SOCURA

The Value of a Security Operations Centre (SOC)

paloalto NETWORKS

Intro

Four in ten businesses (39%) report having cyber security breaches or attacks in the last 12 months.[1] So it's no surprise that three-quarters (77%) of businesses say cyber security is a high priority for their directors or senior managers[1].

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 SOC - that holds responsibility for threat detection and response. However a 2022 SOC Survey revealed that only 47% of respondents indicated that SOC services are obligatory for their organisation[2]. So, right now, not every organisation has a SOC, or understands the requirement for one.

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].

In this eBook we explore:

- What exactly is a SOC
- Why you may need a SOC
- The functions that a SOC performs
- The cost of a SOC
- Why you should consider a managed SOC service
- The cost benefits of our managed service

[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

“A Security Operations Centre can be defined both as a team, often operating in shifts around the clock, and a facility dedicated and organised to prevent, detect, assess and respond to cybersecurity threats and incidents, and to fulfil and assess regulatory compliance.” Gartner

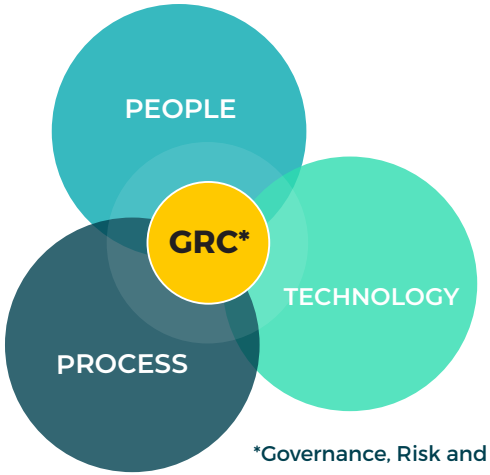
But when can an organisation’s cyber capability be considered a SOC? It’s generally recognised that a SOC should be defined through capabilities and architecture, so, if you’re not performing at least most of the capabilities listed opposite, either internally and/or by outsourcing, that capability couldn’t really be considered a SOC.

With only 35% of organisations even deploying security monitoring tools, and only 32% undertaking any form of user monitoring[4], it’s unlikely that many of the other capabilities are being addressed either.

So what should a SOC look like? 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.

Let’s take a look at the people and technology elements in a little more detail...

Security monitoring and detection	Remediation
Alerting (triage and escalation)	Security road map and planning
Incident response	SOC architecture and engineering (specific to the systems running your SOC)
Vulnerability assessments	Pen-testing
Compliance support	Threat hunting
Data protection	Threat intelligence (production)
Security tool configuration, integration and deployment	SOC maturity self-assessment
Security administration	Threat intelligence (attribution)
Security architecture and engineering (of systems in your environment)	Threat intelligence (feed consumption)
Digital forensics	Red teaming
Threat research	Purple teaming



*Governance, Risk and Compliance

[4] Cyber Security Breaches Survey 2021. GOV.UK

People

The people involved in a SOC must be individuals with the ability to understand, prioritise and investigate security incidents from a selection of appropriate tools. Your people will be your SOC's most valuable asset, and herein lies the challenge:

The people a SOC needs

SOC Manager/ Team Leader

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.

Develops technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.

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.[5]

69% of organisations agree that their security operations have been impacted by the cyber security skills shortage.[6]

70% reported that their organisation does not have enough cyber security employees.[5]

1/2 believe that this puts them at a 'moderate' or 'extreme' risk of a cyber attack.[5]

70% staff turnover for individuals with five or fewer years of experience. [5]

[5] 2022 Cybersecurity Workforce Study. (ISC)2

[6] 2022 SOC Survey. SANS

Technology

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

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

2.Security Orchestration Automation and Response (SOAR) - helps coordinate, execute and automate tasks between various people and tools, within a single platform. This allows SOC teams to quickly respond to cyber incidents, and observe, understand and prevent future incidents.

3.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.

Learn about the tooling that our own analysts chose when building our SOC from the ground up in this article MDR Reimagined & Reinvented, and about the challenges of older ways of working in A New Generation of MDR for a New Era of Threats.

Enterprise customers may be managing 60–80 tools, with those on the higher end of the spectrum possibly managing up to 140[7].

This abundance of tools can itself be a hinderance, often resulting in 'tool sprawl' and the subsequent issues. Read more in this article 'How Information Overload, Talent Retention, and Burnout Impacts SOC Performance'.

Analysts face a deluge of alerts – 11,047 alerts a day on average[8]. Consolidating security tools and suppliers can help you to gain control and reduce risk, look for a partner that can work with you to understand your entire cyber landscape. XDR solutions offer good opportunity for consolidation.

