DigitalXRAID
CYBER SECURITY EXPERTS

MANAGED SOC SERVICES

Respond to Cyber Threats & Protect Your Business 24/7

Security risks are only going to multiply with remote working, stretched IT resources and resourceful attackers

The moves to hybrid working and accelerated cloud adoption and digital transformation have been key disruptors in the cyber security landscape.

However, one thing remains ever-present and proliferates year on year: the risk of a serious security breach.

There are large amounts of breached credentials already being circulated on the dark web – an estimated 27 billion of them. With these credentials, threat actors can access networks under the radar.

On the other hand, cybercriminals may also try to exploit one of the 20,000+ new or unpatched vulnerabilities published over the last year.

Planning for the Future

In times of financial difficulties or recession, it's of the utmost importance that budgets are allocated effectively with maximum ROI.

Some business leaders still view security as a sunk cost. But when you consider that a security breach can cost around £3.18million – or even 10 or 20 times that – investment in prevention is a no brainer.

Facing a determined adversary, no organisation can be 100% breach-proof. This is where the Security Operations Centre (SOC) comes in.

Businesses with a lack of in-house cyber security expertise may struggle to know which avenue to take. Putting more focus on detection and response: finding and resolving breaches before they become serious incidents, takes specialist skill sets.

The smartest decision is to outsource managed SOC services to the experts.

What is a Managed SOC Service and how does it work?

A SOC – or Security Operations Centre – collects an organisation's data logs to detect and protect against cyberattacks. It's made up of a team of security analysts who monitor and analyse a company's security and risk on an ongoing basis.

The SOC function has a vast array of tooling which detects, analyses and responds to cyber threats and incidents.

With all networks, cloud environments and systems monitored 24/7/365, a business remains protected from cyber threats.

A SOC should be an essential part of a company's cybersecurity strategy. Given the current threat landscape, and the ever-expanding corporate attack surface, it has never been more important for businesses to invest in their cyber security posture.

Yet as strategically important as the SOC is, there are major challenges facing CISOs. Skills shortages remain endemic with the current shortfall estimated at over three million globally.

Building an expert team to monitor threats 24/7/365 is not easy with skills and funds in short supply. Let alone the expense of the tooling and resource that is needed to monitor threats 24/7.

That's why many companies are handing this responsibility over to a managed SOC service provider.

A managed SOC service – sometimes referred to as SOC-as-a-Service or SOCaaS – is essentially the same as a fully-fledged in-house function but is operated from an outsourced provider who monitors all networks, systems and applications on behalf of their customers.

Managed SOC service providers have access to the latest technologies and tooling.

They have the aggregate value of refined threat intelligence and response services which they make available to their clients.

These tools include advanced features such as security monitoring and vulnerability monitoring, intrusion detection, SIEM (Security Information and Event Management) and log management, threat intelligence, dark web monitoring, among others.

For any organisation to have the capability and complete visibility to monitor threats and detect breaches on a 24/7 basis before any damage is done, the best solution is to outsource cyber security to a managed SOC service provider.

What does a Managed SOC Service monitor?

Typically, a managed SOC service is situated to monitor all sources of network traffic and activities to detect suspicious activity or anomalies.

The managed SOC service provider will gather all event logs and activity from cloud or network infrastructure, devices, applications, databases, and more, across its client's organisation.

For a managed SOC service to best fulfil its purpose, it requires a constant influx of data. The collected data is then analysed by the managed SOC analysts, through tooling and threat intelligence platforms.

At any and all times of the day or night, threats detected and identified for remediation are responded to before they can cause any disruption to business operations, or damage to reputation.

Data that flows through the network and databases includes:

- Network and DNS logs
- Firewall and intrusion detection/prevention logs
- Email and web logs
- Database activity logs
- Event logs
- And many more

The benefits of a Managed SOC Service

The risk of a security breach has never been higher for businesses across the globe. Governments are seeing an 1885% increase in ransomware attacks. It's extremely difficult for businesses with little or no cyber security expertise to be prepared to deal with security breaches. This is especially true on a 24/7 basis. A managed SOC service can provide the level of security expertise needed to address these challenges.

24/7 Cyber Security

There are many advantages to outsourcing 24/7 cyber security to a managed SOC service provider. A Security Operations Centre can cost upwards of £500,000 to set up.

Aside from that, a SOC will need a minimum of 10 employees to work on 24-hour shift patterns. There are specialised skills needed to manage security operations, and it takes time to acquire and develop these skills.

Never Miss an Alert

With thousands of alerts being delivered to the SOC every day, how can an IT team take on this additional work?

A SOC without enough time or resources becomes vulnerable. The divided attention to security could potentially result in a security risk, as well as a delay in fixing vulnerabilities.

