Threat Protection 3 semanas

Microsoft Defender ATP / Office 365 ATP / Azure ATP / MCAS

KS - Consulting Services

Microsoft Defender es una plataforma orientada a la defensa contra amenazas. Cuenta con soluciones que coordinan la detección, prevención, investigación y respuesta ante diversos tipos de ataque a lo largo de las entidades que conforman a la organización.

Casos de Uso

KS Consulting habilitará el siguiente alcance como parte del ofertamiento:

- **Gestión de incidentes:** Ver, correlacionar, evaluar y administrar alertas y eventos en dispositivos, usuarios y buzones de la red.
- **Auto IR:** uso de herramienta y proceso para investigar y responder automáticamente a eventos maliciosos en la red.
- **Caza avanzada:** Buscar datos del entorno para encontrar amenazas conocidas y potenciales, y actividades sospechosas.

Ámbitos

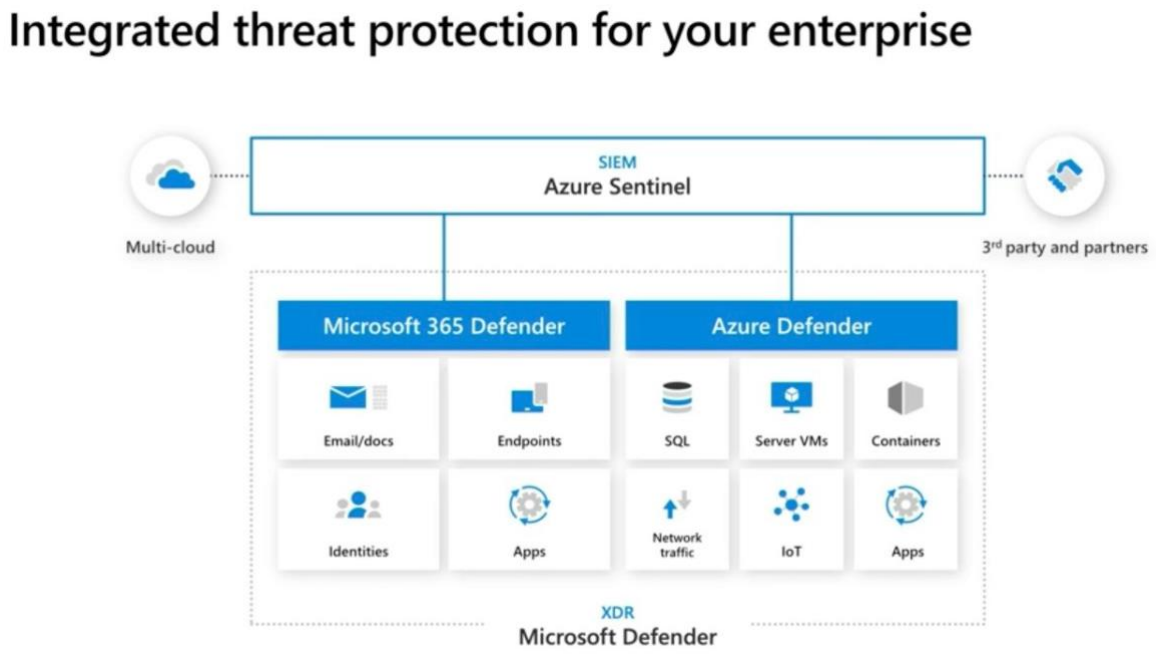
- Entorno de desarrollo o prueba que incluye EndPoints, Servidores, Controladores de Dominio.
- Entorno de producción con Microsoft 365, Azure, servicios de Active Directory, endpoints y servidores.

Alcance

- Planeación **(2 días)**.
- Preparación **(5 días)**.
    - Preparación.
    - Instalación.
    - Configuración y ejecución.
        - **Microsoft 365 Defender.**
        - **Azure Defender.**
        - **MCAS.**
        - **Azure Sentinel.**
- Simular Ataque **(11 días)**.
    - Validación de Requerimientos.
    - Ejecutar la Simulación.
    - Investigar un Incidente.
    - Revisar Alertas Generadas.
    - Revisar la Linea de Tiempo de Dispositivos (MDATP).
    - Revisar la Información de Usuario (MCAS).
    - Investigación y Remediación Automática (Auto IR).
    - Resolución del Incidente.

    - Escenario de Caza Avanzada.
        - Validación de Requerimientos de Caza.
        - Ejecutar la Simulación.
- Cierre y Resumen **(2 días)**.
    - Tablero finalizado.
    - Reporte detallado de lo encontrado.