[7] Have You Experienced 'Tool Sprawl' In Cybersecurity? Seeking Alpha

[8] 2021 State of SecOps Report, Forrester Consulting

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.[9]

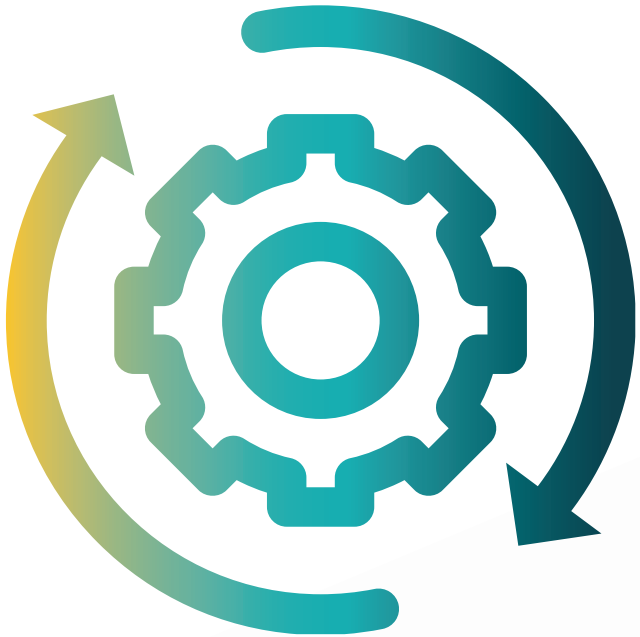
Cyber perils are the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer. The threat of ransomware attacks, data breaches or major IT outages worry companies even more than business and supply chain disruption, natural disasters or the COVID-19 pandemic, all of which have heavily affected firms in the recent years.[10] In fact cyber incidents tops the Allianz Risk Barometer for only the second time in the survey's history (44% of responses).[11]

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:

- Perhaps your organisation (or it's attack surface) has grown – coupled with the security issues surrounding increased remote and hybrid ways of working.
- Perhaps you're holding more sensitive data, and maintaining the confidentiality and integrity of that data, accessible by staff on the premises, by remote staff, or by customers and partners, is critical.
- Perhaps your organisation has grown, or changed in structure meaning it's now operating from numerous locations, where a unified security function could deliver cost savings.
- Perhaps you work in an industry where governance, risk and compliance regulations require a single point of visibility over all threats.
- Or perhaps your current security service provider(s) don't deliver the capabilities you need today.

[9] Cyber Security Breaches Survey 2021
[10] Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. Forbes
[11] Allianz Risk Barometer

The function of a SOC



According to CREST[12], critical functions of a SOC can ultimately be boiled down to a brief list:

Awareness of all IT assets - hardware, software and information or data. Your SOC should have a full, detailed picture of every element running on your infrastructure, including its owner and criticality, to assist in understanding developing threats to them. Assets must include everything, from cloud services to physical infrastructure.

Log management - traffic, incidents and anything of interest must be continuously monitored and logged, so the organisation and any authorities can complete forensics if an incident or breach occurs.

Proactive detection of malicious network and system activity - probably the most critical function of a SOC. Organisations need to know as quickly as possible if there is a breach, or chance of a breach, and what urgent action to take.

Vulnerability management - again, constant work to assess any potential gaps in your network allows for the holistic oversight in terms of organisational vulnerabilities, and which areas might be most vulnerable to existing and emerging threats before you get impacted by them.

Threat awareness - simply put, maintaining keen, constant awareness of the ever-evolving threat landscape allows a SOC to tweak defences - both physical and virtual - before any threat hits the organisation.

[12] What is a Security Operations Centre? CREST

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:

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. *(Investment in log management/correlation, and investigation and response, negligible investment in detection or intel feeds and no investment in workflow/ orchestration or intel management)*

Total Annual Running Cost

£1m to £1.2m

(depending on where the SOC is located)

These are just the annual running costs, and don't include the costs of actually setting up the SOC which includes compiling tactical runbooks, selecting, purchasing and installing security software and the compute it will run on, and calibrating the technology for your specific operations. This could easily cost in the region of £100K.

For many organisations this is simply not realistic, particularly considering the difficulty of recruiting and retaining these 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.

