EDGE TEAM
TECHNOLOGY

WHITE PAPER

Build, buy, or borrow

How to decide between an in-house SOC, an MSSP, and managed detection and response.

For: IT and security leaders deciding who watches the environment around the clock, at organizations of any size.

Reading time: ~12 minutes · May 2026

Executive summary

Every organization eventually faces the same question. Threats do not keep business hours, so something has to watch the environment around the clock and act when an attack is underway. The real question is who does that watching, and how. There are three honest answers. Build the capability in-house, buy it as a service, or borrow it from a partner who already runs one.

This paper is for the IT or security leader weighing that decision. It lays out what round-the-clock detection actually requires, defines the often-confusing menu of options, and offers a framework for choosing among them based on your size, budget, and risk.

The thesis is that the right answer depends far less on technology than on simple arithmetic. Continuous coverage takes a surprising number of people, the talent to staff it is scarce and expensive, and the volume of alerts overwhelms small teams. For most organizations the practical answer is to keep the decisions that require knowing the business and delegate the around-the-clock watching to a partner who can staff it.

What you will leave with

- Why 24/7 coverage is harder and more costly than it first appears.
- Plain definitions of SOC, SIEM, MSSP, MDR, and co-managed models.
- A build, buy, or borrow framework matched to organization size.
- The handful of metrics that tell you whether detection is actually working.

EDGE TEAM
TECHNOLOGY

1. The round-the-clock problem

A security operations center, usually shortened to SOC, is the function that watches for attacks and responds to them. The hard part lives in the phrase round-the-clock. An attack at two in the morning on a holiday weekend needs the same response as one at two in the afternoon on a Tuesday, and attackers deliberately choose the quiet hours.

The shift math

Keeping a single seat staffed every hour of every day takes more people than most leaders expect. Three shifts a day, plus cover for weekends, holidays, vacation, illness, and turnover, works out to a minimum of roughly five to eight analysts simply to keep one chair filled continuously. That is before adding a manager, a detection engineer to tune the tooling, and someone who tracks threat intelligence. A real team is larger still.

The talent is scarce

The cybersecurity workforce gap is measured in the millions of unfilled roles worldwide. Experienced analysts are expensive and in high demand, and the night and weekend shifts that continuous coverage depends on are the hardest of all to hire for and to keep filled. Building a team is not a one-time act of hiring. It is a permanent recruiting and retention effort.

Alert fatigue

Detection tools generate enormous volumes of alerts, and most of them are duplicates or false positives. A small team cannot triage them all, so genuine signals get buried in the noise. The common failure mode is not a missing alert. It is an alert that fired correctly and that no one had the time to open.

> **IN PRACTICE**
> The painful version of this story is the breach that was detected and ignored. The alert was there the whole time, somewhere in the queue behind a thousand others. Coverage is not only about tools that can see. It is about people with the time to look.

2. Sorting out the vocabulary

The market for security operations is crowded with overlapping acronyms, and the words are often used loosely. Getting them straight is the first step toward a clear decision.

In-house SOC

Your own people, processes, and tools running detection and response. It offers maximum control and the deepest understanding of your environment, at maximum cost and staffing burden.

SIEM

Security information and event management. The platform that collects logs from across the environment and correlates them into alerts. It is the backbone of detection, and it is a tool rather than a service. A SIEM with no one watching it is an expensive log archive.

MSSP

A managed security service provider runs broad security operations such as managing firewalls and running scans, and traditionally monitors and forwards alerts for your own team to investigate. The scope is wide, but the engagement often stops at the handoff.

MDR

Managed detection and response sells an outcome rather than a stream of alerts. The provider investigates, hunts for threats, and takes action to contain them, including isolating a compromised machine. The defining difference from a traditional MSSP is that response is included.

SOCaaS and co-managed models

SOC as a service delivers the full function on a subscription. A co-managed model splits the work: you keep your own platform and some staff, and the partner adds around-the-clock analysts and expertise on top.

> **THE KEY DISTINCTION**
> An MSSP tells you something happened. An MDR does something about it. That single difference drives most of the value gap between the two, and it is the first thing to pin down with any provider.

3. Build, buy, or borrow

With the vocabulary clear, the choice reduces to three paths. Each is legitimate, and the right one depends mostly on your size and circumstances.

Build

Stand up your own SOC. This fits larger organizations, often those past several thousand endpoints, that have the budget for a full team and a strong reason to keep everything in-house, such as strict data residency or regulatory requirements. The reward is deep context and direct control. The cost is high and never stops.

