Microsoft

Seguridad, privacidad, cumplimiento y confianza de Microsoft Azure

Instituto Nacional de Aprendizaje
Llave del Progreso

Instituto Nacional de Aprendizaje

Llave del Progreso

Herramientas y características de seguridad

Azure Segurity Center

Exploración de Azure Security Center

- Un servicio de supervisión que ofrece protección contra amenazas en todos sus servicios locales y de Azure.

- Recomendaciones de seguridad
- Supervisión de la configuración de seguridad
- Aplicación automática de sus directivas de seguridad
- Analizar e identificar posibles ataques
- Control de acceso Just-In-time para los puertos

https://azure.microsoft.com/en-us/services/security-center

Escenarios de uso de Azure Security Center

- Puede usar Security Center en las etapas *Detectar*, *Evaluar* y *Diagnosticar* de una contestación a un incidente.

https://docs.microsoft.com/es-es/azure/security-center/security-center-planning-and-operations-guide

Puede usar Security Center durante las etapas de detección, evaluación y diagnóstico.

Detectar. Revisa la primera indicación de una investigación de evento.

Evaluar. Realiza la evaluación inicial para obtener más información sobre la actividad sospechosa.

Diagnosticar. Realiza una investigación técnica e identifica las estrategias de contención, mitigación y solución alternativa.

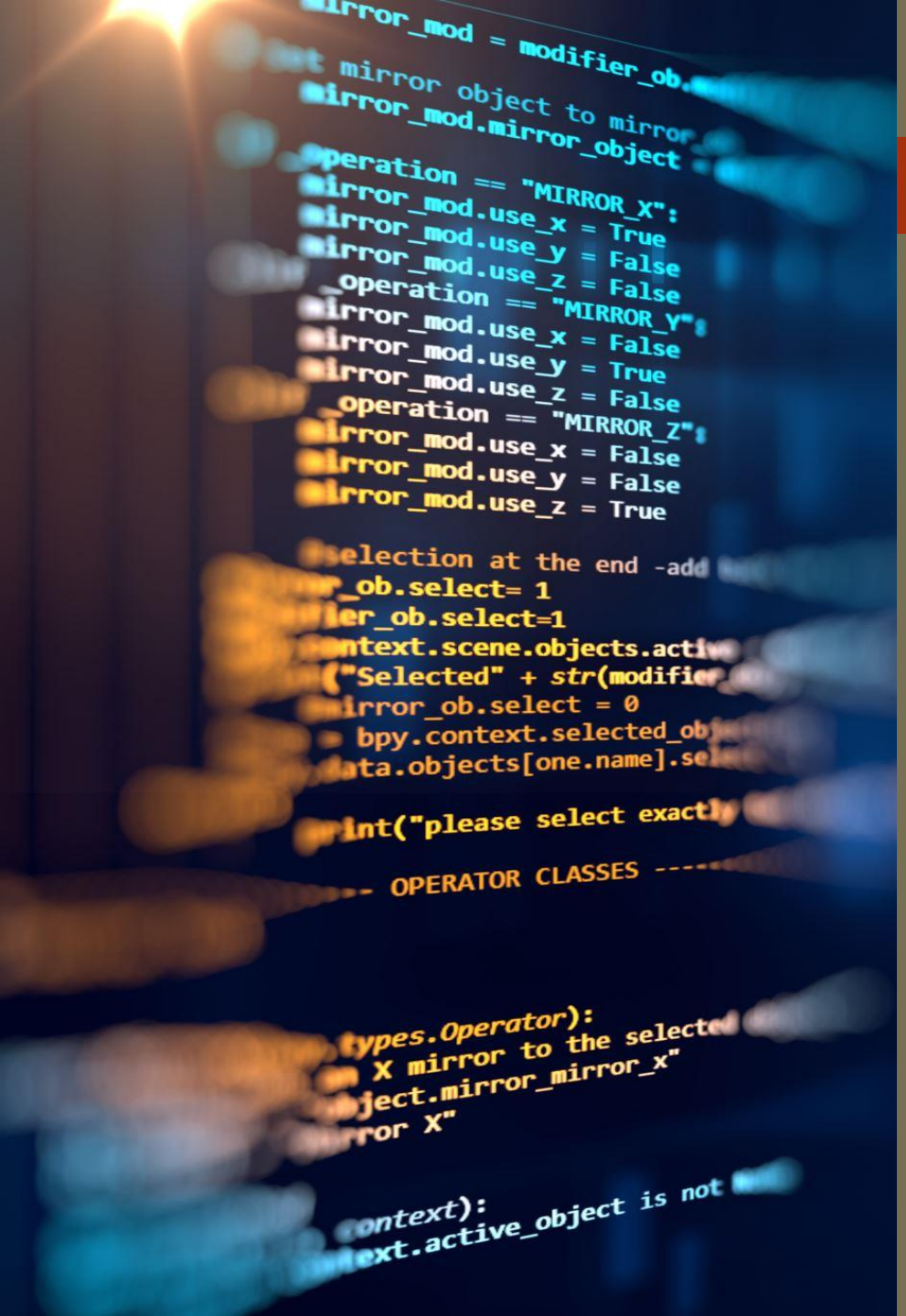
https://azure.microsoft.com/en-us/services/security-center

Exploración de Azure Key Vault

- Es un servicio en la nube que almacena los secretos de las aplicaciones en una ubicación centralizada, para controlar de forma segura los permisos de acceso y el registro de acceso.
Escenarios de uso

- Administración de secretos.
- Administración de claves.
- Administración de certificados.
- Almacenamiento de secretos respaldados por módulos de seguridad de hardware (HSM).

https://azure.microsoft.com/es-es/services/key-vault



Azure Key Vault

- **Administración de secretos**. Puede usar Key Vault para almacenar y controlar de forma segura el acceso a tokens, contraseñas, certificados, claves de interfaz de programación de aplicaciones (API) y otros secretos.

- **Administración de claves.** También puede usar Key Vault como solución de administración de claves. Key Vault facilita la creación y el control de las claves de cifrado que se usan para cifrar sus datos.

https://azure.microsoft.com/es-es/services/key-vault

Azure Key Vault

- **Administración de certificados**. Key Vault le permite aprovisionar, administrar e implementar sus certificados de Capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS), tanto públicos como privados, para sus recursos de Azure, conectados internamente, más fácilmente.

- **Almacenamiento de secretos protegidos con módulos de seguridad de hardware** (HSM). Los secretos y las claves se pueden proteger con software o con HSM validados por el nivel 2 de FIPS 140-2.

Azure Information Protection (AIP)

- Es una solución basada en la nube que ayuda a las organizaciones a clasificar y proteger sus documentos y correos electrónicos mediante la aplicación de etiquetas.

- Usa automáticamente las reglas y condiciones definidas por los administradores.
- De manera manual, por los usuarios.
- O pueden combinar métodos automáticos y manuales, basados en recomendaciones.

Azure Advanced Threat Protection (Azure ATP)

- Solución de seguridad basada en la nube para identificar, detectar e investigar amenazas avanzadas, identidades en peligro y acciones internas maliciosas.

https://azure.microsoft.com/es-es/features/azure-advanced-threat-protection

Componentes Azure Advanced Threat Protection (Azure ATP)

- **Portal:** cuenta con su propio portal dedicado a supervisar y responder a actividades sospechosas.
- **Sensores:** se instalan directamente en sus controladores de dominio. El sensor supervisa el tráfico del controlador de dominio sin requerir un servidor dedicado ni configurar la creación de reflejo de puertos.
- El **servicio en la nube** se ejecuta en la infraestructura de Azure.