

TecnetSOC vs. Wazuh

With Wazuh, you build and run the SOC yourself. TecnetSOC is already the SOC: AI that investigates, people who decide, in your language.

With Wazuh, you install the server, indexer, and dashboard and pay for the storage (or Wazuh Cloud, by agent tiers); your team reviews the alerts because there is no SOC or MDR. With TecnetSOC, you install one agent, the platform deploys itself, and the shift is ours.



44

capabilities where TecnetSOC goes further

6

capabilities where we match

0

capabilities where Wazuh 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 Wazuh: 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

Wazuh is an open SIEM and XDR platform that your team installs and runs; it is not a managed SOC service. Everything else you would need (EDR, RMM, backup) is purchased and run separately, and not everything integrates natively. This comparison shows, capability by capability, how much of what TecnetSOC includes Wazuh covers on its own and what you would have to add in products, contracts, and staff.

— WHAT SETS US APART

Differences you notice day to day

01
Your team runs everything

WITH WAZUH
Your team reviews every alert, tunes rules and decoders, and decides the response, at 3 a.m. too; Wazuh does not offer a SOC or MDR. [1]

WITH TECNETSOC
TecnetOne analysts operate 24/7 in your time zone and in Spanish; for a critical event, they notify you and start the investigation within 30 minutes, as a target.

02
You install and update the servers

WITH SELF-HOSTED WAZUH
You install the server, indexer, and dashboard with root permissions, and every update requires all three on the exact same version, down to the patch. [2]

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

03
You pay for log storage

WITH SELF-HOSTED WAZUH
You buy and manage the storage: the guide estimates 200 GB per 90 days of alerts with up to 100 devices, and it grows with every device. [3]

WITH TECNETSOC
The platform is a cloud service operated by TecnetOne: you don't buy, install, or maintain storage for your logs.

04
Detects vulnerabilities, doesn't patch them

WITH WAZUH
You detect vulnerabilities by CVE, but it doesn't apply patches: installing them, testing them, and scheduling windows is left to your team or another tool. [4]

WITH TECNETSOC
The SOC patches based on real-world exploitation (KEV and EPSS), validates in a pilot group, and closes only when the scanner confirms it.

05
Automated response without human approval

WITH WAZUH
Active Response runs scripts automatically when a rule fires, with no human approval step; isolating a device requires writing your own script. [5]

WITH TECNETSOC
Every alert arrives already investigated by AI agents, and a person approves every critical action before it runs (Human Gate).

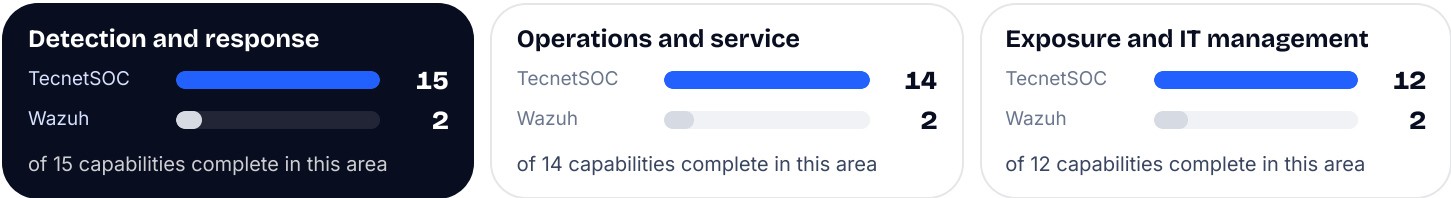
06
Network and email, separately

WITH WAZUH
Seeing network traffic requires installing and configuring Suricata, another product; email security, web filtering, and phishing simulations are not part of the platform. [6]

WITH TECNETSOC
NDR, IDS/IPS, email security, web filtering, and phishing simulations are included in its most complete offering.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Wazuh, side by side

Capability	TecnetSOC	Wazuh Open SIEM and XDR	Evidence on Wazuh
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	2 complete +4 partial	
24/7 security operations center (SOC) with human analysts		Your team provides it	Wazuh does not offer a SOC or MDR; professional support is technical [7]
AI agents that investigate and filter alerts before passing them to an analyst			No AI agents that filter every alert; only a guide for enriching with an LLM [8]
Human Gate: a person approves every critical action before it runs			Active Response fires automatically by rule; there is no human approval gate [9]

