

TecnetSOC vs. Cyrebro

Cyrebro monitors the tools you already have. TecnetSOC brings its own and runs your entire security, in your language.

With Cyrebro, a certified integrator connects your systems, you set aside a dedicated machine as a collector, and patching is not part of the service. With TecnetSOC, you install one agent, see activity within 2 to 4 hours, and the SOC patches.



44

capabilities where TecnetSOC goes further

6

capabilities where we match

0

capabilities where Cyrebro outperforms TecnetSOC

Of the 50: 44 where we go further and 6 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Cyrebro: each one's most complete published offering, with the source for every data point. [How we did it](#)

[Request the 30-day Response trial](#)

[or start free with Visibility, up to 10 devices](#)

tecnetone.com/en/services/soc-as-a-service

- ✓ 24/7 agentic SOC in LATAM, the US, and Europe
- ✓ Native Spanish and multilingual support
- ✓ Human Gate on critical actions
- ✓ ISO/IEC 27001:2022 certified operations
- ✓ Critical: notification and investigation start within 30 min (target)

Public information reviewed as of September 29, 2026. Version 2026.09. Informational comparison prepared by TecnetOne, not affiliated with the brands mentioned.

— BEFORE YOU COMPARE

Cyrebro is a SOC service that connects to the tools you already have; it does not include its own endpoint protection. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01
Integration only through a certified third party

WITH CYREBRO
Your systems can only be connected by a certified integrator from its list, and you must set aside a dedicated machine as an event collector. [1]

WITH TECNETSOC
You install one agent and the rest deploys itself: activity in the portal within 2 to 4 hours, with no implementation project and no servers.

02
Patching and vulnerabilities are left out

WITH CYREBRO
The published service is detection and response; it doesn't document vulnerability management or system patching, so closing those gaps is left to your team. [2]

WITH TECNETSOC
The SOC patches by prioritizing with KEV and EPSS, validates in a pilot group, and considers it closed only when the scanner confirms it.

03
One SOC, a single region

WITH CYREBRO
The SOC operates from Israel in a single region and without shifts that follow the customer's time zone (follow-the-sun), according to an independent directory of MDR providers. [3]

WITH TECNETSOC
Our own analysts operate in LATAM, the US, and Europe, in your time zone and in native Spanish.

04
More data, more cost

WITH CYREBRO
Extending log retention in cold storage comes at an additional cost, and an independent directory warns that the ingested volume can raise the price. [1]

WITH TECNETSOC
You pay per device with stackable plans, and the platform is a cloud service that you don't install or maintain.

05
Email and phishing are not part of the service

WITH CYREBRO
M365 Protect monitors access, apps, and privileges in your suite, but it doesn't document spam or phishing filtering or simulations for your staff. [4]

WITH TECNETSOC
Email security (spam, phishing, malware, BEC) and phishing simulations come in the most complete offering.

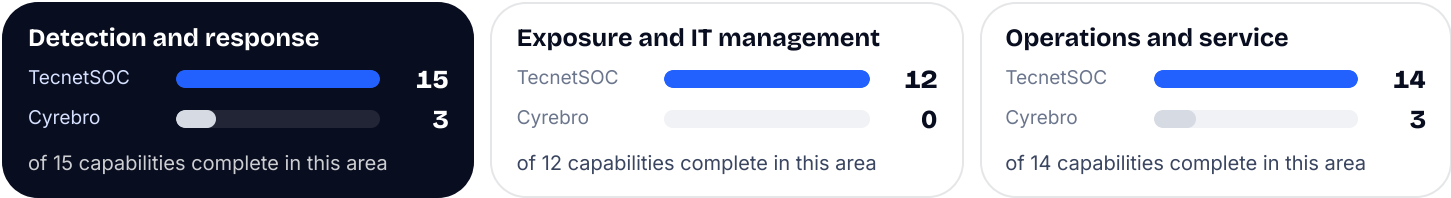
06
You have to request the reports

WITH CYREBRO
You generate the reports yourself with an assistant when you need them; it doesn't publish automated delivery or a compliance platform for your audit. [5]

WITH TECNETSOC
You get an executive summary every morning and automated PDF reports; TecnetGRC is added as an add-on for your audit.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Cyrebro, side by side

Capability	TecnetSOC	Cyrebro SOC	Evidence on Cyrebro
 Offers it  Offers it as an add-on  Partial, limited, or requires another contract  No public evidence			
 Not part of its published offering			
Operations and service	14 of 14	3 complete	
		 +6 partial	
24/7 security operations center (SOC) with human analysts			24/7/365 monitoring with tier 1 to 4 analysts [6]
AI agents that investigate and filter alerts before passing them to an analyst			Presents itself as "AI-native"; AI handles only low-severity investigations [2]
Human Gate: a person approves every critical action before it runs			Automated action by playbook or escalation for approval, according to an independent directory, with no official documentation [3]

