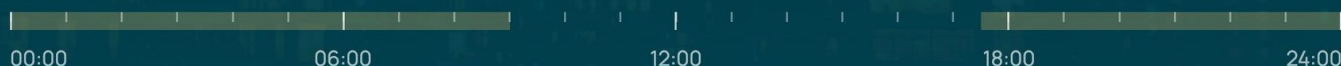


■ THE 24/7 SOC GUIDE

24/7

Do you need **continuous** security monitoring?

What it really takes, and how to choose the right approach.



The office closes at 5.30pm. **Your attack surface stays open.**



Genuine 24/7 security means more than leaving a dashboard open overnight. It takes the right mix of people, processes, technology and the ability to respond, whether that's delivered in-house, with a partner or through a managed detection and response (MDR) service.

A 24/7 SOC isn't automatically the right answer for every organisation, and neither is outsourcing. This guide follows a single night shift to help you work out how much coverage you need, what it has to achieve and how to deliver it sustainably.

READ ONLINE

This eBook accompanies our online guide, which includes an interactive readiness check.

socura.co.uk/blogs/24-7-soc-guide

THE SHIFT LOG

Eleven chapters, from dusk to the next morning.

18:00	01	Why 24/7 coverage matters	p.3
19:30	02	What 24/7 coverage actually means	p.4
21:00	03	What a 24/7 SOC needs	p.5
22:30	04	Does compliance require 24/7 monitoring?	p.6
00:00	05	Do you need 24/7 coverage?	p.7
01:00	06	Where AI and automation fit	p.8
01:30	07	AI you can trust	p.9
02:18	08	The 2am test	p.10
03:30	09	Three ways to deliver 24/7 security	p.11
04:30	10	Choosing the right model	p.12
06:00	11	How Socura approaches 24/7 MDR	p.13
—		Quick answers	p.14
09:00		Clarity, not complexity	p.15

18:00

Why 24/7 coverage matters

The team goes home. Your systems don't.



Your organisation may keep office hours, but your exposure doesn't. A security incident that starts at 2am is no less serious because the team is due back at 9am. Long after everyone has logged off, plenty is still happening:

- Cloud services keep running
- Automated processes keep exchanging data
- Security tools keep generating telemetry, whether or not anyone is looking at it
- Staff keep signing in remotely
- Internet-facing systems stay exposed

75%

of every week falls outside a
9am to 5.30pm, Monday to
Friday working pattern



THE OUT-OF-HOURS CHALLENGE

Cyber security authorities have documented ransomware activity during weekends and public holidays, when fewer defenders and IT staff are available. The NCSC also notes that attackers may act outside normal office hours to reduce the chance of anyone intervening.

A BALANCED VIEW

Not every organisation needs a staffed SOC running around the clock. The NCSC takes a risk-based approach. The real question is whether your model gives you the right level of monitoring and response for the risks you face.

19:30

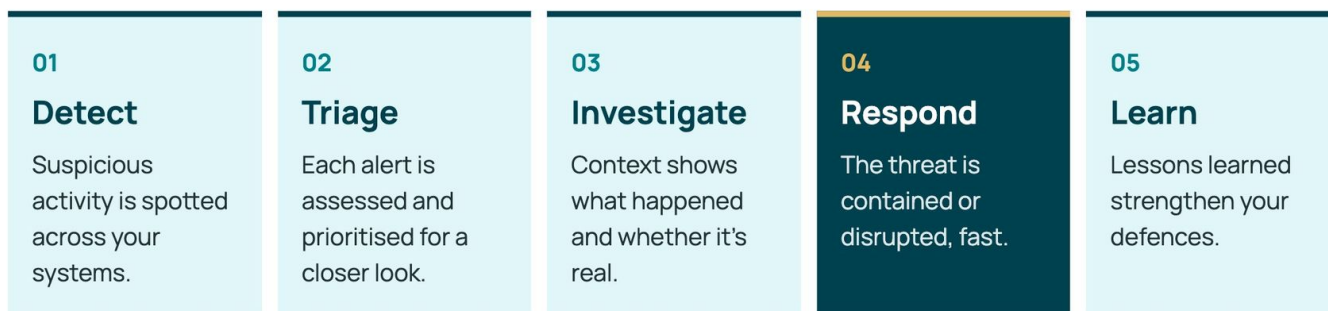
What 24/7 coverage actually means

Tools that run all night aren't the same as people who act.



“24/7 monitoring” can sound more complete than it is. Having security tools switched on around the clock isn't the same as having security operations around the clock. When an alert fires, someone needs to assess it, investigate it, decide whether it's a genuine threat and act. That work follows a cycle.

