

APTO WHITEPAPER

April 2026

The Operator Gap

What true Managed SIEM looks like — and why most MSSPs aren't doing it

A practical guide for security and IT leaders who have invested in SIEM and want it to deliver.

Apto Solutions

aptosolutions.co.uk

Contents

Executive summary	3
1. The Operator Gap	4
2. The Four Pillars of True Managed SIEM.....	6
3. Managed SIEM vs Managed SOC — Two Distinct Layers	8
4. The Industry Confusion — When “Managed SIEM” Isn’t	10
5. How Apto Operates SIEM Differently	12
6. Choosing the Right Engagement Model	13
7. Getting Started.....	14
About Apto Solutions.....	15

Executive summary

UK enterprises have collectively spent hundreds of millions of pounds deploying SIEM platforms over the past decade. Most of those deployments are not delivering proportional security value. The cause is rarely the technology — it is almost always the operating model.

This paper introduces a concept we call the Operator Gap: the missing role between the engineers who deploy a SIEM and the analysts who consume its outputs. We explain what a true Managed SIEM service does, how it differs from a Managed SOC, and why the offering most MSSPs label “Managed SIEM” is something materially different. Finally, we set out the engagement patterns Apto uses to close the Operator Gap on our customers’ own platforms.

Three things to take away:

- A clear definition of the four operational pillars of a true Managed SIEM service.
- A diagnostic for whether your current arrangement is platform operations on your SIEM, or a SOC service on someone else’s.
- A practical starting point — entry-level engagements you can use to test the discipline before committing to a long-term contract.

1. The Operator Gap

You will recognise the pattern. Capital expenditure is approved. The platform is procured, deployed, and connected to its first set of data sources. Dashboards are built. Training is delivered. The project team disbands. There is a launch event, and for a few weeks the new SIEM gets attention from across the security team.

Six months later, a quieter pattern emerges. The detection rules that worked at go-live have not been updated. New data sources have been onboarded but never properly tagged. Search performance has degraded. The licence is creeping toward its limit and nobody is sure why. Analysts have started ignoring entire categories of alert because the signal-to-noise ratio is poor. None of this is dramatic; all of it is corrosive.

The reason this happens so consistently across UK enterprises is structural, not accidental. Every SIEM deployment has three roles that need to be filled, and most organisations have only filled two of them.

The Three Roles Every SIEM Deployment Needs

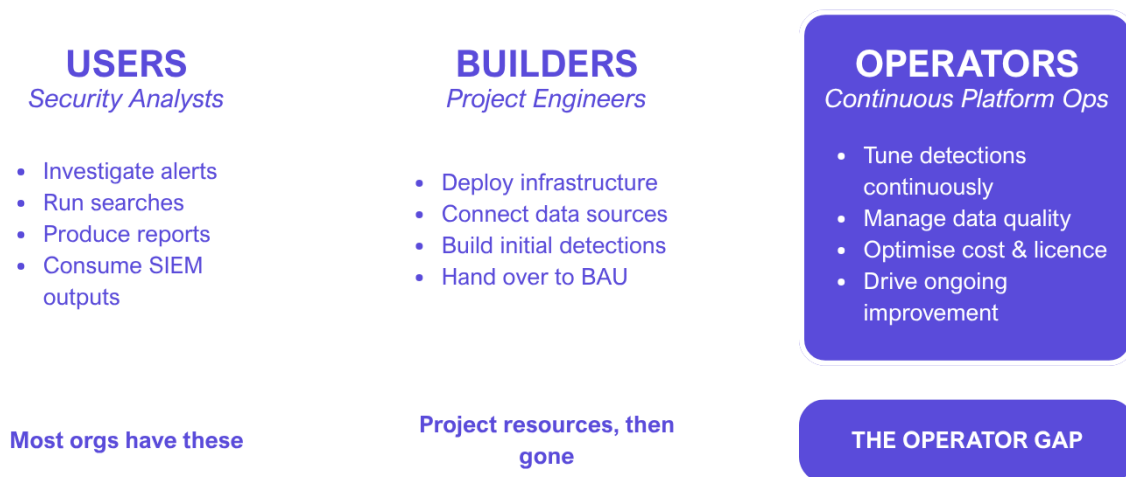


Figure 1. The three roles every SIEM deployment needs. Most organisations have only filled two of them — and that is the Operator Gap.

