyber incidents involving Italian entities were recorded, representing 9.6% of total worldwide incidents, with 241 classified as high severity. While the severity distribution of attacks in Italy remains somewhat below the global average, with 52.5% of Italian incidents classified as Medium or Low⁶, the absolute volume of severe events continues to grow, confirming a structural acceleration in relative cyber risk exposure rather than a temporary spike and maintaining Italy's position as a persistently high-risk environment.

Cumulatively, between 2020 and 2025, the national sample includes 1,432 severe cyber events⁶, highlighting a persistently high level of systemic vulnerability. Most notably, 2025 marks a clear inflection point: the 507 incidents recorded in the year alone account for roughly 35% of all events observed over the entire five-year period, representing a 42% surge compared to full-year 2024, signaling a sharp acceleration in both frequency and impact. At a global level, successful attacks against Italian entities account for 9.6% of total cyber incidents recorded worldwide.

This elevated threat exposure is occurring alongside a material expansion of the regulatory perimeter. Although the national transposition of NIS2 is progressively extending mandatory cybersecurity and incident response requirements to a significantly wider perimeter of Italian entities, structural vulnerability is still at large, particularly evident among small and medium-sized enterprises, which account for approximately 92% of the Italian economic fabric. Despite being increasingly within the scope of NIS2, Italian SMEs show persistent organizational gaps. A recent survey conducted by the Chamber of Commerce of Modena on more than 700 companies indicates that only around 50% of NIS2-regulated firms have a formal incident-management procedure in place, highlighting widespread deficiencies.

Against this backdrop, Italy faces a structural cybersecurity skills gap that materially limits the ability of organizations to internalize security operations. The national ICT workforce represents only 4%¹⁰ of total employment, compared with 5% at EU level, implying a shortfall of more than 236k professionals to close the gap. Each year, roughly 136k job postings for ICT profiles are published¹¹, while the education system supplies only c.70k certified professionals, creating a persistent mismatch between demand and supply. This imbalance is particularly acute in cybersecurity, where demand for Cybersecurity Engineers has increased by 70% between January 2024 and September 2025, while only 14% of organizations report confidence in their ability to manage cyber risks internally.

The skills shortage is especially critical for SMEs, which dominate the Italian productive system and are structurally less equipped to attract and retain specialized talent. Surveys conducted by Il Sole 24 Ore indicate that 18% of Italian SMEs operate without any formal cybersecurity protocol, despite being increasingly exposed to regulatory obligations and cyber threats (OECD). This combination of high exposure, regulatory pressure, and limited internal resources makes fully internalized security models economically and operationally unsustainable for a large share of the market.

In this context, the Italian cybersecurity market reached €2.78bn in 2025¹², growing +12% YoY according to the Osservatorio Cybersecurity & Data Protection of Politecnico di Milano, with

¹⁰ Osservatorio Competenze Digitali 2025

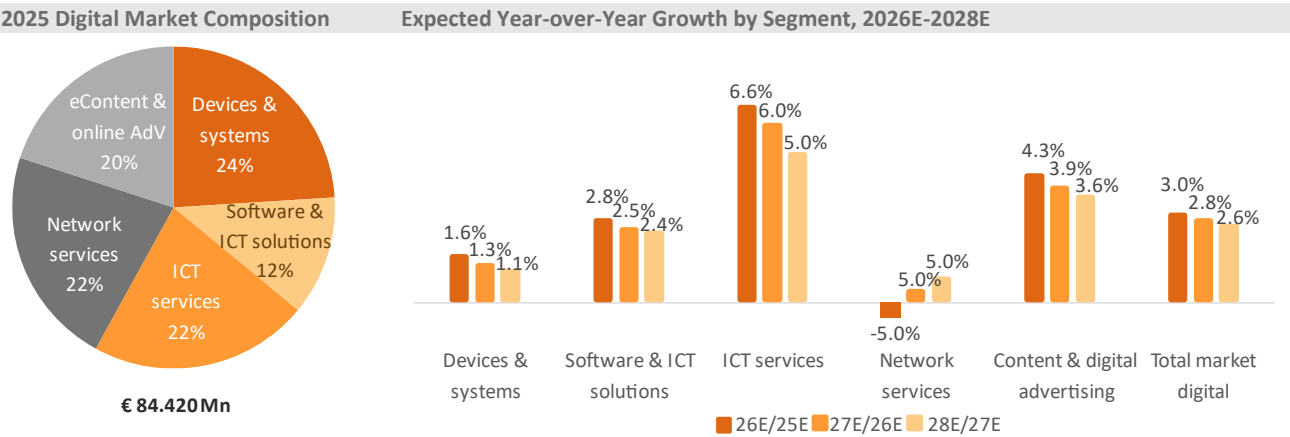
¹¹ Il Digitale in Italia 2025, Anitec-Assinform.

¹² Osservatorio Cybersecurity & Data Protection, Politecnico di Milano, (February 2026).

managed detection and response services representing the fastest growing segment. Looking ahead, the market is expected to sustain double digit growth, with a 2025–2030E CAGR of c.13% according to Mordor Intelligence, confirming cybersecurity as a structural and non-discretionary component of ICT spending for both private enterprises and PA.

Within this framework, market growth is clearly concentrated in Managed Security Services (MSS) and Cloud, the largest and fastest-growing segment, reaching €969mn in 2025, equivalent to c.43% of total cybersecurity spending as measured by Anitec-Assinform, and expanding +13.7% YoY (+13.2% CAGR)¹¹. This segment structurally benefits from the outsourcing of security operations, as organizations increasingly rely on external SOC's, while mitigating the structural shortage of cybersecurity skills and limiting the expansion of internal IT teams.

By contrast, System Integration and other services (which includes training) are expected to reach €817mn in 2025 (c.36% on the same basis), growing +10.4% YoY (+10.3% 2025–2028E CAGR)¹¹, signaling that among the key drivers of future growth is the increasing awareness of the need to strengthen cybersecurity skills across organizations, both within IT teams and among non-technical staff, in order to reduce human-related risk.



Source: KT&Partners' Elaboration on NetConsulting Cube and Anitec-Assinform, October 2025

Competitive Arena

According to Gartner distinction¹³, the MDR offering reaches the client through two operating models: vendors and service-led operators. Vendors develop their technology in-house and sell it as a standardised product, largely through partners. However, the client-specific steps of remediation stay with the customer or move to a third-party MSSP. On the other hand, service-led operators own the client relationship and the delivery, carrying the hands-on work of response through to the client's environment but not owning the technology, rather assembling the offering on proprietary and third-party solutions.

Vendors operate at global scale and share a common cost structure: the platform is built once and sold many times. Service-led operators grow by adding delivery capacity, so revenue and headcount move together and margins compress as the client base widens.

Cyberoo takes the technology side from the vendor model and the client side from the service-led one. Cypeer, CSI and Keatrix are developed in-house and run on the Company's own cloud infrastructure. Like the service-led operators, Cyberoo owns the end client relationship: it runs its own 24/7 I-SOC and handles remediation itself, rather than passing it to the client or to a third party. However, it does not carry their scaling constraint because the service runs on platforms it owns. ORBIS extends that base, facilitating cross-/up-selling so an existing client can be sold into the others without a proportional increase in headcount, sustaining margins.

Cyberoo's Competitive Landscape

Company	Country	Cluster	Rev. growth CAGR FY23-25	EBIT margin avg FY23-25	Rule of 40 Score
Fortinet		Global vendor	+13%	28%	42
Qualys		Global vendor	+10%	31%	41
CrowdStrike		Global vendor	+25%	-3%	22
Rapid7		Global vendor	+5%	-2%	3
SentinelOne		Global vendor	+27%	-44%	-17
Yarix		Service-led	+16%	19%	36
secunet		Service-led	+8%	11%	19
HWG Sababa		Service-led	+13%	4%	17
Tinexta Cyber		Service-led	-3%	0%	-3
Cyberoo			+18%	+25%	42

* Cyberoo's FY25 covers the fifteen months to 31 March 2026 following a change of financial year end.

