THREAT DETECT

A TEAM OF SECURITY SPECIALISTS PROTECTING YOUR BUSINESS 24/7

THREAT DETECT IS NODE4'S MANAGED SECURITY OPERATIONS CENTRE (SOC) AND SIEM (SECURITY INCIDENT AND EVENT MANAGEMENT) SERVICE. POWERED BY MICROSOFT SENTINEL, OUR 24*7 SOC MONITORS YOUR IT ESTATE TO PROTECT CRITICAL ASSETS, DATA, AND INFRASTRUCTURE FROM CYBERATTACKS, ALLOWING YOU TO FOCUS ON RUNNING YOUR BUSINESS.

Establishing a SOC is a costly and time-consuming business. By using Node4's SOC, you are not just benefiting from extensive experience gained from onboarding and managing many clients, but you're benefiting from the financial economies of scale that Node4 achieves by delivering this service to multiple clients.

What's more, by working with multiple clients, it provides Node4 with a much wider perspective and understanding of the different attack vectors that can be utilised to target and exploit customer vulnerabilities, and we use this knowledge to help secure all our security clients. This is a perspective that you simply wouldn't achieve managing your own estate.

Supported by Node4's wider Security specialists that have been providing solutions for over 7 years, the Node4 team have a working knowledge of a range of disciplines and technologies. This is vital given the nature of today's threats and their associated counters constantly changing and developing over time.

Having been able to apply this knowledge during live cyber-attacks, Node4 bring this wealth of experience to bear in a repeatable and systematic way, combining real life experience and automated services to provide a consistent holistic solution, that is not reliant on any single point of failure, 24/7, 365 days a year.

KEY BENEFITS

24X7X365 SERVICE
Our monitored and managed service provides the Node4 Security Operations Centre (SOC) team response to incidents 24*7

SHARED THREAT INTELLIGENCE
Working with multiple Node4 clients from across Node4 group provides a broader and richer understanding of threats than that you would get simply from monitoring your own estate.

COMPLIANCE AND REGULATION
For organisations subject to regulatory requirements (e.g., GDPR, ISO:27001, PCI DSS), a SOC helps ensure compliance with security standards and frameworks.

A SINGLE VIEW
The SOC pulls information from different systems into one place, irrespective of who manages it, providing a single view, making managing risk and issues far more effective.

ENHANCED THREAT INTELLIGENCE
Correlation of threat intelligence from Microsoft and multiple OSINT sources, to give a clear picture of threats.

MONTHLY REPORTING
Monthly reports compiled by an analyst who knows your organisation, rather than through automation, providing visibility of areas for improvement, and an opportunity for dialogue about preventative steps.

SECURITY CLEARED
The Node4 SOC team are police and government security cleared.

DATA SHEET

THREAT DETECT

A TEAM OF SECURITY SPECIALISTS PROTECTING YOUR BUSINESS 24/7

Threat Detect services are connected to global intelligence centres that ensure our threat intelligence is up to date for complete security. And we augment this with additional data from multiple sources, providing us with a broader and clearer picture of threats from which we can protect our clients.

Combined with Node4's ongoing partnerships with other specialist organisations, this ensures that Node4's overall awareness and security posture is ready to meet today's challenges as well as those of the future.

And rather than just waiting for attacks to happen, by continuously monitoring and analysing an organisation's security posture, the SOC team can identify areas for improvement and implement measures to reduce the overall risk of security incidents.

WHAT NODE4'S SOC DOES FOR YOU

- Monitors your public, hybrid cloud and on-premise infrastructure.
- Protects your key business assets.
- Evaluates user behaviour patterns.
- Detects and defeats malware, viruses, ransomware, and Trojans.
- Notes behaviour indicating policy violations, vulnerable software, and suspicious communications.
- Continuously monitors your network for vulnerabilities.

CYBER ESSENTIALS PLUS

Information Security Management ISO 27001 Certified

Member of Microsoft Intelligent Security Association

Microsoft