Users and Builders are familiar shapes in any security organisation. Users are the analysts who consume SIEM outputs — investigating alerts, running searches, producing reports. Builders are the engineers who stood up the platform — racking infrastructure, configuring connectors, writing the first detection rules. They were almost certainly project resources, and almost certainly moved on once the platform went live.

Operators are different. They are the people who run the platform day-to-day. They tune detections as the threat landscape shifts. They police data quality as new sources are added and existing sources change format. They optimise cost as ingestion volumes grow. They make sure the platform improves rather than degrades. They have a playbook of continual indicators that monitor and observe the

platform. They are not analysts and they are not project engineers — they are continuous platform operators, and almost no UK enterprise has them as dedicated, named roles.

That is the Operator Gap. It is why the majority of SIEM deployments under-perform within twelve months of going live. The technology vendor's account team will tell you the answer is more product. The integrator who built the platform will tell you the answer is another project. Neither is wrong, exactly, but neither is sufficient — because the platform does not need another build; it needs an operator.

Why this role is hard to staff in-house

A reasonable response to all of this is, “We will recruit a SIEM engineer.” In practice this is one of the hardest hires in the UK security labour market. The skill profile is rare: someone who understands the platform deeply, can interpret risk registers and threat models (if there is one!), can write detection logic, can manage data engineering, and can hold a conversation with both the SOC and the procurement team. Where they exist, they command salaries that most security functions cannot accommodate within their headcount budget. Where you do hire them, retention is poor — they are heavily targeted by vendors and consultancies, and the role is difficult to make rewarding inside a single end-user organisation because there is rarely enough variety of work. They are also certainly not going to play monitoring platform operations role, they are ‘engineers’.

The result is that most CISOs end up either tolerating the gap, papering it over with rotational secondments from other infrastructure teams, or buying a service. The first option is corrosive; the second is unsustainable; the third is the subject of the rest of this paper.

2. The Four Pillars of True Managed SIEM

A true Managed SIEM service exists to fill the Operator Gap. It is not outsourced SOC — that is a different service, covered in section 3. It is the operating layer that ensures your SIEM platform works effectively so that your analysts can spend their time on threats rather than tooling.

Across our Operate engagements, we see four pillars of activity that define what a real Managed SIEM service does. A provider that does not deliver across all four is offering something narrower — and you should know which one you are buying.

The Four Operational Pillars of a True Managed SIEM Service

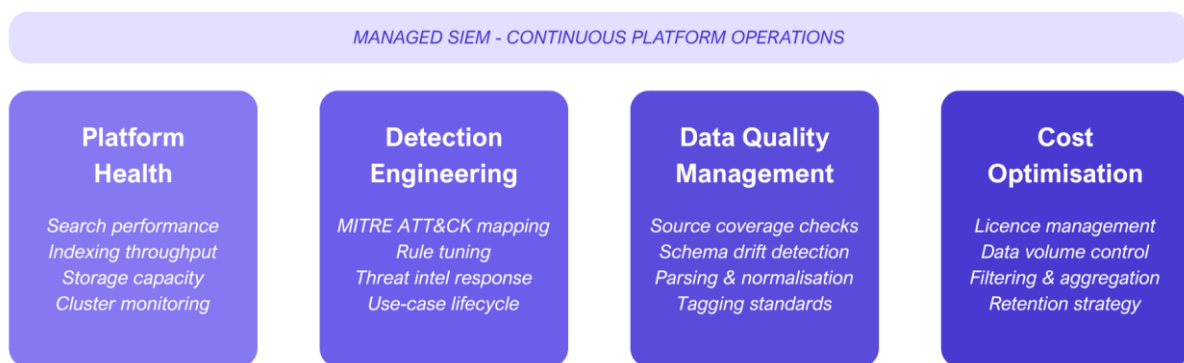


Figure 2. The continuous four operational pillars of a true Managed SIEM service. A provider that does not deliver across all four is offering something narrower.