Source: company filings, KT&Partners elaboration.

¹³ Gartner, *Market Guide for Managed Detection and Response*, Pete Shoard, Andrew Davies, Angel Berrios, 1 October 2025

Historical Financials

We analyze Cyberoo's historical financials over the FY22-FY25 period. The FY25 reporting period spans fifteen months, covering 1 January 2025 to 31 March 2026, following the Group's decision to shift its fiscal year-end from 31 December to 31 March in order to align the reporting calendar with the operating cycles of its commercial partners: with activity historically peaking in December, a 31 December close captured the balance sheet at its most inflated point, and moving the year-end to March, past the seasonal peak, allows working capital to normalize before each reporting date. All prior years (FY22-FY24) are twelve-month periods ending 31 December, making FY25 figures not directly comparable.

Revenues Breakdown Analysis

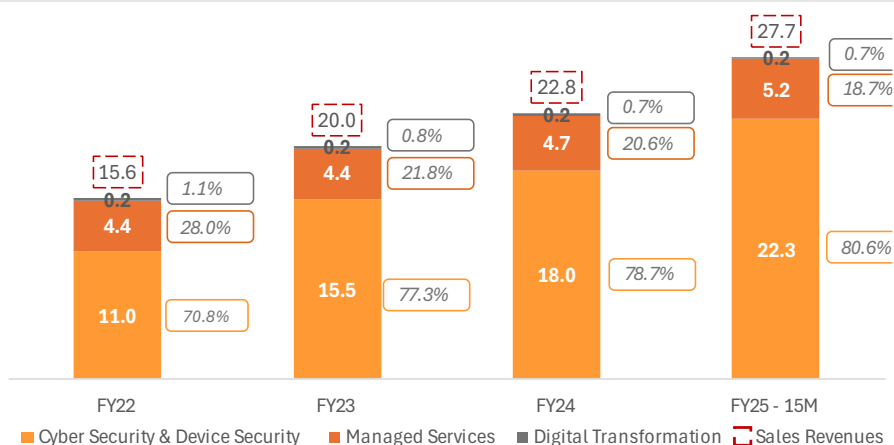
Cyberoo's top line has expanded through a sustained acquisition of new clients on a proprietary technology base built and scaled over the period, with three distinct business units of very different weight and momentum.

Cyber Security & Device Security is the engine of the Group and the source of essentially all its growth. Revenues rose from €11.0mn in FY22 to €18.0mn in FY24 and reached €22.3mn in the fifteen-month FY25, (approximately €20.0mn on a 12-month pro forma, or +15%). Two forces drive this trajectory. First, a rapidly expanding client base: the Italian mid-market is progressively adopting managed cybersecurity as a permanent line item rather than a project spend, and Cyberoo has captured this shift with a distinctive value proposition built around proprietary MDR technology, competitive pricing for the mid-market and a distribution network that reaches customers system integrators do not serve efficiently. Second, the continuous evolution of the technology stack itself: Cypeer, the core of the MDR platform, has been developed since 2016 and scaled commercially from 2021, and each generation of the platform has broadened the addressable use cases and supported the acquisition of larger accounts. Roughly half of divisional revenues in any given year come from the existing client base and half from new logos, a mix that reflects both the recurring nature of the offering and the intensity of commercial acquisition.

Managed Services (monitoring, administration and maintenance of clients' IT infrastructure) and Digital Transformation (digitalization business) are mature, secondary lines with limited strategic weight. Managed Services grew modestly from €4.4mn in FY22 to €5.2mn in the fifteen-month FY25, while Digital Transformation is immaterial at below €0.2mn throughout. Neither has been a growth driver, and their combined weight on Sales Revenues has declined progressively as the cybersecurity franchise has scaled.

The bridge from Sales Revenues to the Value of Production reflects capitalised internal development, which has run at approximately €1.7mn per year through FY22-FY24, stepping up to €3.0mn in the fifteen-month FY25 on the intensification of Keatrix development, and a modest stream of other revenues. On this basis, the Value of Production rose from €17.6mn in FY22 to €25.0mn in FY24 and reached €31.2mn in the fifteen-month FY25, with the underlying twelve-month growth in the mid-to-high teens across the period.

Revenues Breakdown per Business Unit (€mn) – FY22-25 (15M)



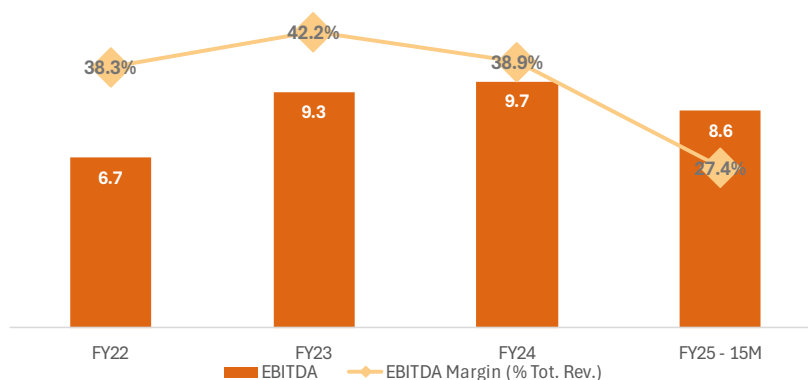
Source: KT&Partners' Elaboration on Company Data (FY22-25)

Profitability Analysis

Cyberoo's cost base reflects a proprietary-product model, in which the dominant cost is the internal development effort behind its own platforms, and the resulting gross margin is structurally high. The cost of goods sold, which captures development activity and the device purchases tied to the MSSP business, is small relative to revenues precisely because the products are proprietary: gross margin has historically stood at high levels, averaging c.75% in the last three years. Below the gross line, personnel is the principal cost, historically at roughly 25-27% of VoP, alongside a services line that captures external collaborators, foreign subsidiaries and the outsourced share of product development, which has run historically at c.7-10% of VoP.

EBITDA grew in absolute terms from €6.7mn in FY22 to €9.3mn in FY23 and €9.7mn in FY24, although margins, after peaking at 42.2% in FY23 and holding at 38.9% in FY24, compressed to 27.4% in FY25 as EBITDA declined to €8.6mn (15 months). This compression is the cost of a deliberate investment cycle rather than a deterioration in the underlying economics. The elevated FY22-FY23 margins reflected the maturity of Cypeer, developed from 2016 and delivering strong returns once its initial investment phase was behind it; from late 2024, the Group layered on a new wave of investment that temporarily depressed profitability, chiefly the Polish expansion, opened in 2023 with the bulk of commercial build-out, marketing and rebate spending concentrated in 2024, the early-stage entry into Spain, and more recently the development of Keatrix and the ORBIS ecosystem, whose returns have yet to materialise.

EBITDA (€mn) and EBITDA margin (on Total Revenues, %) – FY22-25 (15M)



Source: KT&Partners' Elaboration on Company Data (FY22-25).

