SIEM Managed Services

A RICOH Company

Securing your organisation and IT infrastructure against the rising tide of cyber-attacks and online threats has become a major priority. Being able to identify cyber-attacks as early as possible means your organisation can respond more effectively before they develop into a full-blown compromise.

Think of the benefits to your organisation if it had an early warning system, alerting you to potential threats before they could unleash havoc on the business.

The remote collection and analysis of logs using an industry-standard Security Information and Event Management (SIEM) solution does just that. It enables your organisation to store, analyse, and triage log data from infrastructure, operating system and application logs, and be alerted to potential threats.

Many organisations don't have the time or resources to handle this themselves. Our Service Desk can become a cost-effective virtual member of your security team, analysing and notifying you of high-risk events and continually tuning the alerting process to ensure only abnormal events are escalated.

The Service

MTI's SIEM Managed Service is a remote monitoring and security service that can improve visibility of your on-premise and cloud environments and detect when you may be under cyber-attack, or if a user is engaged in potentially malicious activity.

Our managed services team will deploy and configure the SIEM solution into your environment and assume all responsibility for the day-to-day operation, configuration, and management of the service at all times. In the event of a security incident or data breach that falls within the scope of the SIEM service, our team will perform automated and manual responses, available within the SIEM tooling to triage the incident and notify you according to pre-agreed procedures.

Stage 1
Onboarding & Tuning

A client call-out/contact matrix is agreed confirming who MTI will contact based on the severity of the incident and whether it is in working hours or outside working hours.

Sensors deployed into each environment help gain visibility of all your on-premises and cloud environments. Once assets have been identified and configured in the SIEM dashboard, MTI will configure vulnerability scans, asset monitoring and analysis.

Over a transition period of three months, MTI will fine tune event logging and alerting tailored to your specific protected assets. Unnecessary information will be removed and important security events correlated and alerted through Orchestration rulesets.

Once the event logging for the assets has been tuned, MTI will implement Response Action rulesets to execute automatic resolution tasks triggered by specific events or security alarms.

Stage 2
Alerting

Our SIEM solution is compatible with leading IT service desk ticketing applications using ServiceNow, Jira and Email. If an alarm is generated, a ticket will be logged with MTI Managed Services and your own internal IT ticketing system, so all stakeholders are aware of the incident in a timely manner.

If it is a genuine incident, pre-agreed actions to contain or respond to the incident will be invoked by our managed services team.

The ticket will be updated as automated or manual incident response actions are carried out to provide a full audit trail of events in an open and visible manner.

Stage 3
Reporting

MTI will provide you with a named Service Delivery Manager (SDM) as liaison for services delivered who will be available for escalations and concerns. The SDM will generate service reports and provide a comprehensive monthly reporting suite to form the basis of performance reviews.

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

Deliverables

The SIEM Managed Service provides:

- Monthly Reports: Utilisation and incident summaries.
- Quarterly Reviews: Service meetings with ITSM reports to ensure alignment.
- Improvement Opportunities: Suggestions for enhancements or new requirements.
- Technical Summaries: Quarterly key findings and insights.
- Ad-Hoc Reports: Custom SIEM reports as needed.

Outcomes & Benefits

The SIEM Managed Service will deliver the following outcomes:

- Shortened time to respond to any security incident or event.
- The ability to identify security threats and incidents earlier.
- Increased vigilance against threats through MTI's 24x7x365 service.
- An expert virtual member of the security team to analyse and notify you of high-risk events and ensure only abnormal events are escalated.
- The ability to make better use of your internal resources by freeing up technical staff to focus on more valuable tasks.
- Greater peace of mind and reassurance by discovering threats and attacks before they compromise the business.

"Without MTI, we would still be struggling to manage an overwhelming amount of data to review and work out what's a real and significant threat. Working with MTI gives us the peace of mind that we have an expert team making sense of what is noise and what we need to proactively go and do something about.

The relationship I have with MTI is built on trust. MTI have always delivered exactly what they said they would, proactively, truthfully and in the timescales they promised. We're starting to work with MTI on more projects for that reason, I know they will deliver."

Richard Warren,
Head of IT Service Delivery
Merton Council

Why MTI?

MTI has been helping customers become more secure for more than 20 years. We have developed a wealth of knowledge and skills in the tactics used by malicious users to gain access to corporate networks. As the threat landscape expands and the range of cyber-attacks proliferates, we have evolved our expertise to help identify risks to your business earlier and faster. Our SIEM Managed Service can help reduce your cyber security burden and let your IT team focus on more strategic and valuable tasks for your organisation.

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200