Capability	TecnetSOC	Cyrebro SOC	Evidence on Cyrebro
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
AI investigation assistant in the portal that cites its sources	Neo		No evidence of a conversational AI analyst in the portal that cites sources [1]
Operations in LATAM, the US, and Europe, with analysts in your time zone			SOC operated from Israel; no documented follow-the-sun [3]
Analysts, support, and portal in native Spanish			In LATAM, Spanish is provided by the local partner (tiers 1 and 2); tier 3 works from Tel Aviv [7]
Leadership reports in Spanish and in business language			Reports in plain English; no evidence of reports in Spanish [5]
Published notification and investigation start times by severity	Critical: 30 min (target)		Does not publish a notification or response SLA [5]
Executive summary every morning: what happened in the last 24 hours	7:30 a.m.		No evidence of a daily executive summary [5]
Automated weekly, monthly, quarterly, and annual reports			On-demand report assistant; no documented automated cadence [5]
Assigned technical account manager (TAM) and quarterly reviews			Mentions an account manager; no documented quarterly reviews [6]
24/7 contact with support or security staff			Analysts available 24/7 for assistance [5]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	ISO/IEC 27001:2022		States ISO 27001, SOC 2, and ISO 22301 [5]
Fast start with a software agent: your devices' activity, visible within hours	Typical: 2 to 4 hours		Requires an event collector and integrations; an independent directory mentions hours, with no official confirmation [3]
Detection and response	15 of 15	3 complete +8 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Its own data repository (data lake), more than 1,500 detections, MITRE ATT&CK mapping [1]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			No EDR of its own; integrates with SentinelOne, CrowdStrike, Defender; Managed EDR add-on [2]
Web filtering on the device			No native web filtering on the device [2]
Intrusion detection (IDS/IPS)			Only ingests IDS/IPS alerts from third-party firewalls [8]
Threat detection on the internal network (NDR)			No NDR of its own; depends on third-party network logs [8]
Documented investigations enriched with threat intelligence			Threat intelligence and enrichment included in investigations [1]
Incident management with a case log and response time measured per case			Incident management in the platform; no documented MTTR per incident [1]
Response with device isolation and IP address blocking			Isolation and blocking via third-party EDR or firewall [3]
Incident response with root cause analysis			Incident response and digital forensics included [1]
Identity posture: MFA, privileged accounts, and conditional access			M365 Protect detects privilege escalation; it doesn't assess identity posture [4]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			No Zero Trust, secure DNS, or shadow IT offering [2]
Cloud security: alerts and posture			Monitors Azure, AWS, GCP logs; no documented cloud posture [1]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			M365 Protect monitors access and apps; it doesn't filter spam or phishing [4]
Security awareness: phishing simulations and training with metrics			No security awareness offering or phishing simulations [2]

Capability	TecnetSOC	Cyrebro SOC	Evidence on Cyrebro
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence			
Not part of its published offering			
Prioritized security recommendations with an approval workflow			Actionable mitigation steps; no documented approval workflow [2]
Exposure and IT management	12 of 12	0 complete	
		+0 partial	
Unified asset and software inventory			No documented asset and software inventory [2]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)			No documented vulnerability management module [2]
Priority for flaws already being exploited (CISA KEV catalog)			No documented KEV prioritization [2]
Operating system and third-party application patching			Does not offer patching [2]
Provider-operated patching, with published timelines by severity	 Critical: 48 h (target)		Does not offer operated patching with timelines [2]
Closure verification: the scanner confirms the vulnerability is gone			No closure verification scanner [2]
Patch validation in a pilot group before rollout			No patching, no pilot group [2]
External attack surface: what your company exposes on the internet, with a risk score	 Score from 0 to 100		No external attack surface management (EASM) or exposure score [2]
Alerts for domains that imitate your brand and for exposed credentials or keys			No typosquatting or exposed secrets detection [2]
Annual penetration test (pentest)	 Annual		No documented pentesting [2]
Remote monitoring and management (RMM)			Does not offer RMM [2]
Uptime monitoring (NOC)			Does not offer NOC or uptime monitoring [2]
Backup and continuity	3 of 3	0 complete	
		+0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	Add-on		Does not offer backup [2]
Immutable backup vault (cannot be altered or deleted), isolated per customer	Add-on		Does not offer an immutable vault [2]
Disaster recovery with drills and measured recovery time (RTO)	Add-on Measured RTO		Does not offer disaster recovery [2]
Compliance	6 of 6	0 complete	
		+1 partial	
Monthly evidence ready for auditors and insurers	 Monthly		Reports and data lake queries serve as evidence; no monthly delivery [5]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	Add-on		No GRC platform [2]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	Add-on		No coverage of Mexican regulations [2]
Risk management, controls, statement of applicability, and internal audits	Add-on		No risk management, controls, or SoA [2]
Auditor portal with an evidence room and a public trust page (trust center)	Add-on		No auditor portal or Trust Center for customers [2]
Business continuity, vendor risk, and data breach management	Add-on		No continuity, vendor, or breach modules [2]