Lower Total Cost of Ownership

To match the capability of a managed SOC service, an in-house SOC would also need to invest in all the tools, systems and software needed. This is why many organisations choose a managed SOC service at a fraction of the cost.

SOC managed services improve security by providing the necessary resources and expertise 24/7/365, allowing the organisation to avoid spending large sums on hiring and maintaining security staff and tools.

Free Internal Resources

Outsourcing to a managed SOC service provider frees internal IT staff to pursue important operation and digital transformation tasks while safe in the knowledge that their security is being monitored.

Most importantly, an organisation can achieve world-class threat detection and response without high upfront costs or the stress of hiring, training and retaining talented analysts.

The benefits of a managed SOC service include:

- Cost efficiencies compared with building a function in-house
- Access to highly qualified cyber security experts
- The economies of scale your managed SOC provider offers, and the extra insight they gain into the threat landscape across their customer base
- Upgrades to tooling are all taken care of
- Knowing that your business is protected against cyber threats 24/7/365
- If you're just starting out and don't have the expertise in-house, outsourcing will give you the flexibility to build your resources without constraints
- If your company changes direction, you can more easily change what you need to monitor without adding additional workload to your already stretched in-house team

A study by IBM revealed that human error is responsible for 95% of breaches.

This will always be an obstacle for organisations to navigate. With attacks on the rise, business leaders need to train staff and prioritise a security-focused mindset to create the first line of defence in teams that would otherwise be unaware of the risks when clicking malicious links.

When an organisation outsources SOC managed services, the smaller details that can be overlooked due to a lack of time or expertise are taken care of. The risk that an understaffed SOC becomes a bottleneck in attack prevention and overall security posture is also eliminated.

Can a Managed SOC Service support compliance requirements?

A managed SOC service brings together an organisations people, processes and technology, using tools and practices to respond to security incidents.

Event monitoring and data logging are some of the key components of any managed SOC.

Many compliance standards require security monitoring and data logging, including ISO 27001 and Cyber Essentials. It's the role of the managed SOC service provider to keep any system and tooling up to date and to comply with regulations such as GDPR.

A key function of a managed SOC service is to provide required incident response data for evidence and auditing purposes.

A managed SOC is the perfect way to meet these compliance management business requirements without adding extra burden to your staff. Managed SOC service providers will support with reporting for audit purposes and for stakeholder visibility.

Is a Managed SOC Service right for my business?

Gain specialist skills

The cyber security industry as a whole is short of 2.7 million workers, and SOC analysts are arguably among the hardest to come by.

This is coupled with stress and burnout associated with alert overload. This usually comes down to cheap tooling spitting out false positives with no way to prioritise signals.

Get the right tools

This leads on to another challenge: the cost of technology investments. Organisations must find the right blend of tools to provide the insight their analysts need.

That's not always easy in a crowded market where vendor hype is sometimes difficult to penetrate. The financial burden is growing.

Better ROI

Perceived ROI is dropping in over half of organisations due to management complexity. Security engineering costs are creeping towards $3m annually, but only 51% rate these efforts as effective.

The best way to support in-house teams during the mass exodus of cyber talent is to outsource to experts.

Wider knowledge of the threat landscape

This is especially pertinent for smaller organisations that simply do not have the resource in house for constant threat monitoring of suspicious activity, and considering the continued growth of the cyber skills gap.

Expert partner:

Security partners bring industry-wide insight and extensive knowledge of the entire threatscape and it therefore makes sense for organisations to invest in this aggregate value.

Finding the right partner is a higher stakes game than many realise. Get it wrong and cyber risk and costs could quickly spiral out of control.

DigitalXRAID
CYBER SECURITY EXPERTS

How can we help?

DigitalXRAID's CREST accredited managed SOC operates 24/7/365, with a dedicated team of analysts monitoring customers' networks, systems and applications, keeping them secure and responding to security events in real time.

The service helps customers understand and reduce risk. Our security services operate as an extension of your own team, working seamlessly to provide world-class threat detection and response to identify and neutralise an attack in just 8 minutes.

As a fully managed security service, customers don't need to update or configure any tooling.

The service uniquely provides the complete spectrum of advanced threat detection and response capabilities, more recently coined as XDR (extended detection and response).

Services include vulnerability management, IDS & IPS, threat mining, SOAR, SIEM & log management, endpoint D&R, file integrity monitoring, dark web monitoring and full compliance reporting.

What's different about our managed SOC service?

The service provides state of the art tooling and expertise, for less than the cost of one InfoSec employee.

DigitalXRAID's SOC service is completely impartial, not looking to push any particular security software or solution sale but is able to offer advice which is in the best interests of the customer.

The managed SOC service operates 24/7/365 with some of the highest qualified security professionals in the world, holding CCIE Security and CISSP certifications, amongst others.

The SOC is one of the first in the world to hold CREST certification and continues to be in the top 1% of providers globally with this certification.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com