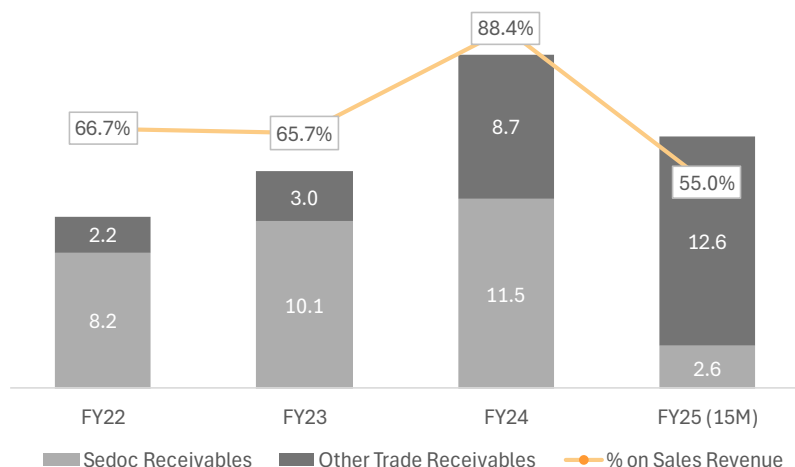
Below EBITDA, the picture is consistent with a technology group that capitalises a meaningful share of its development effort. D&A reflects the amortisation of the capitalised platforms, and net financial charges have remained contained. Net income declined to €2.6mn in the fifteen-month FY25 from €4.4mn in FY24, tracking the same investment-driven compression visible at the EBITDA level.

Capital Structure & Cash Flow Analysis

Cyberoo runs a proprietary-technology balance sheet, in which fixed assets are dominated by the intangible base that houses its own platforms. Net fixed assets reached €22.5mn at FY25, up markedly from prior years on the increase in intangibles connected to software, artificial intelligence, Keatrix, ORBIS and R&D. This reflects a business that consistently allocates a significant share of revenues to capital expenditure: capex ran at roughly €4.3mn in FY23 and €5.2mn in FY24, before stepping up to €13.7mn in the fifteen-month FY25, a figure that includes the €4.7mn shareholder loan extended to Cyberoo Capital and captures the peak of the Group's investment cycle. Roughly a fifth of revenues is directed to investment in any given year, almost entirely on the internal development of proprietary products rather than on tangible assets.

Working capital, and trade receivables specifically, was the focus of investors in recent years. Receivables built up materially through the growth phase, rising from roughly €13mn in FY23 towards €20mn in FY24, with DSO peaking at around 265 days in FY24 against a historical average just above 200 days, driven by a structural payment mismatch: end clients have progressively shifted from upfront licence fees to instalment payments spread over the contract duration, while Cyberoo continues to pay its own suppliers on ordinary terms, and the timing gap accumulated on the balance sheet. The dynamic was compounded by the concentrated exposure to related party Sedoc Digital Group, which peaked at €14.2mn in 1H24.

Both pressures have since eased visibly: the Sedoc exposure was cut to €2.6mn at FY25, down roughly 78% from €11.5mn at FY24 and running ahead of the agreed repayment schedule, and net working capital fell to €4.7mn at FY25 from €11.9mn at FY24, evidence of the success of the wind-down strategy and of the structural measures put in place to contain the receivables build-up. Chief among these is Cyberoo Capital, the vehicle through which the Group offers its solutions under operating lease arrangements: in FY25, still outside the consolidation perimeter, it began to absorb the client shift toward instalment-based payments, moving the associated exposure out of consolidated trade receivables. From FY26 the vehicle is consolidated, bringing its assets back into the Group perimeter, but the exposure re-enters as a leased-asset book rather than as trade receivables.

Trade Receivables Breakdown (FY22-25 15M): Focus on Sedoc & Incidence on Sales

Source: KT&Partners' Elaboration on Company Data (FY22-25).

Over the three years the Group's net cash position moved from €3.9mn at FY23 to a near-neutral level at FY24, before settling at €0.8mn at FY25, a trajectory that reflects the receivables cycle far more than the underlying profitability. FY24 was the year in which the build-up of trade receivables absorbed cash most heavily, compressing operating cash flow to just €1.7mn despite EBITDA of €9.7mn, and eroding the net cash accumulated in prior years. FY25 reversed that dynamic: operating cash flow recovered to €14.1mn, drawn roughly half from EBITDA and half from the release of working capital as total trade receivables fell to €15.2mn from €20.2mn and the fifteen-month period closed past the seasonal December peak. Cyberoo Capital, still outside the consolidation perimeter at FY25, had by then begun to absorb part of the instalment-based demand, with the Group carrying an intercompany receivable of c.€1.2mn toward the vehicle: a first, still-limited sign of the structural role it is expected to play in containing trade receivables from FY26 onwards. The FY25 reduction itself was driven mainly by the Sedoc operation and factoring, and this cash was almost entirely reinvested, with €13.7mn of capex spanning the peak of internal development and the €4.7mn deployed into Cyberoo Capital (to be eliminated in FY26E through the vehicle's consolidation), leaving free cash flow only marginally positive and the net cash position essentially unchanged year-on-year, an investment-intensive period funded in full from internally generated resources.

Deconstructing Forecasts

Our forecasts are built bottom-up and reflect organic growth only, though Cyberoo's positioning does not exclude expansion through external lines.

We expect Value of Production to grow from c.€31.8mn in FY26E at a 14% CAGR over the forecasted period, driven by the ORBIS model under which each product becomes an entry point into the full portfolio. Regulatory compliance is the demand engine we expect to feed this hardest, with NIS2 entering through Docetz and pulling clients toward monitoring (Cypeer and the Cyber Security Suite), training (Keatrix) and regulator-compliant reporting (Titaan) under an ongoing maintenance requirement that makes the demand recurring.

The same logic drives international growth: Keatrix, a shelf product that opens foreign markets at low cost, gains the initial foothold, and ORBIS then extends the relationship into cross- and up-selling of the higher-value lines.

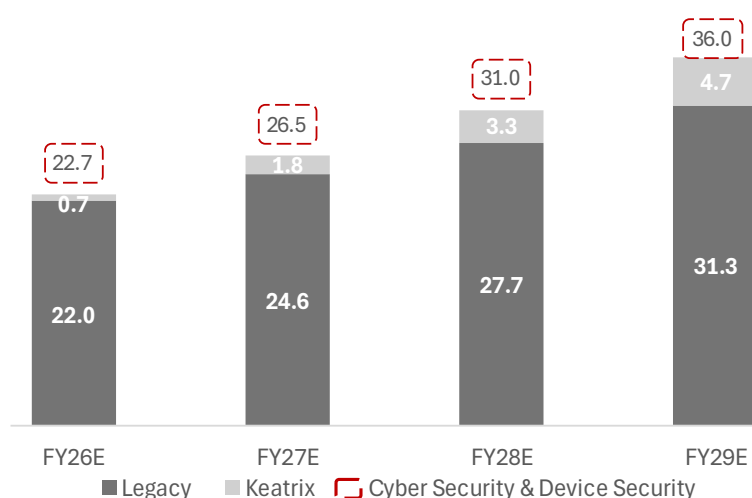
As mix shifts toward these proprietary, scalable products, we expect EBITDA margin to gradually return to pre-FY25 levels, reaching c.40% by FY29E, while the structural measures on working capital keep the balance sheet in a growing net-cash position.

We model Cyber Security & Device Security revenues of approximately €22.7mn in FY26E (12 months ending March 2027), growing to €36.0mn by FY29E at a 16.6% FY26-29E CAGR, with both legacy business and new products driving growth.

The **core MDR business**, which we model at c.€22.0mn in FY26E, up 10% YoY against a twelve-month FY25 base of c.€20mn (€22.3mn on a reported 15-month FY25). From FY27E we assume linear organic growth of 12-13% per year, reaching c.€31.3mn by FY29E, broadly in line with the pace of the Italian cybersecurity market (c.13% 2025-30E CAGR¹⁴): we assume no market share gains, reflecting an ongoing rationalization of commercial intake, with tighter pricing discipline on new-client acquisition and the sacrifice of selected lower-value contracts in favour of a higher-quality, higher-margin client base.

