KTL SOLUTIONS

Secure Enclave: 12-Week Implementation

$30,000 (plus GCC High Licenses and Azure Services)

Product Azure Sentinel

Secure Enclave: KTL will configure and implement Office 365, Enterprise Mobility & Security, and Windows 10 Enterprise features in a Virtual Desktop Infrastructure (VDI) in Azure Government and configure Azure Sentinel services.

Services provided will cover:

- Deployment of Azure Active Directory Domain Services.
- Deployment of Azure Virtual Desktops within supported Azure Government regions.
- Azure Virtual Desktops will be configured such that
  - They follow industry security best practices.
  - The execution of applications is prevented unless whitelisted by an administrator.
  - They allow users to utilize any available session host through profile mapping.
  - Office 365 Apps for Enterprise are installed
  - Teams is configured for remote/VDI environment.
- Deployment of a next generation network security appliance to protect devices within the enclave.
- Configuration of routing and access control lists to limit connectivity to only services identified as required.
- Configuration of conditional access policies to:
  - Block connectivity to all services other than the Azure Virtual Desktop's from outside the environment.
  - Allow connectivity to Office 365 only from within the Azure Virtual Desktop network
  - Enforce MFA for all users
  - Allow administrative access for a named account (break glass account) to be used outside the enclave in the event something goes wrong.
- Deployment and configuration of Azure Sentinel to:
  - Audit Office 365 activity.
  - Audit Azure Active Directory sign-ins.
  - Audit Azure Active Directory events.
  - Audit Azure activity events.
  - Audit Azure Virtual Desktop events.
  - Audit network security appliance events.
- Configuration of up to five Azure Sentinel analytic rules.
- Configuration of up to five Azure Information Protection (AIP) labels
  - Public, Confidential, FCI, CUI, CUI – EXPT
- Deployment of Microsoft Defender for Endpoint on supported systems within the environment.
- Configuration of Microsoft Defender for Office 365 following industry and vendor best practices
- Configuration of backups for user data within Office 365 and Azure

- Configuration of Azure AD Privilege Identity Management features if Azure AD P2 licenses are purchased.
- Configuration of Office 365 B2B features to restrict the ability to collaborate with external users without administrative approval.
- Configuration of Azure AD user settings following industry and vendor security best practices.
- Creation of a System Security Plan (SSP) to document CMMC practices/objectives satisfied completely or partially through technical configurations.
- Identification of CMMC practices/objectives that customer is responsible for or can be met using additional third-party services.
- Set up of VDI for users in Azure Government
- Configuration of services and document configurations mapped to CMMC/NIST 800-171
    - Azure Active Directory
    - Azure Information Protection (Configuration of 2 policies)
    - Intune
    - Windows 10 Enterprise
    - Windows Virtual Desktop for users
- Determining and Configuration of Required Compliance Policies
- Determining and Configuration of Required and Supportable Configuration Policies
- Configuration of Conditional Access Policies
- Configuration of Exchange DLP rules
- The following services will be disabled:
    - Mobile device access
    - Access by any device not utilizing the VDI environment except for access to the VDI environment itself.
- Configuration of Azure Sentinel to ingest log data from the Microsoft cloud services listed:
    - Exchange Online
    - SharePoint Online
    - OneDrive for Business
    - Azure AD
    - VDI Machines
- Configuration of up to 5 log alerts for potential security incidents
- Documentation for configurations of cloud environment with mapping to CMMC/NIST 800-171 controls