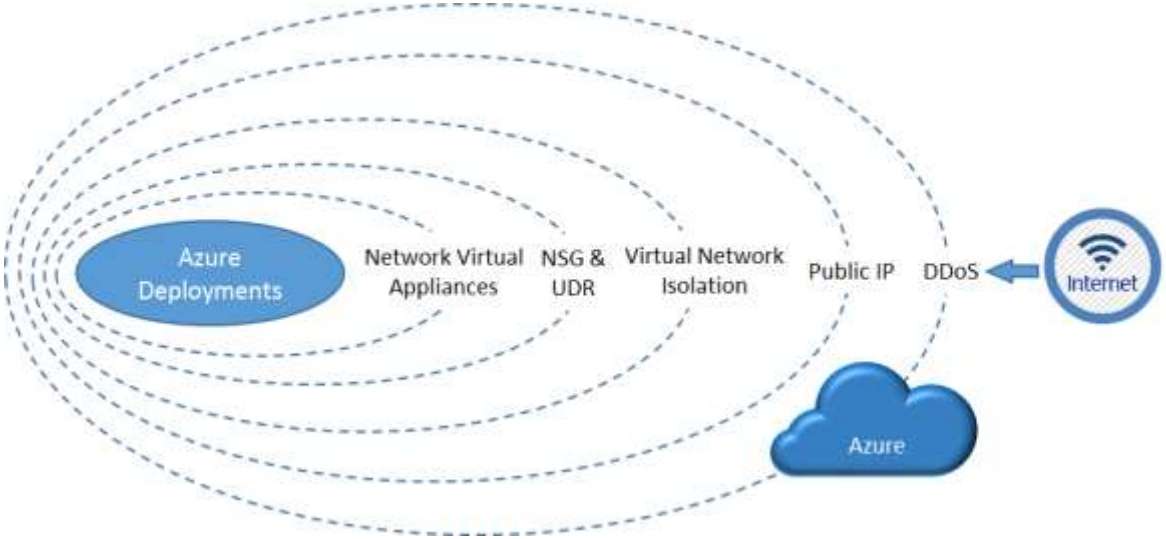
Agenda

- Presentación.
- Servicios de Seguridad en Azure
- ¿Que es Azure Security Center?
- ¿Por qué tenemos que usarlo?
- ¿Qué necesitamos para empezar?
- Free vs Estándar
- Recolección de datos.
- Setting - Funcionalidades.
- Demo.

Servicios de Seguridad de Azure



https://docs.microsoft.com/en-us/azure/best-practices-network-security

Servicios de Seguridad de Azure

- Servicios generales de Seguridad en Azure.
  - Azure Security Center
  - Azure Key Vault
  - Azure Disk Encryption
  - Log Analytics
  - Azure Dev/Test Labs
- Azure Identity and Access Management
  - Azure Role Based Acces Control (RBAC).
  - Azure Active Directory /B2C /B2B
  - Azure Multi-Factor Authentication
- Azure Networking
  - Azure Security Gropus
  - Azure VPN Gateway
  - Azure Load Balancer
  - Azure Applicantion Gateway
  - Azure Applicantion Proxy
- Seguridad en Azure Storage
  - Azure Storage Service Encryption
  - Store Simple Encrypted Hybred Storage
  - Azure Client-Side Encryption
  - Azure Storage Shared Access Signatures
  - Azure Sotrage Account Keys
  - Azure Files Shres wit SMB 3.0 Encryption
  - Azure Storage Analytics
- Seguridad en Azure Database.
  - Azure SQL Firewall
  - Azure SQL Authentication
  - Azure SQL Trasnsparent Data Encryption
  - Azure SQL Database Auditing
- Backup and Disaster Recovery
  - Azure Backup
  - Azure Site Recovery

¿Que es Azure Security Center?

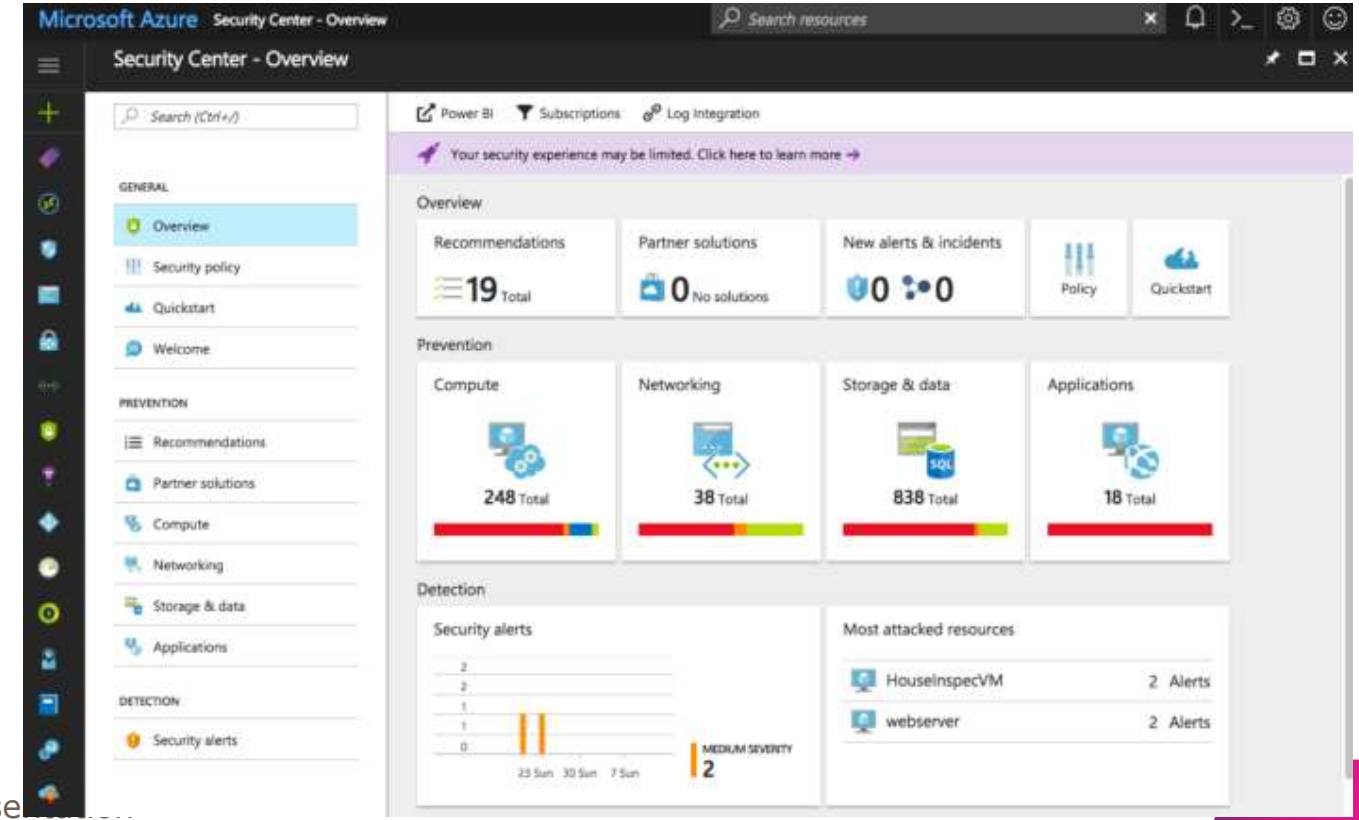
Azure Security Center nos ofrece una solución de administración unificada de la seguridad en Azure, además de protección contra amenazas avanzadas para todas nuestras cargas de trabajo o servicios que se ejecutan tanto en la nube, Azure, Amazon, Google, como On-Premise, o sea, de forma local en nuestro centro de datos.

