

TecnetSOC vs. Stellar Cyber

Stellar Cyber unifies your tools in a platform that your team or your provider operates. TecnetSOC brings the tools and operates them for you, in your language.

With Stellar Cyber, device protection comes from another vendor's EDR, email is filtered by another product, and the license is measured by GB or assets per day. With TecnetSOC, EDR, email, and patching are part of the service, and TecnetOne analysts respond 24/7.



44

capabilities where TecnetSOC goes further

6

capabilities where we match

0

capabilities where Stellar Cyber 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 Stellar Cyber: 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 October 14, 2026. Version 2026.09. Informational comparison prepared by TecnetOne, not affiliated with the brands mentioned.

— BEFORE YOU COMPARE

Stellar Cyber is an open security operations platform (SIEM, NDR, UEBA, and ITDR) that your team or a certified service provider operates; Stellar Cyber doesn't offer its own SOC. Device protection, email filtering, and vulnerability scanning come from other vendors' integrated products. Here we compare the platform with what TecnetSOC includes, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01

The platform is not the service

WITH STELLAR CYBER
You buy a platform: monitoring, investigating, and responding around the clock is done by your team or a certified service provider (MSSP) that you hire separately; Stellar Cyber doesn't operate its own SOC. [1]

WITH TECNETSOC
TecnetOne analysts monitor, investigate, and respond 24/7, in your time zone and in Spanish; for a critical incident, they notify you and start investigating within 30 minutes, as a target.

02

You buy the EDR from another vendor

WITH STELLAR CYBER
Protection for each device comes from an EDR you buy from another vendor: its model is to bring your own EDR and integrate it, from 32 options such as CrowdStrike, SentinelOne, or ESET. [2]

WITH TECNETSOC
Advanced protection on every device (EDR/XDR) and web filtering are part of the most complete offering, with one agent and activity usually visible in 2 to 4 hours.

03

You pay for ingested data, not per device

WITH STELLAR CYBER
The license is measured by daily GB ingested or by active assets per day, and its documentation sets compliance rules for the contracted limit, with overage charges. [3]

WITH TECNETSOC
You pay per device with stackable plans; the SIEM and retention are included in the service.

04

Sees vulnerabilities, doesn't patch them

WITH STELLAR CYBER
Vulnerabilities come from other vendors' integrated scanners, and its license (SIEM, NDR, UEBA, threat intelligence, IDS, sandbox, orchestration, and file integrity) doesn't include installing patches. [4]

WITH TECNETSOC
The SOC patches based on real-world exploitation (KEV and EPSS), with target timelines by severity, validates in a pilot group, and marks an item closed only when the scanner confirms it.

05

Another product filters your email

WITH STELLAR CYBER
The AI analyzes emails your users report as suspicious; asked whether you still need Mimecast or Proofpoint for inbound filtering, its answer is yes. [5]

WITH TECNETSOC
Protection against spam, phishing, malware, and impersonation (BEC) is included in the service, with self-service quarantine and phishing simulations with per-user metrics.

06

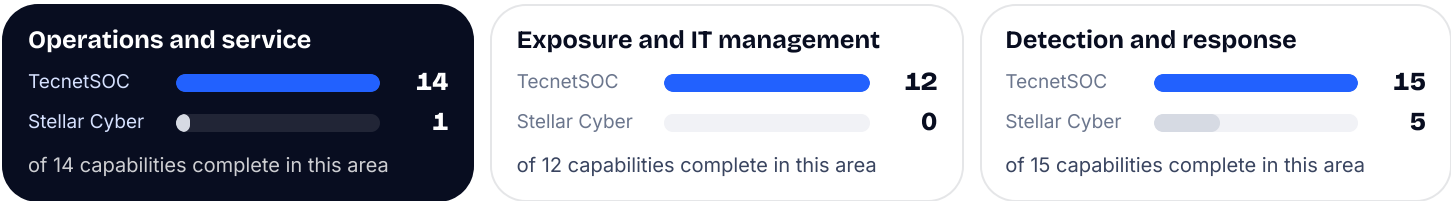
Detects attacks, doesn't back up your data