THE SECURITY OPERATIONS LIFECYCLE



MONITORING VS RESPONSE

24/7 monitoring

- Tools collect data and raise alerts all night
- Alerts may wait until someone is next available
- You find out what happened, after it happened

24/7 detection and response

- People assess alerts as they arrive
- Genuine threats are investigated straight away
- Agreed actions contain the threat, whatever the hour

KEY TAKEAWAY

Technology alone doesn't create a 24/7 security operation. Tools need people and processes behind them that can turn security data into meaningful action.

21:00

What a 24/7 SOC needs

Five components that have to work together.



Whichever model you choose, these five components need to be in place. If one is missing, the others can't make up for it.

01

People

SKILLS AND COVER

Analysts who can monitor, triage and investigate, plus specialists in detection engineering, threat hunting and incident response. In-house, that also means recruitment, skills development, shift patterns and cover for holidays and sickness.

02

Technology

TOOLS AND AUTOMATION

Platforms such as SIEM, EDR, XDR and SOAR, increasingly supported by AI, provide visibility, detection and automation. They don't remove the need for people who understand your environment and can interpret what the tools report.

03

Visibility

THE RIGHT TELEMETRY

Useful signals can come from endpoints, servers, identity systems, cloud platforms, email, networks and key applications. There's no universal list. Prioritise what supports meaningful detection, rather than collecting everything.

04

Response

A CLEAR ROUTE TO ACTION

Know who is notified when a threat is confirmed, which containment actions can be taken straight away, which need approval and how incidents escalate. Monitoring is far less useful if nobody knows what happens next.

05

Improvement

TUNING AND HUNTING

Detection rules need tuning, threat intelligence suggests new use cases and threat hunting finds what detections missed, with AI assisting analysts' research. A SOC can't be built once and left unchanged.

ALERT FATIGUE

A flood of poorly prioritised alerts eats analyst time and hides genuine threats. The goal isn't more alerts. It's better signals.

22:30

Does compliance require 24/7 monitoring?

No blanket rule, but plenty to consider.



It's one of the most common questions we hear. The short answer: there's no blanket UK rule that says every organisation must run a 24/7 SOC. But the frameworks you follow, and the people you answer to, can still shape what "appropriate" looks like.

Cyber Essentials

Sets a baseline of technical controls. It doesn't require a round-the-clock SOC.

ISO/IEC 27001

Requires an information security management system, including monitoring and evaluating performance, but doesn't prescribe a SOC model or universal 24/7 monitoring.

UK NIS Regulations

For organisations in scope, require appropriate and proportionate measures to manage risk and minimise the impact of incidents. Not a blanket 24/7 SOC requirement.

NIS2

An EU directive, not UK domestic law. Check which UK legislation and sector-specific rules actually apply to you.

WHERE CONTINUOUS MONITORING MAY BE EXPECTED

Contracts

Terms agreed with clients or partners

Insurance

Cyber insurer requirements

Customers

Supply chain assurance requests

Your sector

Industry-specific rules and regulators

KEY TAKEAWAY

Compliance can be part of the decision, but it shouldn't be the whole of it. Weigh it alongside your actual risk and security needs.

This chapter is general guidance, not legal advice. Check the specific obligations that apply to your organisation.

00:00

Do you need 24/7 coverage?

Six honest questions to answer first.



Deciding whether you need round-the-clock coverage isn't about ticking a compliance box. It means taking a practical look at how your business runs when your IT team is offline, on leave or asleep.

01 Do you know what needs protecting?

Critical data, devices and cloud platforms such as Microsoft 365 or AWS should all be clearly mapped.

02 Are you looking for the right signs?

Your tools should surface real malicious activity, not bury your team in harmless noise.

03 Who is watching at 2am?

And on weekends and bank holidays, when attackers know you're most likely to be offline.

04 Is anyone authorised to act?

Can someone isolate a device or lock an account immediately, without waiting for permission?

05 Can your team sustain a 24/7 rota?

Including sickness, holidays and the toll that alert fatigue takes on a small team.

06 Can you prove it works?

Do you know how fast you detect and contain incidents, if your board or insurer asks?

QUESTION 05, IN NUMBERS

$$168 \div 37.5 = 4.5 \rightarrow 6+$$

hours a week to cover contracted hours per analyst analysts on paper analysts in reality, with leave and sickness

Keeping one seat filled around the clock takes **6+ dedicated analysts** at a minimum, before adding specialist roles.

01:00

Where AI and automation fit

Helping analysts, never replacing them.



Your security tools generate far more data overnight than any team could read. AI and automation help analysts work through the volume faster, so they can spend their time on the decisions that matter. They assist people; they don't replace them. And used carelessly, they simply create a new kind of noise.