Asimismo, nos da visibilidad y control sobre las cargas de trabajo de nube hibrida, defensas activas que reducen la exposición a las amenazas y una detección inteligente, lo que nos permitirá mantenernos al día de los ciberataques.

A través del panel principal y de un vistazo tendremos un resumen de la situación de seguridad de las cargas de trabajo permitiéndonos detectar y evaluar su seguridad pudiendo identificar y mitigar riesgos.

¿Qué pinta tengo?

.

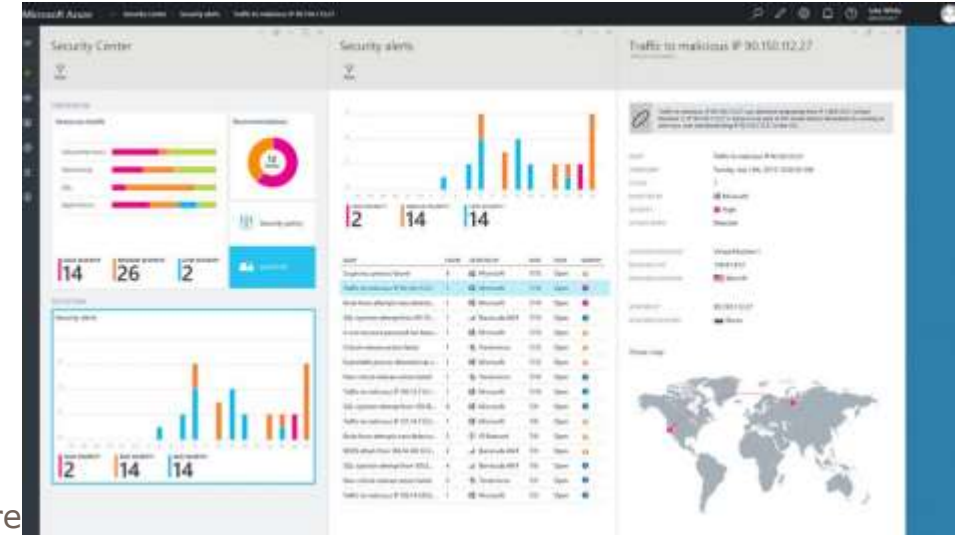


Insight Prese...

Insight

¿Por qué tenemos que utilizarlo?

- **Ventajas de Control y visibilidad.**
- **Prevención de amenazas adaptable.**
- **Detección y respuesta inteligente ante amenazas**



Insight Pre

Insight

¿Por qué tenemos que utilizarlo?

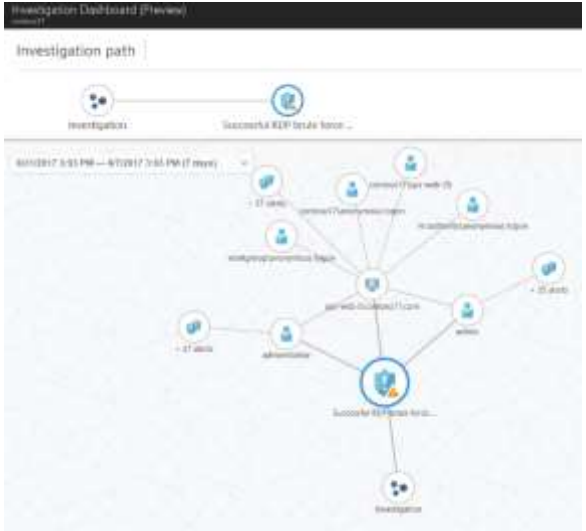
Ventajas de Control y visibilidad.

- **Comprensión del estado de seguridad de las cargas de trabajo híbridas**. A través de una única consola podemos administrar la seguridad de todas las cargas de trabajo en la nube híbridas (locales, de Azure y de otras plataformas en la nube, como en de nuestros centros de datos). Los paneles integrados nos proporcionan información al instante sobre los problemas de seguridad que requieren atención.
- **Integración con los flujos de trabajo de seguridad existentes**. Nos permite integrar y analizar la información de seguridad usando las API REST que nos conectará con los procesos y las herramientas existentes.
- **Visibilidad en las cargas de trabajo en la nube**. Ante los cambios en los despliegues, altas y bajas de servicios, nuevos desarrollos, nuevos proyectos, seguir detectando automáticamente e incorporándolos a nuestro control en cuanto se crean.
- **Administración de directivas centralizada**. Nos permite garantizar el cumplimiento de los requisitos de seguridad normativos administrando las directivas de seguridad de forma centralizada.
- **Datos de seguridad procedentes de muchos orígenes**. Recopila, buscar y analizar los datos de seguridad procedentes de una gran variedad de orígenes, incluidas soluciones de terceros, como firewalls, etc.
- **Informes de cumplimiento**. Nos proporciona información y datos relativos a la seguridad para demostrar el cumplimiento y generar fácilmente pruebas para los auditores.

¿Por qué tenemos que utilizarlo?

