

TecnetSOC vs. Expel

Expel runs the tools you bought. TecnetSOC comes with everything included and runs it for you, 24/7.

With Expel, you buy and renew the licenses for your EDR and your SIEM, and its analysts get access to your consoles and your devices. TecnetSOC brings its own platform, doesn't ask for credentials to your consoles, and you can try Response for 30 days.



41

capabilities where TecnetSOC goes further

9

capabilities where we match

0

capabilities where Expel outperforms TecnetSOC

Of the 50: 41 where we go further and 9 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Expel: 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

Expel is a managed SOC service that works on top of the security tools you already have; you provide the device protection, the SIEM, and email security. Here we compare each one's most complete published offering, capability by capability.

— WHAT SETS US APART

Differences you notice day to day

01
You pay for the tools

WITH EXPEL
You buy and renew the licenses for your EDR, your SIEM, and other tools; Expel connects via API and works on top of what you already have. [\[1\]](#)

WITH TECNETSOC
The most complete plan already includes a SIEM with MITRE ATT&CK correlation, EDR/XDR, NDR, IDS/IPS, and web filtering.

02
It recommends, your team patches

WITH EXPEL
You receive remediation recommendations and root cause analysis; applying and testing patches is left to your team. [\[2\]](#)

WITH TECNETSOC
The SOC patches: it prioritizes by KEV and EPSS, validates in a pilot group, and closes only when the scanner confirms it.

03
Its analysts get into your consoles and devices

WITH EXPEL
Your team hands over credentials and gives its analysts access to your EDR and SIEM console, including the remote terminal on your devices. [\[3\]](#)

WITH TECNETSOC
You install one agent, the rest of the platform deploys on its own, and you don't hand over administrator credentials.

04
Analysts in the US and support in English

WITH EXPEL
All of its analysts work from the US, and its website and documentation are in English; it doesn't publish support in Spanish or operations in LATAM. [\[4\]](#)

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

05
Phishing as a separate add-on

WITH EXPEL
Phishing is an add-on that investigates the emails your employees report; it doesn't publish its own anti-spam filter or phishing simulations for your staff. [\[5\]](#)

WITH TECNETSOC
The most complete plan includes email security (spam, phishing, malware, BEC) and phishing simulations for your staff.

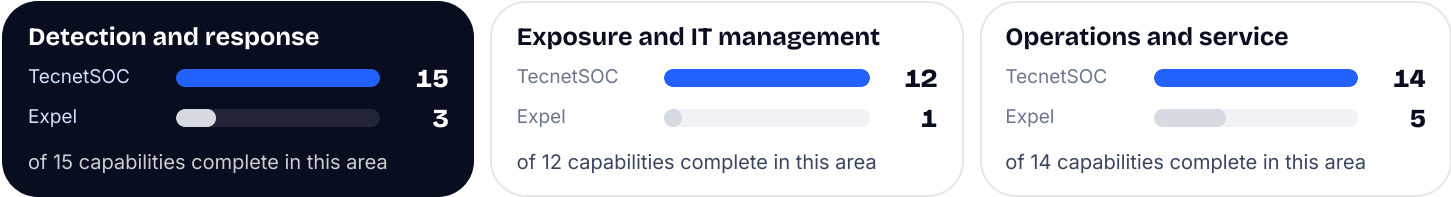
06
Demo, quote, and upfront payment

WITH EXPEL
You get a custom quote, and its website offers a demo, with no published free trial; on AWS Marketplace you sign up for 12 to 36 months, paid upfront, with no refunds. [\[6\]](#)

WITH TECNETSOC
You pay per device, Visibility is free for up to 10 devices, and you try Response for 30 days in your real environment.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Expel, side by side

Capability	TecnetSOC	Expel SOC	Evidence on Expel
 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			24×7×365 SOC with human analysts and direct access to them [1]
AI agents that investigate and filter alerts before passing them to an analyst			Ruxie and its triage and correlation agents investigate alerts before the analyst [7]
Human Gate: a person approves every critical action before it runs			Analysts validate the threat before Ruxie runs containment [1]
AI investigation assistant in the portal that cites its sources	 Neo		Ruxie as an "AI SOC manager"; no evidence of an on-demand conversational assistant that cites sources [8]