Keatrix is the second driver and the new layer within the division. We model the contract book billed each year, from c.€1.8mn in FY26E to c.€7.0mn by FY29E, and we model these as revenues as follows: 40% in the year of billing, 30% in the following year and the remaining 30% in the third. Each year's P&L therefore combines 40% of the new book with the deferred portions released from prior years, while the unrecognised balance sits as deferred income.

Cyber Security & Device Security Revenue Breakdown by Offering (€mn), FY26E-FY29E



Source: KT&P's Estimates (FY26E-29E).

¹⁴ Osservatorio Cybersecurity & Data Protection, Politecnico di Milano, (February 2026); Mordor Intelligence.

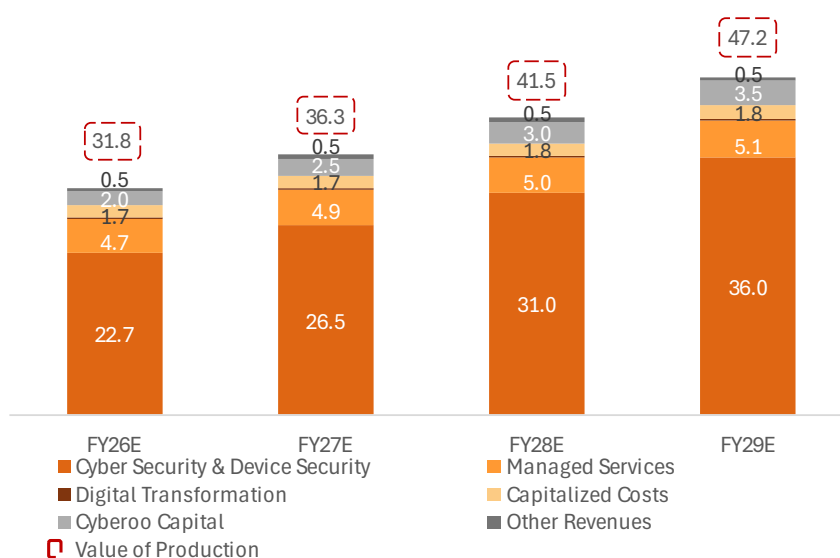
Managed Services and Digital Transformation are mature, stable lines in our estimates. We model Managed Services revenues of c.€4.7mn in FY26E, from €5.2mn 15M FY25 base, growing 5% in FY27E and 2% per year thereafter; Digital Transformation remains stable at c.€0.2mn throughout the plan. Both serve legacy client relationships and complete the Group's ability to act as a single technology partner, while commercial focus and investment concentrate on the cybersecurity ecosystem, so their combined weight on Sales Revenues declines from roughly 18% in FY26E to 13% by FY29E.

From FY26E, a new revenue stream enters the Group's accounts with the consolidation of **Cyberoo Capital**. The subsidiary acquires eligible multi-year rights, licenses or bundles from third-party suppliers, resellers or market counterparties, making them available to final customers through operating-lease structures, and earns periodic fees that embed both a capital and an interest component, recognized on an accrual basis. We model the €15mn facility approved for the subsidiary as being deployed over the four-year plan and captured within capex, of which, given the deferred profile of the rental fees, roughly two-thirds is progressively recognized through the P&L over the same horizon, starting at c.€2.0mn in FY26E and rising by around €0.5mn per year thereafter.

Other Revenues, comprising ancillary income and operating contributions, are held at their historical level of approximately €0.5mn per year throughout the plan.

Finally, we keep capitalised development costs broadly stable in absolute terms at their historical annual level of approximately €1.7-1.8mn (excluding the exceptional €3.0mn recorded in the fifteen-month FY25), consistent with the Group's steady investment in research and development on its proprietary platforms. Overall, we estimate a **Value of Production** of c.€31.8mn in FY26E, up against the fifteen-month FY25 base of €31.2mn, and reaching c.€47.2mn by FY29E, at a 14% FY26-29E CAGR.

Value of Production Breakdown (€mn), FY26E-FY29E



Source: KT&P's Estimates (FY26E-29E).

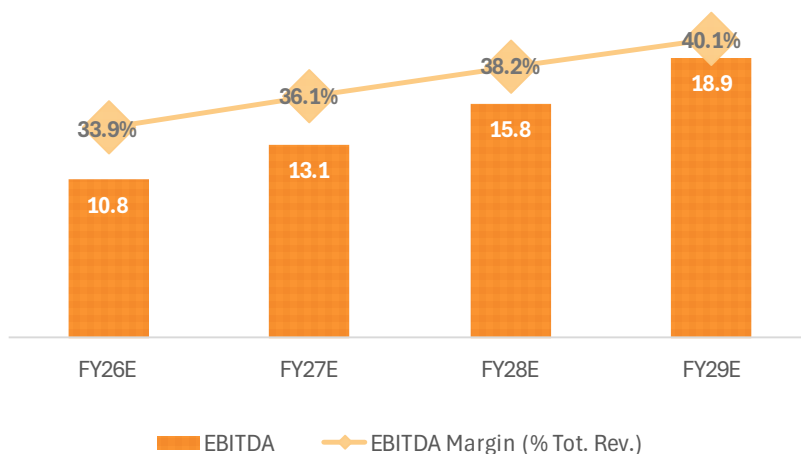
EBITDA: Margin Recovery First, Expansion Later

We estimate EBITDA of approximately €10.8mn in FY26E, +26% YoY against the €8.6mn of 15M FY25, with the margin on Value of Production recovering to 33.9% from 27.4% as the investment cycle that compressed FY25 profitability normalizes. From there, we model EBITDA reaching €18.9mn by FY29E, a CAGR of roughly 20%, with the margin reaching gradually c.40%.

The expansion rests on two layers. First, operating leverage on a largely fixed cost base. Personnel, modelled at c.€8.0mn in FY26E (€9.4mn in 15M FY25), grows around 5% per year in absolute terms, well below the pace of the top line as its incidence on VoP is expected to decline from roughly 25% toward 20% between FY26E and FY29E. Services costs, at c.€2.9mn in FY26E (€3.5mn in 15M FY25), improve only slightly as a share of VoP, from c.9% in FY26E to c.8% by FY29E, remaining above the c.7% of FY23-24 as the externalised development effort tied to Keatrix keeps them structurally higher than in the past. The remaining cost lines, from raw materials to rentals, are held broadly flat as a share of VoP. This operating leverage is partly the nature of a proprietary-software business, where incremental volumes carry little variable cost, and partly the growing weight of shelf products like Keatrix, which scale through the existing commercial structure with no additional headcount.

Second, part of the expansion is structural to Cyberoo Capital, whose lease revenues flow to EBITDA at what we assume being c.80% margin: its own service costs, which we model at roughly 20% of the vehicle's revenues (c.€0.4-0.7mn per year over the plan), sit above the line, while the bulk of the acquisition cost of the contract book is capitalised and surfaces below the operating line as D&A.

EBITDA (€mn) and EBITDA margin (on Total Revenues, %) – FY26E-29E



Source: KT&P's Estimates (FY26E-29E).

D&A steps up over the plan, from approximately €5.9mn in FY26E (€4.2mn in 15M FY25) to €7.9mn by FY29E, absorbing both the amortisation of the capitalised development and the depreciation of Cyberoo Capital's contract book, which we model at roughly 70% of the vehicle's revenues each year. The remaining c.10% of those revenues flows as an interest expense on the funding, so that net financial charges increase over the plan, and the two together reabsorb almost the entire c.80% EBITDA margin of Cyberoo Capital, leaving its contribution to net income essentially null.