Prevención de amenazas adaptable

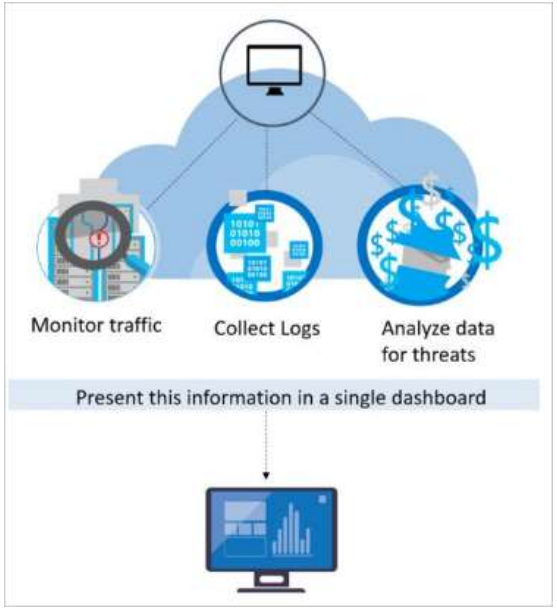
- **Evaluación de la seguridad continua**. Supervisa la seguridad de los equipos, redes y servicios de Azure con cientos de evaluaciones de seguridad integradas, o bien nos permite crear las suyas propias. Asimismo nos facilita identificar el software y las configuraciones que son vulnerables a ataques.
- **Controles de aplicación adaptables**. Bloquear el malware y otras aplicaciones no deseadas aplicando recomendaciones de inclusión en lista blanca adaptadas a nuestras cargas de trabajo de, basándonos en el aprendizaje automático.
- **Seguridad de acceso a la red**. Reducimos la superficie expuesta a ataques de red con el acceso gestionado y controlado "***Just-In-Time***" a los puertos de administración de las máquinas virtuales de Azure, lo que reducirá drásticamente la exposición a ataques por fuerza bruta y otros tipos de ataques de networking.
- **Recomendaciones prácticas**. Fácil, nos da recomendaciones de seguridad prácticas ordenadas por prioridad, importante detalle, y guías de automatización integradas para corregir las vulnerabilidades de seguridad antes de que puedan ser usadas por los "malos".



¿Por qué tenemos que utilizarlo?

Detección y respuesta inteligentes a amenazas

- **La inteligencia sobre amenazas más exhaustiva del sector**. Nos podemos beneficiar de la seguridad inteligente de Microsoft, que emplea trillones de señales de sistemas y servicios de Microsoft despelgados en todo el mundo para identificar las nuevas amenazas que están en constante evolución.
- **Investigación optimizada**. Realiza una evaluación del ámbito y el impacto de un ataque a través de la experiencia visual e interactiva del portal. Podemos usar las consultas predefinidas o "ad hoc" para explorar los datos de seguridad en mayor profundidad.
- **Alertas e incidentes clasificados por orden de prioridad**. Insistor, muy importante primero centrarnos en las amenazas más graves gracias a las alertas de seguridad prioritarias. También puede crear sus propias alertas de seguridad personalizadas.
- **Detección de amenazas avanzada**. Esta funcionalidad de análisis del comportamiento y aprendizaje automático sirve para identificar ataques y vulnerabilidades de seguridad de día cero (0 day), supervisando tanto las redes, máquinas asi como servicios en la nube para detectar ataques entrantes y actividad posterior, cuidadito.
- **Inteligencia contextual sobre amenazas**. Nos permite visualizar el origen de los ataques en un mapa del mundo interactivo, usar informes de inteligencia sobre amenazas integrados para obtener información valiosa sobre las técnicas y objetivos de actores malintencionados conocidos, los malos "malosos".



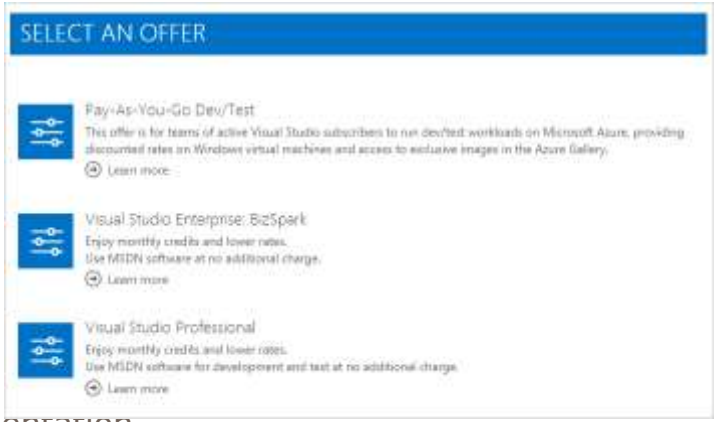
¿Qué necesitamos para empezar?

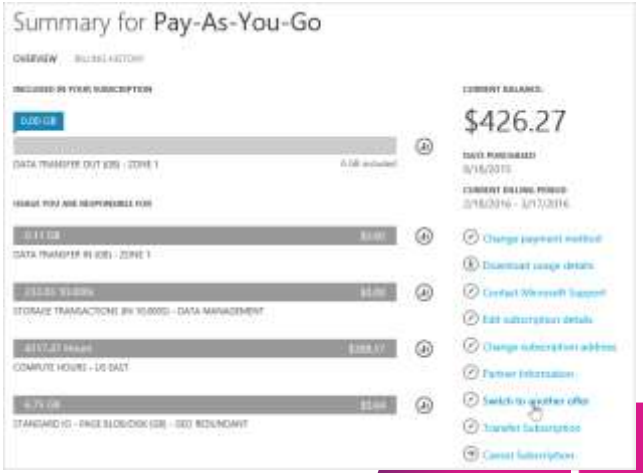
MUNDOSQL.ES

Para empezar a trabajar con el Centro de seguridad, necesitamos….

- Una suscripción a Microsoft Azure.

Nota: Recordar que, por defecto, se habilita la versión Azure Security Center Free





Insight

Versiones: Free vs Standard

- https://azure.microsoft.com/es-es/pricing/details/security-center/

CARACTERÍSTICAS	GRATIS (SOLO RECURSOS DE AZURE)	ESTÁNDAR (RECURSOS DE AZURE E HÍBRIDOS)
Directiva de seguridad, evaluación y recomendaciones	✓	✓
Soluciones de asociados conectados	✓	✓
Búsqueda y colección de eventos de seguridad	- -	✓
Acceso a CM Just-in-Time	- -	✓
Controles de aplicación adaptables	- -	✓
Detección de amenazas avanzada en redes, máquinas virtuales y servidores, y servicios de Azure	- -	✓
Alertas integradas y personalizadas	- -	✓
Información sobre amenazas	- -	✓
Datos incluidos	No aplicable	500 MB por día[1]
Precio	Gratis	€12,65 / nodo[2] / mes

Recolección de datos de ASC

¿Cómo recopila Security Center los datos de los equipo en Cloud y On-Premise?

