SOCURA

The Value of a SOC

The reliance on digital infrastructure, the rise in handling of sensitive data, and the continually evolving threat landscape mean that today, a majority of organisations should consider a formal organisational structure - a Security Operations Centre (SOC) - that holds responsibility for threat detection and response.

39%

Four in ten businesses (39%) report having cyber security breaches or attacks in the last 12 months.[1]

77%

77% of businesses say cyber security is a high priority for their directors or senior managers.[1]

47%

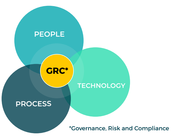
However a 2022 SOC Survey revealed that only 47% of respondents indicated that SOC services are obligatory for their organisation.[2]

A CREST internal survey revealed increasing boardroom buy-in to the concept, but there's a gap in understanding, and funding, for a fully functioning SOC. Some organisations may feel it doesn't make (financial) sense to have a dedicated SOC team, but as organisations grow and evolve, so do the risks and cost of cyber threats. Failing to prepare, organise, and arm a team of qualified security operations professionals can become an expensive mistake[3]

[1]Cyber Security Breaches Survey 2021: GOV.UK
[2]2022 SOC Survey, SANS
[3]What is a Security Operations Centre? CREST

What is a SOC

There's no one answer, they can be internal or external, and they can be virtual or hybrid, but whichever model you decide is best for your organisation, CREST breaks the core elements into three distinct building blocks, **people**, **processes**, and **technology**, all of which come together to form a crucial part of an organisation's compliance and risk management strategy.



*Governance, Risk and Compliance

The People a SOC needs

SOC Manager
Oversees defensive teams and strategies. Manages resources, priorities and projects.

Analysts
Create threat detection content, triage and investigate alerts, tune detection rules, and neutralise threats.

Security Engineer
Implements, configures, supports, and monitors security controls and tools.

The challenge we're all facing

3.4m workers are needed worldwide, to close the workforce gap and secure assets effectively, up 26% on a year ago.[4]

69% of organisations agree that their security operations have been impacted by the cyber security skills shortage.[2]

70% reported that their organisation does not have enough cyber security employees.[4]

1/2 believe that this puts them at a 'moderate' or 'extreme' risk of a cyber attack.[4]

70% staff turnover for individuals with five or fewer years of experience.[4]

[4]2022 Cybersecurity Workforce Study: ISC12

The Technology

From a technology perspective the tools available to cyber security teams are abundant. Key technologies include:

Security Information and Event Management (SIEM)
Gathers and analyses activity from different resources across the organisation's IT infrastructure.

Security Orchestration Automation and Response (SOAR)
Helps coordinate, execute and automate tasks within a single platform. Allows SOC teams to quickly respond to cyber incidents, and observe, understand and prevent future incidents.

Extended Detection and Response (XDR)
Delivers visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyse, hunt, and remediate threats.

Why you may need a SOC

The answer is quite simple; the stakes have never been higher. Among organisations that have identified cyber breaches or attacks around a quarter (27%) experience them at least once a week, and among the 39% of businesses that identify breaches or attacks, one in five (21%) end up losing money, data or other assets.[1]

Cyber perils are the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer.[1] So whilst you may have some form of operational security now, there are many reasons to re-evaluate the effectiveness and capabilities of what it provides your organisation, including:

- Your organisation (or it's attack surface) has grown
- You're holding more sensitive data
- Your organisation has grown, or changed in structure
- You need a single point of visibility over all threats

[1]Allianz Risk Barometer

Cost of a SOC

What a SOC costs has a very similar answer to what one looks like, there's no one answer, it will depend on how you choose to operate it (internal or external, virtual or hybrid, and the level of SOC operations that you are trying to achieve. If you do decide to build your SOC in house, here's one example of what costs may look like

These are just the annual running costs, and don't include the costs of actually setting up the SOC. This could easily cost in the region of 100K.

Let's assume 24/7 operations, which in our experience would require a minimum of 8 staff, and 1 SOC team leader.

And let's suppose this costing is based on an organisation of 2,500 employees, and we're building out an intermediate level SOC in terms of tooling.

Total Annual Running Cost
£1m to £1.2m
(depending on where the SOC is located)

For many organisations this is simply not realistic, particularly considering the difficulty of recruiting and retaining the in-demand security analysts. A managed SOC gives your organisation access to both superior technology and a professional cyber security team, without the associated full-time costs, all whilst providing a higher level of experience and expertise than might be immediately available to an internal SOC.

Our service offers seamless setup and implementation and will have you up and running in a matter of weeks. All delivered from an ISO 27001 and Cyber Essentials Plus accredited organisation – meaning that you can trust us to do it right, every time.

For more detail on all of this, and to learn more about the Socura difference, please download the full eBook.

Download the eBook

SOCURA