Microsoft Sentinel Accelerator

ANS

Think Bigger.

What are ANS Accelerators?

Our Accelerators are high-value, low-cost solutions which can be delivered in less than 6 weeks, making them ideal if you're on a tight deadline or don't want to make a significant investment.

What is the Microsoft Sentinel Accelerator?

The Microsoft Sentinel Accelerator is to enable you to accelerate your modern SecOps journey into the cloud at pace. This Accelerator is focused on the Microsoft Sentinel technology and best practice architecture, creating the foundation for you to fully adopt a SecOps process through all your infrastructure at cloud scale, enabling you to see and stop threats before they cause harm.

Who is this suitable for?

This Accelerator is ideal for organisations that are looking to modernise their security practice, have a SecOps-driven initiative or have multiple data sources with limited visibility. It is also suitable for businesses with legacy security/SIEM capabilities.

What will this solution enable me to do?

1. Collect data at cloud scale

Collect data across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

2. Detect threats

Detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft.

3. Investigate threats

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

4. Respond to incident

Rapidly respond to incidents with built-in orchestration and automation of common tasks.

What outcomes can I expect?

We will deliver a fully functioning Microsoft Sentinel platform ready for data to be ingestedand served. This can either be for a PoC / proof of value or at an enterprise scale.This includes identities, security, connectors, monitoring, auditing & logging.

This Accelerator will be delivered with infrastructure as code allowing the future possibility for agile iteration using SecDevOps, be that PoC to production or another environment for the enterprise scale version. For the enterprise scale version, all environments are backed by Azure DevOps and using code repositories to allow configuration and pipelines to flow from Dev to UAT, and UAT to Production seamlessly.

We will provide 5 custom connectors to illustrate the compatibility and agility of the Microsoft Sentinel Platform.

How do ANS deliver this Accelerator?

Delivered using a standardised statement of work, build process and engagement means we can get you up and running with a fully functioning Microsoft Sentinel platform in under 6 weeks. Using our mature remote delivery capability, we can ensure a quality build from our UK-based 24x7x365 operations centre, without requiring significant input from you.

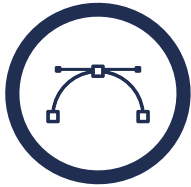# What are the benefits of using an ANS Accelerator?

Rapid time to value

Depending upon if a landing zone is required, ans can deliver this within 2-6 weeks

Fully extendable

As well as easy to integrate with other services.

Proven architecture

Provisioned with proven success and stable functionality.

High-touch project support

A dedicated Project Manager and short project kick off lead times will get your project off the ground quickly and smoothly

Want to get started?

Get in touch.

Telephone

0800 458 4545

Web

www.ans.co.uk

Address

ANS Group

ANS Campus

Birley Fields

Manchester

M15 5QJ

ANS

Think Bigger.