

TecnetSOC vs. Arctic Wolf

Arctic Wolf detects and alerts you. TecnetSOC runs your entire security for you, in your language and in your time zone.

With Arctic Wolf, forensic analysis inside your environment is purchased separately, through a prepaid block of hours (retainer), and your team applies operating system patches. With TecnetSOC, response with forensic analysis and patching are already included.



35

capabilities where TecnetSOC goes further

15

capabilities where we match

0

capabilities where Arctic Wolf outperforms TecnetSOC

Of the 50: 35 where we go further and 15 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Arctic Wolf: 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

Arctic Wolf is a managed SOC service, like TecnetSOC. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01

Response with forensic analysis, under another contract

WITH ARCTIC WOLF
Its managed detection and response (MDR) service detects, contains, and guides remediation; response with forensic analysis inside your environment is a separate service, through a prepaid block of hours (retainer) or billed hourly. [1]

WITH TECNETSOC
Incident response with forensic analysis is part of the most complete offering, and a person approves every critical action.

02

Patching for supported applications only

WITH ARCTIC WOLF
Its Resolve license patches only supported third-party applications that don't require a restart; it doesn't document operating system patches or timelines. [2]

WITH TECNETSOC
The SOC prioritizes patching based on what is already being exploited in the real world (KEV and EPSS), validates it in a pilot group, and closes only when the scanner confirms the fix.

03

Security yes, IT operations no

WITH ARCTIC WOLF
Its portfolio doesn't include RMM, uptime monitoring, or an IT help desk, and for pentesting it may refer you to third parties: another contract. [3]

WITH TECNETSOC
The most complete offering includes RMM, uptime monitoring (NOC), a 24/7 help desk, a TAM, and annual pentesting.

04

Every data source, another license

WITH ARCTIC WOLF
Its public sector price list charges separate licenses for users, servers, each cloud, and each application, such as Microsoft 365 or Google Workspace. [4]

WITH TECNETSOC
You pay per device with stackable plans; Visibility is free for up to 10 devices, and Response comes with a 30-day trial.

05

No operations in Latin America

WITH ARCTIC WOLF
Its published SOC's are in North America, Europe, and Asia Pacific, none in Latin America, and its technical documentation has no Spanish version. [5]

WITH TECNETSOC
We operate in LATAM, the US, and Europe, with analysts in your time zone and support in native Spanish.

06

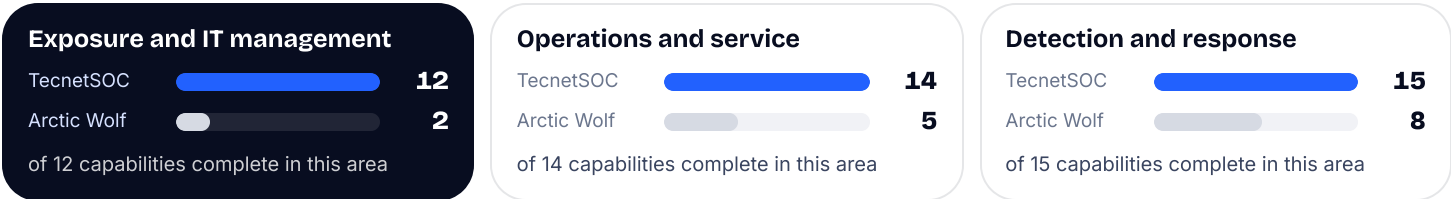
Compliance without Mexican regulations

WITH ARCTIC WOLF
Its compliance reports cover frameworks such as NIST, PCI DSS, HIPAA, or GDPR, with no Mexican regulations and no GRC platform for your audit. [6]

WITH TECNETSOC
You add TecnetGRC as an add-on with CNBV, LFPDPPP, NOM-024, ISO 27001, and an auditor portal; each regulatory framework is purchased separately.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Arctic Wolf, side by side

Capability	TecnetSOC	Arctic Wolf SOC	Evidence on Arctic Wolf
 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	5 complete  +6 partial	
24/7 security operations center (SOC) with human analysts			24x7 monitoring with an assigned Concierge Security Team [7]
AI agents that investigate and filter alerts before passing them to an analyst			Aurora Agentic SOC: Triage Agent and Investigation Agent analyze and prioritize alerts [8]
Human Gate: a person approves every critical action before it runs			Humans approve high-impact or low-confidence actions; others run on their own [8]

