DigitalXRAID
CYBER SECURITY EXPERTS

SECURITY OPERATIONS CENTRE

Complete 24/7 Security Protection

When it comes to security, you need to make sure that your organisation is prepared to face any threat at any time, not just when the lights are on.

What is a Security Operations Centre (SOC)?

As the sophistication and proliferation of cyberattacks increases, businesses must put more focus on detection and response techniques so they can identify and respond to breaches when they inevitably happen.

A Security Operations Centre (SOC) monitors cyber threats, detects any suspicious activity and ultimately protects businesses against cyberattacks.

A Security Operations Centre should be the key piece in any company's cybersecurity strategy.

For a business to ensure complete cyber security protection, a Security Operations Centre must operate around the clock to address any incidents as quickly and effectively as possible.

A Security Operations Centre (SOC) unifies threat detection, prevention and response capabilities with technology, tooling and business operations. A SOC is made up of a team of security analysts who will monitor and analyse security risk on a 24/7 basis plus utilise a range of advanced tooling to detect and respond to cyber security incidents in real time.

There are some key roles that a Security Operations Centre (SOC) must include:

- SOC manager – overseeing the whole operation and liaising directly with the CISO for any reporting to the board
- SOC analysts – These are the team members who are on the front line detecting and responding to cyber security threats

A Security Operations Centre may also include Threat Hunters

Threat Hunters specialise in advanced threats and offensive cyber security techniques and a range of junior to senior positions working alongside each other.

How does a SOC protect your business?

A Security Operations Centre is tasked with safeguarding a company's cyber security by monitoring people, processes and technology across the business.

By using advanced technology and security tools, a Security Operations Centre can continuously analyse and improve the organisation's security posture.

A Security Operations Centre will identify the primary cause of any cyberattack – sometimes called root-cause analysis – and provide a detailed report on how, when, and why a security breach was successful. Any indicators of compromise that are identified are then addressed appropriately so a similar cyberattack won't happen again in the future.

Ultimately SOC teams must detect, respond to, and prevent any cybersecurity incidents from jeopardising business operations, customer data, and brand reputation.

Security Operations Centre teams continually work through 5 key phases:

Prevention

As the saying goes, prevention is always better than cure. That goes for cybersecurity too.

By implementing proactive detection techniques, a SOC will detect malicious activity to prevent a breach from occurring

Regular Testing

SOC analysts will continually perform vulnerability assessments to identify potential threats.

Any newly identified threat will be added to the company's risk register. Any associated damage or remediation costs will also be outlined.

The SOC team will conduct testing services that simulate specific attacks on systems and fine tune security policies and incident response plans.

Monitoring & Detection

For most Security Operations Centres, the core technology or tool used for monitoring, detection and response is Security and Event Management (SIEM).

As SOC capabilities evolve, more detailed telemetry and monitoring tooling has become available. Advanced extended detection and response (XDR) technology expands on traditional SIEM functions and can automate incident response for a faster neutralisation of an attack.

Investigation

The Security Operations Centre services will analyse any suspicious activity that has been identified.

It is not enough to simply view the log files of a SIEM tool. The key finding in this phase is whether any part of the IT infrastructure has been penetrated.

Following a triage of the incident, the SOC analyst will outline how to effectively respond.

Response

Once the investigation is complete the threat contained, the SOC team must remediate the issue.

This could include isolating endpoints, closing down permissions to edit or delete files, terminating processes that could be harmful and ensuring that attackers are not able to move laterally through the network.

But SOC responsibilities don't end there.

What does a Security Operations Centre monitor?

Typically, a Security Operations Centre monitors all sources of traffic across the network and any user activities to detect suspicious activity or anomalies.

The Security Operations Centre team will gather all event logs and activity from cloud environments, network infrastructure, devices, applications, and databases to build a thorough picture of the organisation's security posture.

The collected data is analysed by SOC analysts in the Security Operations Centre, using tooling and threat intelligence platforms.

For a Cyber Security Operations Centre to best fulfil its purpose, it requires a constant influx of data. This can be log data in the form of:

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

At all times of the day or night, any threat detected for remediation is responded to before it can cause any disruption to business operations, or damage to reputation.

A fully fledged Security Operations Centre has a vast array of tooling and functionality which detects, analyses and responds to cyber threats and incidents.