Pillar 1 — Platform Health and Performance

The first pillar is the unglamorous one: making sure the platform itself continues to perform. Search latency, indexing throughput, storage capacity, cluster health, upgrade lifecycle. Most internal teams reach for this category last because it feels like infrastructure work, not security work. The result is that performance issues are usually detected by analysts complaining that searches are slow — by which point the problem has been live for weeks.

A managed SIEM operator monitors platform health proactively. Capacity is forecast. Upgrades are planned and rehearsed. Performance regressions are caught at the infrastructure layer before they show up in the analyst experience. The platform feels reliable, and reliable platforms get used.

Pillar 2 — Detection Engineering

The second pillar is the most visible one: detection logic. Rules, correlation searches, risk scores, alert thresholds — the working content that turns raw data into security signals. This is where the Operator Gap shows up most painfully, because detection content has to evolve continuously to keep pace with two moving targets: the threat landscape, and the customer’s own environment.

A managed SIEM operator runs a detection engineering lifecycle. New use cases are designed against frameworks like MITRE ATT&CK and your own threat models. Existing rules are tuned to reduce false

positives. Threat intelligence is ingested into detections rather than left to rot in a feed. Retired use cases are documented and removed cleanly. The detection library is treated as a product, not as a static configuration. Analysts feel the difference within weeks.

Pillar 3 — Data Quality Management

The third pillar is the one most often missed entirely: data quality. The most beautifully tuned detection rule in the world produces nothing if the data it depends on stops arriving, changes format silently, or is mis-tagged at source. Data quality drift is the single biggest cause of detection coverage degradation we see in legacy SIEM environments.

A managed SIEM operator monitors data quality continuously. Source coverage is tested — every expected source is reporting, on schedule, in the expected format. Schema drift is detected, owned, and resolved. Parsing and normalisation pipelines are validated end-to-end. Tagging standards are enforced at ingest, not retrofitted later. This is unglamorous work, and it is where managed SIEM most clearly differs from any other service tier.

Pillar 4 — Cost Optimisation

The fourth pillar is the one that pays for the others. SIEM costs grow faster than security budgets, almost without exception. Volume-based licensing creates a perverse incentive — the easiest way to “use the platform more” is to ingest more data, regardless of value. Within two or three years, most UK enterprises are spending a meaningful share of their security budget on data they are not actually using to detect anything.

A managed SIEM operator manages cost as a continuous discipline. Data volumes are reviewed by source. Low-value data is filtered, aggregated, or routed to cheaper tiers. Retention policies are tied to detection requirements, not to default settings. Licence headroom is monitored and forecast, not discovered the week before renewal. In several of our engagements, this pillar alone has paid for the rest of the service many times over. But does every pound saved also reduce coverage? Increase risk, its not a simple formula.

These four pillars are not optional extras. They are the working definition of a true Managed SIEM service. When you evaluate a provider, the question to ask is not “Do you do Managed SIEM?” — every provider says yes — but “Show me how you deliver each of these four pillars on my platform.” The answers will be revealing.

3. Managed SIEM vs Managed SOC — Two Distinct Layers

The terms Managed SIEM and Managed SOC are routinely used interchangeably in vendor marketing. They describe fundamentally different services, and confusing them is the most common source of bad procurement outcomes we see in this market.

What a Managed SOC provides

A Managed SOC is a service that provides human security analysts, (yes with some automation!). They monitor your environment, triage alerts, investigate incidents, and coordinate response. The focus is on the security workflow — the people-and-process layer that turns detections into action. A typical Managed SOC offering covers 24/7 monitoring and triage, incident investigation and escalation, threat hunting, response coordination, and regular reporting on security posture.

What a Managed SIEM provides

A Managed SIEM service focuses on the platform itself — the technology that collects, correlates, and presents the data on which the SOC depends. The focus is on the operating layer beneath the workflow. A typical Managed SIEM offering covers the four pillars described in section 2: platform health, detection engineering, data quality, and cost optimisation.

The relationship between them

The relationship between them is hierarchical, not lateral. A SOC needs a well-operated SIEM to be effective — without one, the analysts spend their day fighting tooling rather than threats. But a well-operated SIEM does not automatically give you a SOC: it gives the SOC something good to work with.