Capability	TecnetSOC	Arctic Wolf SOC	Evidence on Arctic Wolf
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		Cipher / Aurora Security Assistant answers on demand; dated source citations are not documented [9]
Operations in LATAM, the US, and Europe, with analysts in your time zone			No SOC or office in LATAM; SOC's in North America, Europe, and Asia Pacific [10]
Analysts, support, and portal in native Spanish			No public evidence of Spanish-speaking analysts or support for the region; its portal is offered in English, Japanese, German, and French, with no Spanish [11]
Leadership reports in Spanish and in business language			Executive reports exist; no evidence of a Spanish version [12]
Published notification and investigation start times by severity	Critical: 30 min (target)		Does not publish notification times by severity; the available figures come from third parties [7]
Executive summary every morning: what happened in the last 24 hours	7:30 a.m.		No evidence of a daily executive summary [7]
Automated weekly, monthly, quarterly, and annual reports			Detailed reports and dashboards on demand; does not publish automated periodic reports [7]
Assigned technical account manager (TAM) and quarterly reviews			Named Concierge Security Team with periodic strategic reviews [7]
24/7 contact with support or security staff			Concierge team and SOC available 24x7 [7]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	ISO/IEC 27001:2022		Arctic Wolf is ISO 27001 certified and has a SOC 2 Type II report [13]
Fast start with a software agent: your devices' activity, visible within hours	Typical: 2 to 4 hours		Typical deployment of about 10 days; MDR Connect for IT providers "in hours" [14]
Detection and response	15 of 15	8 complete +4 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Proprietary platform for log ingestion, correlation, and search, with more than 250 integrations [8]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			Aurora Protect and Endpoint Defense (Cylance) against malware and ransomware [15]
Web filtering on the device			No evidence of web filtering in the endpoint agent [15]
Intrusion detection (IDS/IPS)			Monitors the customer's IDS/IPS and traffic with a sensor; does not sell its own IPS [7]
Threat detection on the internal network (NDR)			A physical or virtual network sensor detects threats on the internal network, including devices without an agent [7]
Documented investigations enriched with threat intelligence			Investigations with its own Threat Intelligence and Threat Intelligence Plus [16]
Incident management with a case log and response time measured per case			Creates the incident with a ticket and guidance; response time per incident not documented [7]
Response with device isolation and IP address blocking			Managed Containment isolates at the network and host level; Dynamic Block Lists [7]
Incident response with root cause analysis			Incident360 and IR JumpStart Retainer: response and forensic analysis, purchased separately [1]
Identity posture: MFA, privileged accounts, and conditional access			M365/Google identity monitoring and integrations; identity posture not detailed [16]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			No native secure DNS, ZTNA, or shadow IT control [15]
Cloud security: alerts and posture			MDR and CSPM modules for Azure, AWS, and GCP [4]

Capability	TecnetSOC	Arctic Wolf SOC	Evidence on Arctic Wolf
✓ Offers it ⊕ Offers it as an add-on ⦿ Partial, limited, or requires another contract ? No public evidence ✗ Not part of its published offering			
Email security: spam, phishing, malware, and impersonation fraud (BEC)	✓	✗	Only monitors M365/Google mailboxes; no native anti-spam gateway or quarantine [4]
Security awareness: phishing simulations and training with metrics	✓	✓	Managed Security Awareness and Plus with simulated phishing [4]
Prioritized security recommendations with an approval workflow	✓	⦿	AI remediation guidance and ITSM integration; no documented approval workflow [17]
Exposure and IT management	12 of 12	2 complete	
		+4 partial	
Unified asset and software inventory	✓	✓	Continuous asset inventory (Sevco technology) in Attack Surface Management [12]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	✓	⦿	Internal and external scanning with likelihood of exploitation; EPSS not explicit [17]
Priority for flaws already being exploited (CISA KEV catalog)	✓	⦿	Prioritizes with exploitation intelligence; use of KEV not documented in the product [18]
Operating system and third-party application patching	✓	⦿	Resolve patches only supported third-party software, not the operating system [2]
Provider-operated patching, with published timelines by severity	✓ Critical: 48 h (target)	✗	Does not publish provider-operated patching or timelines [2]
Closure verification: the scanner confirms the vulnerability is gone	✓	⦿	Mentions remediation verification tracking; rescan mechanics not detailed [12]
Patch validation in a pilot group before rollout	✓	?	No evidence of a pilot group before patch rollout [2]
External attack surface: what your company exposes on the internet, with a risk score	✓ Score from 0 to 100	✓	External scanning and Aurora Attack Surface Management with risk prioritization [12]
Alerts for domains that imitate your brand and for exposed credentials or keys	✓	?	No evidence of typosquatting or exposed secrets detection [17]
Annual penetration test (pentest)	✓ Annual	?	No evidence of its own pentesting service [12]
Remote monitoring and management (RMM)	✓	✗	Does not offer RMM [19]
Uptime monitoring (NOC)	✓	✗	Does not offer NOC or uptime monitoring [19]
Backup and continuity	3 of 3	0 complete	
		+0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	⊕ Add-on	✗	No backup offering [19]
Immutable backup vault (cannot be altered or deleted), isolated per customer	⊕ Add-on	✗	No backup vault [19]
Disaster recovery with drills and measured recovery time (RTO)	⊕ Add-on Measured RTO	✗	No disaster recovery; its financial warranty does not replace a recovery plan [20]
Compliance	6 of 6	0 complete	
		+2 partial	
Monthly evidence ready for auditors and insurers	✓ Monthly	⦿	Its Concierge team offers support with audits and reports; no monthly evidence package [7]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	⊕ Add-on	⦿	Compliance reports by framework; not a GRC platform with mapping [6]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	⊕ Add-on	✗	No coverage of Mexican regulations [6]
Risk management, controls, statement of applicability, and internal audits	⊕ Add-on	✗	No risk management, SoA, or internal audits for the customer [6]
Auditor portal with an evidence room and a public trust page (trust center)	⊕ Add-on	✗	Its own Trust Center, not offered to the customer [21]