Structural De-Risking of Working Capital

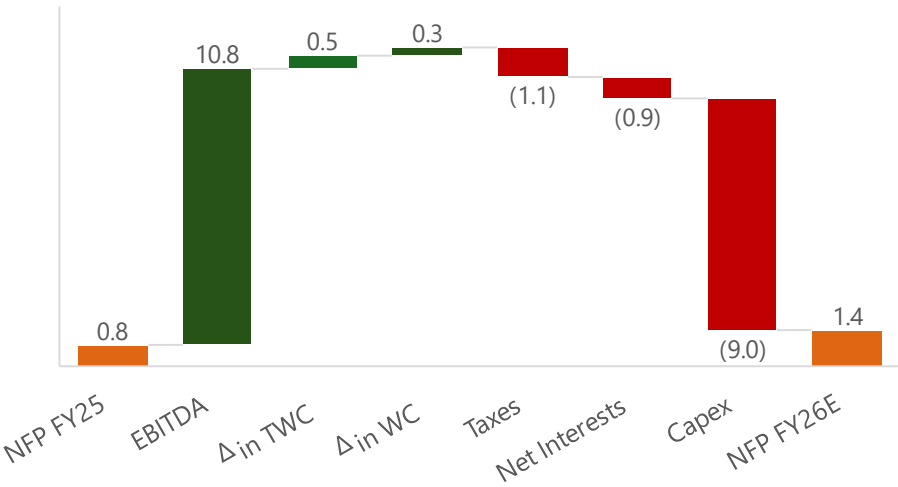
Net fixed assets reach c.€25.6mn in FY26E (ending March 2027), driven by the intangible base. The consolidation of Cyberoo Capital is, in cash terms, largely a reclassification: the €4.7mn intercompany financing carried among financial assets at FY25 is eliminated and replaced by the vehicle's contract book within intangibles, with no cash outflow at Group level.

Beyond this reclassification, we estimate FY26E capex of c.€9.0mn, comprising c.€5.2mn of organic intangible investment, still elevated by ongoing R&D, c.€3.0mn related to Cyberoo Capital's lease book, and c.€1.0mn of tangible capex broadly in line with previous years. Thereafter we assume organic intangible capex normalizes to c.€4mn in FY27E and grows 10% p.a. in FY28-29E, tangible capex holds at c.€1mn, and Cyberoo Capital adds new lease investments that bring the vehicle to its €15mn budgeted cumulative deployment by the end of the plan.

Trade receivables are the key working-capital item and the clearest evidence of the Group's structural de-risking. Having peaked during the past investment cycle, receivables are set on a normalizing path: we model a DSO of approximately 160 days in FY26E, standing at roughly €14.7mn, growing organically with the business thereafter. Two dynamics underpin this. First, the Sedoc receivable, already down to €2.6mn at FY25 ahead of its repayment schedule, continues to decline in FY26E, while remaining a physiological component of the balance sheet given that Sedoc is also a commercial client. Second, and more structurally, the measures put in place to address the payment mismatch, Cyberoo Capital, pro-soluto factoring and the shift toward distributors that better manage credit, move the growing client preference for instalment-based payments off trade receivables and into the leased-asset book, so that top-line growth no longer translates mechanically into receivables inflation. As a result, trade working capital stabilizes at around 33-34% of Value of Production over the plan, well below the historical average of the last three years (c.50%).

Operating cash flow forecasted at €9.6mn in FY26E funds the investment plan internally, and consistent with the Group's track record we assume no dividend distribution. The net financial position thus improves to c.€1.4mn of net cash at FY26E, from €0.8mn at FY25, and improve progressively thereafter, on Free Cash Flow conversion (from EBITDA) averaging c.15% in FY27-29.

Net Financial Position (NFP) Bridge – FY25-26E



Source: KT&Partners' Elaboration on Company Data (2025), KT&P's Estimates (2026)

FY22-FY29E Income Statement (€mn)

€ Million	FY22	FY23	FY24	FY25 (15M)	FY26E	FY27E	FY28E	FY29E
Sales Revenues	15.6	20.0	22.8	27.7	27.6	31.6	36.2	41.4
<i>Cyber Security & Device Security</i>	11.0	15.5	18.0	22.3	22.7	26.5	31.0	36.0
<i>Managed Services</i>	4.4	4.4	4.7	5.2	4.7	4.9	5.0	5.1
<i>Digital Transformation</i>	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Other Revenues	0.3	0.3	0.4	0.5	0.5	0.5	0.5	0.5
Cyberoo Capital	-	-	-	-	2.0	2.5	3.0	3.5
Capitalized costs	1.7	1.7	1.7	3.0	1.7	1.7	1.8	1.8
Total Revenues	17.6	22.0	25.0	31.2	31.8	36.3	41.5	47.2
Growth %	n.m.	25.4%	13.6%	24.8%	1.7%	14.3%	14.3%	13.8%
COGS	(3.8)	(5.0)	(6.3)	(8.7)	(8.7)	(10.0)	(11.4)	(13.0)
Gross Profit	13.8	17.0	18.7	22.5	23.0	26.3	30.1	34.2
Gross Margin (% on Tot. Rev.)	78.3%	77.3%	74.8%	72.1%	72.5%	72.5%	72.5%	72.5%
Services	(2.0)	(1.6)	(1.8)	(3.5)	(2.9)	(3.2)	(3.5)	(3.8)
Rental Costs	(0.3)	(0.3)	(0.4)	(0.5)	(0.5)	(0.6)	(0.7)	(0.8)
Personnel Expenses	(4.6)	(5.6)	(6.6)	(9.4)	(8.0)	(8.4)	(8.8)	(9.3)
Other Expenses	(0.1)	(0.2)	(0.2)	(0.5)	(0.5)	(0.5)	(0.6)	(0.7)
EBITDA	6.7	9.3	9.7	8.6	10.8	13.1	15.8	18.9
EBITDA Margin (% on Tot. Rev.)	38.3%	42.2%	38.9%	27.4%	33.9%	36.1%	38.2%	40.1%
Growth %	n.m.	37.8%	4.7%	-12.0%	25.6%	21.9%	20.9%	19.5%
D&A and Provisions	(2.4)	(3.2)	(3.3)	(4.2)	(5.9)	(6.8)	(7.3)	(7.9)
EBIT	4.3	6.1	6.5	4.3	4.8	6.3	8.5	11.0
EBIT margin (% on Tot. Rev.)	24.7%	27.6%	25.9%	13.8%	15.2%	17.4%	20.6%	23.3%
Financial Income/(Expenses)	(0.2)	(0.4)	(0.2)	(0.5)	(0.9)	(0.9)	(1.0)	(1.0)
EBT	4.1	5.7	6.2	3.8	4.0	5.4	7.6	10.0
Taxes	(1.3)	(1.7)	(1.9)	(1.2)	(1.1)	(1.5)	(2.1)	(2.8)
Tax Rate	32.0%	30.2%	29.8%	32.7%	28.0%	28.0%	28.0%	28.0%
Net Income	2.8	4.0	4.4	2.6	2.9	3.9	5.5	7.2
Net margin (% on Tot. Rev.)	15.9%	18.0%	17.5%	8.2%	9.0%	10.7%	13.1%	15.2%

Source: KT&Partners' Elaboration on Company Data (2022-2025), KT&P's Estimates (2026-2029)

FY22-FY29E ND Bridge (€mn)