The need for best in class technology

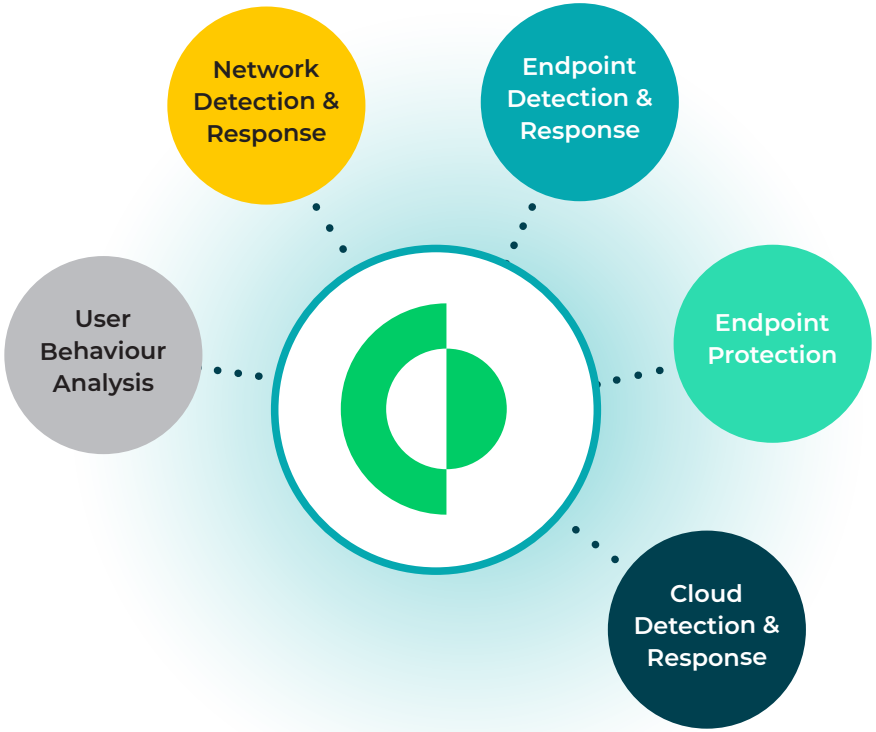
Even in organisations fortunate enough to have SOC capability, the chances are high that siloed tools force analysts to pivot from console to console to verify threats, often resulting in missed attacks. Visibility gaps are common, making it harder for analysts to correlate and prioritise events and alerts pertaining to threats. Exhausted analysts and longer mean time to respond (MTTR) will usually follow.

A lack of orchestration and automation is often part of the problem. It opens the door to extra complexity, human error, slow and manual response, in turn resulting in attacker dwell time being lengthy enough for the threat actor to achieve their objectives (lateral movement, encryption, ransom demands, data destruction, data exfiltration, and extortion).

To reduce the risk of a successful attack, you need a holistic approach to detection and response that eliminates blind spots, increases accuracy, and streamlines investigations. You need to stitch together events across cloud, network, and endpoint layers for comprehensive insight - an approach we mentioned earlier, XDR.

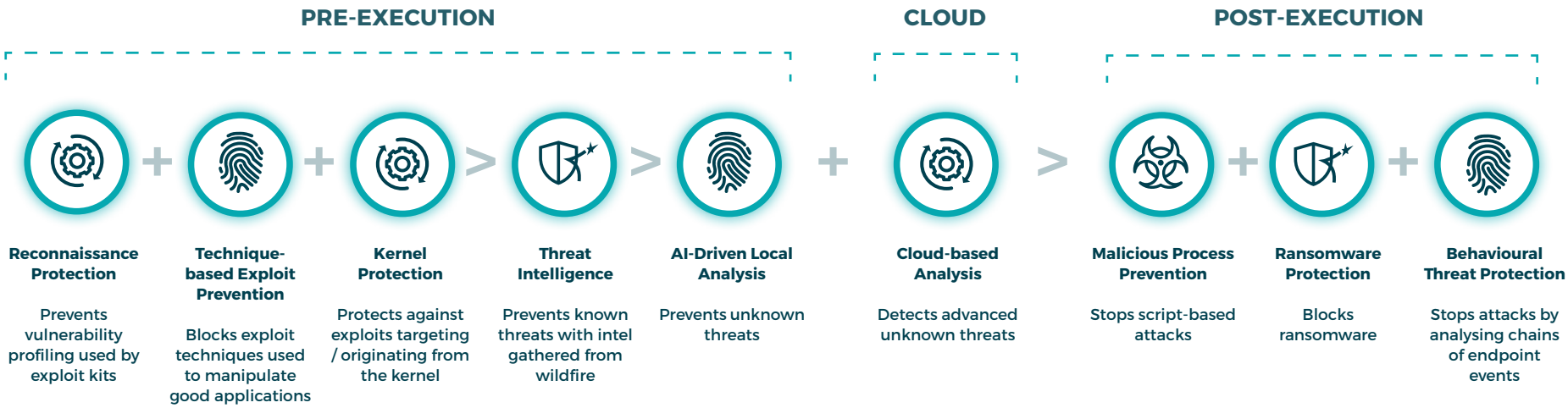
XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause. Intelligent alert grouping and alert deduplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

CREST suggest that if appropriate hardware and software lie beyond your budget, you should consider an outsourced SOC function via a Managed Service Provider (MSP). Over the next few pages we'll strengthen the argument for outsourcing, and explain why we think you should choose Socura.



