THREAT DETECT

24/7 DEFENCE FROM CYBERATTACKS THROUGH EXPERT OVERSIGHT.

Threat Detect is Node4's managed SIEM service - Security Information and Event Management (SIEM), with event and alert triage all overseen by our Security Operations Team.

With Threat Detect and Node4's honed insights into the threat landscape your IT estate, critical assets, data, and infrastructure benefit from 24/7 alerting and once configured to match your organisational risk can forewarn of likely cyberattacks – we'll triage our intel so that you know when to act and when you can focus on running your business.

Our approach uses your existing Microsoft Sentinel subscription to offer a managed SIEM with outputs fed directly to Node4's Security Operations Team. With Node4 focused on managing the SIEM platform, surfacing and prioritising the likely risks, your own internal cyber security expert can focus on the particular risk to your business and its mitigation.

Lean into our expert team of cyber analysis who keep their skills and insights honed through regular training and professional development; 'doing the do'. By supporting Node4's wide and diverse clientele and running numerous managed security services they are highly effective experts in triaging high volumes of events and alerts. Tailored, and tuned to the likely risks and concerns of your business, our analysts can separate out the important actions and tasks that your team must focus on first. We'll check in with you regularly and offer supporting advice on security best practice. Node4 has a wide net of detection capabilities to support a robust and proactive defence of your environment against known attacks. Continuously improving our defensive capabilities and knowledge that will deter or minimise any novel approaches.

HOW WE STAY VIGILANT

With years of experience managing security operations, our team have gained an in-depth understanding of the different attack vectors that can be used to target and exploit customer vulnerabilities. Our work supporting a wide variety of clients has proven vital for shaping our understanding of the nature of today's threats which are constantly changing and developing over time.

KEY BENEFITS

- **24/7/365 Service**
  Our managed SIEM service provides a Node4 Security Operations Team response to incidents 24/7, 365 days a year.
- **Shared Threat Intelligence**
  Our shared experience working with multiple clients provides a broader and richer understanding of threats in comparison to a clients own inhouse monitoring, risk evaluation and mitigation.
- **Compliance And Regulation**
  For businesses subject to regulatory requirements (e.g. GDPR, ISO:27001, PCI DSS, Cyber Essentials Plus), a Managed SIEM helps ensure compliance with security standards and frameworks.
- **A Single View**
  The Node4 Security Operations Team pulls information from different systems into one place, irrespective of who manages them, providing a single view that makes assessing and alerting risk far more effective.
- **Guiding Your Inhouse Team Into Action**
  Threat Detect will surface and prioritise likely risks, so your own internal cyber security expert knows what to tackle first.
- **Enhanced Threat Intelligence**
  Correlation of threat intelligence from Microsoft and multiple OSINT sources gives 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 And Uk Based**
  The Node4 Security Operations Team are police and government security cleared and UK based.

Our Security Operations Team are connected to global intelligence centres that help ensure our threat intelligence stays ahead of the threat. We augment this with over 400 additional data sources, providing us with a broader and clearer picture of threats to look out for.

We've applied our ever-evolving knowledge of security threats to helped us forge a repeatable and systematic way to surface and alert clients as to threats of this nature. With Threat Detect, our real-life experience and automated services have been combined to provide a consistent, holistic solution that is not reliant on any single point of failure, 24/7, 365 days a year.

Combine this with Node4's ongoing partnerships with other specialist organisations, and this ensures our 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 your businesses security posture, the Security Operations Team can identify areas for improvement and advise you on how best for you to implement measures to help reduce your overall risk of security incidents.

WHAT NODE4'S THREAT DETECT DOES FOR YOU

- Management of your Microsoft Sentinel SIEM.
- Monitors your public, hybrid cloud and on-premise infrastructure through one platform
- Monitors and advises on the alerts you need in place in order for you to reduce the risk to your key business assets.
- Evaluates user behaviour patterns.
- Uses the alerts and events configured to assess behaviour, and surface policy violations and suspicious communications.