Managed SOC vs Managed SIEM – Two Distinct Layers



Figure 3. Two distinct layers. A Managed SOC handles the security workflow. A Managed SIEM handles the platform operations the SOC depends on.

You can buy these layers separately, and many UK enterprises do. A common pattern is an organisation with a strong internal SOC team — well staffed, well trained, capable of investigation and response — but no dedicated platform engineer. They buy Managed SIEM to fill the platform layer while keeping security operations in-house. Another common pattern is an organisation with no internal analyst capacity that buys both layers from one or more partners. Both are valid; the important thing is to know which problem you are buying a solution to. But again, an operational model orchestrating those layers is not present, managed SIEM demands, offers and delivers that.

A short decision aid

A short diagnostic helps. If your symptoms are alert fatigue, cost creep, detection drift, or poor coverage of your own data sources — the platform is the problem, and you need Managed SIEM. If your symptoms are insufficient analyst hours, no out-of-hours coverage, slow incident response, or inability to hire SOC staff — the workflow is the problem, and you need Managed SOC. Most organisations have some of both. Buying Managed SOC when your real problem is platform operations is the most expensive way to find out you needed Managed SIEM all along.

4. The Industry Confusion — When “Managed SIEM” Isn’t

This is the section we most need this paper to land. The marketing language used by managed SOC providers makes Managed SIEM sound like a feature of their service. In our experience working alongside our customers’ existing providers, this is rarely true in the substantive sense — and the conflation is costing UK enterprises real money and real visibility.

How the pattern works

The pattern works like this. The provider sells a Managed SOC service. Inside that service is a SIEM — but it is the provider’s SIEM, on the provider’s licence, configured to the provider’s standards, with the provider’s detection content. Your data is shipped to that platform. The provider’s analysts run their workflow on top of it. From the customer’s perspective, the provider “does Managed SIEM” because there is, somewhere, a SIEM being managed. But it is not your SIEM, it’s theirs, and the operating discipline being applied to it has very little to do with the four pillars described earlier in this paper.