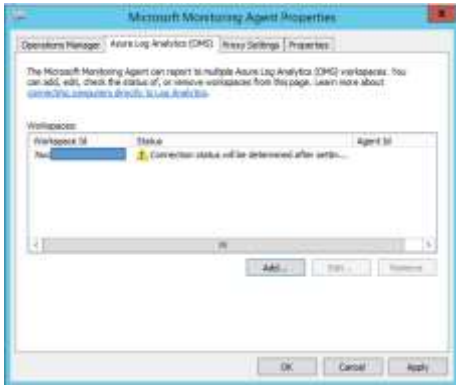
Me alegro que me hagas esa pregunta

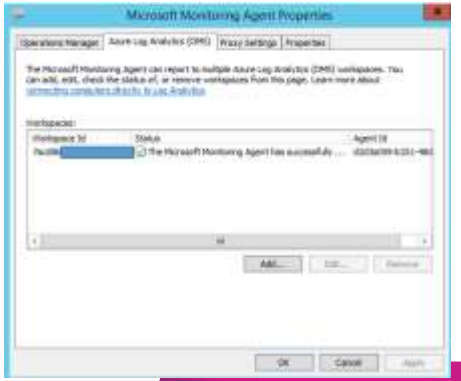
La recolección de datos se realiza a través de …..

Microsoft Monitoring Agent, que tiene la capacidad de leer distintas configuraciones relacionadas con la seguridad y distintos registros de eventos de la máquina y copia los datos en el área de trabajo para analizarlos.

Estos son algunos ejemplos de dichos datos:

- tipo y versión del sistema operativo,
- registros del sistema operativo (registros de eventos de Windows),
- procesos en ejecución,
- nombre de la máquina,
- direcciones IP,
- usuario conectado e identificador de Tenant.
- Asimismo, copia los archivos de volcado de memoria en dicha área de trabajo.





Como funciona el agente de ASC.

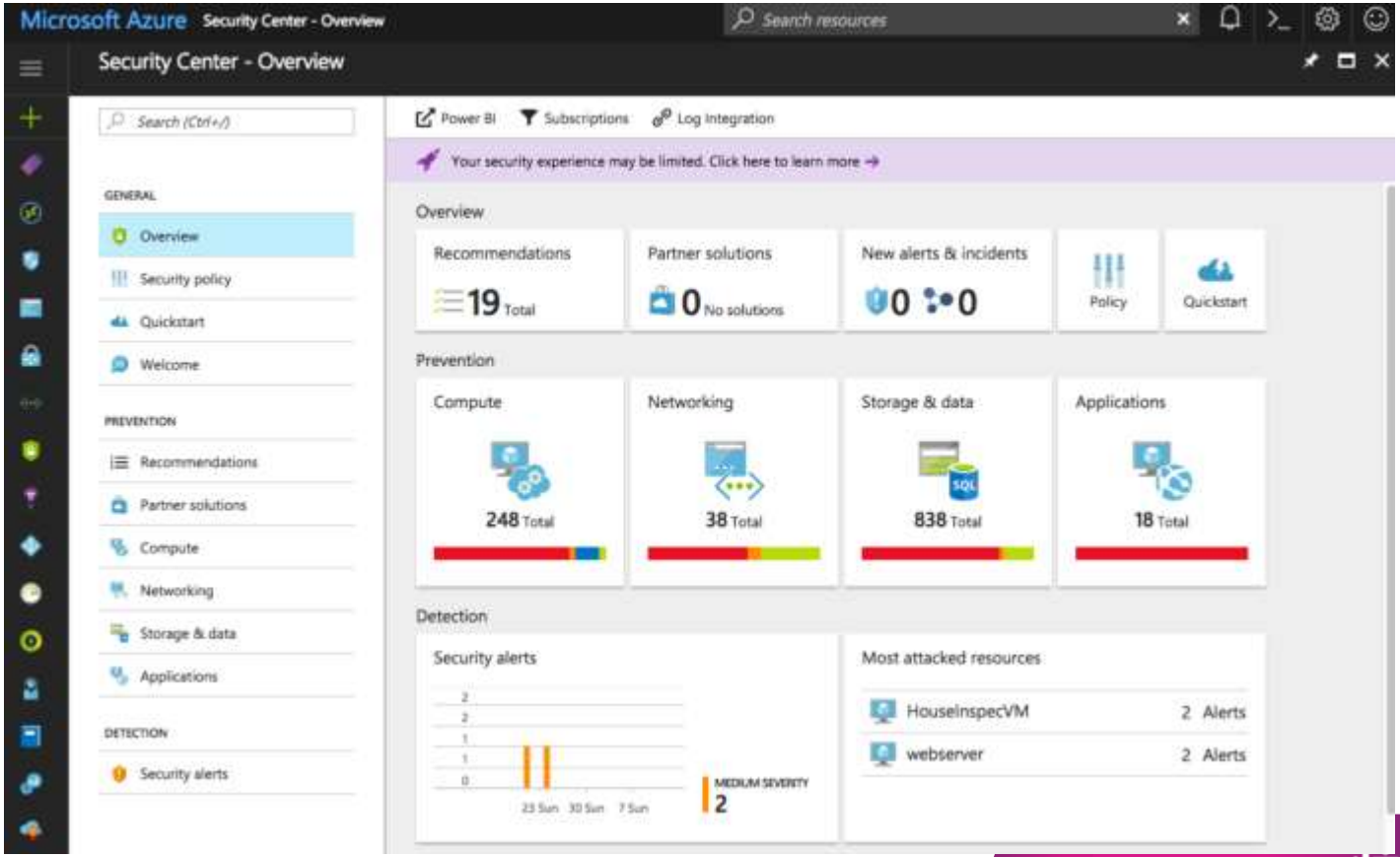
- Aprovisionamiento automático.
  - Cuando el aprovisionamiento automático está habilitado en la directiva de seguridad, Microsoft Monitoring Agent, tanto para Windows como para Linux, se instala en todas las máquinas virtuales de Azure admitidas (ver cuales abajo), y en las nuevas que se vayan desplegando, sin tener que realizar una configuración adicional.
    La ejecución del agente está diseñado para que no sea invasivo y tenga un impacto mínimo sobre el rendimiento de la máquina virtual.
  - Microsoft Monitoring Agent para Windows requiere el uso del puerto TCP 443.
  - Si en algún momento nos interesa deshabilitar la recopilación de datos de un agente, podemos desactivarla en la directiva de seguridad. Hay que tener en cuenta si estamos utilizando el agente para otros servicios por lo que no se desinstalará dicho agente.
- Aprovisionamiento manual.- Instalar directamente el agente.

Para encontrar una lista de máquinas virtuales admitidas, lea las preguntas frecuentes sobre Azure Security Center.

