Gold Microsoft Partner

Cyber Advisory
ADVISORY PAPER

MICROSOFT SENTINEL SMART INGESTION

Align your security posture and understand your data, agent deployment and usage options to optimise investments within Microsoft Sentinel.

Microsoft Sentinel is a powerful tool, however to maximise its benefits and your total cost of ownership, there is a need to continually ‘right size’ and tune your data sources, agent deployment, usage options, and your ingestion policies to align with your business’s security and risk posture.

This does not mean enabling every single data source to send the maximum amount of information or copying traditional NOC/SOC/SIEM ingestion practices. Ingestion of log data can become expensive and require significant effort and resources to sift through the information to glean the right intelligence that drives correct responses. Therefore, maintaining control of ingestion levels without compromising your policies on risk and compliance is key.

ITC can tailor your data sources to gather the correct amount of information at the right time and can further be tuned “up or down” depending on known threats.

SOLUTION OVERVIEW

As an MSSP ITC understands data log ingestion as a function of our own security operations and on behalf of our customers. We observe trends, efficiencies and models across a range of company sizes and industries, and continuously test, feedback and deploy the latest enhancements and best practices.

Delivered through an ITC workshop, our experts will discuss your organisation’s security and audit postures and policies, taking into account budgetary constraints. We then set up and conduct the discovery and provide a quick overview of the anticipated deliverables, before diving deep in to your Sentinel data to provide a report of actionable insights and summary roadmap of potential savings across various sources through ingestion optimisation, maximising licensing-related benefits and Azure offers.

KEY FEATURES AND BENEFITS

Situational Analysis

- Examination of current threat posture
- Compliance and risk appetite against policy
- Review of tooling and data sources

Actionable Recommendations

- Recommendations for reducing data “noise”
- Optimising information provided to Sentinel
- Prioritisation of data sources and volume against budget

Post-Improvement Reporting

- Guidance on source ‘tuning’ against threat levels
- Guidance on any appropriate tooling or licence changes to add improvement
- Considerations for Azure reserved capacity and other cost management measures

Risk profile and security policy review

A view of current data sources and the usefulness of the information provided

Key ingestion management recommendations and ‘tuning’ advice

Report providing details of actions to reduce cost and complexity

WHY ITC

Gold Microsoft Partner Microsoft

Member of Microsoft Intelligent Security Association Microsoft

ITC Secure is an advisory-led cyber security services company.

We have a 25+ year track record of delivering business-critical services to over 300 blue-chip organisations - bringing together the best minds in security, a relentless focus on customer service, and advanced technological expertise to help businesses succeed.

With our integrated delivery model, proprietary platform, and customer-first mindset, we work as an extension of your team throughout your cyber journey and always think not only about you but also your customers and the reputation of your brand.

ITC Secure is a certified Great Place to Work® and is headquartered in London, UK. With a dynamic balance of the best in people, technology, and governance, we make cyber resilience your competitive advantage.

For more information, please contact us: **enquiries@itcsecure.com** or **020 7517 3900**