COMTACT
Cloud. Security. Delivered.

Microsoft Sentinel Health Check

A one-day assessment service to improve your Microsoft Sentinel deployment

The basic set-up of Microsoft Sentinel enables you to handle security incidents and receive data analysis right out of the box. However, expert advice is needed to ensure full game-changing capabilities are leveraged, aligned and activated for your specific use cases. Effectively assessing and deploying Microsoft Sentinel into our client's businesses is what we do each day – and we have the awards and customer recommendations to validate this.

Common issues addressed

- A legacy SIEM may still be in use. This mandates a "swivel chair" operational model, which is both time-consuming and costly
- Desired or required non-Azure cloud platforms may be partially integrated or not at all
- 3rd party solutions or software may not be integrated with your Microsoft Sentinel platform
- Security appliances sending syslog and Common Event Format (CEF) signals may be volumetrically large and noisy, carrying with them hefty time and cost implications
- Alert fatigue may be setting in as analysts spend excessive time handling thousands of alerts with poor prioritisation and poor visibility across the business

How our one-day health check can help

Our security engineers interrogate and analyse your Microsoft Sentinel environment using a view-only access permission. The results are collated and prioritised across several key areas: threat intelligence, data sources, logs and connectors, fidelity and visibility, investigation and data enrichment, as well as advising on overall health and tuning.

Included in the service

- Scoping session to fully understand your business requirements and infrastructure
- Gap analysis of all current log sources for fidelity, visibility and value against the desired end state
- Subsequent logging strategies and recommendations
- Assessment of your current threat hunting and gathering of threat intelligence and recommendations on how to improve
- Review of your alerting rules and playbooks
- Recommendations on response automation and MDR
- A full automated cloud security assessment

Clear improvement roadmap

The results of the health check are presented back to you on completion. Our recommendations include a clear priority-led roadmap to help you improve the deployment of Microsoft Sentinel, the connecting components, and the telemetry collected. We help ensure the full capabilities are being leveraged, are operating efficiently and delivering maximum value to your business.

Please get in touch to find out more about how our Health Check can help take your Microsoft Sentinel Deployment to the next level.