SIEM/SOAR Managed Service

Microsoft Sentinel

In today's digital realm, the early detection of cyber threats is paramount for effective response. However, many organisations struggle with limited visibility across their on-premises and cloud environments. That's where our Microsoft Sentinel SIEM/SOAR managed service comes in. As an integral part of our MTI offering, Microsoft Sentinel seamlessly integrates with your infrastructure to provide comprehensive monitoring and detection capabilities. Leveraging advanced analytics and automation, Sentinel swiftly identifies anomalies and potential threats, empowering your team to respond proactively.

Our remote monitoring and security service delivers intelligent security analytics and threat intelligence across your enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and response.

Integrated with MTI's Service Desk, our 24x7x365 service acts as a virtual member of your security team, analysing high-risk events and fine-tuning alerts. Combined with our Microsoft Sentinel SIEM/SOAR managed service, we offer advanced threat detection and swift response mechanisms, ensuring unparalleled security for your enterprise. With our MTI service featuring Microsoft Sentinel, you can fortify your defences and stay ahead of evolving cyber threats.

What MTI Provides

MTI's managed services team will fully configure Azure Sentinel and assume all responsibility for the day-to-day operation and management of the service at all times.

Among other things, the service provides security orchestration, automation, and response (SOAR), detection of previously undetected threats and minimising false positives using Microsoft's analytics and threat intelligence. It will investigate threats with artificial intelligence, hunt for suspicious activities at scale, and respond to incidents rapidly with built-in orchestration and automation of common tasks.

In the event of a security incident or data breach that falls within the scope of assets monitored by the Managed Service, the service team will perform automated and or manual responses (via the Sentinel tooling) to triage the incident and notify the correct contact in line with pre-agreed procedures.

The managed service includes:

- Full Incident handling
- Customer callout / contact matrix to cover 24x7x365 notifications
- Ongoing rule configuration
- Ongoing fine tuning, Incident suppression, Data filtering
- Unlimited ad-hoc reporting
- Regular production of required reports from ingested data
- Automated and immediate email / ticketing alerts in the event of a security incident
- SLA backed notification of Alerts and Security Events (exact SLAs are agreed during the onboarding process, and systematically monitored)
- Full access to Workbooks for data analysis and rich visual reports

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

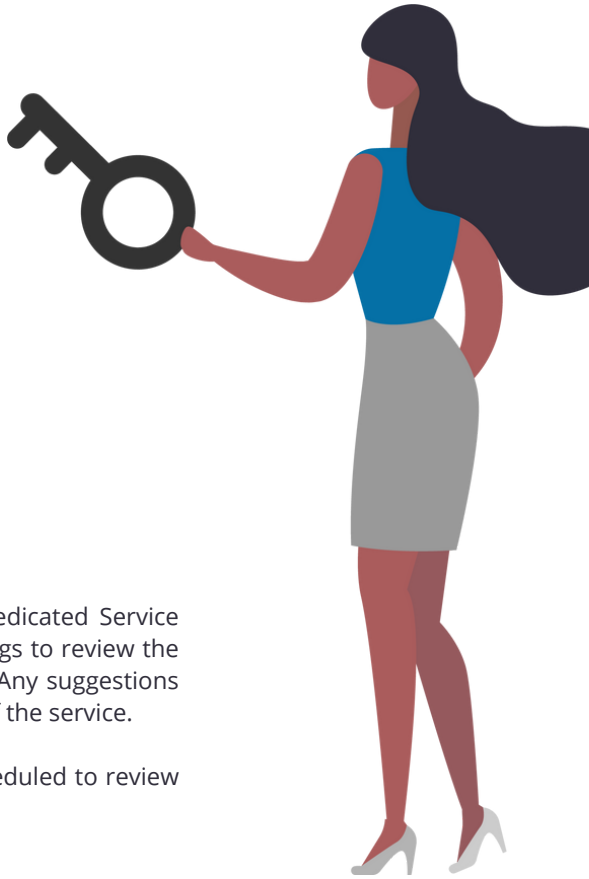
Service Transition Period

A transition period, typically lasting for six months, is vital to implementing a successful Sentinel solution and includes a range of tasks for your onboarding process:

Health Checks

If MTI did not deploy the Sentinel solution, we will perform an initial health check of the existing installed solution to baseline the environment upon award of the contract. This health check will be conducted annually.

Once the health check of the solution has been completed, we will generate a full report on findings and remediation to ensure awareness is raised of the overall health of the Sentinel deployment. Any remediation or changes will be documented and agreed with you and implemented by our skilled engineers, following approval of a quotation for remediation works.



Service Delivery

After the initial design, onboarding and transition phase is completed, your dedicated Service Delivery Manager will host regular monthly service delivery management meetings to review the operation of the managed service and ensure it continues to meet your needs. Any suggestions for improvement or additional requirements will be factored into the operation of the service.

In addition to monthly service reviews, a bi-weekly technical meeting will be scheduled to review security threats and stay up to date on outstanding actions.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Reporting and Performance Reviews

MTI provides you with a named Service Delivery Manager as a liaison for the services delivered and to be available for escalations and concerns, in addition to generating service reports, providing a comprehensive monthly reporting suite that will form the basis of performance reviews.

The service report will include but not be limited to the following:

Monthly ITSM Report

- Report on performance against agreed KPIs across all disciplines
- Account Relationship Status
- Service Status
- Commercial Status
- Business/IT Transformation Status
- Provide interpretation / analysis of reports
- Use of Egress and ServiceNow Dashboard
- Client Feedback
- Incident and Service Request Breakdown
- Change Management reporting as required

Monthly Technical Report

- Orchestration Rule Summary
- Alarm & Threat Summary
- Summaries by Device Group
- Vulnerability Summary
- Data ingestion/Capacity GB Available/Used

The MTI Service Delivery Manager will be responsible for conducting all service reviews which will be a forum to discuss performance, escalations, risk, issues, and other salient matters.

> “MTI are our strategic cyber security partner of choice. Working together for over 10 years as an extension of our team. Our relationship is built on trust of the people we work with, experts in their field that we know will have our back.”
>
> **Abba Abbaszadi**
> IT Director, Charles Russell Speechlys
>
> Charles Russell Speechlys

Why MTI

With over 20 years of security experience, MTI brings a wealth of expertise to safeguard your organisation's digital assets. As award winners in the field and with extensive experience in security solutions and penetration testing, we offer a comprehensive suite of services designed to fortify your defences.

As a founding member of the global cybersecurity body, CREST, we have developed a deep understanding of the tactics employed by malicious users to infiltrate corporate networks, allowing us to identify and mitigate any risks to your business.

ISO 9001 QUALITY MANAGEMENT | ISO 27001 INFORMATION SECURITY MANAGEMENT | ISO 14001 ENVIRONMENTAL MANAGEMENT | ISO 45001 HEALTH & SAFETY MANAGEMENT | ISO 45001 HEALTH & SAFETY MANAGEMENT

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Data Centre Modernisation
Data & Cyber Security
Managed Services
IT Transformation