€ Million	FY23	FY24	FY25 (15M)	FY26E	FY27E	FY28E	FY29E
EBITDA	9.3	9.7	8.6	10.8	13.1	15.8	18.9
Income Taxes	(1.7)	(1.9)	(1.2)	(1.1)	(1.5)	(2.1)	(2.8)
Change in TWC	(4.1)	(6.8)	5.7	0.5	(1.8)	(2.0)	(1.6)
Other Changes in WC	1.7	0.6	1.5	0.3	0.9	0.9	0.5
Net Financial Income (Expenses)	(0.4)	(0.2)	(0.5)	(0.9)	(0.9)	(1.0)	(1.0)
Operating Cash Flow	4.8	1.5	13.9	9.6	9.9	11.6	14.0
Capex	(4.3)	(5.2)	(13.7)	(9.0)	(8.0)	(9.4)	(10.8)
Free Cash Flow	0.5	(3.8)	0.2	0.6	1.9	2.2	3.2
Change in Equity	1.5	-	(0.4)	-	-	-	-
Adjustments	-	-	1.0	-	-	-	-
Change in NFP	2.1	(3.8)	0.8	0.6	1.9	2.2	3.2
Begin NFP	(1.9)	(3.9)	(0.0)	(0.8)	(1.4)	(3.3)	(5.5)
End NFP	(3.9)	(0.0)	(0.8)	(1.4)	(3.3)	(5.5)	(8.7)

Source: KT&Partners' Elaboration on Company Data (2022-2025), KT&P's Estimates (2026-2029)

Valuation

Based on Cyberoo's projected financials, we performed a valuation of the company using two standard methodologies: market multiples and Discounted Cash Flow (DCF).

- **Market Multiples (EV/EBITDA, EV/EBIT and P/E):** using a peer group of seven listed comparables, we applied the median FY26E and FY27E EV/EBITDA, EV/EBIT and P/E multiples to Cyberoo's forecasted financials, with a 25% liquidity and size discount. Averaging the results of the three multiples yields an implied equity value of €100.6mn.
- **Discounted Cash Flow (DCF):** we projected Cyberoo's Free Cash Flows over the FY26E to FY29E period, extended them over FY30E to FY33E at a 10% annual growth rate, and discounted them using a WACC of 9.0% and a terminal growth rate of 3.0%. This approach returns an implied equity value of €73.1mn.

Valuation Recap

	Equity Value (€mn)	Value per share (€)
EV/EBITDA	102.6	2.51
EV/EBIT	111.9	2.74
P/E	87.2	2.13
Average Multiples	100.6	2.50
DCF	73.1	1.80
Average	86.8	2.15

Source: KT&P's estimates, Factset consensus data

By averaging the outputs of both methodologies, we derive a fair equity valuation of €86.8mn, corresponding to a fair value of €2.15 per share, 68% upside on the current share price of €1.28. This implies an EV/EBITDA multiple of 8.0x on FY26E.

KT&Partners' Implied Multiples

	FY25	FY26E	FY27E
EV/EBITDA implied	10.0x	8.0x	6.6x
EV/EBIT implied	19.9x	17.8x	13.6x
P/E implied	33.8x	30.3x	22.2x

Source: KT&P's estimates, Factset consensus data

Peers Overview

To assess Cyberoo's valuation, we selected a peer group of seven listed companies that reflects its hybrid model, which combines proprietary technology with managed services. The sample includes two clusters. The first comprises cybersecurity vendors that develop their own technology platforms: Fortinet, Okta, F-Secure and CY4Gate. The second comprises Italian IT operators with a high share of recurring managed and cloud services: WIIT, Sys-Dat and DHH. The two clusters differ in scale, product focus and geographic reach, but together they cover the two components of Cyberoo's business model, its technology and its service delivery.

Tinexta, historically one of the main listed Italian players in digital trust and cybersecurity with FY25 revenues around €450mn, was taken private in July 2026 by Advent International and Nextalia at 10.6x FY25 adjusted EBITDA multiple, and is therefore excluded from our sample.

The selected sample includes:

Fortinet, Inc.: listed on NASDAQ (FTNT-US), with a market capitalization of c.€110bn, Fortinet is a US cybersecurity group headquartered in Sunnyvale, California. The company positions itself at the convergence of networking and security, with an offering built around its FortiGate firewalls and expanding into Unified SASE and Security Operations. Its model combines hardware, software and subscription services sold mainly through channel partners. While operating on an entirely different scale, Fortinet shares with Cyberoo a strategy based on proprietary technology and a growing contribution from security operations services. In FY25, the group reported revenues of \$6.80bn, up 14% YoY.

Okta, Inc.: listed on NASDAQ (OKTA-US), with a market capitalization of c.€29.1bn, Okta is a US software company specializing in identity and access management. The company defines itself as the leading independent identity partner, providing cloud based solutions that allow organizations to secure access for employees, customers and, increasingly, AI agents. Its business is almost entirely subscription based. Okta shares with Cyberoo a focus on a specific layer of the cybersecurity stack delivered through a recurring revenue model. In FY26 (ended January 31st, 2026), total revenue reached \$2.919bn, up 12% YoY, with subscription revenue of \$2.855bn.

F-Secure Oyj: listed on Nasdaq Helsinki (FSECURE-FI), with a market capitalization of €246mn, F-Secure is a Finnish cybersecurity company focused on consumer security. The group distributes its solutions mainly through partners such as telecom operators and financial institutions, with the partner channel accounting for 82% of FY25 revenue, and is focusing its growth on Embedded Security and Scam Protection. F-Secure shares with Cyberoo a proprietary technology base and a go to market model that relies on indirect channels rather than direct sales. In FY25, the group reported revenues of €145.7mn, broadly stable YoY, with an adjusted EBITA margin of 34.5%.

CY4Gate S.p.A.: listed on Euronext STAR Milan (CY4-IT), with a market capitalization of €248mn, CY4Gate is an Italian group active in cyber intelligence and cybersecurity. Its offering spans forensic intelligence, decision intelligence and security solutions, serving mainly government, defence and enterprise customers. In FY25, revenues were split 49% in Italy and 51% abroad. CY4Gate is the Italian listed player closest to Cyberoo in terms of sector and technology development, although with a stronger exposure to the public and defence segments. In FY25, the group reported operating revenues of €99.1mn, up 37% YoY, and EBITDA of €20.8mn, with a 20.4% margin.

WIIT S.p.A.: listed on Euronext STAR Milan (WIIT-IT), with a market capitalization of €755mn, WIIT is an Italian provider of cloud computing services for critical enterprise applications, operating mainly in Italy and Germany, where it has grown through acquisitions. Its model is

based on owned data centers and managed services, with recurring revenues of €136.6mn representing 88.7% of the total. WIIT shares with Cyberoo a high value managed services model aimed at enterprise customers and a strong weight of recurring revenues. In FY25, the group reported adjusted revenues of €167.9mn, up 5.9% YoY, with an adjusted EBITDA margin of 39.8%.

Sys-Dat S.p.A.: listed on Euronext STAR Milan (SYS-IT), with a market capitalization of €271mn, Sys-Dat is an Italian ICT group. Its offering includes ERP, CRM and process management software, business intelligence, cloud services, cybersecurity, document management and networking, with vertical solutions for sectors such as manufacturing, retail, healthcare and fashion. The group combines organic growth with a buy and build strategy. Sys-Dat shares with Cyberoo a customer base of Italian companies and a service model with a high share of recurring revenues, which rose to 83% of the total in FY25. In FY25, revenues reached €89.6mn, up 55.9% YoY, driven by 9.8% organic growth and the acquisition of A&C Group, with EBITDA of €17.1mn.

Dominion Hosting Holding S.p.A. (DHH): listed on Euronext Growth Milan (DHH-IT), with a market capitalization of €130mn, DHH is an Italian group that provides integrated B2B cloud and internet services in Italy, Croatia, Slovenia, Serbia, Switzerland and Bulgaria. Its activities include cloud computing, hosting, business connectivity and AI infrastructure. DHH shares with Cyberoo its listing on the same market, a comparable size and a subscription based model with 91% of revenues deriving from subscriptions. In FY25, the group reported revenues of €41.8mn, up 13% YoY.