Buy

Purchase the SOC function as a service. You gain the capability without hiring and retaining the entire team yourself, while still standing up the surrounding program and governance. This suits organizations that want the function in place quickly without building it from nothing.

Borrow

Use managed detection and response, very often alongside a small internal team. This is the practical answer for most small and mid-size organizations. It reaches full coverage quickly, carries a predictable cost, and fills the nights and weekends an internal team cannot. A common and effective arrangement is hybrid: the internal team works business hours, and the partner covers everything outside them.

Size is the simplest guide. The smaller the team, the stronger the case for borrowing. The larger and more heavily regulated the organization, the more building can be justified. Most organizations land in the middle, with a co-managed or hybrid arrangement that blends internal knowledge with external coverage.

EDGE TEAM
TECHNOLOGY

4. Knowing whether it works

Whichever path you choose, a few metrics reveal whether detection is actually working. They matter just as much when judging a partner as when running your own team, so learn them before you sign anything.

Mean time to detect

The average time from when an attack begins to when it is noticed. Lower is better, because everything an attacker accomplishes happens inside that window. A long detection time means the intruder had room to work.

Mean time to respond

The average time from a confirmed incident to containment. This is where managed detection and response earns its name, because fast containment is what limits the damage once something is found.

Dwell time

How long an attacker stays in the environment undetected. The longer the dwell, the more time to move laterally, steal data, and establish persistence. Industry reporting now places the global median dwell time at roughly eleven days, down sharply from the weeks or months common a decade ago, largely because detection has improved.

When you evaluate a provider, ask how they measure these and what their targets are. A credible partner answers in minutes and hours, commits to specific containment actions, and reports on them honestly. A weaker one talks mainly about how many alerts it forwarded to you.

> **THE TEST**
> The right question for any provider is simple. When you find something at three in the morning, do you act, or do you send me an email and wait for a reply? The answer separates real detection and response from alert forwarding.

5. What to keep, what to delegate

Borrowing detection does not mean outsourcing responsibility. The work splits cleanly into what only you can own and what a partner is better placed to run.

Keep in-house

- Governance, risk, and compliance, and the security strategy that sets the priorities.
- Architecture and tool decisions, including which platforms you standardize on.
- Business context and the final call on response actions that affect operations, plus an internal liaison to the partner.

Delegate to a partner

- Around-the-clock monitoring and triage, especially during nights and weekends.
- Threat hunting and first-line investigation of the alerts that matter.
- Active containment during a live incident, which is what managed detection and response provides.

A note on cost

Building a SOC is a seven-figure commitment in most cases once you add the platform, the licensing, and a team large enough to cover every hour of the year. Borrowing through managed detection and response typically runs a fraction of that, scaled to the size of your environment, with a predictable annual cost. A hybrid model sits in between. For most organizations the arithmetic points in the same direction.

This is the value-added reseller model. EdgeTeam helps you run the build, buy, or borrow decision honestly, designs the architecture and logging that detection depends on, recommends the right managed partner for your environment without loyalty to any single vendor, and stays involved as your architect of record. You keep the decisions that require knowing your business. We bring the design and coordinate the specialists who watch the environment.

Conclusion

Round-the-clock security comes down to arithmetic more than technology. Continuous coverage takes more people than most teams can hire, the talent is scarce, and the alerts pile up faster than a small team can read them. Recognizing that early is what turns a vague sense of exposure into a clear and defensible decision.

For a few large, well-funded, heavily regulated organizations, building makes sense. For most, the honest answer is to keep the decisions that require knowing the business and borrow the around-the-clock watching from a partner who can staff it. The goal is simple: make sure someone is always watching and always ready to act, whoever that someone turns out to be.

Next step

EdgeTeam's Security Posture Review includes a detection readiness check: a look at what you can see today, where the coverage gaps are, and whether building, buying, or borrowing fits your size and budget. We will scope it to your environment on the first call.

Request a posture review: edgeteam.com/cybersecurity

Or call the bridge: 1.866.EDGETEAM, available 24/7.

About EdgeTeam Technology

EdgeTeam is a value-added reseller and architect of record for organizations across K-12, Higher Education, SMB, Enterprise, and Local Government. We design, recommend, and coordinate cybersecurity, infrastructure, and connectivity engagements with vendor-neutral partners. We do not run an in-house SOC. We pair our architecture team with the right managed partner for your environment.

edgeteam.com · sales@edgeteam.com · 1.866.EDGETEAM