

Gold  
Microsoft Partner



# ITC Sentinel SIEM Managed Security Service

ITC Sentinel SIEM provides a comprehensive approach to data collection, threat detection, incident investigation and rapid response.

Whether your business adheres to NIST, CIS Top 20, ISO or is yet to adopt a framework, to further establish the cyber security of your business and achieve regulatory compliance requirements, centralised logging, event correlation and incident investigation are key.

The skills gap in the cyber security industry is ongoing; recruitment and retaining the right experts within a business can be challenging.

# SOLUTION OVERVIEW


ITC has developed a multi-layered approach which utilises the industry's first cloud native SIEM technology; Microsoft Azure Sentinel. By combining advanced machine learning and artificial intelligence with human expertise and insight, our solution enables businesses to defend against the cyber threats of tomorrow.

ITC puts experienced security analysts at the heart of its service. Delivering credible security, our SOC analysts provide depth to incidents and alerts raised; carrying out initial investigation, assessing the urgency and severity, ultimately providing contextual information on the impact to your business.


Furthermore, incident remediation, mitigation assistance and root cause analysis complete the process, enabling you to respond to the incident and taking the necessary steps to ensure it doesn't happen again. This in turn reduces the number of false positives reported, giving you the confidence that each alert reported matters.

## KEY FEATURES AND BENEFITS

 **24x7x365 management, detection and response**

 **Access to fully qualified, expert analysts**

 **Automation of common tasks and incident response**

 **Easy integration into behavioural analytics tools, workflow management systems (ServiceNow etc.)**

 **Simple and scalable pricing**

## HOW WE DO IT

 **COLLECT**

 **DETECT**

 **INVESTIGATE**

 **RESPOND**

## WHY ITC

ITC has over two decades of experience delivering cyber security solutions to organisations in over 180 countries. Delivered and managed through our world-class, London-based, Security Operations Centre, we utilise Microsoft's cloud-native technology to automate and orchestrate an all-encompassing security information and event management solution.

Combining advanced machine learning and artificial intelligence with human expertise and insight, this multi-layer approach enables businesses to defend against the cyber threats of tomorrow.

## CONTACT US

Don't just take our word for it, get in touch about a proof of value today and see the benefits for yourself. Find out how ITC Sentinel SIEM can deliver next-generation security incident response for your business.

***ITC is making the digital world a safer place to do business.***