Work Package: Threat Protection Consultancy

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 Defender	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
Defender Consultancy	Support with the planning, implementation and deployment of Microsoft Defender components.	Once	Implementation

f. Service Specification – Microsoft Threat Protection Consultancy

Module Overview: Provide a workshop session to explore the capabilities of Microsoft Defender. Following this, consultancy will be provided to increase the utilisation of Microsoft Defender. Knowledge Transfer and documentation will be provided to capture configuration and provide handover to the customer.

Inclusions	**Defender for Endpoint:** • Feature configuration, device grouping & device tagging • Device enrolment & testing • Endpoint policy setup, testing & tuning (up to 10 policies per activity) • Vulnerability management review & remediation planning • Knowledge transfer **Defender for Office 365:** • Attack simulation training & campaign creation • Threat/alert policy setup, testing & tuning (up to 10 policies per activity) **Defender for Cloud Apps:** • Connection & application review • Policy setup, testing & tuning (up to 10 policies per activity) • Knowledge transfer **Defender for Cloud:** • Defender for Cloud planning, setup & knowledge transfer **Defender for Identity:** • Planning & sizing • Deployment & installation (up to 4 servers per activity) • Platform configuration & tuning • Knowledge transfer **Defender for Servers:** • Feature configuration, device grouping & device tagging • Azure Arc enrolment & deployment (up to 10 servers per activity) • Knowledge transfer
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 to the target environment • Individual attending sessions has Security and Compliance Administrator roles • Customer has access to M365 E5 or equivalent licenses (already in their environment or via a trial)
Key Information / Assumptions	• Customer can make agreed changes to their Defender environment

	• Customer wants to expand their utilisation of their Microsoft Defender environment
Product(s)	N/A
Bytes Resource	Microsoft Consultant
Customer Resource	Resource with access and permissions for the necessary work.