Market Multiples Valuation

The selected peer group trades at a median FY26E EV/EBITDA of 12.2x, EV/EBIT of 29.8x and P/E of 37.8x. On the same metrics, Cyberoo trades at 4.8x, 10.6x and 18.2x, discounts of 61%, 64% and 52% respectively. We do not believe the gap is explained by fundamentals. Cyberoo's average FY25 to FY27E EBITDA margin of 37.1% sits well above the peer median of 30.1%, while its 2024 to 2027E sales CAGR of 11.4% is in line with the peer median of 11.7%. The main differentiating factor is scale: Cyberoo's market capitalization of €52mn compares with a peer median of €271mn. We therefore apply a 25% liquidity and size discount to the peer multiples.

We base our valuation on median rather than average multiples. The two US vendors in the sample, Okta and Fortinet, trade at FY26E EV/EBITDA multiples of 34.6x and 39.0x, which lift the peer average to 18.4x against a median of 12.2x. The median neutralizes this skew without requiring the exclusion of companies that are relevant benchmarks for the cybersecurity software segment.

Peers Comparison

Company Name	Exchange	Market Cap	Avg. EBITDA Margin (25-27)	CAGR Sales (24-27)	EV/EBITDA			EV/EBIT			P/E		
					2025	2026	2027	2025	2026	2027	2025	2026	2027
WIIT SpA	Milan	755	41.9%	4.7%	16.8x	15.6x	14.0x	34.2x	29.8x	24.0x	66.7x	48.7x	31.7x
Okta, Inc. Class A	NASDAQ	29,092	27.7%	8.3%	39.6x	34.6x	30.4x	41.0x	36.5x	32.3x	52.2x	45.3x	40.7x
CY4Gate SpA	Milan	248	21.2%	19.7%	12.3x	10.3x	8.9x	n.m	48.8x	24.6x	n.m.	n.m.	68.2x
F-Secure Oyj	Helsinki	246	32.9%	2.3%	7.5x	8.4x	7.5x	11.0x	12.5x	10.8x	11.0x	15.4x	10.4x
Sys-dat S.p.A.	Milan	271	19.7%	26.0%	14.2x	12.2x	10.7x	23.3x	19.0x	16.2x	36.1x	29.9x	25.3x
Fortinet, Inc.	NASDAQ	110,275	37.9%	11.7%	49.8x	39.0x	35.0x	52.5x	41.2x	37.0x	61.9x	48.5x	44.3x
DHH S.p.A	Milan	130	30.1%	20.1%	9.6x	8.8x	7.3x	17.1x	16.5x	13.4x	29.2x	30.4x	23.4x
Average Peer Group		20,145	30.2%	13.2%	21.4x	18.4x	16.3x	29.8x	29.2x	22.6x	42.8x	36.3x	34.9x
Median Peer Group		271	30.1%	11.7%	14.2x	12.2x	10.7x	28.7x	29.8x	24.0x	44.1x	37.8x	31.7x
Cyberoo S.p.A.	Milan	52	37.1%	11.4%	6.0x	4.8x	3.9x	11.9x	10.6x	8.1x	20.3x	18.2x	13.4x

Source: Factset data, KT&Partners' elaboration

Applying the FY26E and FY27E median multiples, net of the 25% discount, we obtain an equity value of €102.6mn (€2.51ps) through EV/EBITDA, €111.9mn (€2.74ps) through EV/EBIT and €87.2mn (€2.13ps) through P/E.

Valuation Multiples

EV/EBITDA			EV/EBIT			P/E		
Multiple Valuation (€mn)	2026E	2027E	Multiple Valuation (€mn)	2026E	2027E	Multiple Valuation (€mn)	2026E	2027E
EV/EBITDA Comps	12.2x	10.7x	EV/EBIT Comps	29.8x	24.0x	P/E Comps	37.8x	31.7x
Cyberoo EBITDA	10.8	13.1	Cyberoo EBIT	4.8	6.3	Cyberoo Net Income	2.9	3.9
Enterprise value	130.8	140.6	Enterprise value	144.0	152.1	Equity Value	108.5	123.9
Average Enterprise value	135.7		Average Enterprise value	148.1		Average Equity value	116.2	
Liquidity/Size Discount	25%		Liquidity/Size Discount	25%		Liquidity/Size Discount	25%	
Enterprise Value Post-Discount	101.8		Enterprise Value Post-Discount	111.0		Equity Value Post-Discount	87.2	
FY25 Net Debt	(0.8)		FY25 Net Debt	(0.8)		Number of shares (mn)	40.9	
FY25 Minorities	-		FY25 Minorities	-		Price per Share	2.13	
Equity Value	102.6		Equity Value	111.9				
Number of shares (mn)	40.9		Number of shares (mn)	40.9				
Price per Share	2.51		Price per Share	2.74				

Source: Factset data, KT&Partners' elaboration

DCF Valuation

We have conducted our valuation using an eight-year DCF model, based on 9.0% WACC.

In our DCF model, we start from EBIT, taxed at 28% to derive NOPAT, then add back D&A and account for changes in working capital and capex. Consistently, in the bridge from Enterprise Value to Equity Value we use FY25 NFP, a net cash position of €0.8mn as of March 31st, 2026.

We discounted FY26E to FY29E annual cash flows derived from our estimates. Over FY30E to FY33E, we extended FCF at a 10% annual growth rate. This rate sits below both our FY26E to FY29E VoP CAGR of c.14% and the expected growth of the Italian cybersecurity market (c.13%¹⁵). We then applied a terminal growth rate of 3.0%, reflecting the structural, regulation driven demand for cybersecurity services. Finally, we carried out a sensitivity analysis on the terminal growth rate (+/- 0.25%) and on WACC (+/- 0.25%).

According to our valuation method, our estimated fair value is equal to €1.80ps.

FY26-FY233E ND Bridge (€mn)

€mn	Mar '27E	Mar '28E	Mar '29E	Mar '30E	Mar '31E	Mar '32E	Mar '33E	Mar '34E
EBIT	4.8	6.3	8.5	11.0				
- Taxes on EBIT	(1.4)	(1.8)	(2.4)	(3.1)				
Tax rate (%)	28%	28%	28%	28%				
NOPAT	3.5	4.6	6.1	7.9				
+ D&A	5.9	6.8	7.3	7.9				
+ Other Value adjustments	-	-	-	-				
Net operating cash flow	9.4	11.3	13.5	15.9				
-/+ Change in working capital	0.8	(0.8)	(1.2)	(1.1)				
- CAPEX	(9.0)	(8.0)	(9.4)	(10.8)				
Free Cash Flow	1.2	2.5	2.9	3.9	4.3	4.7	5.2	5.7
growth rate (g)	3.0%							
WACC	9.0%							
FCF discounted	1.2	2.2	2.3	2.9	2.9	3.0	3.0	3.0
Discounted Cumulated FCFO	20.5							
Terminal Value	98.3							
Discounted TV	51.7							
Enterprise Value	72.2							
NFP FY25	(0.8)							
Minorities FY25	-							
Equity Value	73.0							
# Shares Outstanding (mn)	40.9							
Fair value per share (€)	1.80							

Source: KT&P's Estimates (2026-2033)

Sensitivity Analysis

€ Millions		WACC				
Terminal growth Rate		8.50%	8.75%	9.00%	9.25%	9.50%
	2.50%	75.0	71.8	68.8	66.1	63.5
	2.75%	77.4	74.0	70.8	67.9	65.2
	3.00%	80.1	76.4	73.0	69.9	67.0
	3.25%	83.0	79.0	75.4	72.1	69.0
	3.50%	86.3	81.9	78.0	74.4	71.1

Source: KT&P's Estimates

¹⁵ Osservatorio Cybersecurity & Data Protection, Politecnico di Milano; Mordor Intelligence

DISCLAIMER

THIS DOCUMENT WAS PREPARED BY MICHELE FILIPPIG – VICE PRESIDENT – AND CARLO ALBERTO MORLETTO – SENIOR ANALYST – ON BEHALF OF KT&PARTNERS S.R.L., WITH REGISTERED OFFICE AT VIA DELLA POSTA 10, MILAN, ITALY, MILAN COMPANY REGISTER NO. 1926922, SPECIALIZING IN FINANCIAL RESEARCH AND ANALYSIS (HEREINAFTER, “KT&PARTNERS”).