Capability	TecnetSOC	Cyrebro SOC	Evidence on Cyrebro
✓ Offers it ✗ Not part of its published offering	ⓘ Offers it as an add-on ⓘ Partial, limited, or requires another contract	? No public evidence	
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✓ Per device	✗	Custom quote; no public pricing or plans [2]
Free plan to get started	✓ Up to 10 devices	✗	No free plan [2]
Free trial in your real environment	✓ 30 days	ⓘ	No public free trial; proof of value on request, according to an independent directory [3]
Available under your IT provider's brand	✓	✓	"Your brand, powered by CYREBRO": the partner sells under its own brand [6]
Full coverage	50	6 +15 partial	

— NEXT STEP

See it in your own operations

Try it in a real environment, without changing what already works for you.

The first agentic SOC in Spanish: platform, analysts, and support.

Request the 30-day Response trial

Start free with Visibility (up to 10 devices)

Or talk to a specialist

tecnetone.com/en/services/soc-as-a-service

HOW THE RESPONSE TRIAL WORKS

1

You install a single agent

2

You get the executive summary every morning

3

You decide with data from your environment

— APPENDIX

Methodology and sources

Who prepared it and how

We prepared it at TecnetOne and show you the source for every data point. The list of capabilities is based on the TecnetSOC catalog. We evaluated each provider's most complete published offering, including its own add-ons, and ours with the same rigor. We used only public information (official websites, documentation, and press releases) reviewed as of September 29, 2026.

What each status means

Offers it: the provider delivers it, operates it, and is accountable for it within its service, wherever the technology comes from. Add-on: available at an additional cost. Partial: limited scope, or requires another contract or another operator. No public evidence: no public information confirms it at the time of review; this does not mean the provider doesn't offer it. Not part of its published offering: its documentation indicates it is not included. Your team provides it: with a tool, that capability depends on your staff, your shifts, and your response times, not on the provider. When in doubt between two values, we chose the more conservative one.

How we make corrections

A provider may offer something it doesn't publish: confirm it directly with them. If you see outdated or incorrect information, write to us through our contact form and we'll correct it in the next version. We review this comparison every quarter and whenever a provider's published offering or our catalog changes.

Evaluated for Cyrebro: CYREBRO AI-Native MDR (full SOC platform + M365/Workspace Protect + Managed EDR + co-branded IT provider program), reviewed Sep 29, 2026

Evaluated for TecnetSOC: TecnetSOC in its most complete offering (Compliance plan, with the TecnetProtect and TecnetGRC add-ons), platform catalog soc.catalogo.tecnetone.com and tecnetone.com/servicios/soc-as-a-service, reviewed Sep 29, 2026. Same standard as the others. Add-ons at an additional cost count as part of the offering, just like the other providers' own add-ons.

1. [www.cyrebro.io/why-cyrebro/solution-description/](#) (Differences you notice day to day)

2. [www.cyrebro.io/](#) (Differences you notice day to day)

3. [mdrproviders.io/providers/cyrebro](#) (Differences you notice day to day)

4. [www.cyrebro.io/cyrebro-m365-protect/](#) (Differences you notice day to day)

5. [www.cyrebro.io/faqs/](#) (Differences you notice day to day)

6. [www.cyrebro.io/partners/](#) (24/7 security operations center (SOC) with human analysts)

7. [tiinside.com.br/en/03/12/2025/cyrebro-chega-ao-brasil-com-apoio-da-...](#) (Analysts, support, and portal in native Spanish)

8. [www.cyrebro.io/integrations/](#) (Intrusion detection (IDS/IPS))

Sources and date. This comparison is informational and is prepared by TecnetOne so you can compare, capability by capability, what TecnetSOC includes versus the most complete published offering of each provider mentioned. The list of capabilities is TecnetOne's own catalog and may not include every feature of each provider. We used only public information (official websites, technical documentation, and press releases) reviewed as of September 29, 2026; version 2026.09, reviewed quarterly. "No public evidence" means that no public

information confirms it at the time of review, not that the provider cannot offer it in another way: confirm every detail directly with them. The sources for each data point are in each provider's individual comparison, linked at the bottom of the table.

Trademarks. Third-party names and trademarks belong to their respective owners and are used only to identify them and for informational comparison. None of these providers is affiliated with TecnetOne or sponsors or endorses this document.

TecnetSOC scope. Backup and the compliance platform (TecnetGRC) are add-ons at an additional cost. Our times are service targets for notification and investigation start, not for resolution (critical: 30 minutes, as a target). Patching is subject to the maintenance windows agreed with you and to the applications included in your profile. Compliance is delivered as readiness and evidence, not as certification. TecnetSOC is a TecnetOne service, with ISO/IEC 27001:2022 certified operations, available directly or through your IT provider.