WITH STELLAR CYBER
Its license alone brings together detection and response capabilities, but it doesn't include server backup, an immutable vault, or disaster recovery for your systems. [4]

WITH TECNETSOC
You can add TecnetProtect (at an additional cost): backup to an immutable vault per customer and disaster recovery with drills and measured RTO.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Stellar Cyber, side by side

Capability	TecnetSOC	Stellar Cyber Open XDR	Evidence on Stellar Cyber
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering Your team provides it			
Operations and service	14 of 14	1 complete +7 partial	
24/7 security operations center (SOC) with human analysts		Your team provides it	No SOC of its own; 24/7 monitoring is provided by your team or a certified service provider you hire separately [1]
AI agents that investigate and filter alerts before passing them to an analyst			Auto Triage prioritizes and filters alerts; the analyst who decides is provided by your team or your provider [6]
Human Gate: a person approves every critical action before it runs			Automated or human-in-the-loop playbooks, your choice; your team or your provider runs them [7]
AI investigation assistant in the portal that cites its sources	 Neo		AI Investigator answers in natural language with editable queries; in early access, with no documented source citations [8]
Operations in LATAM, the US, and Europe, with analysts in your time zone		Your team provides it	No analysts of its own; according to Stellar Cyber, LATAM providers operate its platform and you choose one [9]
Analysts, support, and portal in native Spanish			Website in Spanish; console and support language not published; analysts are provided by your team or your provider [10]
Leadership reports in Spanish and in business language			Customizable reports that your team or your provider builds; executive reports in Spanish not documented [11]
Published notification and investigation start times by severity	 Critical: 30 min (target)	Your team provides it	Only platform support times (from one hour to business days); security times depend on your provider [12]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.	Your team provides it	No documented daily executive summary; your team or your provider puts it together [13]
Automated weekly, monthly, quarterly, and annual reports			Weekly or monthly scheduled reports that your team or your provider configures; quarterly and annual reports not documented [13]
Assigned technical account manager (TAM) and quarterly reviews		Your team provides it	Assigned customer success manager for the platform; TAM and quarterly reviews not documented [14]
24/7 contact with support or security staff			24x7 platform support via portal; the 24/7 security contact is provided by your team or your provider [15]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		Its trust center lists ISO/IEC 27001 and SOC 2, with a SOC 2 report available [16]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		Its own sensor only for Windows Server and Linux; on workstations it relies on another vendor's EDR [17]
Detection and response	15 of 15	5 complete +6 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Correlates alerts into cases and maps them to its XDR Kill Chain, based on MITRE ATT&CK [18]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			No EDR of its own: integrates 32 EDRs from other vendors, such as CrowdStrike, SentinelOne, and ESET [2]
Web filtering on the device			No evidence of web filtering on the device [4]
Intrusion detection (IDS/IPS)			The sensor detects intrusion attempts in files and network traffic (IDS); blocking goes through your firewall [19]
Threat detection on the internal network (NDR)			Its own NDR: modular sensor with network traffic analysis, IDS, and malware sandbox [19]
Documented investigations enriched with threat intelligence			Built-in threat intelligence platform that enriches logs and cases with indicators [20]