Capability	TecnetSOC	Wazuh Open SIEM and XDR	Evidence on Wazuh
☒ 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			
AI investigation assistant in the portal that cites its sources	☒ Neo	☐	AI Analyst (Wazuh Cloud only) generates periodic reports; it doesn't investigate on demand or narrate cases [10]
Operations in LATAM, the US, and Europe, with analysts in your time zone	☒	Your team provides it	No security operations; global "follow the sun" support, not from LATAM [7]
Analysts, support, and portal in native Spanish	☒	☐	Does not publish Spanish-language support or analysts [7]
Leadership reports in Spanish and in business language	☒	☐	Technical PDF reports and AI Analyst in English; no executive report in Spanish [10]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	Only a technical support SLA (Premium, 4 h for critical), not for security incidents [7]
Executive summary every morning: what happened in the last 24 hours	☒ 7:30 a.m.	Your team provides it	AI Analyst sends periodic emails with a posture summary; it is not a daily summary [10]
Automated weekly, monthly, quarterly, and annual reports	☒	☐	PDF reports from the dashboard and scheduled AI reports; no fixed weekly-to-annual schedule [10]
Assigned technical account manager (TAM) and quarterly reviews	☒	☒	Professional support includes a dedicated customer success manager and 4 health checks per year (Premium) [7]
24/7 contact with support or security staff	☒	☐	Premium is 24/7 only for critical issues; Standard is 8x5 [7]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	☒ ISO/IEC 27001:2022	☒	Wazuh Cloud states SOC 2 and PCI DSS; no published ISO 27001 [11]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☐	Wazuh Cloud starts quickly; the self-hosted version requires installing and sizing servers [11]
Detection and response	15 of 15	2 complete +7 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)	☒	☒	Core of the product: SIEM with rules, correlation, and MITRE ATT&CK mapping [12]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☐	Detects malware and rootkits with YARA rules and VirusTotal; no native vulnerability exploitation prevention or anti-ransomware [13]
Web filtering on the device	☒	☐	Does not offer web filtering on the device [14]
Intrusion detection (IDS/IPS)	☒	☐	Native host IDS; network IDS only by integrating Suricata (third party) [15]
Threat detection on the internal network (NDR)	☒	☐	No native NDR; depends on Suricata; agentless monitoring limited to SSH [15]
Documented investigations enriched with threat intelligence	☒	☒	Enrichment with CDB lists, VirusTotal, and Wazuh's own CTI [13]
Incident management with a case log and response time measured per case	☒	☐	Does not include case management or MTTR per incident; integrates with third parties [13]
Response with device isolation and IP address blocking	☒	☐	IP blocking included (firewall-drop, netsh); device isolation only with your own script [9]
Incident response with root cause analysis	☒	Your team provides it	Does not offer an incident response or forensics service [7]
Identity posture: MFA, privileged accounts, and conditional access	☒	☐	Ingests Entra ID logs via MS Graph; does not assess posture; no Google Workspace [16]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	Does not offer secure DNS, Zero Trust access, or shadow IT control [14]
Cloud security: alerts and posture	☒	☐	Monitors Azure and Microsoft 365 logs; posture documented only for GCP [17]
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☐	Does not offer email security [14]

Capability	TecnetSOC	Wazuh Open SIEM and XDR	Evidence on Wazuh
☒ 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			
Security awareness: phishing simulations and training with metrics	☒	☐	Does not offer security awareness or phishing simulations [14]
Prioritized security recommendations with an approval workflow	☒	☒	SCA provides hardening recommendations; no business prioritization or approval workflow [13]
Exposure and IT management	12 of 12	2 complete +2 partial	
Unified asset and software inventory	☒	☒	Syscollector inventories hardware, system, packages, ports, and processes [13]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	Detection by CVE with CVSS and severity; no published EPSS [18]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☒	CISA is listed as a data source; no documented explicit prioritization by KEV [18]
Operating system and third-party application patching	☒	☐	Detects vulnerabilities but does not apply patches [14]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	No patching or operated service with published timelines [14]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	Detects Windows hotfixes and marks as resolved the CVEs the patch fixes [18]
Patch validation in a pilot group before rollout	☒	☐	No patching, so no pilot group [14]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	Does not offer external attack surface management (EASM) [14]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	Does not detect lookalike domains; GitHub is monitored only through activity auditing [19]
Annual penetration test (pentest)	☒ Annual	Your team provides it	Does not offer pentesting [7]
Remote monitoring and management (RMM)	☒	☐	It is not an RMM tool [14]
Uptime monitoring (NOC)	☒	☐	No NOC-style uptime monitoring [14]
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 [14]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	Does not offer an immutable backup vault [14]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	Does not offer disaster recovery [14]
Compliance	6 of 6	0 complete +2 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	Compliance dashboards (PCI DSS, HIPAA, NIST, GDPR, TSC); does not deliver monthly evidence [20]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Maps alerts to PCI DSS and TSC (SOC 2); no ISO 27001 or GRC platform [20]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican frameworks (CNBV, LFPDPPP, NOM-024) [20]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	Does not manage risks, SoA, or internal audits [20]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	No auditor portal or Trust Center for the customer [20]
Business continuity, vendor risk, and data breach management	☒ Add-on	☐	No continuity, vendor, or breach management modules [20]

