Managed Microsoft Azure Sentinel Service

Expert management of Microsoft's leading SIEM technology.

Threat detection to stay ahead of modern-day attacks

With cyber threats growing rapidly in volume and sophistication, and a cloud-enabled and mobile workforce restricting visibility and control, protecting your systems, data, and users has never been more challenging.

Organisations already using Microsoft systems are switching to use Microsoft Sentinel as their cloudnative SIEM that aggregates data from multiple sources, including users, applications, servers, and devices running on-premises or in any cloud, allowing for the analysis of millions of records.

Microsoft Sentinel addresses many of the issues that plague traditional SIEMs – eliminating the cost and time associated with deploying hardware or virtual data collection appliances, allowing for speedy connectivity to security logs data sources, and providing quick visibility into risk and security threats across multi-cloud and hybrid environments.

Microsoft Sentinel offers a birds-eye view across an organisation, giving them the visibility to combat the modern-day threat landscape. But, all the data that the SIEM is providing must be understood and acted on! Our highly accredited (CREST, ISO 9001, ISO 27001) penetration testing team (CNS, part of Flow group) will audit your entire estate to enable us to scope our managed service to suit your organisational needs, following the Mitre attack / cyber kill chain framework.

This managed service provides continuous monitoring, filtering of false positives and trend analysis to enable rapid detection and escalation of significant alerts whilst recommending strategic security improvements. Offering threat detection in a structured and deterministic way.

Benefits of trusting Flow to manage your Microsoft Sentinel environment:

- **Improved threat detection** - put yourself in a better position to detect a threat against your estate
- **De-risking your organisation** - maximise your ability to speedily detect a breach to reduce cost and damage
- **Cost effective service** - expert advice and monitoring from Flow, with a clear ROI
- **Why Flow?** - Highly accredited penetration testing team and an expert service desk with over 10 years experience

Have peace of mind that your alerts will be actioned 24x7x365

In an ideal world...

1. Know your estate
Know what your attack surface is and how to protect it

2. Secure your estate
Understand attacker behaviour to know how to defend against them

3. Detect any threats
Assess alerts without getting overwhelmed by false positives

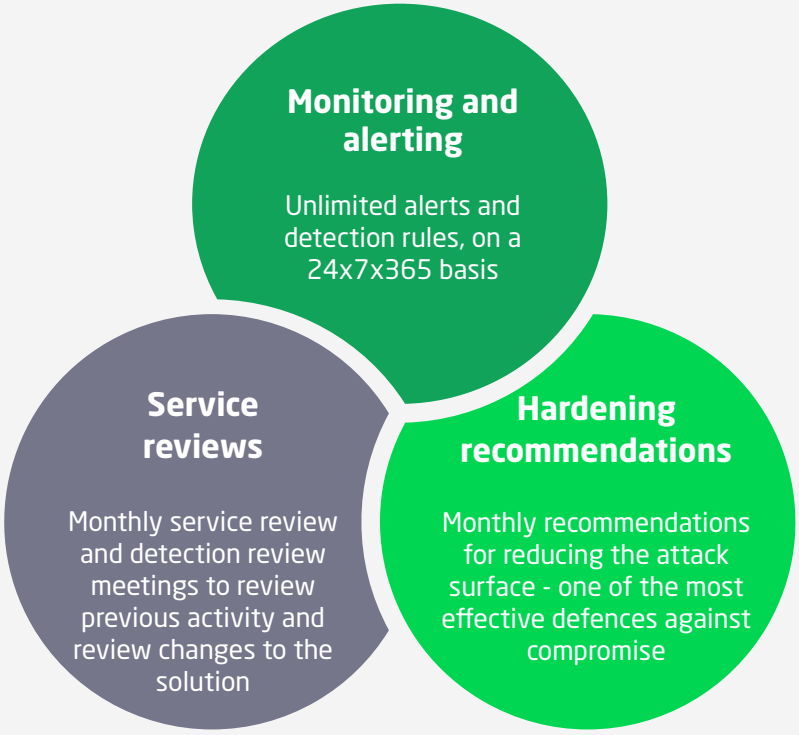
T: (0) 1442 927 996
info@flowtransform.com
flowtransform.com

FLOW
the smart choice

Rely on us for continuous smart defence

Access our expert cyber team to bolster your skills, knowledge and time constraints with both our core service and optional add ons.

The Flow approach to threat detection



Vulnerability scanning
Monthly scanning to tune the detection environment to ensure it is detecting exploits from known vulnerabilities

Managed breach detection
A fully managed breach detection solution with 5 decoys and 80 tokens within the customer environment

Purple teaming
Annual penetration test learning to ensure that a determined attacker is detected

Incident response
A bespoke package to assist with potential incidents identified

security

Security is built into the fabric of our solutions, enabling organisations to do business in confidence and without fear of a cyber attack

Flow's managed threat detection built on Microsoft Sentinel

Microsoft

for managed breach detection

THINKST CANARY

for vulnerability scanning

tenable

T: (0) 1442 927 996
info@flowtransform.com
flowtransform.com