Capability	TecnetSOC	Stellar Cyber Open XDR	Evidence on Stellar Cyber
☒ Offers it ☒ Offers it as an add-on ☐ Partial, limited, or requires another contract ☐ No public evidence ☐ Not part of its published offering ☐ Your team provides it			
Incident management with a case log and response time measured per case	☒	☒	Cases with an activity log and a record of creation, acknowledgment, and closure [21]
Response with device isolation and IP address blocking	☒	☐	Blocks IPs with your firewall and contains devices with your EDR, both connected products from other vendors [22]
Incident response with root cause analysis	☒	Your team provides it	Tools to investigate; response with root cause analysis is provided by your team or your provider [23]
Identity posture: MFA, privileged accounts, and conditional access	☒	☐	ITDR detects identity abuse in AD, Entra ID, and Okta; posture (MFA, conditional access) not documented [24]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	No evidence of secure DNS, Zero Trust access, or shadow IT control [25]
Cloud security: alerts and posture	☒	☐	Ingests logs from AWS, Azure, Google Cloud, and OCI; posture comes from integrating other vendors' CSPM [26]
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☐	Analyzes emails your users report; inbound filtering stays with Mimecast or Proofpoint [5]
Security awareness: phishing simulations and training with metrics	☒	☐	No phishing simulations or user training among its license capabilities [4]
Prioritized security recommendations with an approval workflow	☒	☐	Its MITRE coverage analyzer suggests where to invest to expand detection; no approval workflow [27]
Exposure and IT management	12 of 12	0 complete +2 partial	
Unified asset and software inventory	☒	☐	Discovers assets by IP and MAC and lets you import your inventory; software inventory not documented [28]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☐	No scanner of its own; integrates Tenable, Qualys, and Rapid7; use of EPSS not documented [29]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☐	No evidence of prioritization by the CISA KEV catalog [28]
Operating system and third-party application patching	☒	☐	No evidence of patching; its license capabilities don't include installing patches [4]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	No patching operated by Stellar Cyber; your team or your provider handles it [23]
Closure verification: the scanner confirms the vulnerability is gone	☒	☐	No evidence of vulnerability closure verification [4]
Patch validation in a pilot group before rollout	☒	☐	No evidence of patch validation in a pilot group [4]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	No evidence of monitoring what your company exposes on the internet [25]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	No evidence of alerts for domains that imitate your brand or for exposed credentials [25]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting as its own service; your team or your provider handles it [23]
Remote monitoring and management (RMM)	☒	☐	No evidence of remote monitoring and management (RMM) [29]
Uptime monitoring (NOC)	☒	☐	No evidence of uptime monitoring for your systems (NOC) [25]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	☒ Add-on	☐	No backup of its own; the capabilities of its license alone don't include backup [4]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	No backup vault of its own [4]

Capability	TecnetSOC	Stellar Cyber Open XDR	Evidence on Stellar Cyber
☒ Offers it ☒ Offers it as an add-on ☒ Partial, limited, or requires another contract ☐ No public evidence ☐ Not part of its published offering ☐ Your team provides it			
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	No disaster recovery for your systems; on-premises, disaster recovery for the platform is on you [30]
Compliance	6 of 6	0 complete +2 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Ready-made PCI and HIPAA reports, customizable; no monthly evidence package [11]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Ready-made PCI DSS reports; ISO 27001 or SOC 2 readiness not documented [11]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No evidence of Mexican regulations [11]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	No risk management, controls, or internal audits for your company [11]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	Stellar Cyber's own trust center; no portal for your auditor or trust page of your own [16]
Business continuity, vendor risk, and data breach management	☒ Add-on	☐	No evidence of business continuity, vendor risk, or breach management [11]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	☒ Per device	☒	License by active assets per day or by daily GB ingested; no stackable plans [31]
Free plan to get started	☒ Up to 10 devices	☐	No published free plan [4]
Free trial in your real environment	☒ 30 days	☒	Proof of concept with your data and in your environment; duration and cost not published [32]
Available under your IT provider's brand	☒	☒	Multi-tenant platform for MSSPs, with reports carrying the provider's brand [11]
Full coverage	50	6 +17 partial	

What your team would have to provide to run it 24/7: people, shifts, response times, a daily summary, incident response, and operated patching. TecnetSOC includes them in the service.

— NEXT STEP

From tool to service, with no implementation project

You install a single agent, see your devices' activity within hours, and our analysts operate 24/7 in your language.

