Managed Security Service

Not just another Security Operations Centre

From the move by many organisations to Cloud-based remote working, to the rollout of 5G making our mobile devices better connected, we are more vulnerable to cyber attacks than ever before. This has made businesses step up their efforts to remain secure, with many exploring the benefits of Security Operations Centres.

Traditionally, a SOC is highly reactive; rapidly reacting to alerts and incidents as they are generated. But wouldn't it be better if these incidents didn't happen in the first place?

What is a Security Operations Centre?

Put simply, a Security Operations Centre consists of highly-trained cyber security professionals who are responsible for monitoring an organisation's security posture, analysing, responding to and remediating any cyber security incidents.

There are a number of reasons why you might be considering a SOC for your organisation; for example, if you...

- Run a service for the public which can be accessed online
- Host sensitive info for access on site or remotely
- Have different office locations with a unified security function
- Share large amounts of sensitive info between organisations
- Require a single point of visibility to detect and manage all threats

Our approach

For Transparity, the requirements for a SOC represent the bare minimum to meet your organisation's security needs. Our Managed Security Service has been built on three core principles, as the traditional perimeter defence model is no longer sufficient:

- **Zero Trust:** Never trust, always verify
- **Least privilege:** Provide only the access required, and only for the duration needed
- **Assume breach:** Always be ready for the worst, assuming users or systems will fail

Microsoft Sentinel

Named a leader in The Forrest Wave: Security Analytics platform providers, Q4 2020, Q4 2020 - and ranking top in Strategy - Sentinel is Microsoft's best-in-class, Cloud-native SIEM. The solution is leveraged by Transparity as it provides overarching security management, harvesting enriched signalling and telemetry data from all of your critical resources, not just from Azure and Microsoft 365.

Taking this data and supplemented by Machine Learning and Artificial Intelligence, it is able to correlate alerts from disparate sources and products to provide highly accurate incident detection. These incidents provide our SOC with a detailed understanding of the threat timeline, point of entry, entities involved and impact.

But Transparity are not only proactive in implementing and configuring defensive products to best practices standards; we take a holistic approach to security, ensuring we adhere to best practices across the board; from processes and frameworks to end user education and awareness training.

Here's what we do differently...

In addition to direct access to our highly-skilled and experienced Security Operations Centre engineers and analysts, along with dedicated 24/7/365 support should a breach occur via our Security Incident and Response Team, Transparity's Managed Security customers receive:

Continuous improvement

- Industry-standard security best practices are continually reviewed and evaluated against your infrastructure, not "set and forget"
- Security hardening beyond the defaults
- Microsoft Secure Score improvement and management
- Regression remediation to maintain your security posture
- When your security posture has improved to the point of maintaining, our Security Analysts will perform proactive threat hunting

Equal protection for all resources

- To protect your organisation from an attacker, we must think like an attacker. This means paying careful attention to all internal and external attack vectors
- Attackers will leverage any attack vector possible, including users, IT, OT and IoT devices, regardless of location
- We will protect your users and resources across Microsoft Azure and M365, as well as third-party Cloud, on-premises and Private Cloud workloads
- This protection covers not only Windows-based devices, but alternative OS such as Linux, Unix and VMware, plus devices like firewalls and switches

SOC capability

- Dedicated Security Analysts monitor your organisation 24/7/365
- Our Security Incident and Response Team will investigate and mitigate threats as they occur
- Should recovery be required, we will support you by creating and implementing a remediation and recovery plan to get you up and running again as quickly as possible
- Rapid escalation to Microsoft if required
- Maximise adoption and usage of your product licensing for great ROI
- New features implemented on release

Alignment to our evergreen blueprint

- Our recommended settings are derived from industry best practices and our highly-skilled analysts' experience
- These settings make up the Transparity "Secure by Design" blueprint, which is continually reviewed and evaluated
- Any configuration drift will be flagged by our SOC and regressions remediated

Best-of-breed tooling

- Utilising leading-edge Microsoft-centric security products
- Backed by constantly-evolving Artificial Intelligence and Machine Learning
- Harnessing the power of the Microsoft Graph Security API to improve threat protection, detection, and response capabilities

Unrivalled end-to-end integration

- Delivered by Microsoft's XDR Defender products and Microsoft Sentinel SIEM
- Alerts and incidents are created directly into our Datto Autotask Professional Services Automation (PSA) platform

Additional benefits of our Managed Security Service

- Vulnerability assessment and management: Microsoft Defender for Endpoint will continually scan your devices and report on any threats detected. A monthly external scan of your public facing resources will also be performed, with a remediation plan will be generated if any vulnerabilities are detected
- Service Management System: Your sensitive documents and passwords will be stored securely in our IT Glue documentation and management system
- Optional penetration testing: Red team testing from of our select technology partners, giving you additional peace of mind
- User education and awareness training: Bi-yearly training provided by one of our security experts, including documentation to take away so users have a point of reference after the session
- Threat intelligence: The security landscape is constantly changing with new, zero-day threats being discovered daily. Our Security Analysts constantly review a wide range of security feeds to detect new threats and ensure you are protected
- Remote Service Delivery Manager (SDM): A security-centric SDM will own the security war room should an incident occur, providing you with constant updates, plus a remediation and recovery plan. They will also create and discuss your monthly Security Service report, which will show month-on-month improvements to your security posture

Get in touch

Ready to speak to Transparity about your Managed Security strategy? Just email hello@transparity.com or call us on 01202 800000 to book a complimentary virtual consultation.

transparity

transformation • partnership • clarity

* Security Operations Centre Buyer's Guide - National Cyber Security Centre

Microsoft Partner | Azure Expert MSP

Microsoft

Windows and SQL Server Migration Advanced Specialisation
Teamwork Deployment Advanced Specialisation
Calling for Microsoft Teams Advanced Specialisation
Meeting and Meeting Rooms Advanced Specialisation
Adoption and Change Management Advanced Specialisation
Threat Protection Advanced Specialisation
Identity and Access Management Advanced Specialisation
Information Protection and Governance Advanced Specialisation
Cloud Security Advanced Specialisation
Azure Virtual Desktop Advanced Specialisation
Modernise Endpoints Advanced Specialisation