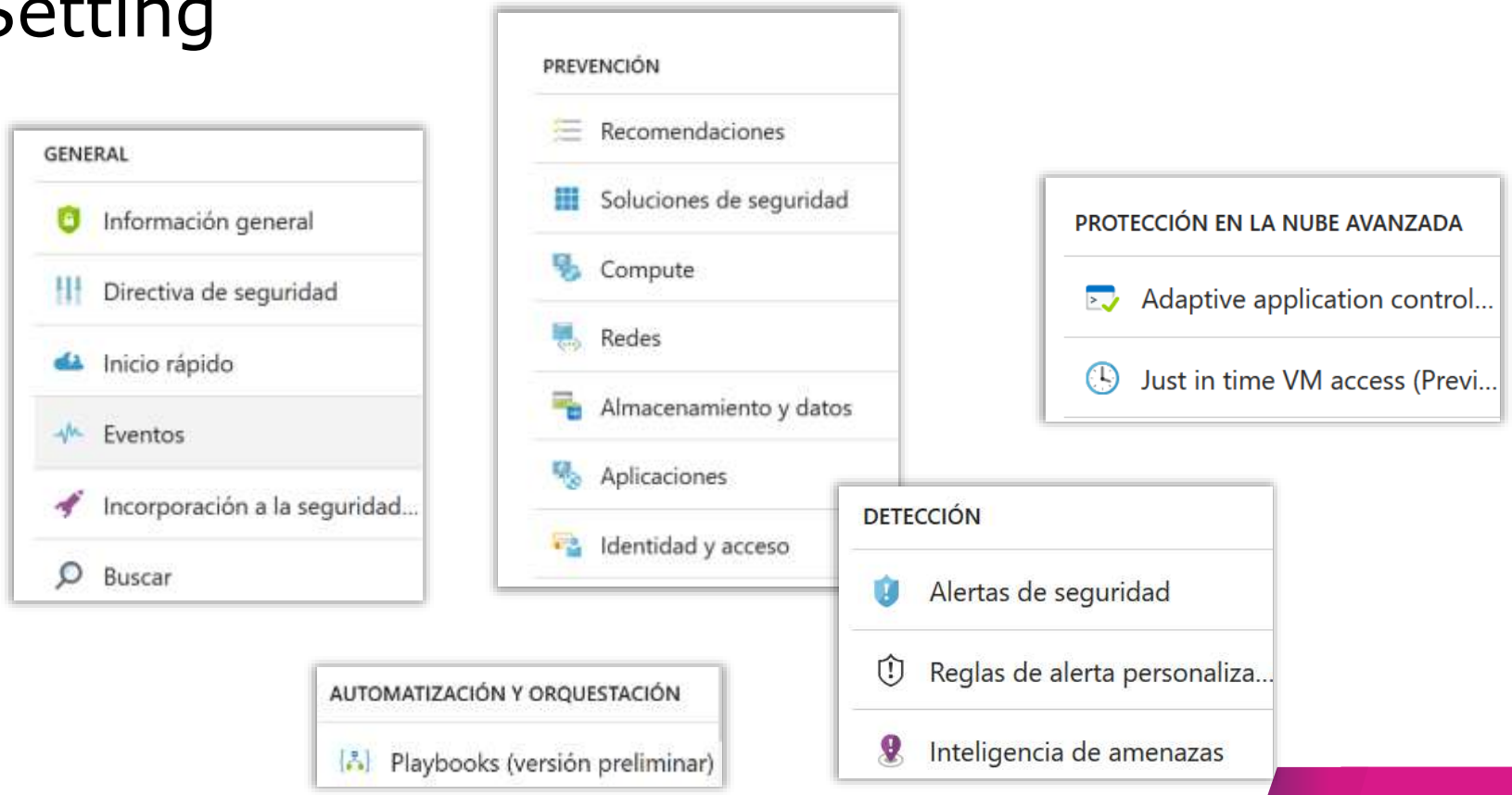
Insight Presentation

Setting

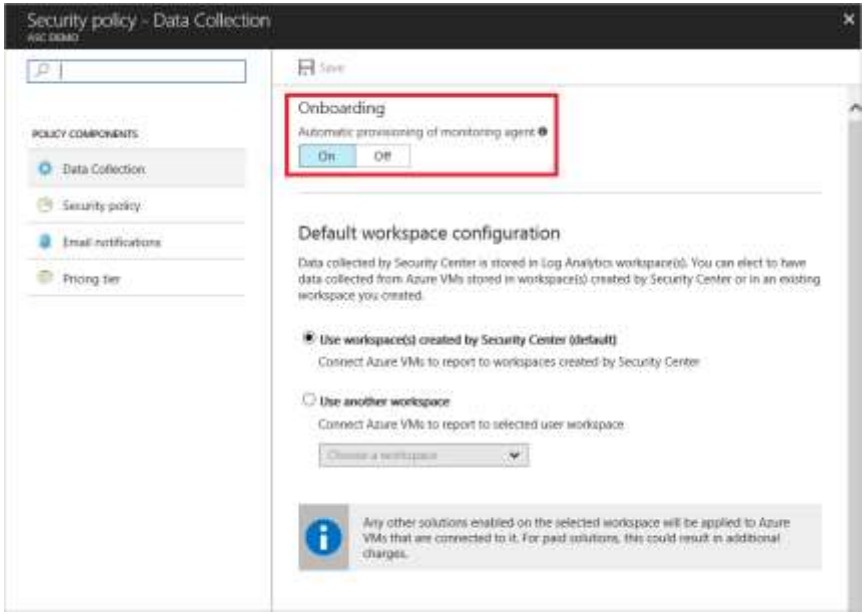
- General
- Prevención
- Protección en la nube Avanzada
- Detección