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

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

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

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 October 14, 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 Stellar Cyber: Stellar Cyber, most complete published offering (Open XDR platform with NG-SIEM, NDR with IDS and sandbox, UEBA, ITDR, threat intelligence, Auto Triage, AI Investigator, and automated response; no SOC of its own: operation is provided by your team or a certified service provider), reviewed Oct 14, 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.

- stellarcyber.ai/partners/find-mssp/ (Differences you notice day to day)
- stellarcyber.ai/platform/universal-endpoint-detection-and-response-... (Differences you notice day to day)
- docs.stellarcyber.ai/6.6.x/Configure/Adm-in-Licensing-Compliance.htm (Differences you notice day to day)
- stellarcyber.ai/resources/stellar-cyber-pricing/ (Differences you notice day to day)
- stellarcyber.ai/automatically-triage-phishing-emails-with-stellar-c-... (Differences you notice day to day)
- stellarcyber.ai/platform/capabilities-autonomous-soc/ (AI agents that investigate and filter alerts...)
- stellarcyber.ai/platform/automated-threat-hunting/ (Human Gate: a person approves every...)
- stellarcyber.ai/ai-investigator-natural-language-threat-hunting/ (AI investigation assistant in the portal that...)
- stellarcyber.ai/news/press-releases/stellar-cyber-becomes-a-platfor... (Operations in LATAM, the US, and Europe, with analysts...)
- stellarcyber.ai/es/ (Analysts, support, and portal in native Spanish)
- stellarcyber.ai/enterprise/compliance-and-reporting/ (Leadership reports in Spanish and in business...)
- success.stellarcyber.ai (Published notification and investigation...)
- docs.stellarcyber.ai/6.6.x/Using/Respond/Reports-Scheduled.htm (Executive summary every morning: what happened...)
- stellarcyber.ai/customer-success/ (Assigned technical account manager (TAM) and...)
- stellarcyber.ai/customer-support/ (24/7 contact with support or security staff)
- security.stellarcyber.ai/ (Independent certification of operations (ISO 27001...)
- docs.stellarcyber.ai/prod-docs/6.5.x/Installation/Server-Sensor-OS.htm (Fast start with a software agent: your...)
- docs.stellarcyber.ai/6.6.x/Common/Hom-e-XDR-Kill-Chain-Understanding... (Continuous monitoring and event correlation...)
- docs.stellarcyber.ai/6.6.x/Installation/Sensor-Types-Introduction.htm (Intrusion detection (IDS/IPS))
- stellarcyber.ai/threat-intelligence-built-in-not-bolted-on/ (Documented investigations enriched...)
- docs.stellarcyber.ai/6.6.x/Using/Cases/Cases-Main.htm (Incident management with a case log and response time...)
- docs.stellarcyber.ai/6.6.x/Using/Cases/Case-Detail-Response-Tab.htm (Response with device isolation and IP...)
- stellarcyber.ai/stellar-cyber-services/ (Incident response with root cause analysis)
- stellarcyber.ai/identity-threat-detection-response-itdr/ (Identity posture: MFA, privileged accounts...)
- stellarcyber.ai/platform/ (Zero Trust: secure DNS, application access, and...)
- stellarcyber.ai/uc/multi-cloud-security/ (Cloud security: alerts and posture)
- stellarcyber.ai/mitre-attck-coverage-analyzer/ (Prioritized security recommendations with an...)
- docs.stellarcyber.ai/6.6.x/Using/Investigate/Asset-Analytics-Main.htm (Unified asset and software inventory)
- docs.stellarcyber.ai/6.6.x/Configure/Connectors/1-Connectors-List.htm (Vulnerabilities prioritized by severity...)
- doc-server.stellarcyber.ai/6.4.xs/Common/Stellar-Description.htm (Disaster recovery with drills and...)
- docs.stellarcyber.ai/6.6.x/Configure/System-Licensing.htm (Per-device pricing, with plans that stack)
- stellarcyber.ai/schedule-proof-of-concept/ (Free trial in your real environment)

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 October 14, 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.



A SOC that speaks your language.

See outdated or inaccurate information? Write to us and we'll correct it.