

# Azure Sentinel Engineering

The cloud-native SIEM solution from a major cloud provider, Microsoft Azure Sentinel is making strong inroads into the SIEM space, particularly in organisations making use of Microsoft threat protection technology or the Azure platform itself.

And it's not confined to Azure: Sentinel integrates with other cloud services, applications, services, devices and users under a variety of operating models. And of course, it offers all the advantages of a cloud service – cost, flexibility, billing, availability, ease of scaling, and more.

As always, turning potential value into measurable results can be a challenge.

Implementing a public cloud SIEM service like Azure Sentinel takes a different set of skills and experience than in-house teams may have – and they'll often have a backlog of changes or other commitments that make meeting business timelines impossible.

Plus, charging models can sometimes complicate onboarding data from Azure Sentinel and vice-versa – assuming that they're compatible with cloud-based solutions at all.

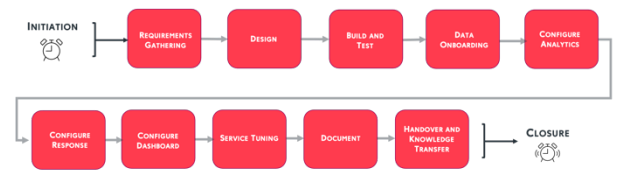
Adarma can help.

## Adarma Sentinel Engineering

Adarma Azure Sentinel Engineering is a fixed time, price, and outcome implementation of Azure Sentinel service covering a single tenant and integration with Microsoft Office365 and other supported data sources.

The engagement runs over three months, taking care of design, implementation and tuning, and handover = getting you out of the starting gate, past implementation hurdles and into the home straight to value.

An Adarma project manager oversees throughout, initiating a kick-off workshop to gather and refine requirements as rapidly and efficiently as possible. If your service requires customisation for additional data sources, rules and integrations, they'll be identified, discussed, and agreed here.



ENGAGEMENT RUNS ACROSS THREE MONTHS WITH ADARMA PROJECT MANAGEMENT



**FIXED TIME, PRICE, AND OUTCOME IMPLEMENTATION OF AZURE SENTINEL SERVICE, SINGLE TENANT AND INTEGRATION WITH MS O365 AND OTHER SUPPORTED DATA SOURCES.**  
ADDITIONAL CUSTOMISED RULES / INTEGRATIONS / DATA SOURCES AVAILABLE

Throughout the engineering process, our experienced SIEM engineers will work collaboratively with your teams to design and implement based on best practice and in line with your change control processes to protect your operational environments.

(And when we say collaboratively, we mean collaboratively. Partnership and trust aren't just "nice to have" extras – they're the foundation of Adarma's approach.)

We'll make sure knowledge is transferred throughout the engagement, so handover to your operational team is simple and stress-free.

And whenever you're ready to delve deeper into Azure Sentinel, we'd love to work with you again as you define your roadmap for the onward Azure Sentinel journey.

# Azure Sentinel Engineering

## Why Adarma?

Adarma is registered as a Microsoft Solution Partner with skills and capabilities in Azure, Security, Sentinel and Services. All Adarma's Azure Sentinel engineers have successfully completed Microsoft's training programme.

Microsoft Partner Center Adarma Limited

Additionally, each one has passed Adarma's in-house Sentinel/Azure training, drawn from best practice in the field, years of expertise onboarding, engineering, and maintaining SIEM systems for a range of FTSE-350 clients, and our experience as an elite partner for other major SIEM vendors.

You'll reap dual benefits: specific expertise with Azure Sentinel, and the wide-ranging knowledge and experience, toolkits and artefacts of a wider Security practice to reinforce it.

- **We've got the expertise you need** to successfully build and integrate solutions – our engineers are qualified security professionals backed by a wider practice of diverse skills that let us identify the challenges others miss - and implement solutions that only we can.
- **We understand the platform** and the infrastructure, familiar with engineering across multiple SIEM platforms, the Azure cloud, and the benefits Incident Response technology can bring to your organisation. We speak your SMEs

language because we're natives.

- **We partner with best of breed** solutions to deliver world class services, delivering rapid value through the service we implement and deliver.

And it's not just our technology:

- Our professional services are backed up by a wider practice of accredited experts across disciplines and technologies – all with native security backgrounds.
- Our SOAR lead is the one of only two accredited Phantom trainers in Europe.
- Our Managed Services Product Lead sits on the customer advisory board of a market-leading SIEM technology provider.

## About Adarma

We're one of the largest independent security services companies in the UK. A business formed and run by experienced senior security leaders, we know security and how to deliver real value in the real world. This is why our clients are successful FTSE 350 organisations from all industry sectors.

Adarma delivers innovative tailored solutions for some of the world's biggest companies. Our teams are a diverse group of technical experts and consultants, all with the same objective and united by the same goal: to help our clients prepare for attack and stand side-by-side with them when it happens.

Helping make the world a safer place.

Contact us to discuss your Azure Sentinel Engineering requirements [enquiries@adarma.com](mailto:enquiries@adarma.com)

[www.adarma.com](http://www.adarma.com)