DigitalXRAID

CYBER SECURITY EXPERTS

Microsoft Sentinel

SECURITY OPERATIONS CENTRE

Managed Microsoft Sentinel Service

Protect & Secure Your Business

Respond to Threats in Real Time

24/7/365 Complete Protection

DigitalXRAID's Managed Microsoft Sentinel Service

info@digitalxraid.com

In today's fast-paced digital landscape, security threats are evolving at an unprecedented rate. DigitalXRAID, with its CREST certified Security Operations Centre (SOC), offers a cutting-edge Managed Microsoft Sentinel service for proactive threat detection, investigation, and response.

Protected and Secured Every Day of the Year

DigitalXRAID's Managed Microsoft Sentinel Service is designed to provide businesses with the most advanced threat detection, event management, and response services – while maximising Microsoft investment – ensuring that your organisation's security posture remains robust and resilient against cyber threats.

By trusting DigitalXRAID to manage your Sentinel platform, you can free internal resources to work on growth projects, while gaining access to a team of highly qualified cyber security experts, that will monitor your business 24/7.

We are certified members of CREST

To become a CREST certified Security Operations Centre (SOC), the service provider must undergo a thorough assessment process that evaluates their technical capabilities, processes, and procedures. The assessment is carried out by CREST-accredited assessors who are experts in the field of cybersecurity.

With DigitalXRAID's CREST Accredited Managed MS Sentinel service, you're not just getting a SIEM; you're investing in a partnership that prioritises your business's security and growth.

Why Choose a CREST Accredited SOC?

Trusted and validated expertise:

A CREST certified managed SOC is backed by a globally recognized and respected organization that provides independent validation of the SOC's capabilities, processes, and procedures. This ensures that the SOC has the necessary expertise and skills to effectively manage security threats.

Stringent standards and best practices:

CREST certification requires adherence to strict standards, best practices, and guidelines for managing security incidents. This ensures that the SOC is using the latest techniques and technologies to detect, prevent and respond to security threats.

Enhanced credibility and trust:

A CREST certification provides a stamp of approval that enhances the credibility and trust of the SOC. This can give customers and stakeholders the confidence that their security needs are being managed by a competent and reliable team.

Better threat detection and response:

A CREST certified managed SOC is equipped with the latest tools, technologies, and methodologies to detect and respond to security incidents quickly and effectively. This can help to minimize the impact of security breaches and reduce downtime.

Continuous improvement:

CREST certification requires ongoing monitoring and testing of the SOC's capabilities to ensure that it is continuously improving its security posture. This ensures that the SOC is always up to date with the latest threats and technologies.

info@digitalxraid.com

By having our system and processes independently checked and audited, we can not only prove that we offer a world-leading, gold standard service, but also ensure that we continue to improve our service - all making us a better company.

MICROSOFT SENTINEL

KEY FEATURES

Data Collection and Analysis:

Microsoft Sentinel collects data from across all of your users, devices, applications, and infrastructure, both from Microsoft and third-party sources. It uses advanced analytics and machine learning to identify threats quickly and accurately so your SOC team can take action.

Threat Detection and Response:

Microsoft Sentinel offers built-in templates and workflows so your SOC analysts can get your infrastructure onboarded smoothly and respond to incidents fast. It also supports creating custom workflows to automate responses to specific threats according to your unique requirements.

Proactive Hunting:

Your SOC team can proactively search for security threats using built-in query tools and custom queries to offer you better security protection.

Incident Management and Investigation:

Microsoft Sentinel provides tools so your new SOC team can investigate incidents and understand the scope and impact of threats to your business. It also offers visualisation tools so the SOC team can analyse and interpret data related to your security incidents swiftly.

Integration and Automation:

Microsoft Sentinel integrates with your various Microsoft and third-party security tools and services. It supports automation for routine tasks and orchestrates complex workflows to improve your SOC team's security response times and efficiency.

Overall, Microsoft Sentinel is designed to support DigitalXRAID's SOC analysts in detecting, investigating, and responding to threats in real-time, enhancing your overall enterprise cybersecurity management.

info@digitalxraid.com

Key Cabapilities of the Managed Microsoft Service

- SIEM & Log Management
- Intrusion Detection
- Threat Hunting
- Vulnerability Management
- Asset Discovery
- Behaviour Monitoring
- SOAR Capabilities
- Dark Web Monitoring
- Security & Compliance
- Endpoint Detection & Response
- Incident Response
- Data Loss Prevention
- Use Case Development
- XDR Capabilities
- Threat Intelligence

> "We are immediately made aware of any security threats and know they are being investigated by DigitalXRAID, eliminating the risk of lasting damage to our business."

