satisnet
streamlining security management

Microsoft

Microsoft Azure Sentinel
FREE SIEM Health Check

Maximise The Value Of Your SIEM…
…All At No Cost!

Achieve maximum value from your Azure Sentinel SIEM investment with a free half-day health check from the UK's leading SIEM provider and Microsoft Security Ecosystem Partner.

Maximise Value.
Achieve ROI.
Increase Security.

Data connectors – other Azure sources and third-party feeds

Customised workbooks and reports – e.g. PCI, NIST, ISO 27001 and CIS20

Advanced threat hunting using KQL and Jupyter Notebooks

Tuning of incidents and alerts including Breach and Attack Simulations (BAS) to tune against latest attacks and TTPs

What Do *You* Get?

Understand and gain visibility of your current Azure Sentinel instance

Azure Sentinel license costs reduction – optimise log sources and storage

SIEM gap analysis

Current configurations of alerts, incidents, feeds, and incident response processes

Recommendations to achieve SIEM optimisation and capacity planning

All At NO Cost!

How The Health Check Works

Satisnet helps you fully understand the configuration and operation of your Azure Sentinel instance and provides recommendations to address any gaps discovered by investigating the below aspects.

Understand

KPIs identified and configured
Use-cases
SLAs
Incident management review
Current alerts
Types of incidents
Process and people
Log sources are configured and optimised
Data connectors – other Azure sources and third-party feeds
Workbooks (dashboarding)
Reporting

Investigate

Networking traffic analysis
Threat intelligence
Ticketing system and vulnerability management integration
Audit rules and analytics detections
Entity review/watchlists
Customised workbooks, reports, and use-cases
UEBA
Skills analysis and training requirements

Optimise

Tuning of incidents and alerts
Red Teaming/breach simulation to tune against latest attacks and TTPs
Capacity planning
Playbooks – automation of IR
Advanced threat hunting using KQL and Jupyter Notebooks
Workflow automation – power BI-integration with Teams, O365, etc.
Operating Azure Sentinel in the SOC BAU activities

After the initial 2-3 hours of auditing your Azure Sentinel instance, Satisnet will produce a report of recommendations – prioritised accordingly.

Request Your FREE Azure Sentinel Health Check Now!

www.satisnet.co.uk
+44 (0) 1582 369330

satisnet
streamlining security management