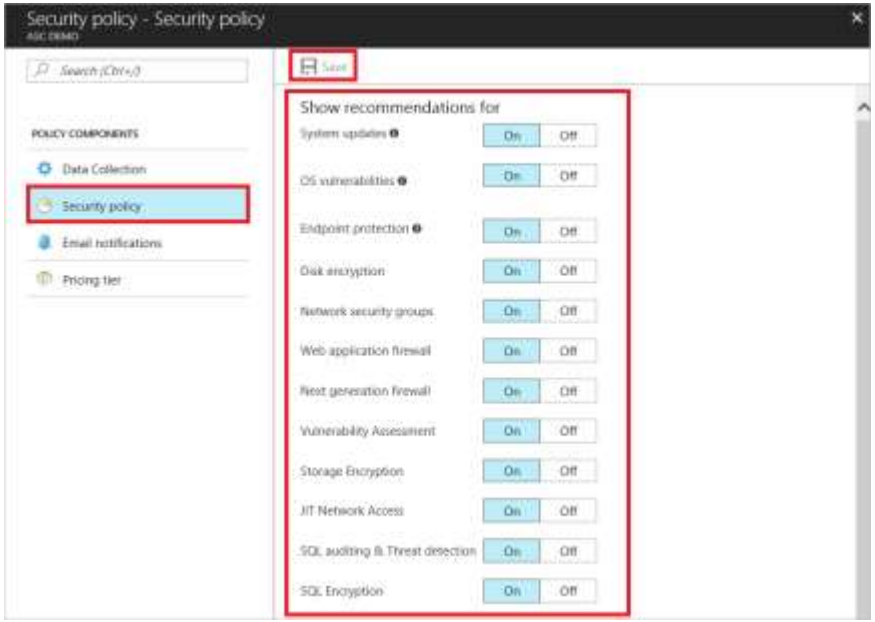


Setting



Directivas de Seguridad

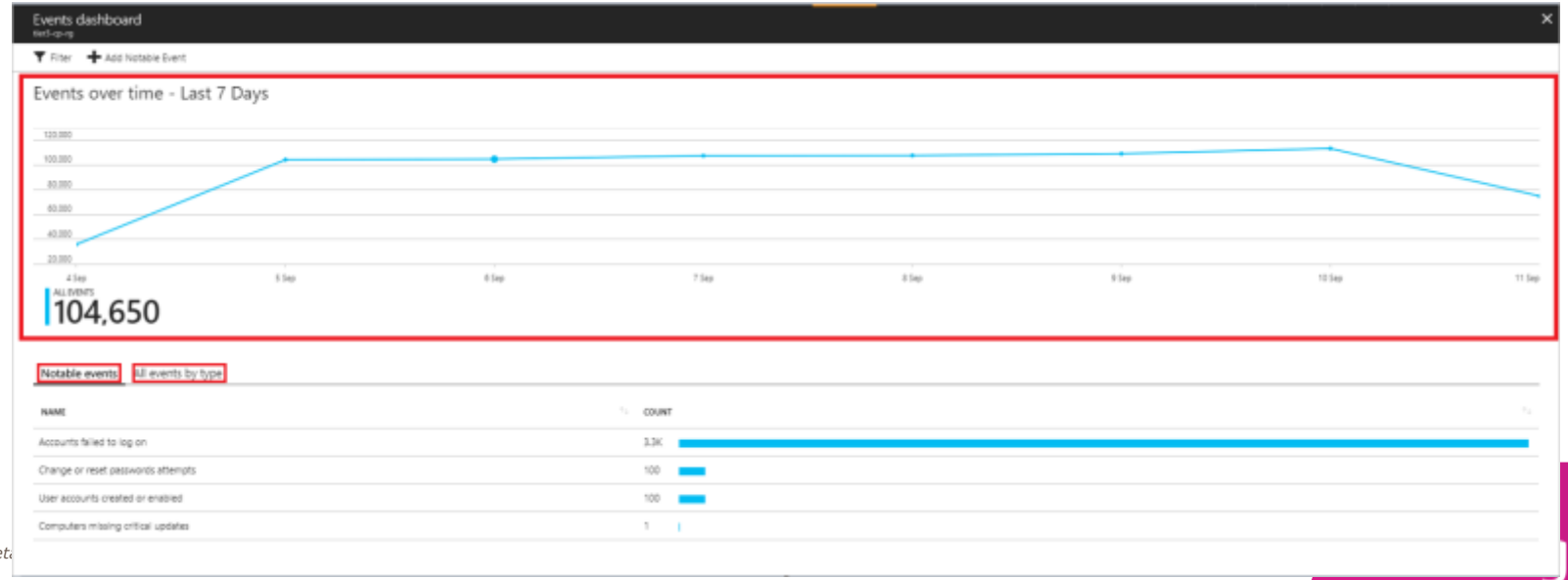




Eventos

Nos permite capturar todos los datos de registros y eventos necesarios para obtener información general sobre seguridad y asi, conseguir un set completo de datos en un formato en el que se podemos realizar búsquedas.

En el panel se muestra una recopilación de eventos a lo largo del tiempo y permite ver rápidamente los eventos importantes que se han producido en nuestro entorno.



Nivel de recopilación de datos

Security Center puede reducir el volumen de eventos manteniendo suficientes eventos para la investigación, la auditoría y la detección de amenazas. Podemos elegir la directiva de filtrado adecuada para nuestras suscripciones y áreas de trabajo (workspaces) entre cuatro conjuntos de eventos que recopilará el agente.

- **Todos los eventos**: Para los clientes que quieren asegurarse de que se recopilan todos los eventos. Este es el valor predeterminado.
- **Común**: Se trata de un conjunto de eventos que satisfacen a la mayoría de los clientes y les permite efectuar una prueba de auditoría completa.
- **Mínimo**: Es un conjunto más pequeño de eventos para los clientes que quieren reducir el volumen de eventos.
- **Ninguno**: Se deshabilita la recopilación de eventos de seguridad de los registros de seguridad y de AppLocker. Para los clientes que elijan esta opción, sus paneles de seguridad solo tendrán registros del Firewall de Windows y evaluaciones preventivas, como el antimalware, la línea base y las actualizaciones.

Nivel de recopilación de datos

Para determinar los eventos que formarán parte de los conjuntos de eventos **Común** y **Mínimo**, Microsoft ha colaborado con los clientes y los estándares del sector para obtener información sobre la frecuencia sin filtrar de cada evento y su uso. En este proceso se han empleado las siguientes directrices:

Mínimo: Asegúrese de que este conjunto abarque solamente los eventos que podrían indicar una brecha correcta y eventos importantes que tengan un volumen muy bajo. Por ejemplo, este conjunto contiene un inicio de sesión de usuario correcto y uno erróneo (identificadores de evento 4624 y 4625), pero no contiene el cierre de sesión, que es importante para la auditoría pero no lo es para la detección y tiene un volumen relativamente alto. La mayor parte del volumen de datos de este conjunto son los eventos de inicio de sesión y el evento de creación de proceso (Id. de evento 4688).

Común: Proporcione una pista de auditoría de usuario completa en este conjunto. Por ejemplo, este conjunto contiene los inicios de sesión y los cierres de sesión de usuario (Id. de evento 4634). Se incluyen acciones de auditoría como cambios en los grupos de seguridad, operaciones de Kerberos en los controladores de dominio de clave y otros eventos que recomiendan las organizaciones del sector.

Los eventos que tienen un volumen muy bajo se han incluido en el conjunto Común, ya que la motivación principal para elegirlo respecto de todos los eventos pasa por reducir el volumen, y no por filtrar eventos específicos.

Nivel de recopilación de datos

Los eventos que tienen un volumen muy bajo se han incluido en el conjunto Común, ya que la motivación principal para elegirlo respecto de todos los eventos pasa por reducir el volumen, y no por filtrar eventos específicos.