Capability	TecnetSOC	Expel SOC	Evidence on Expel
Offers it Offers it as an add-on Partial, limited, or requires another contract No public evidence Not part of its published offering			
Operations in LATAM, the US, and Europe, with analysts in your time zone			SOC focused on North America; no operations in LATAM [9]
Analysts, support, and portal in native Spanish			No evidence of Spanish-speaking analysts or support [10]
Leadership reports in Spanish and in business language			Reports in English; no Spanish version [1]
Published notification and investigation start times by severity	 Critical: 30 min (target)		Mean response time of 14 min and a 5 min target cited by third parties; no published contractual commitment [11]
Executive summary every morning: what happened in the last 24 hours	 7:30 a.m.		No evidence of a daily executive summary [1]
Automated weekly, monthly, quarterly, and annual reports			Monthly metrics report only; no published weekly, quarterly, or annual reports [1]
Assigned technical account manager (TAM) and quarterly reviews			Dedicated relationship manager in Premium; quarterly reviews not confirmed [2]
24/7 contact with support or security staff			24x7 support from onboarding to day-to-day questions, with direct access to SOC experts [2]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	 ISO/IEC 27001:2022		ISO 27001, ISO 27701, and SOC 2 Type II certified (Trust Center) [12]
Fast start with a software agent: your devices' activity, visible within hours	 Typical: 2 to 4 hours		API connection in minutes with no agent, but requires the customer to have its own tools [13]
Detection and response	15 of 15 	3 complete +9 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)			Correlation in Workbench and Managed SIEM on the customer's Sentinel or Splunk [14]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation			No EDR of its own; works on the customer's CrowdStrike, Defender, SentinelOne [11]
Web filtering on the device			No native web filtering on the device [1]
Intrusion detection (IDS/IPS)			Monitors network alerts from third-party firewalls or sensors; no IDS of its own [1]
Threat detection on the internal network (NDR)			Network coverage only through integrated third-party tools [1]
Documented investigations enriched with threat intelligence			Investigations enriched with intelligence and full traceability in Workbench [1]
Incident management with a case log and response time measured per case			Workbench logs every action; monthly report with MTTD and MTTR [1]
Response with device isolation and IP address blocking			Automated remediation: isolate a device, disable an account, and block, through the customer's tools [11]
Incident response with root cause analysis			Full forensic response separately or under a prior contract, according to an independent directory; no official confirmation [9]
Identity posture: MFA, privileged accounts, and conditional access			Identity detection (Okta, Entra); no posture management or privileged accounts [1]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)			No secure DNS, Zero Trust access, or shadow IT control [1]
Cloud security: alerts and posture			Detection in Azure, AWS, GCP, and OCI; cloud posture not evidenced [1]
Email security: spam, phishing, malware, and impersonation fraud (BEC)			Triage of the reported phishing mailbox; no anti-spam or quarantine of its own [5]
Security awareness: phishing simulations and training with metrics			No phishing simulations or user training [5]