Using these security tools, Security Operations Centres can identify and neutralise an attack in less than 6 minutes.

What are the benefits of a Security Operations Centre?

Over the last few years, ransomware attacks have increased by over 1885%. For any business with little or no in-house cybersecurity expertise, it's very difficult to defend against the rising tide of cyber threats. This is even more pertinent when you consider that attackers don't confine themselves to working hours to launch their attacks.

A Security Operations Centre can provide the level of advanced security protection needed to address these challenges.

The SOC will bring assurance to the business that cyberattacks will be detected and prevented in real-time. SOC analysts can respond faster, protect customer and sensitive data, while costing less than the cost of lost business and fines associated with an attack.

.

The Security Operations Centre will:

- Provide proactive, 24/7 threat detection and incident response.
- Monitor and manage firewall and intrusion prevention systems/intrusion detection systems
- Help with patch management and whitelisting
- Provide deep analysis of security log data from various sources across the business
- Analyse, investigate and document security trends
- Investigate security breaches to understand the root cause of attacks and prevent future breaches
- Enforce security policies and procedures

Why should you outsource your Security Operations Centre?

Building a Security Operations Centre team of SOC analysts to monitor threats 24/7/365 is not easy with skills and funds in short supply. Let alone the expense of the tooling and technology associated.

That's why many companies are choosing to outsource their Security Operations Centre to a specialist provider.

A managed SOC provider monitors all networks, systems and applications on behalf of their customers.

With security being a highly dynamic area, businesses should consider outsourcing their security operations to expert professionals with specific knowledge, experience, qualifications such as CREST and CHECK accreditations, and expertise.

For any organisation to have the capability and complete visibility to monitor threats and detect breaches on a 24/7 basis, one of the best solutions is to outsource your Security Operations Centre

What can a managed Security Operations Centre provide?

Managed SOC – also known as SOC-as-a-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.

Partnering with a Security Operations Centre service provider makes cybersecurity a priority without over-spending on in-house tools. It can also free up time for business leaders to focus on building their enterprise.

The Security Operations Centre service will take care of security monitoring, vulnerability and malware detection, managed detection and response, threat monitoring, incident response, security audits, and much more.

The benefits of a managed SOC include:

- Cost efficiencies compared with building a function in-house
- Access to highly qualified cyber 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

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 Security Operations Centre 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.

Therefore, many organisations choose a managed SOC service at a fraction of the cost.

Security Operations Centre services improve security by supplying the necessary resources and capability 24/7/365, allowing the organisation to avoid spending large sums on hiring and maintaining security staff and tools.

Gain specialist skills

The cyber security industry 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 SOC analysts need.

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

Better ROI

According to one study, perceived ROI is dropping in over half of organisations due to management complexity. The same report claims security engineering costs are creeping towards $3m annually, but only 51% rate these efforts as effective.

It is not always possible for smaller organisations to tackle the digital skills gap by investing in a larger security analyst team or a wider technology stack.

As a result, the best way to support in-house teams during this mass exodus of cyber talent is to outsource to Security Operations Centre experts.

Wider knowledge of the threat landscape

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

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.

Free Internal Resources

Outsourcing to a managed Security Operations Centre 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.

DigitalXRAID's Security Operations Centre (SOC) service

DigitalXRAID's 24/7 Security Operations Centre (SOC) is a leading cyber security service that analyses, manages, and responds to all aspects of your IT infrastructure's security every day of the year.