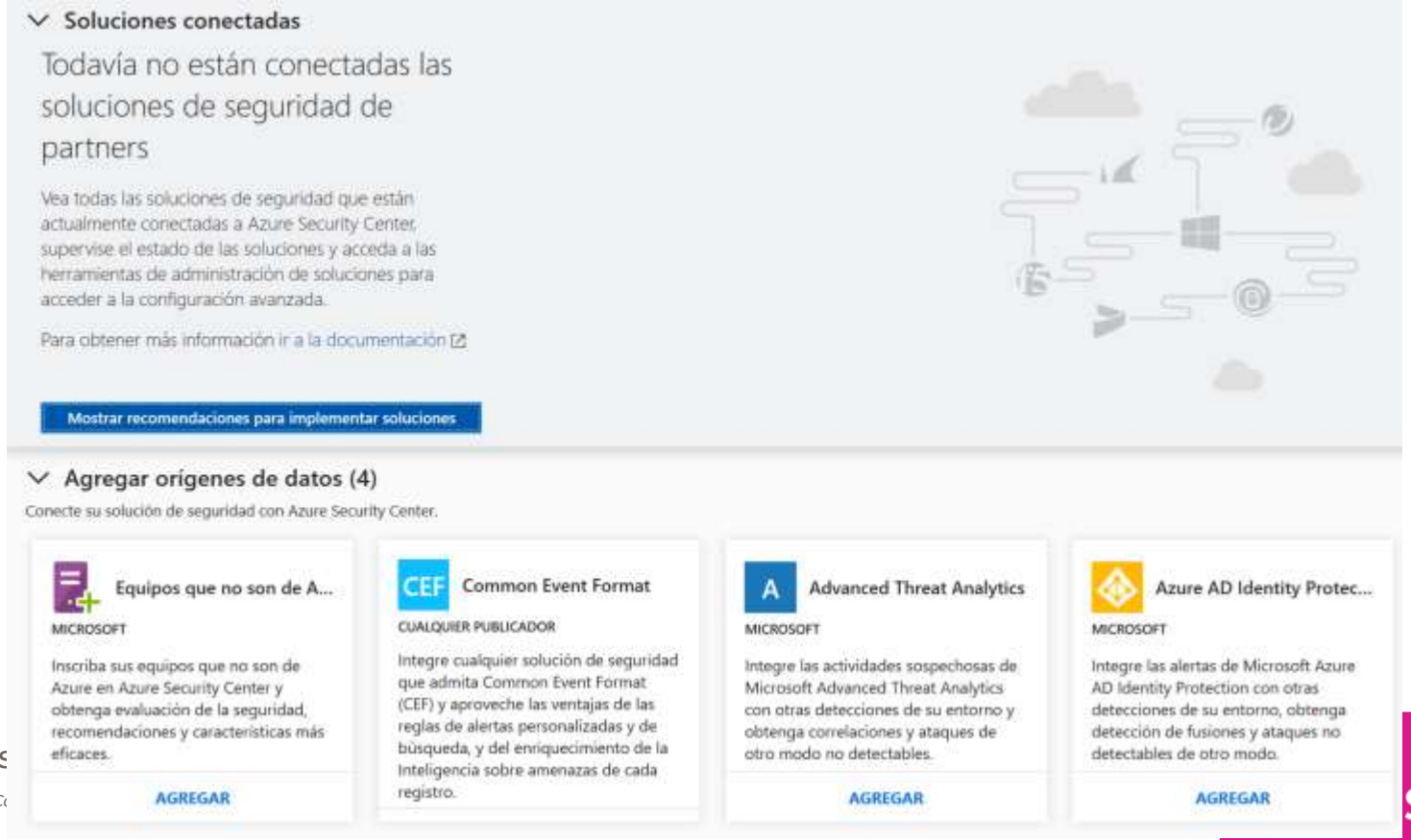
A continuación se muestra un desglose completo de los identificadores de evento de seguridad y de AppLocker para cada conjunto:

Common	All events in minimal plus the following: 299, 300, 324, 340, 403, 404, 410, 411, 412, 413, 431, 500, 501, 1100, 1107, 1108, 4608, 4610, 4611, 4614, 4616, 4622, 4634, 4647, 4648, 4649, 4658, 4661, 4662, 4665, 4666, 4667, 4670, 4673, 4674, 4675, 4689, 4690, 4697, 4704, 4705, 4716, 4717, 4718, 4725, 4726, 4729, 4733, 4738, 4742, 4744, 4745, 4746, 4750, 4751, 4752, 4757, 4760, 4761, 4762, 4764, 4768, 4771, 4774, 4778, 4779, 4781, 4793, 4797, 4798, 4799, 4800, 4801, 4802, 4803, 4826, 4870, 4886, 4887, 4888, 4893,
	4898, 4902, 4904, 4905, 4907, 4931, 4932, 4933, 4985, 5059, 5136, 5137, 5140, 5145, 5632, 6144, 6145, 6272, 6273, 6278, 8222, 26401, 30004
Minimal	1102, 4624, 4625, 4657, 4663, 4688, 4700, 4702, 4719, 4720, 4722, 4723, 4724, 4727, 4728, 4732, 4735, 4737, 4739, 4740, 4754, 4755, 4756, 4767, 4825, 4946, 4948, 4956, 5024, 5033, 8001, 8002

