

Azure Sentinel Quick Start

Take the first steps to gain a bird's eye security view across your enterprise

The importance of security response and taking quick action has never been more critical. Solutions built for yesterday's environments struggle to keep the pace with today's challenges, let alone tomorrow's unimagined risks.

Get a jump start on the next generation solution for Security Information and Event Management (SIEM) and Security Orchestration and Automated Remediation (SOAR) with our **Azure Sentinel Quick Start**.

WHAT WE DO



Analyze your requirements and priorities for your SIEM deployment.



Define and deploy Azure Sentinel in your environment.



Configure Sentinel to immediately process your entire Microsoft footprint (M365, Azure, Dynamics) as your baseline starting point.



Discover threats and learn how to automate responses.



Recommend next steps on how to proceed with a production implementation of Azure Sentinel.

PRICE: \$25,000

WHAT YOU GET

Deployment: We help you set it up

With expertise in Microsoft's expansive security stack, Catapult's Spyglass team helps you get your Azure Sentinel instance up and running the right way, the first time.

Workshop: We teach you the basics

Learning about planning your log storage to match your requirements, configuring event sources, developing hunting queries with Kusto Query Language (KQL) and the basics of threat hunting.

MAIN OBJECTIVES

Plan your deployment and provide information to build a business case for a production deployment of Azure Sentinel, including a technical roadmap.

Understand how to mitigate threats in Microsoft 365 and Azure security as your first step, with review of additional event sources that can be seamlessly integrated.

Learn about threat hunting and how to mitigate and protect against threats found.