Capability	TecnetSOC	Wazuh Open SIEM and XDR	Evidence on Wazuh
✔ Offers it ✗ Not part of its published offering	⊕ Offers it as an add-on ⦿ Your team provides it	⦿ Partial, limited, or requires another contract	❓ No public evidence
How it's purchased	Not counted		
Per-device pricing, with plans that stack	✔ Per device	⦿	Free open source; Cloud by agent tiers (100, 250, 500), not stackable per-device pricing [11]
Free plan to get started	✔ Up to 10 devices	✔ No license cost	The open source platform is free with no device limit, self-hosted [14]
Free trial in your real environment	✔ 30 days	⦿	14-day Wazuh Cloud trial (21 via a partner), not 30 [11]
Available under your IT provider's brand	✔	✔	Partner program with a multi-tenant console and authorized white labeling [21]
Full coverage	50	6 +15 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.

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 Wazuh: Wazuh, open source platform (free, self-hosted, installed and run by the company itself) and Wazuh Cloud (SaaS from Wazuh Inc. by agent tiers, with a price published by the vendor; Wazuh maintains the platform, the company runs security), with Premium professional support and Wazuh Cloud AI Analyst. Offering evaluated as a company adopts it on its own, without a managed security provider partner. 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. documentation.wazuh.com/current/user-manual/ruleset/index.html (Differences you notice day to day)
2. documentation.wazuh.com/current/upgrade-guide/index.html (Differences you notice day to day)
3. documentation.wazuh.com/current/quickstart.html (Differences you notice day to day)
4. documentation.wazuh.com/current/user-manual/capabilities/vulnerabil... (Differences you notice day to day)
5. documentation.wazuh.com/current/user-manual/capabilities/active-res... (Differences you notice day to day)
6. documentation.wazuh.com/current/proof-of-concept-guide/integrate-ne... (Differences you notice day to day)
7. wazuh.com/services/professional-support/ (24/7 security operations center (SOC) with human analysts)
8. documentation.wazuh.com/4.14/proof-of-concept-guide/leveraging-llms... (AI agents that investigate and filter alerts...)
9. documentation.wazuh.com/4.14/user-manual/capabilities/active-respon... (Human Gate: a person approves every...)
10. documentation.wazuh.com/4.14/cloud-service/ai-analyst.html (AI investigation assistant in the portal that...)
11. wazuh.com/cloud/ (Independent certification of operations (ISO 27001...))
12. wazuh.com/platform/siem/ (Continuous monitoring and event correlation...)
13. documentation.wazuh.com/4.14/user-manual/capabilities/index.html (Advanced protection on every device (EDR/XDR)...)
14. wazuh.com/platform/overview/ (Web filtering on the device)
15. documentation.wazuh.com/4.14/proof-of-concept-guide/integrate-netwo... (Intrusion detection (IDS/IPS))
16. documentation.wazuh.com/4.14/cloud-security/azure/monitoring-ms-gra... (Identity posture: MFA, privileged accounts...)
17. documentation.wazuh.com/4.14/cloud-security/azure/index.html (Cloud security: alerts and posture)
18. documentation.wazuh.com/4.14/user-manual/capabilities/vulnerability... (Vulnerabilities prioritized by severity...)
19. documentation.wazuh.com/4.14/cloud-security/github/index.html (Alerts for domains that imitate your brand...)
20. documentation.wazuh.com/4.14/compliance/index.html (Monthly evidence ready for auditors and insurers)
21. wazuh.com/partners/ (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.](#)