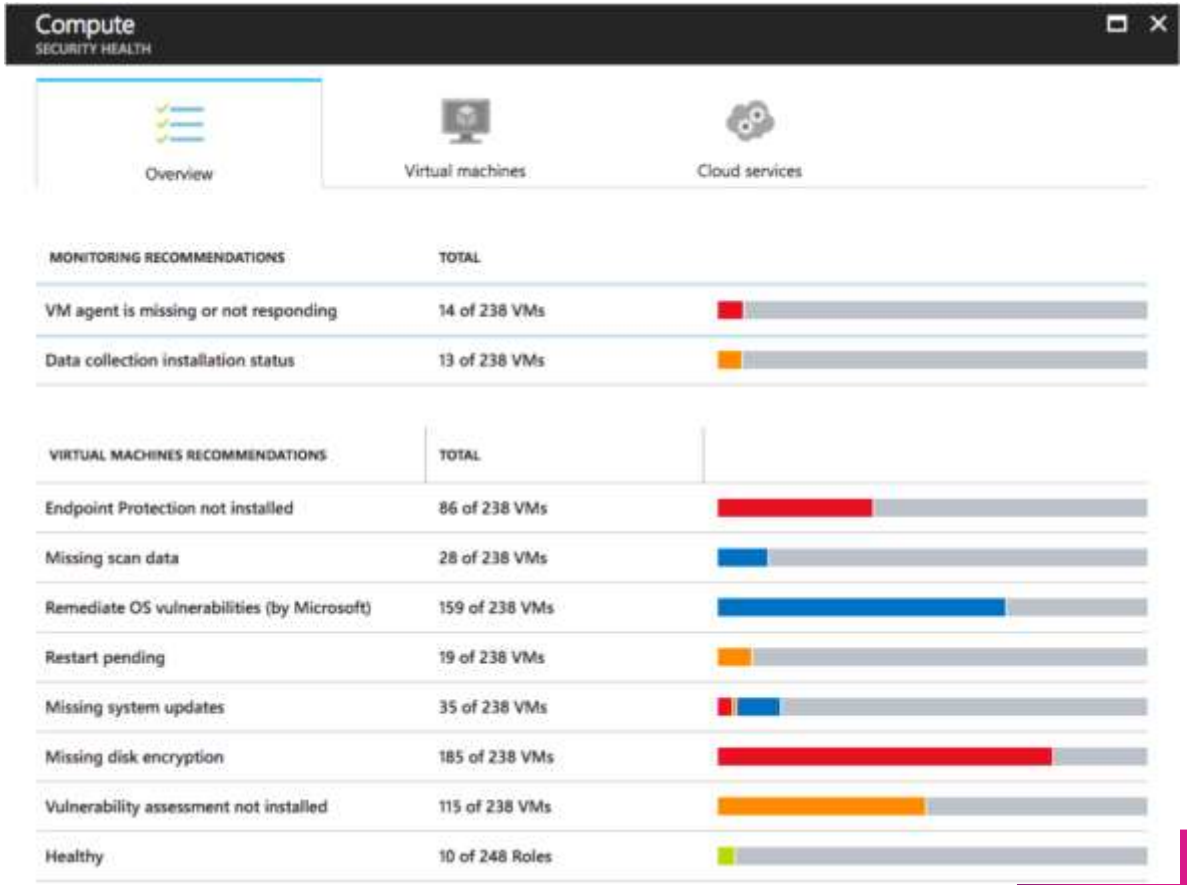
Recomendaciones

DESCRIPCIÓN	RECURSO	ESTADO	GRAVEDAD
Habilitar la seguridad avanzada para las suscripciones	2 suscripciones	Abierto	Alta
Endpoint Protection no está instalado en máquinas virtuales de Azure	3 máquinas virtuales	Abierto	Alta
Habilitar la auditoría y la detección de amenazas en servidores SQL	serversqlprueba	Abierto	Alta
Habilitar la auditoría y la detección de amenazas en bases de datos de SQL	SQLDatabase	Abierto	Alta
Aplicar cifrado de discos	2 máquinas virtuales	Abierto	Alta
Proporcionar detalles de contacto de seguridad	1 suscripciones	Abierto	Media
Habilitar la recopilación de datos de las suscripciones	2 suscripciones	Resuelto	Alta
Agregar un firewall de última generación	Ivan01-ip	Resuelto	Alta
Habilitar los grupos de seguridad de red en subredes	default	Resuelto	Alta
Restringir el acceso a través de un punto de conexión accesible desde Internet	Ivan01	Resuelto	Media
Agregar una solución de evaluación de vulnerabilidad	Ivan01	Resuelto	Media

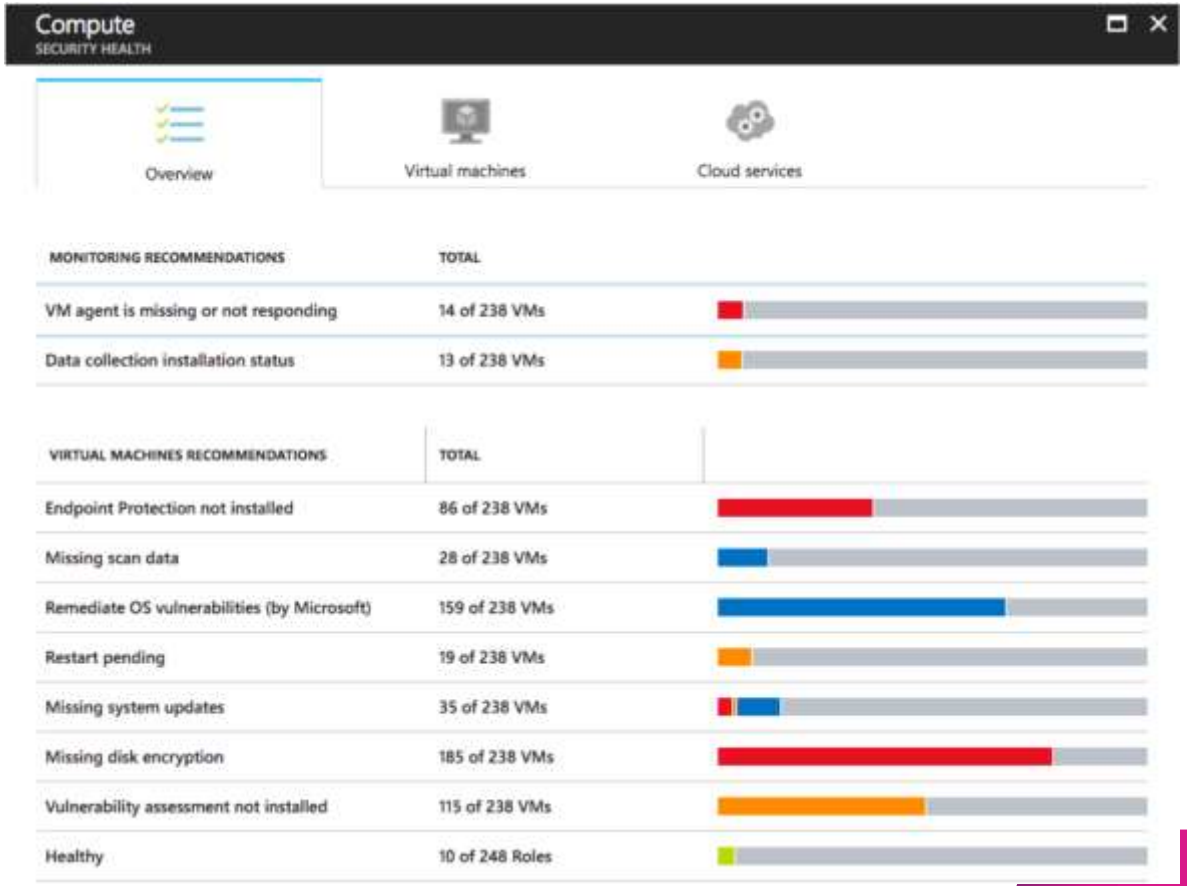
Soluciones de Seguridad.



Compute



Redes



Muchas gracias por asistir

Roberto Tejero
@robtejero