Mayor Información:



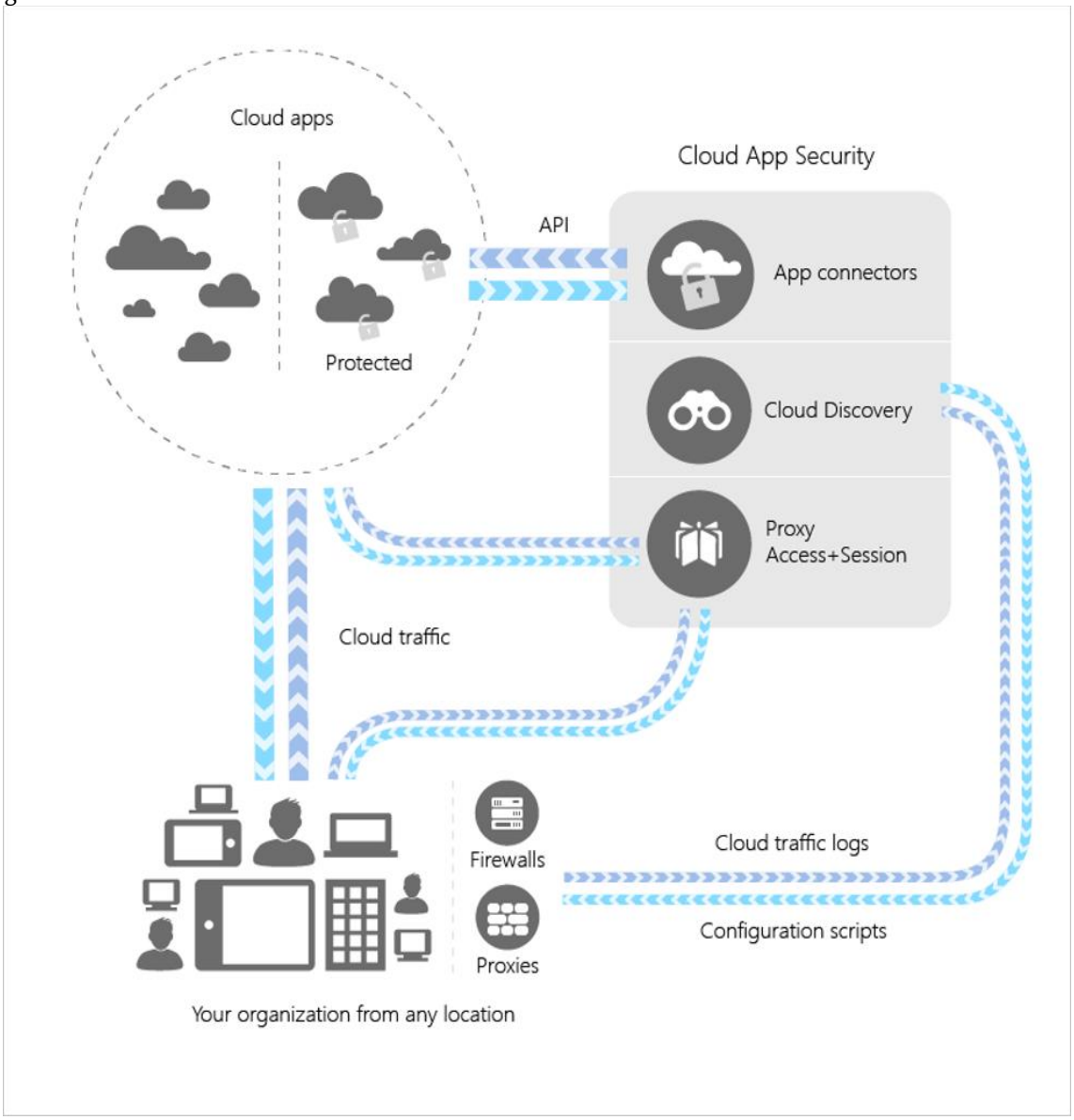
Microsoft 365 Defender

Integra herramientas que permiten combatir amenazas dentro del ambiente de Office 365. Cuenta con directivas que regulan la interacción por email y herramientas colaborativas como SharePoint Online y OneDrive for Business, además de generar alertas personalizadas para notificar eventos de riesgo.

Directivas de Protección en Office 365 ATP:

Microsoft Cloud App Security

MCAS es un Cloud Access Security Broker (CASB), el cual permite la integración de recopiladores de logs, conectores API y reverse proxy para el monitoreo de actividad dentro de la organización. Además de contar con directivas de acceso que regular el comportamiento de los usuarios dentro de las aplicaciones en la nube organizacional.



Microsoft Defender

Microsoft Defender es una plataforma diseñada para prevenir, detectar, investigar y responder ante amenazas avanzadas a lo largo de la red corporativa.

Microsoft ATP utiliza tecnología integrada en los sistemas Windows 10, la cual recolecta y procesa las señales de comportamiento del dispositivo y las envía a la instancia en la nube de Windows Defender ATP de la organización. En la nube la información recolectada en los endpoints es procesada para generar estadísticas y recomendaciones para prevenir amenazas.

Azure Defender

Azure Defender previene amenazas como amenazas de desplazamiento lateral, robo de credenciales, ataques de fuerza bruta, ejecución sospechosa de scripts dentro del entorno On-premises de la organización.

Esta solución contempla la instalación de un sensor en cada uno de los controladores de dominio que posea la organización. Estos sensores registran la actividad y reportan los incidentes al portal de Azure ATP, además de contar con integración a Cloud App Security.