True Managed SIEM vs MSSP Bundled SOC

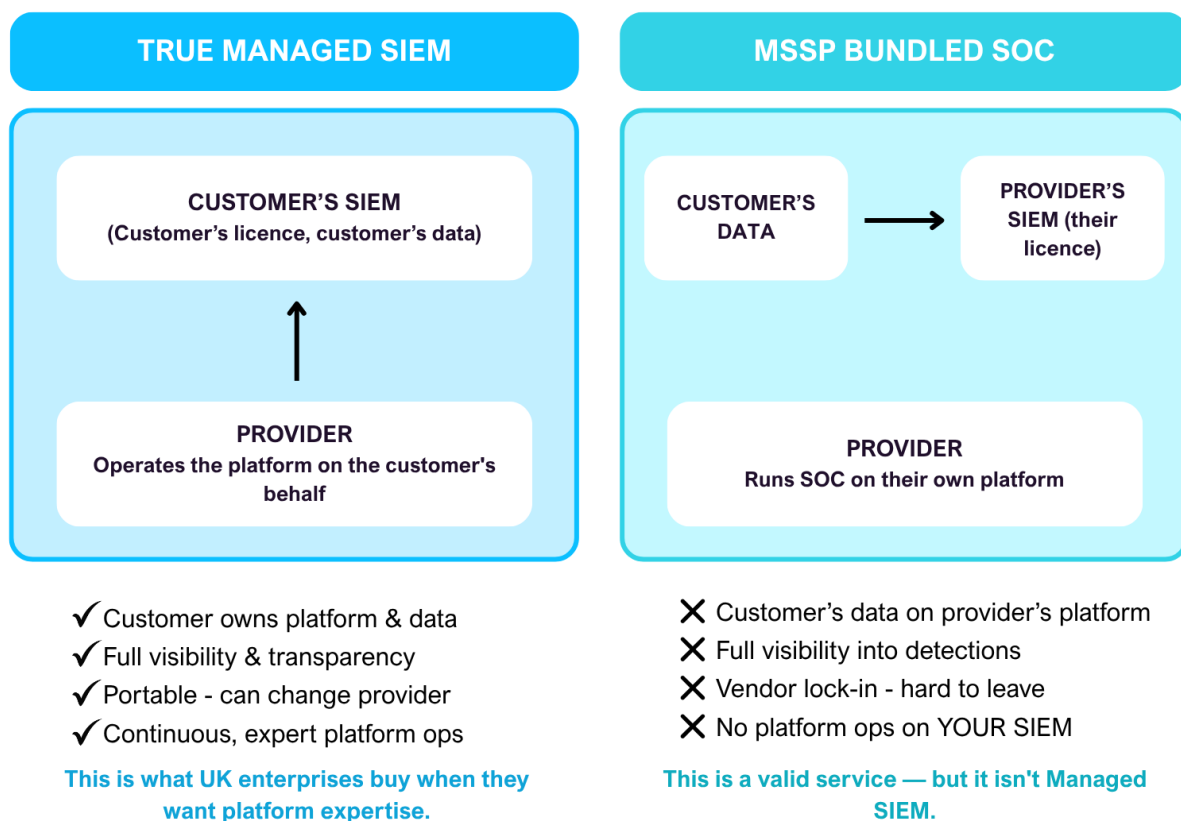


Figure 4. The two service shapes side by side. Both are valid commercially — but only one is Managed SIEM.

This is a perfectly valid commercial offering. For organisations with no internal capability and no desire to own a platform, an outsourced SOC running on a provider-managed SIEM can be the right answer. Where the conflation becomes a problem is when an organisation has invested in its own SIEM — has

paid for the licence, accumulated the data, trained its analysts on the tooling — and then buys a service it believes will operate that investment, only to discover that the provider is actually running a parallel service on a different platform.

The hidden costs of bundled SOC dressed as Managed SIEM

The hidden costs of this pattern are usually four:

- Visibility. You see the alerts the provider chooses to surface, but you do not see how the underlying detection logic is constructed, evaluated, or evolved. Decisions about what counts as a threat are being made on a platform you cannot inspect.
- Portability. Switching providers means re-onboarding your data and rebuilding institutional knowledge. The longer the engagement runs, the higher the lock-in becomes — not because the contract is restrictive, but because the operational state of the service lives inside the provider’s platform.
- Cost transparency. The provider’s licence economics are opaque. As your data volumes grow, you cannot tell whether the price increases you receive are tracking your actual ingestion or the provider’s internal margin.
- Skills retention. Your team does not develop expertise in the platform you are paying for. When the contract ends or the partnership sours, you are starting from a lower base than when you began.

Diagnostic — which service are you actually receiving?

A six-question diagnostic will tell you which kind of service you are actually receiving. If the answer to most of these is “the provider”, you have an outsourced SOC. If the answer is “us”, you have Managed SIEM.

Question	True Managed SIEM	MSSP bundled SOC
1. Whose SIEM licence is the service running on?	Yours	The provider’s
2. Whose tenancy holds the indexed data?	Yours	The provider’s
3. Can you inspect the detection rules in production today?	Yes, directly	Only via the provider’s reports
4. If you ended the contract, would the platform still work the next morning?	Yes	No — re-onboard required
5. Is data quality monitored against your source coverage requirements?	Yes, continuously	Mostly the provider’s feed
6. Are licence and ingestion costs visible to you in real time?	Yes	No — billed by provider

None of this is an argument against outsourced SOC. It is an argument for honest labelling — and for buyers to know which problem they are paying to solve. A true Managed SIEM provider will be able

to walk you through the four pillars on your platform, name the engineers responsible, and show you the operating cadence. A bundled SOC provider will struggle, because the service is structured around their platform, not yours.

5. How Apto Operates SIEM Differently

Apto's Operate service is built around the four pillars on the customer's own platform — Splunk, Microsoft Sentinel, any SIEM platform, or the Cribl pipelines that increasingly sit alongside them. We do not run a parallel SIEM. We do not pipe customer data into our environment. The discipline is applied where the licence and the data live: on your tenancy.

Engagement model — Discover, Design, Deploy, Operate

The engagement model follows our published methodology of Discover, Design, Deploy, and Operate. Most customers begin with a Discover engagement — a structured baseline of the current state, covering architecture, detection coverage, data quality, and cost posture. Where the baseline reveals architectural changes are required, a Design phase follows. Where new operating practices need to be put in place, a Deploy phase stands them up. Then the Operate phase begins, and runs continuously.