WHO DOES WHAT

WHERE AI ASSISTS

WHERE ANALYSTS LEAD

Detect

- Help sift large volumes of telemetry and highlight unusual activity.

- Decide which signals matter, and why.

Triage

- Add useful context to alerts and filter known, harmless noise.

- Judge whether it's a genuine threat.

Investigate

- Help connect related activity and speed up research.

- Interpret what happened and what's at risk.

Respond

- Suggest possible containment steps for analysts to review.

- Decide on, carry out and lead every response action.

Learn

- Suggest improvements to detection rules.

- Test, verify and own every rule before it goes live.

KEY TAKEAWAY

AI doesn't replace the need for skilled people around the clock. What it can do is help those people see more, and act faster.

01:30

AI you can trust

Ask how it's governed, not just whether it's used.



“AI-powered” is easy to claim. What matters is how AI is governed: what it's allowed to do on its own, who checks its work and what happens to your data along the way.

Confident, but wrong

AI models can present false information with total confidence. That's why AI output needs human verification before anyone acts on it.

Hard to see inside

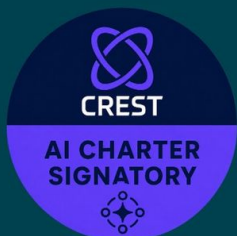
It isn't always clear why AI flagged something. Good providers make AI explain its reasoning, so analysts can check it.

QUESTIONS TO ASK ANY PROVIDER ABOUT AI

- | | |
|--|---|
| <p>01 Which actions can AI or automation take without a human?</p> | <p>02 Who verifies AI-generated detections before they go live?</p> |
| <p>03 Is our data ever used to train public AI models?</p> | <p>04 Where is our data processed and stored?</p> |
| <p>05 Can you explain why AI flagged a particular alert?</p> | <p>06 Which standards govern your use of AI?</p> |

HOW SOCURA APPROACHES IT

We're a founding signatory of the CREST AI Charter, a commitment to using AI responsibly, transparently and accountably.



- Governance aligned with UK government codes of practice
- UK data sovereignty principles
- Customer data never used to train public AI models
- Strict data isolation and security
- Analysts verify all AI output before anything is acted on

02:18

The 2am test

One incident. Two very different outcomes.



AN ILLUSTRATIVE SCENARIO

It's the early hours of Saturday. An attacker signs in to an administrator account using stolen credentials, and your security tools raise an alert for the unusual sign-in. What happens next depends entirely on who is there to see it.

If nobody is watching

- 02:18** The alert lands in a queue and waits.
- 03:40** The attacker explores your network and looks for backups.
- 05:50** Ransomware starts spreading across servers.
- Mon** The team arrives to a major incident, not an alert.

With 24/7 detection and response

- 02:19** An analyst picks up the alert, already enriched with context.
- 02:28** Investigation confirms the account is compromised.
- 02:34** Following a pre-agreed playbook, the analyst locks the account and isolates the device.
- Mon** The team reads a clear incident report and next steps.

WHAT MADE THE DIFFERENCE

Not the alert. Both organisations had the same one. The difference was people ready to act, with the right tools and the authority to contain the threat without waiting until Monday.

THE QUESTION TO ASK

If this alert fired at 2am tonight, which of these two outcomes would your organisation face?

03:30

Three ways to deliver 24/7 security

In-house, co-managed or MDR.



BUILD

In-house SOC

High control and deep knowledge of your environment. The challenge is sustaining true 24/7 cover: shifts, rotas, recruitment, training and absence, plus the engineering to keep detections current.

BLEND

Co-managed SOC

Your team keeps key decisions while a partner extends cover out of hours, supports triage or adds specialist skills. Agree from the start who investigates, who can contain and who gets called.

PARTNER

MDR service

A provider combines technology, specialist analysts and proven processes to deliver detection and response, without you hiring every role. It's a partnership, not handing security over and walking away.

How they compare	In-house	Co-managed	MDR
Who delivers	Your internal team	Your team plus a partner	A specialist provider
24/7 monitoring	Your own shift rotas	Shared, e.g. the partner covers nights	Provided around the clock
Control	Maximum	Shared, through agreed escalation rules	Collaborative, through agreed actions
Organisational knowledge	Retained internally	Retained through joint working	Retained through close partnership
Resource requirement	Higher	Medium	Lower

KEY TAKEAWAY

No model is right for everyone. Each one can work, as long as responsibilities are clear and the coverage can be sustained.

04:30

Choosing the right model

Come back to the fundamentals.