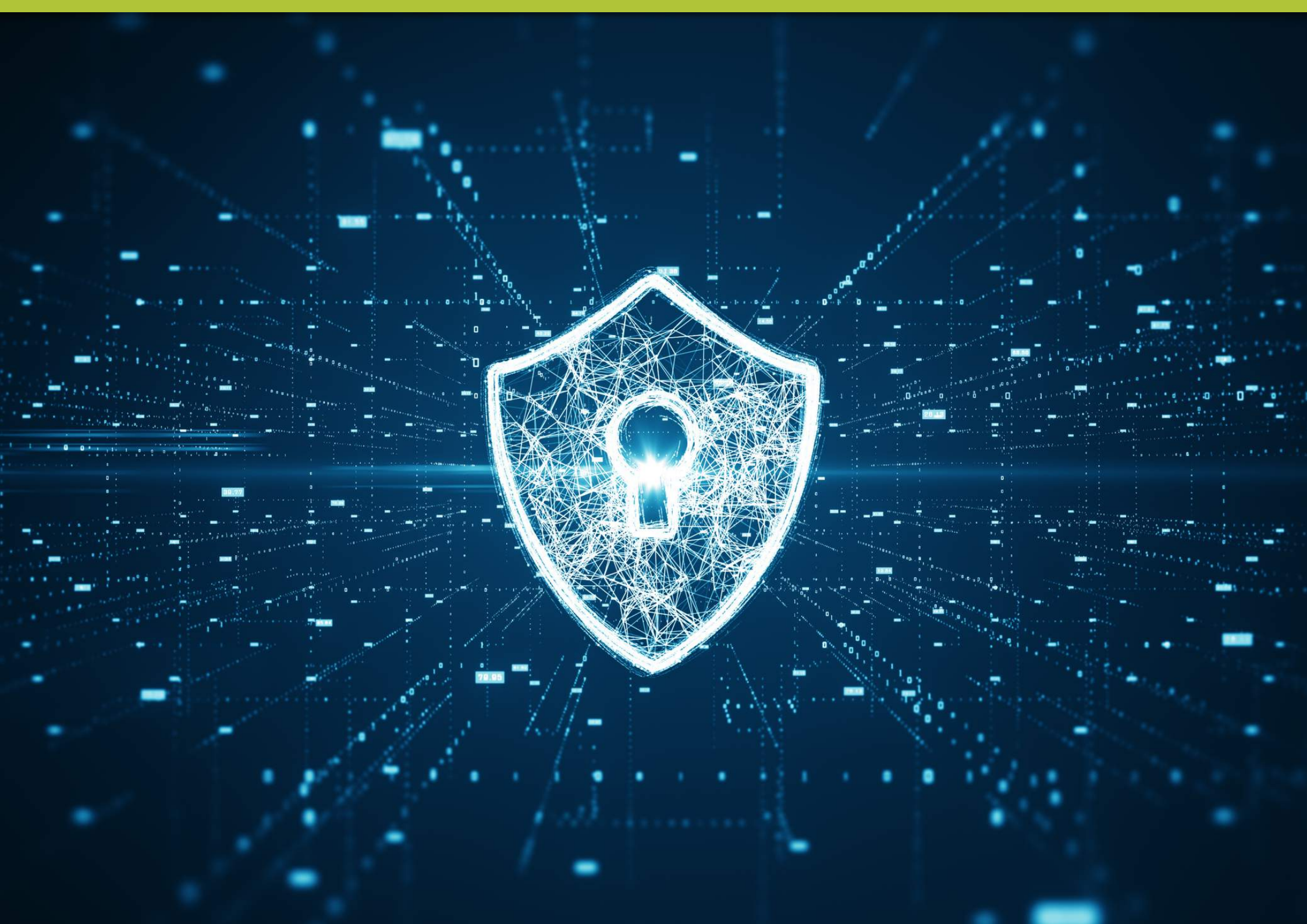
DigitalXRAID's CREST accredited Security Operations Centre operates on a 24/7/365 basis, with a dedicated team of analysts monitoring networks, systems and applications, keeping them secure and responding to security events in real time.

The flagship managed SOC 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.

The service uniquely supplies 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 (Secure Orchestration and Response), SIEM & log management, endpoint D&R, file integrity monitoring, dark web monitoring and full compliance reporting.

Our world-leading, CREST accredited Security Operations Centre can identify and neutralise threats in under six minutes.



DigitalXRAID's CREST Security Operations Centre operates 24/7/365

What's different about our managed SOC service?

The managed Security Operations Centre (SOC) service provides state of the art tooling and expertise, for less than the cost of one InfoSec employee.

This supports increased new business through supply chain assurance. Risk reduction and advanced cyber protection is accessible for all businesses, without expanding in-house operations or straining existing teams

DigitalXRAID's Security Operations Centre service is completely impartial.

The service is not looking to push any particular security software or solutions 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% globally with this certification

Unlike other providers, DigitalXRAID has achieved government-grade security accreditations on top of the elite CREST certification.

We also have ISO 9001 for Quality Management Systems, ISO 20000 for IT Service Management and Cyber Essentials data security certifications added for complete peace of mind for customers

DigitalXRAID

CYBER SECURITY EXPERTS

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

info@digitalxraid.com digitalxraid.com