Best in class attack prevention

The Socura service is built upon Cortex XDR, the industry's first extended detection and response platform that natively integrates endpoint, network and cloud data to stop sophisticated attacks. By correlating and analysing threats across networks, cloud, identity, and endpoint you can simplify and strengthen threat protection.



Cortex XDR provides everything you need for threat prevention, detection and response with a single, cloud-native agent. It safeguards your endpoints with battle-tested and proven next-gen antivirus.

paloalto® NETWORKS | CORTEX® BY PALO ALTO NETWORKS

Simplified Investigations

Today's siloed security tools generate endless alerts with limited context. To reduce response times, security tools must provide a complete picture of incidents with rich investigative details.

By aggregating alerts and indicators of compromise (IoCs) from detection sources - XDR, SIEM, security analytics solutions, network security tools, threat intelligence feeds, mailboxes and more - and then executing automatable, process-driven playbooks to enrich and respond to these incidents, you can streamline security processes and connecting disparate security tools.

These playbooks coordinate across technologies, security teams, and external users for centralised data visibility and action. Cortex XDR also helps to simplify investigations by automatically revealing the root cause, sequence of events, and threat intelligence details of alerts from any source.

Socura's MDR service benefits from simplified security operations by unifying case management, real-time collaboration, threat intelligence management, and automation of containment actions.

88%

Reduction in investigation time

with Cortex XDR by revealing the root cause of alerts from any source.

98%

Alert reduction

due to intelligent alert grouping and deduplication using Cortex XDR.

Security Automation

Manual processes slow down incident response and increase the cost of security operations. To move at pace, analysts need to be able to:

- Automatically collect and update incident information from the XDR tool
- Present detailed context including the severity, timeline and affected hosts and users of security incidents
- Use incident playbooks to streamline investigations by automatically assigning owners to incidents, performing enrichment and reputations checks, plus much more
- Receive notifications, review incidents and perform tasks from their mobile device

The Socura MDR service is built from the ground up on a security orchestration, automation and response (SOAR) platform that will deliver all of the above and allow our team to support yours by helping to manage alerts from any source, standardise processes to act upon those alerts using playbooks, act upon threat intelligence, and automate response for any security use-case.

Our analysts, and the rest of the team, stay well informed on the latest security innovations, cyber crime issues and trends, and any new threats on the horizon. This vigilance can help inform creation of your security roadmap, to deliver direction in your ongoing cyber security efforts.

Why Socura?