Capability	TecnetSOC	Arctic Wolf SOC	Evidence on Arctic Wolf
✓ Offers it ✗ Not part of its published offering	ⓘ Offers it as an add-on ⓘ Partial, limited, or requires another contract	? No public evidence	
Business continuity, vendor risk, and data breach management	+ Add-on	✗	No continuity, vendor, or breach modules [6]
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✓ Per device	ⓘ	Charges per user or server plus a base fee; the endpoint protection module is charged per device; Silver to Platinum tiers [4]
Free plan to get started	✓ Up to 10 devices	✗	No free plan; base fee with a price published by the vendor [4]
Free trial in your real environment	✓ 30 days	ⓘ	Only a 30-day evaluation of its attack surface module, through its channel partners; no free trial of the SOC [22]
Available under your IT provider's brand	✓	✗	Sold through the channel with co-branded marketing materials; the service keeps the Arctic Wolf brand [23]
Full coverage	50	15 +16 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 Arctic Wolf: Arctic Wolf, most complete offering (Aurora MDR "Total" Platinum + Aurora Endpoint Security + Exposure Management with Resolve + Awareness Plus + Incident360 + Threat Intelligence Plus), 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. [arcticwolf.com/solutions/incident-response-retainer/](#) (Differences you notice day to day)

2. [docs.arcticwolf.com/en/arctic-wolf-unified-portal/unified-portal/au...](#) (Differences you notice day to day)

3. [arcticwolf.com/resources/blog-uk/an-in-depth-guide-to-pen-tests/](#) (Differences you notice day to day)

4. [www.freeitdata.com/wp-content/uploads/2025/01/AW-Public-Sector-Pric...](#) (Differences you notice day to day)

5. [arcticwolf.com/resources/press-releases/arctic-wolf-security-operat...](#) (Differences you notice day to day)

6. arcticwolf.com/compliance/ (Differences you notice day to day)
7. arcticwolf.com/solutions/managed-detection-and-response/faq/ (24/7 security operations center (SOC) with human analysts)
8. arcticwolf.com/aurora-soc/ (AI agents that investigate and filter alerts...)
9. www.globenewswire.com/news-release/2025/04/28/3069280/0/en/Arctic-Wolf-launches-aurora-soc/ (AI investigation assistant in the portal that...)
10. arcticwolf.com/company/overview/ (Operations in LATAM, the US, and Europe, with analysts...)
11. arcticwolf.com/es/ (Analysts, support, and portal in native Spanish)
12. arcticwolf.com/solutions/exposure-management/ (Leadership reports in Spanish and in business...)
13. arcticwolf.com/information-security/ (Independent certification of operations (ISO 27001...))
14. arcticwolf.com/resources/press-releases/arctic-wolf-launches-aurora-soc/ (Fast start with a software agent: your...)
15. docs.arcticwolf.com/en/aurora-endpoint-security/overview-and-architecture/ (Advanced protection on every device (EDR/XDR)...))
16. arcticwolf.com/resources/blog/arctic-wolf-product-updates-may-2026/ (Documented investigations enriched...)
17. arcticwolf.com/solutions/exposure-management/faq/ (Prioritized security recommendations with an...)
18. arcticwolf.com/resources/blog/vulnerability-prioritization-requires-advanced-technologies/ (Priority for flaws already being...)
19. arcticwolf.com/partners/ (Remote monitoring and management (RMM))
20. arcticwolf.com/why-arctic-wolf/security-operations-warranty/ (Disaster recovery with drills and...)
21. trust.arcticwolf.com/ (Auditor portal with an evidence room and a...)
22. www.channelinsider.com/security/arctic-wolf-new-partner-program-cyb/ (Free trial in your real environment)
23. arcticwolf.com/resources/press-releases/arctic-wolf-launches-new-an-soc/ (Available under your IT provider's brand)

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.



A SOC that speaks your language.

[See outdated or inaccurate information? Write to us and we'll correct it.](#)