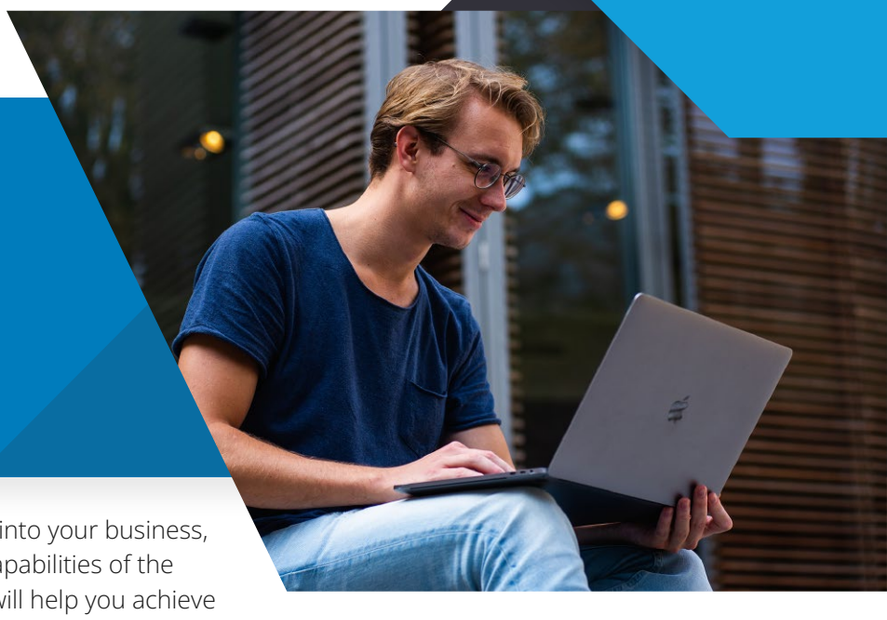
COMTACT
Cloud. Security. Delivered.

Microsoft Security



Microsoft Sentinel Accelerator

A two-month Microsoft Sentinel deployment service

If you've made the wise decision to bring Sentinel into your business, you will want to ensure that the game-changing capabilities of the solution are fully leveraged from the outset. This will help you achieve maximum security capability, value from your investment and optimal efficiency within your team.

While the basic Sentinel features can be understood and leveraged quite quickly, it can take 6 months to tune and deploy to an optimal level and may even be years to fettle it like a pro. Our Microsoft Sentinel Accelerator was created to fast-track deployment and get you to the pro stage sooner and with minimal hassle. We help you filter out noisy alerts from the outset, so they don't overwhelm your team. This includes optimal tuning of the system so valid attacks are flagged and dealt with immediately. We also help you transition from your previous SIEM and aggregate your entire estate across all clouds, IPaaS, IaaS, SaaS and 3rd party products.

Comtact support our customers with complex deployments of Microsoft Sentinel into their business each and every day, making complex tasks almost as simple as flicking a switch – and we have the awards and customer recommendations to prove it.

Our initial 5-day deployment includes

- Scoping session to understand your business requirements and infrastructure
- Integration with your Microsoft estate, 3rd party solutions and across multiple clouds
- Set-up of all log sources for optimal fidelity, visibility and value
- Configuration of threat intelligence sources and hunting capability
- Set-up of alert rules and playbooks
- Integration with your MISP threat intelligence environment

Our 2-month delivery includes

- Dedicated level 1 support and level 2 escalation
- Continual tuning and refinement of log sources
- Implementation of MDR use cases identified during deployment
- Continual categorisation and prioritisation of alerts
- Optimisation of data enrichment tools
- Configuration of watchlists
- Development of custom automation workflows
- Development of bespoke and dynamic playbooks
- 24x7x365 MDR and SOC option with triage and ticket resolution
- Creation of custom reports and dashboards within Sentinel
- Weekly 2-hour reviews and a final service review and summary report
- Easy transition to a full managed service should you wish to continue with Comtact after the Accelerator period

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