NO OTHER PEOPLE OR COMPANY CONTRIBUTED TO THE RESEARCH. NEITHER THE MEMBERS OF THE RESEARCH TEAM, NOR ANY PERSON CLOSELY ASSOCIATED WITH THEM HAVE ANY RELATIONSHIPS OR ARE INVOLVED IN CIRCUMSTANCES THAT MAY REASONABLY BE EXPECTED TO IMPAIR THE OBJECTIVITY OF THE RESEARCH, INCLUDING INTERESTS OR CONFLICTS OF INTEREST, ON THEIR PART OR ON THE PART OF ANY NATURAL OR LEGAL PERSON WORKING FOR THEM, WHO WAS INVOLVED IN PRODUCING THE RESEARCH.

FOR THIS PURPOSE, THE MEMBERS OF THE RESEARCH TEAM CERTIFY THAT: (I) THEY HAVE NOT RECEIVED AND WILL NOT RECEIVE ANY DIRECT OR INDIRECT COMPENSATION IN EXCHANGE FOR ANY VIEWS EXPRESSED IN THE RESEARCH; (II) THEY DO NOT OWN ANY SECURITIES AND/OR ANY OTHER FINANCIAL INSTRUMENTS ISSUED BY THE COMPANY OR ANY FINANCIAL INSTRUMENT WHICH THE PRICE DEPENDS ON, OR IS LINKED TO ANY SECURITIES AND/OR ANY FINANCIAL INSTRUMENTS ISSUED BY THE COMPANY; (III) NEITHER THE ANALYSTS NOR ANY MEMBER OF THE ANALYST’S HOUSEHOLD SERVE AS AN OFFICER, DIRECTOR OR ADVISORY BOARD MEMBER OF THE COMPANY.

KT&PARTNERS HAS IN PLACE AN EQUITY RESEARCH POLICY, IN ORDER TO RULE RESEARCH SERVICES IN COMPLIANCE WITH PARLIAMENT REGULATION (EU) NO.596/2014 AND COMMISSION DELEGATED REGULATION (EU) NO. 958/2016 ON MARKET ABUSE. IN THIS POLICY, THERE ARE ALSO DESCRIBED THE ORGANIZATIONAL MECHANISMS ADOPTED BY KT&PARTNERS TO PREVENT AND PROFESSIONALLY MANAGE CONFLICTS OF INTEREST THAT MAY BE ARISE DURING THE PERFORMANCE OF THE RESEARCH. IN ANY CASE, CHINESE WALLS AND OTHER INFORMATION BARRIERS ARE IN PLACE TO AVOID THE EXCHANGE OF CONFIDENTIAL INFORMATION BETWEEN THE EQUITY RESEARCH DEPARTMENT AND OTHER SERVICES AREAS.

KT&PARTNERS PREPARED THIS DOCUMENT ON BEHALF OF CYBEROO S.P.A. ACCORDING TO AN AGREEMENT ENTERED WITH THE SAME AND ON THE BASIS OF THE DATA AND PUBLIC INFORMATION PROVIDED BY THE SAME OR DERIVED FROM SOURCES DEEMED SERIOUS AND RELIABLE ON THE FINANCIAL MARKET BUT WHOSE ABSOLUTE TRUSTWORTHINESS, COMPLETENESS, AND ACCURACY CANNOT BE GUARANTEED. THE FEES AGREED FOR THIS RESEARCH DO NOT DEPEND ON THE RESULTS OF THE RESEARCH.

KT&PARTNERS RELEASE THIS DOCUMENT AS INITIATION OF COVERAGE ON CYBEROO S.P.A., NO OTHER DOCUMENTS WERE ISSUED BEFORE.

THIS DOCUMENT IS A SOURCE OF INFORMATION ONLY, AND IS NOT PART OF, AND IN NO WAY MUST BE CONSIDERED AN OFFER TO SELL, SUBSCRIBE OR TRADE, OR A SOLICITATION TO PURCHASE, SUBSCRIBE OR TRADE, FINANCIAL INSTRUMENTS/PRODUCTS, OR IN GENERAL TO INVEST, NOR MUST IT BE CONSIDERED ANY FORM OF CONSULTING FOR AN INVESTMENT IN FINANCIAL INSTRUMENTS.

THE INFORMATION PROVIDED IN THIS DOCUMENT MUST NOT BE UNDERSTOOD AS A REQUEST OR SUGGESTION TO CONDUCT OR CARRY OUT A SPECIFIC TRANSACTION.

EACH INVESTOR MUST FORM HIS/HER OWN OPINION BASED EXCLUSIVELY ON HIS/HER ASSESSMENT OF THE ADVISABILITY OF INVESTING. ANY INVESTMENT DECISION MADE ON THE BASIS OF THE INFORMATION AND ANALYSES IN THIS DOCUMENT IS THE EXCLUSIVE

RESPONSIBILITY OF THE RECIPIENTS OF THIS DOCUMENT, WHO MUST CONSIDER THIS DOCUMENT MERELY AS A SOURCE OF INFORMATION AND ANALYSIS TO SUPPORT SUCH DECISION.

ANY OPINIONS, FORECAST OR ESTIMATES CONTAINED HEREIN CONSTITUTE A JUDGEMENT AS AT THE DATE OF THIS DOCUMENT, AND THERE CAN BE NO ASSURANCE THAT THE FUTURE RESULTS OF THE COMPANY AND/OR ANY FUTURE EVENTS WILL BE CONSISTENT WITH ANY OF SUCH OPINIONS, FORECAST OR ESTIMATES.

KT&PARTNERS MAKES NO EXPLICIT OR IMPLICIT GUARANTEE WITH RESPECT TO PERFORMANCE OR THE OUTCOME OF ANY INVESTMENT OR PROJECTIONS MADE.

THEREFORE, KT&PARTNERS, ITS REPRESENTATIVES AND/OR EMPLOYEES WILL NOT BE LIABLE FOR ANY EFFECT DERIVING FROM THE USE OF THIS DOCUMENT, AND HEREBY DECLINE ALL LIABILITY FOR ANY DIRECT OR INDIRECT DAMAGES, FINANCIAL OR OTHERWISE, DERIVING FROM ANY USE OF THE INFORMATION IT CONTAINS.

KT&PARTNERS AIMS TO PROVIDE CONTINUOUS COVERAGE OF THE COMPANY IN CONJUNCTION WITH ANY EXCEPTIONAL EVENT THAT OCCURS AFFECTING THE ISSUER'S SPHERE OF OPERATIONS AND IN ANY CASE AT LEAST TWICE PER YEAR.

IN THIS STUDY DCF AND MULTIPLE VALUATION MODELS HAVE BEEN USED. RECOMMENDATIONS FOLLOW THE FOLLOWING RULES:

- ADD - FOR A FAIR VALUE > 15% ON CURRENT PRICE
- HOLD - FOR A FAIR VALUE <15% o >-15% ON CURRENT PRICE
- REDUCE - FOR A FAIR VALUE < -15% ON CURRENT PRICE

