La seguridad de Google Cloud se compone por un equipo de los mejores expertos de la seguridad de la información, la seguridad de aplicaciones, la criptografía y la seguridad de redes, manteniendo los sistemas de defensa, desarrollando procesos de revisión de seguridad, creando una infraestructura segura e implementando las políticas de seguridad.

De esta manera, ejecutan equipos como Project Zero, que es un equipo de investigadores de seguridad enfocado en investigar las vulnerabilidades de cero días.

Ademas, tiene un programa de recompensas por detección de vulnerabilidades, que ofrece recompensas de decenas de miles de dólares por cada vulnerabilidad confirmada.

De esta manera, todos los empleados de Google son capacitados arduamente para formar parte del equipo, y lograr cumplir con los objetivos y el código de conducta.

El diseño de la infraestructura de la seguridad se compone en varias capas.

- La infraestructura de bajo nivel, la implemetnacion de servicios, el almacenamiento de datos, la comunicación en internet y la Seguridad Operativa.

La infraestructura de bajo nivel habla sobre cómo se protegen las instalaciones físicas de los centros de datos, el hardware que se utiliza y la pila de software que se ejecuta en el hardware. El acceso a estos centros está muy controlado, se utiliza identificación biométrica, detección de metales, cámaras, barreras para vehículos y sistemas de detección de intrusiones con láser.

Cada servidor del centro de datos tiene una identidad única, lo que le permitirá autenticar las llamadas a la API, la autenticación mutua del servidor y la encriptación del transporte.

La implementación de servicios, consiste en la política de seguridad de confianza cero, que consiste en que ningún dispositivo o usuario es de confianza de forma predeterminada, aun asi estuviera en la red.

Los datos nunca se agruparán en una o un conjunto de máquinas, sino que estarán en decenas de miles de máquinas homogéneas.

El almacenamiento de datos se maneja a través de la encriptación en reposo, que quiere decir que se utilizan varias capas de encriptación para proteger aquellos datos que se encuentran almacenados. Para lograr esta tarea, se establecen claves, permitiendo que la infraestructura se aisle de amenazas como el firmware de disco malicioso.

Por otro lado, la comunicación segura en internet, que se desarrolla a través de multiples maquinas interconectadas en la LAN y WAN. La infraestructura de internet se da en un espacio de direcciones IP privadas, solo algunas son expuestas al exterior para establecer mas medidas de seguridad, como la protección a los ataques DoS.

De esta manera, vemos que se llevan a cabo muchísimos sistemas de seguridad que van teniendo en cuenta todo tipo de ámbitos. Por otro lado, los servidores llevan a cabo otro tipo de controles de forma automática en el espacio fisicologico.

Preguntas: ¿Cuales son los controles fisicologicos que comentaste?

El endurecimiento del hardware, que reduce las rutas de acceso físico de cada maquina, reduciendo los puertos, y bloqueando rutas de acceso en el nivel de firmware.

Genera alertas cuando los controles físicos a lógicos cuando estos detectan eventos anómalos, y la defensa del sistema, que reconoce un cambio en el entorno físico y responde las amenazas con acciones defensivas.

¿Cómo esto se trataba de una venta para una empresa, Google ofrece alguna facilidad para estas en cuanto a temas de seguridad?

Si, google ofrece diferentes cursos o capacitaciones on-line a través de las cuales se desarrolla de que maneras se pueden establecer los servicios de seguridad de google, con diferentes planes recomendados, como por ejemplo la ruta de aprendizaje de security engineer, la ruta de aprendizaje de DevSecOps y la ruta de aprendizaje de SIEM y SOAR de google.

¿Qué seria SIEM y SOAR?

Estas son herramientas de ciberseguridad indispensables que atienden distintas funciones, SOAR automatiza y coordina la respuesta a incidentes de seguridad, lo que reduce la carga de trabajo a los equipos, y SIEM combina la gestión de información de seguridad y la gestión de eventos en un sistema, analizando datos en para detectar eventos en tiempo real.

El Cloud Bursting se trata de usar de forma temporal un entorno de computación privado para la carga y el aumento de actividad en un modelo de referencia en la nube cuando necesites una capacidad adicional. Esto quiere decir que cuando la capacidad de datos esta al limite en un entorno privado se puede obtener una capacidad adicional en un entorno de google cloud cuando sea necesario. De esta manera, se adapta a los tiempos de alta demanda de un servicio, en los que se podrá hacer uso de esta herramienta. Unicamente se facturará el tiempo de uso de esta capacidad adicional, logrando permitir que el servicio se encuentre activo aunque falte capacidad.

Para implementarlo, se logra ya sea a través de cargas de trabajo interactivas o por lotes. Hay varios sistemas de balanceo como Cloud Load Balancing, que permite determinar este tipo de actividades.

De esta manera este sistema ofrece una serie de ventajas, tales como aprovechar de una forma más óptima los entornos de computación privados, al aprovechar en tiempos de alta demanda el servicio de cloud bursting, y tener en cuenta que el patrón de picos de actividad permite que los recursos de procesamiento no se utilicen en exceso.