Compliant With:

GDPR READY · HIPAA COMPLIANT · AICPA SOC · PCI DSS COMPLIANT · ISO 27001 · amazon web services Partner Network · Microsoft Azure Certified

info@digitalxraid.com

Security Operations Centre Service Packages

	ESSENTIALS	CORE	PROACTIVE
Design, HLD & Install	✓	✓	✓
XDR	✓	✓	✓
Monthly Reporting	✓	✓	✓
Monthly Service Review		✓	✓
Quarterly Reviews	✓		
Incident Response		✓	✓
SOAR Capabilities		✓	✓
Full MS Defender Management		✓	✓
DLP		✓	✓
Threat Hunting		✓ Quarterly	✓ Unlimited
Unlimited Use Case Development		✓	✓
Threat Intelligence			✓
Dark Web Monitoring			✓
Unlimited SOC Engineering			✓

To provide flexibility for our customers, our pricing structure is offered across three solution types: Essentials, Core, and Proactive SOC. These offerings allow customers to choose the correct solution that meets their specific needs and budget, rather than being forced into a one-size-fits-all solution.

info@digitalxraid.com

Why not visit our Security Operations Centre

Call us on 0800 090 3734 to book an appointment and see how we can help you.

Build vs Outsource

Creating your own in-house Microsoft Sentinel powered Security Operations Centre is a huge undertaking. Before embarking on such an ambitious project, you'll need specialist skills to deploy the solution and to prepare a comprehensive budget.

To ensure the full financial support of your executive management team, it's imperative that you consider several key elements:

- The initial investment required for building the SOC (construction costs, equipment, staffing)
- Recurring expenses for operating the SOC (salaries, maintenance & upkeep, utilities, training)
- A buffer for any unexpected expenses (new technologies, staff replacements, repairs)

What You'll Need...

Expensive Tooling

SIEM & Log Management

Intrusion Detection

Threat Hunting

Vulnerability Management

Asset Discovery

Behaviour Monitoring

SOAR Capabilities

Dark Web Monitoring

Threat Intelligence

Endpoint Detection & Response

+

Highly Skilled Employees

Minimum Cost £500,000pa

info@digitalxraid.com

Expert Knowledge

Our cyber security experts are some of the best in the business. We'll safeguard your digital assets and shield you from every conceivable online threat.

The Personal Touch

Here at DigitalXRAID, we understand that no two companies are the same. With our dedicated, fully tailored service, we'll provide you with the best possible cyber security programme for your business. Our goal is to be an extension of your team.

24 Hour Protection

Cyber criminals don't sleep, so neither do we. Our Security Operations Centre provides round-the-clock protection 24 hours-a-day, 365 days-a-year.

Peace of Mind

When you choose DigitalXRAID, you're choosing the best. With our dedicated, industry-leading SOC service, you'll have the peace of mind that your digital assets are in the safest possible hands.

The Hive: Threat Intelligence

DigitalXRAID's CTI specialists are fed data from the entire internet, every day, to map out adversaries and their infrastructure. This gives them greater visibility into the hidden sites where cybercriminals instigate their attacks and enhances proactive threat protection.

Flexibility & Customer First

With DigitalXRAID's Managed Microsoft Sentinel service, rest assured that your organisation's security is fortified against the ever-evolving landscape of cyber threats. Partner with us and experience the future of cybersecurity today.

Staying Two Steps Ahead of the Hackers

Cyber criminals are always looking for new and inventive ways to bypass your security. Using state-of-the-art, up-to-the-minute security techniques and leading tooling from Microsoft, we'll identify potential threats and prevent security breaches before they happen.

info@digitalxraid.com

Proud to be Highly Certified as Cyber Experts

At DigitalXRAID, we specialise in providing cutting-edge, market-leading cyber security solutions. We're experts in our field, and our skills and experience are backed up by our extensive awards and certifications. We're serious about security and compliance and have some of the finest security professionals in the country.

CREST VA PEN TEST CSIR SOC

Crown Commercial Service Supplier

bsi ISO/IEC 20000-1 Service Management CERTIFIED

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 2)

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

info@digitalxraid.com

Proud to Partner with Industry-Leading Vendors & Technology

Microsoft Partner

LevelBlue

SentinelOne

SEARCHLIGHT CYBER

tenable

SpyCloud

DigitalXRAID

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence

Against Cyber Threats?

Call us now on 0800 090 3734

---

info@digitalxraid.com **digitalxraid.com**