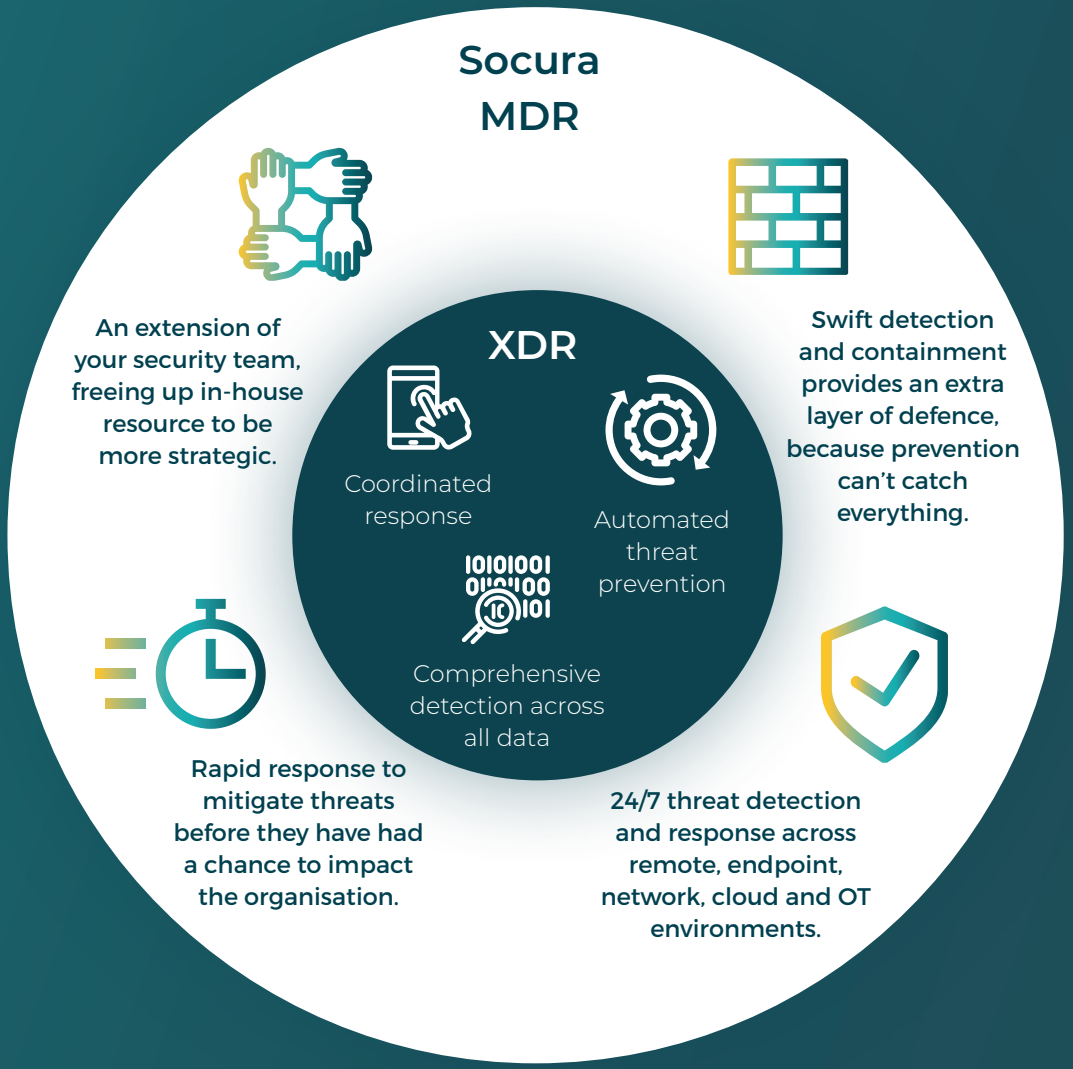
Managed Detection and Response (MDR) is increasingly favoured, as building and manning a 24/7 security operations centre (SOC) in-house is hard to justify from a cost perspective. Organisations can instead utilise the economies of scale that a specialist provider offers, and the enhanced visibility they have into multiple customer environments.

The Socura Managed SOC Service offers a 24/7 proactive threat detection, hunting and response capability that identifies and contains cyber threats in near real-time.

Our service is designed to protect organisations of all sizes from data breaches, reduce attacker dwell time, and negate the impact of any malicious activity on your business operations. Our partnership approach makes this happen by collecting the right data, at the right time - with no compromises.

- Detection and response
- Monitoring and triage
- Expert security analysis
- Dedicated, proactive threat hunting
- Guided remediation actions

This is MDR built for a world of heightened digital risk. With Socura you get a trusted partner that works as an extension of your own security team, but with the support of the latest cloud-based and machine-powered security technologies.



About Socura

We're here to help make the digital world a safer place; changing the way organisations think about cyber security through a dynamic, innovative, and human approach. Our forward-thinking services help organisations to not only detect advanced threats and targeted attacks, but contain them too.

We are a team that cares: about the quality of what we do, the priorities of our clients, the service we deliver and the outcomes we achieve for everyone involved. We've developed a service that we have absolute confidence in. And we never stand still.

To independently demonstrate the quality of its Security Operations Centre (SOC), Socura has undertaken and successfully passed the CREST SOC Accreditation.

The CREST SOC Accreditation process involved an in-depth review of the operating processes of Socura's 24/7 SOC, which delivers monitoring and protection of its customer base, including FTSE 250 companies, central government and critical health infrastructure.

The accreditation process reviews the technologies selected, the threat intelligence and context available, and the ability of the Socura team to bring this together to deliver a robust threat detection and response service to protect its customers operating capabilities.

We've also achieved certification to the internationally recognised ISO 9001:2015, ISO 27001:2017 standards and Cyber Essentials Plus. Achieving these certifications shows our commitment to continually improving systems to deliver the highest quality services. This provides confidence for our clients that the information and systems we hold are secure, and services received from Socura will be of the highest standard.

CREST

CYBER ESSENTIALS CERTIFIED PLUS

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 9001 QUALITY MANAGEMENT

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 27001 INFORMATION SECURITY MANAGEMENT