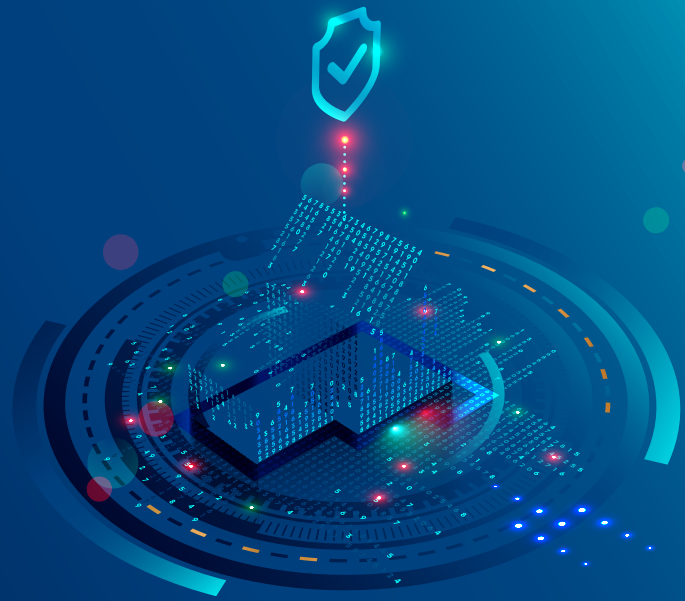


Microsoft Sentinel Quickstart

Gain a bird's eye view across your enterprise with SIEM for a modern world



Solution Brief

Background and business challenge

As IT becomes more strategic, the importance of security grows daily. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks.

Investigation is complex and time-consuming

Every second counts when SecOps personnel are handling a threat that might jeopardize their organization. The clock is ticking fast, but investigation requires highly skilled security analysts and can often take days or weeks.

There is a global shortage of security analysts and experience

The need for skilled security professionals has greatly increased, and supply cannot meet current or future demand.

Current solutions are not architected for today's demands, or tomorrow's

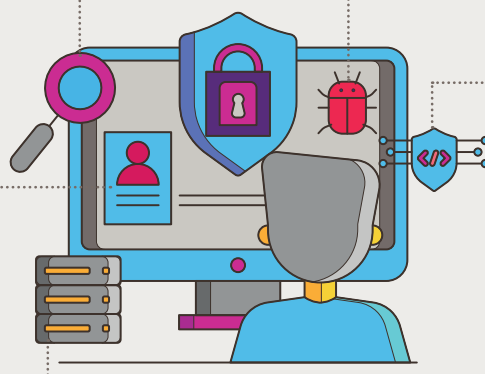
Legacy on-premises SIEMs require powerful hardware and extensive maintenance that make them expensive to operate. Storage and compute needs increase dramatically during an incident, which is difficult for an on-prem footprint to accommodate. The move to the cloud has enabled a new degree of enterprise scale-out, and with the explosion of cloud-born data, legacy SIEMs are less and less able to cope with the demand.

Threats continue to grow in complexity and volume

Attacks are increasingly heterogeneous. A typical attack spans different parts of the enterprise and crosses various resource types: it might start from an IoT device, proceed to an endpoint, spread to a cloud service or to a database, involve multiple user accounts or tenants, and so on.

Alert fatigue: Security Operation Centres (SOC) see too many alerts from disconnected products

SOCs typically have dozens of security products, each producing a large volume of alerts. In isolation, these products often have high false positive rates and poor response prioritisation, resulting in deafening alert noise. Attacks fall through the cracks despite generating alerts. Unfortunately, legacy SIEMs are functioning only as aggregators and don't increase response capabilities. SOC's need a way to integrate their security products to reduce the noise, prioritize alerts, and enable investigation and hunting across the entire dataset.



That's why Microsoft developed Azure Sentinel, a fully cloud-native SIEM.

Our solution

The Microsoft Sentinel Quickstart service provides a fixed price, fixed scope implementation of the Microsoft Sentinel SIEM/SOAR (Security Orchestration, Automation, and Response) platform. It is designed to provide the initial set up of the platform, the pre-requisite log analytics workspace, and a default set of data connectors to enable ingestion of a basic set of Microsoft log sources. There is also the option to ingest other log sources however this would be subject to additional cost.

On completion of this module, you will have a configured Sentinel platform on which you can perform your own security analytics function.

Business outcomes

See and stop threats before they cause harm with Insight Microsoft Sentinel Quickstart.

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Speedy and cost effective deployment

- Be up and running within a day with an the initial set of logs
- No need to order hardware or pay for lengthy consultancy engagements

Focus on security, unburden SecOps from IT tasks:

- No infrastructure setup or maintenance
- SIEM Service available in Azure portal
- Scale automatically, put no limits to compute or storage resources
- Respond rapidly with built in automation and orchestration

Reduce security and IT costs with a cost-effective SIEM:

- No infrastructure costs, only pay for what you use
- Bring your Office 365 Data for free
- Predictable Billing with capacity reservations
- Flexible model, no annual commitments

Collect security data at cloud scale from all sources across your enterprise:

- Pre-wired integration with Microsoft solutions
- Connectors for many Microsoft partner solutions
- Standard log format support for all sources

Detect threats and analyse security data quickly with AI:

- Machine Learning (ML) models based on decades of Microsoft security experience and learnings and your own Threat Intelligence
- Millions of signals filtered to few correlated and prioritised incidents
- Get prioritised alerts and automated expert guidance
- Visualise the entire attack and its impact
- Hunt for suspicious activities using pre-built queries and Azure Notebooks

Our partner












Related Services

- Managed Detection and Response Service
- Security Awareness Program
- Managed Device Service

Why Insight?

Today, technology isn't just supporting the business; it's becoming the business. At Insight, we help you navigate complex challenges to develop new solutions and processes. We will help you manage today's priorities and prepare for tomorrow's needs.

 Global scale & coverage	 Operational excellence & systems	 Software DNA	 Services Solutions	 Data centre transformation	 Next-generation tech skills	 App dev & IoT expertise	 Insight Digital Workspace™	 Partner alignment
--	---	---	---	---	--	--	---	--

For more information, please contact your Insight Account Manager.

0344 846 3333 | uk.insight.com