There's no single operating model that suits every organisation. Whichever direction you're leaning, the decision should come back to the same six questions.

01

What risks are you trying to manage?

02

What capability do you already have?

03

Where are the gaps?

04

What would it take to close them internally?

05

Which responsibilities do you want to keep?

06

What level of coverage do you actually need?

IF YOU'RE SPEAKING TO PROVIDERS, ASK

- | | |
|--|--|
| <ul style="list-style-type: none"> ■ Are analysts actively working overnight, or only on call? | <ul style="list-style-type: none"> ■ Which containment actions can you take, and which need our approval? |
| <ul style="list-style-type: none"> ■ Which systems will you monitor: endpoints, identity, cloud, email? | <ul style="list-style-type: none"> ■ How will incidents be communicated and escalated to us? |
| <ul style="list-style-type: none"> ■ How do you tune detections and reduce noise over time? | <ul style="list-style-type: none"> ■ Is your SOC independently accredited, for example by CREST? |

KEY TAKEAWAY

The right model gives you the capability you need today, and can keep up as your organisation, technology and threats change.

06:00

How Socura approaches 24/7 MDR

An extension of your team, not a black box.



Socura's Managed Detection and Response service is built for organisations that need continuous detection and response, without necessarily building the whole operation themselves. We monitor your digital estate around the clock, investigate alerts and respond to genuine threats.



UK-based analysts

Working from our CREST-accredited SOC, with AI governed under the CREST AI Charter.



AI-assisted detection

Analysts use AI to support threat research, then test and verify every rule themselves.



Proactive threat hunting

Looking for activity that automated detections may have missed.



Response that acts

Analysts contain genuine threats using actions agreed with you, and our Incident Management Portal keeps you informed.

HOW WE WORK WITH YOU

01

Onboarding

Understanding your environment

02

Configuration

Agreeing actions and escalation

03

Tuning

Cutting noise, sharpening signals

04

Service reviews

Regular, open conversations

05

Improvement

Evolving as you do

The result shouldn't be more alerts. It should be **greater visibility, faster response and a clearer view** of your security, around the clock.

[Explore Socura MDR](#)

The questions we're asked most often.

What's the difference between a SOC and MDR?

A SOC is the capability itself: the people, processes and technology that monitor and respond. MDR is a service in which a provider delivers that detection and response for you.

Is 24/7 coverage worth it for a smaller organisation?

It depends on your risk, data and systems, not your size. Smaller teams often find MDR or a co-managed model more realistic than building a 24/7 SOC in-house.

Should a SOC monitor cloud services too?

If critical data, identities or business services live in the cloud, they belong in scope alongside your devices and networks.

We already have an IT security team. Do we need 24/7 cover?

Possibly not, if they can sustain out-of-hours cover. If not, a partner can extend their reach overnight without replacing them.

Is 24/7 monitoring the same as 24/7 response?

No. Monitoring means data is collected and alerts raised around the clock. Response means someone assesses those alerts and acts on genuine threats as they happen.

Do I need a SIEM if I already have EDR?

EDR gives deep visibility of endpoints. A SIEM brings together signals from many sources, such as identity, cloud, email and network. The right mix depends on what you need to see.

Can a SOC prevent a cyber attack?

No SOC can stop every attempt. What it can do is detect activity early and contain it quickly, so an intrusion doesn't become a serious incident.

How do I know if my monitoring is good enough?

Ask how quickly you'd detect and contain an incident at 2am on a Saturday, and whether you could evidence it.

More questions are answered in our online guide.

socura.co.uk/blogs/24-7-soc-guide



END OF SHIFT

09:00

24/7 security should bring **clarity, not complexity.**

Round-the-clock security can feel complicated at first, with people to consider, technology to evaluate, processes to define and costs to understand. But underneath it all sits one simple question.

For some, the answer will be a stronger internal SOC. For others, a co-managed model or an MDR service. The aim isn't to build a SOC because 24/7 sounds impressive. It's to have the right capability in place when it matters.

THE QUESTION THAT MATTERS

When something important happens out of hours, what happens next?

If you have a clear, tested and sustainable answer, you have the foundations of an effective security operation.



SOCURA

Always watching. **Always ready.**

hello@socura.co.uk

socura.co.uk

 Socura

READ THE ONLINE GUIDE socura.co.uk/blogs/24-7-soc-guide

This guide shares general guidance drawn from our experience and does not constitute legal or compliance advice. It isn't tailored to any specific organisation, so for advice on your own environment and obligations, please get in touch. References to standards and regulations reflect our understanding at the time of publication.

Socura Limited · Registered in England and Wales No. 12200836 · © Socura. All rights reserved.