Work Package: Modern SecOps

a. Scope

i. Customer Scope

Customer Variable	In Scope
Organisation (s)	<<ClientName>>
Location	<<CustomerCountry>>

ii. Service Scope

Service Variable	In Scope	Out of Scope
Resources	Microsoft Sentinel	All other resources

b. Service Term (Project)

i. Service Start Date: Within ten (10) days from countersign date of this Statement of Work

ii. Service Expiration Date: 12 months from the Service Start Date

All Services must be consumed within 12 months from the Service Start Date. Services not consumed by the Expiration Date are terminated, and any Fees paid for such Services will be deemed earned by Bytes and no refund will be provided. The reinstatement of expired Services will require the execution of a Change Order or new SOW prior to delivery and may be subject to additional Fees.

c. Agreed Work Location

Work delivered for the Service will be conducted remotely from Bytes' registered offices, or proxy locations of employees.

d. Prerequisites

Item	Responsibility
Provide a single point of contact (SPOC) for all engagement queries and concerns. The SPOC must identify relevant technical and business stakeholders as requested, and ensure they are available to assist with this engagement if required.	Customer
Identify maintenance/implementation window(s) appropriate for this project	Customer
Identify appropriate individuals to involve in each phase of the project, and ensure they are available as needed.	Customer
Provide or facilitate access to any systems, information or individuals that is required	Customer

e. Deliverables

This Service will produce the following Deliverable(s):

Deliverable	Description	Frequency	Sign-Off
Microsoft Sentinel Consultancy	Provide professional services to support with the planning, implementation and knowledge transfer of Microsoft Sentinel.	Once	Implementation

f. Service Specification – Microsoft Modern SecOps Consultancy

Module Overview: The Microsoft Modern SecOps engagement covers the following key areas: Planning, Activation, Initial Configuration and Knowledge Transfer on Microsoft Sentinel.

Inclusions	**Plan:**
	• Microsoft Sentinel overview
	• Cost estimation
	• Business case building
	• Architect workshop & high-level design
	Implement:
	• Microsoft Sentinel instance creation
	• Azure Lighthouse configuration
	• Defender XDR integration
	• Microsoft Sentinel Data Lake setup & bulk retention changes to tables
	• Data connector configuration (Microsoft Cloud Services)
	  ○ Defender XDR
	  ○ Microsoft 365 Activity
	  ○ Entra ID
	  ○ Azure Activity
	• Data connector configuration for Windows Server (DCRs only)
	• Data connector configuration for 3rd party solutions (Max 1)
	• Analytical rule implementation (Max 20)
	• Workbook configuration (Max 30)
	• Automation rules & playbook implementation (Max 3)
	Health check & validate:
	• Check retention & archive settings
	• Check costs & billings settings
	• Validate Analytical Rule usage & health
	• Validate Workbook usage
	• Check Automate Rule health
	• Check Playbook usage & health
	Optimise & learn:
	• Cost & consumption optimisation
	• Data ingestion optimisation
	• Extending automation
	• SOC activity review & processes
	• Knowledge transfer – Analytical Rules
	• Knowledge transfer – Workbooks & reporting
	• Knowledge transfer – Automation
	• Knowledge transfer – Incident Management
	• Knowledge transfer – KQL
	• Analytical Rule tuning

Exclusions	• Procurement of hardware, software and licensing unless explicitly stated in this document • Follow on tasks or documentation, unless explicitly stated in this document. • Configuration of Servers • Configuration/deployment of applications

	• Configuration of on-premises Firewall(s)
Dependencies	Contributor RBAC Access of the target Azure subscription. Global Administrator Access of the target Entra ID Tenant. **Note:** The configuration of Microsoft Sentinel can be performed on a remote session with the customer resource with the correct permissions.
Key Information / Assumptions	Customer has an Azure agreement and can provision one or more Azure Subscriptions. Customer retains ownership and responsibility for Sentinel Workspaces and associated objects created.
Product(s)	N/A
Bytes Resource	Microsoft Security Consultant
Customer Resource	Resource with access and permissions to: Microsoft365, Entra ID and the relevant Azure subscriptions.