Capability	TecnetSOC	Expel SOC	Evidence on Expel
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			Resilience recommendations in Workbench; no evidenced approval workflow [1]
Exposure and IT management	12 of 12	1 complete	
		+1 partial	
Unified asset and software inventory			No asset and software inventory of its own [15]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)			Prioritizes with the customer's Qualys, Tenable, or Rapid7 data; doesn't scan [15]
Priority for flaws already being exploited (CISA KEV catalog)			Vulnerability Prioritization evaluates every update to the KEV catalog and EPSS [16]
Operating system and third-party application patching			Doesn't patch; only recommends, the customer executes [15]
Provider-operated patching, with published timelines by severity	 Critical: 48 h (target)		No operated patching or published timelines [15]
Closure verification: the scanner confirms the vulnerability is gone			No closure verification of its own [15]
Patch validation in a pilot group before rollout			No patch validation in a pilot group [15]
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 [10]
Alerts for domains that imitate your brand and for exposed credentials or keys			No typosquatting or exposed secrets detection [10]
Annual penetration test (pentest)	 Annual		No pentesting [10]
Remote monitoring and management (RMM)			No RMM [10]
Uptime monitoring (NOC)			No NOC or uptime monitoring [10]
Backup and continuity	3 of 3	0 complete	
		+0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	Add-on		No backup [10]
Immutable backup vault (cannot be altered or deleted), isolated per customer	Add-on		No immutable vault [10]
Disaster recovery with drills and measured recovery time (RTO)	Add-on Measured RTO		No disaster recovery [10]
Compliance	6 of 6	0 complete	
		+0 partial	
Monthly evidence ready for auditors and insurers	 Monthly		No monthly evidence for auditors or insurers [10]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	Add-on		No GRC platform for the customer [10]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	Add-on		No Mexican regulations [10]
Risk management, controls, statement of applicability, and internal audits	Add-on		No risk management, SoA, or internal audits [10]
Auditor portal with an evidence room and a public trust page (trust center)	Add-on		The Trust Center belongs to Expel, not a service for the customer [12]
Business continuity, vendor risk, and data breach management	Add-on		No business continuity or vendor management [10]

Capability	TecnetSOC	Expel SOC	Evidence on Expel
✓ 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 by integrations and volume, not per device [17]
Free plan to get started	✓ Up to 10 devices	✗	No free plan [6]
Free trial in your real environment	✓ 30 days	✗	Online demo only; no published free trial [18]
Available under your IT provider's brand	✓	✗	No IT provider branding or multi-tenant console; announced as a future plan according to MSSP Alert [19]
Full coverage	50	9 +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 Expel: Expel MDR Premium package plus Managed SIEM, Phishing, Vulnerability Prioritization, and AI surface coverage, 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. [expel.com/services/managed-detection-response/](#) (Differences you notice day to day)

2. [expel.com/mdr-packages/](#) (Differences you notice day to day)

3. [docs.expel.io/connect-your-technology/about-integrations/why-expel-...](#) (Differences you notice day to day)
4. [expel.com/meet-the-soc-experts/](#) (Differences you notice day to day)

5. [expel.com/services/phishing/](#) (Differences you notice day to day)

6. [aws.amazon.com/marketplace/pp/prodview-65wyj23v3b3ea](#) (Differences you notice day to day)

7. [expel.com/blog/what-we-built-july-2026/](#) (AI agents that investigate and filter alerts...)
8. [expel.com/blog/new-ruxie-power-up-ai-detection-agent/](#) (AI investigation assistant in the portal that...)

9. [mdrproviders.io/providers/expel](#) (Operations in LATAM, the US, and Europe, with analysts...)

10. [expel.com/](#) (Analysts, support, and portal in native Spanish)

11. [expertinsights.com/endpoint-security/expel-mdr-par](#) (Published notification and investigation...)

12. [security.expel.com/](#) (Independent certification of operations (ISO 27001...))

13. [expel.com/resource/expel-mdr-onboarding-get-up-and-running-in-7-min...](#) (Fast start with a software agent: your...)

14. [www.prnewswire.com/news-releases/expel-launches-managed-siem-to-hel...](#) (Continuous monitoring and event correlation...)

15. [expel.com/services/vulnerability-prioritization/](#) (Unified asset and software inventory)

16. [expel.com/blog/mdr-insights-using-vulnerability-data-to-inform-reme...](#) (Priority for flaws already being...)

17. [mdrcost.com/expel-pricing](#) (Per-device pricing, with plans that stack)

18. [expel.com/on-demand-mdr-demo/](#) (Free trial in your real environment)

19. [www.msspalert.com/news/expel-expands-mdr-coverage-across-the-ai-att...](#) (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.](#)