The Operate phase is where the four pillars become a service rather than a deck. We provide named platform engineers, working under a published operating cadence, against agreed measures across detection coverage, data quality, performance, and cost. We do not separate platform health from detection engineering from data quality from cost optimisation, because none of them work in isolation; the service is delivered as a single continuous operating discipline.

What customers experience in the first ninety days, and at month twelve

What customers experience in the first ninety days is consistent across our engagements. The early weeks are dominated by visibility: getting an honest picture of what is and is not working on the current platform. Source coverage is mapped against the security strategy and the gaps are documented. Detection rules are inventoried, scored, and prioritised. Cost trajectories are pulled apart by source and by use case, often for the first time. None of this is dramatic, but it is the basis for everything that follows.

By month three the operating cadence is in place. Detections are tuned on a published schedule. New use cases are being designed and deployed against MITRE ATT&CK. Data quality is being monitored continuously and drift is being caught early. Cost is being managed actively rather than reactively. The platform feels different to the analysts using it, and there are usually measurable changes in alert volumes, false positive rates, and licence headroom.

By month twelve the customer has the operational discipline they could not staff internally, on the platform they already own, with the visibility and portability they would not have had under a bundled SOC arrangement. That is the value proposition.

6. Choosing the Right Engagement Model

There is no single right way to consume Managed SIEM. The choice depends on what you have internally and what problem you are trying to solve. Three patterns are most common in the UK enterprises we work with.

Pattern 1 — Health Check + Quarterly Operate

Suited to organisations with a strong internal team that handles platform operations day-to-day but lacks an expert backstop. We deliver a structured Health Check at the start, then a quarterly cadence of platform reviews, detection updates, and cost optimisation work. Lighter weight, lower cost, and useful for organisations whose platform is healthy but whose discipline is at risk of slipping.

Pattern 2 — Continuous Operate

Suited to organisations that have lost — or never had — a dedicated platform engineer, and where the SIEM is showing clear symptoms of the Operator Gap. Apto provides the operating layer continuously, working alongside the customer's analysts. This is the most common model in our customer base and is the closest match to the four-pillar definition above.

Pattern 3 — Co-managed Operate alongside an internal or external SOC

Suited to organisations that are building internal SOC capability, or that already buy SOC services from another provider, and need platform discipline alongside. Apto runs the four pillars; the SOC team — wherever it sits — runs the workflow. This is the cleanest separation of concerns, and the easiest to govern over time.

Whichever pattern fits, the underlying discipline is the same: continuous platform operations on the customer's own SIEM, delivered by named engineers against published measures.

7. Getting Started

We have designed several entry-point engagements to give prospective customers clarity before commitment. Each one is short, structured, and produces a written output you can take to your board or your CISO regardless of whether you go on to engage Apto for an ongoing service.

Free Assessment

A no-obligation conversation with one of our platform specialists to understand your current state, identify quick wins, and decide whether a deeper engagement is worth your time.

SIEM Health Check

A structured review of your existing SIEM deployment covering architecture, detection coverage, data quality, and operational efficiency. Produces a written report and a prioritised action list.

Observability Maturity Assessment

A framework-driven evaluation of your monitoring and observability capabilities against industry best practice, producing a maturity score and a roadmap to the next level.

Data Mapping and Discovery

An analysis of your telemetry data flows, identifying redundancy, gaps, and optimisation opportunities. Often pays for itself in the first cycle of cost reductions.

Book a free SIEM Health Check

The fastest way to start is the Free Assessment. Email enquiries@aptosolutions.co.uk or call +44 (0)845 226 3351 and we will arrange a thirty-minute conversation with one of our platform specialists.

About Apto Solutions

Apto Solutions is a UK platform-engineering specialist focused on Splunk, Microsoft Sentinel, and Cribl. We help our customers extract more security value from the SIEM platforms they have already invested in, through a structured methodology of Discover, Design, Deploy, and Operate. Our headquarters are in Bristol; we work with customers across the UK in financial services, retail, the public sector, and critical national infrastructure.

Read more at <https://www.aptosolutions.co.uk/> or follow our writing at <https://www.aptosolutions.co.uk/insights/>.