Integración con Cloud Security Command Center

Prisma Cloud se integra con Cloud Security Command Center de Google para proveerle visibilidad sobre los riesgos de seguridad y de cumplimiento a través de todo su entorno GCP. Esto significa que sus equipos de seguridad pueden recopilar los datos rápidamente, identificar amenazas y tomar acciones antes de que se produzcan daños o pérdidas comerciales.

Desarrollo de un Mapa de Defensa de Amenazas en la Nube para GCP

Prisma le permite desarrollar un programa de defensa de amenazas en la nube a través de todo su entorno GCP, desde la concepción hasta su plena madurez, con las siguientes capacidades:

- **Garantía de cumplimiento.** El mapeo de configuraciones de recursos en la nube con marcos de cumplimiento (como CIS, GDPR, PCI DSS y HIPAA) puede consumir mucho tiempo. Al utilizar políticas preempaquetadas, Prisma permite el monitoreo continuo, la reparación automática y la generación de informes con un clic; y, a la vez, simplifica el proceso para mantener el cumplimiento.
- **Control de seguridad.** Una visibilidad incompleta y un impreciso control de cambios en los dinámicos entornos informáticos en la nube pública pueden dificultar los procesos de control de la seguridad. Prisma habilita la validación de arquitectura al establecer protecciones de políticas para detectar y reparar automáticamente riesgos a través de las configuraciones de recursos, arquitecturas de redes y actividades de usuarios. Con Prisma, finalmente puede compatibilizar la agilidad de DevOps sin comprometer la seguridad.
- **Habilitación de SOC.** Los equipos de operaciones de seguridad están desbordados de alertas que incluyen poco contexto sobre los problemas, lo que dificulta solucionarlos oportunamente. Prisma permite identificar vulnerabilidades, detectar amenazas, investigar incidentes actuales o pasados, y solucionar problemas a través de todo su entorno GCP en minutos.

Etapa 1: Adoptar	Etapa 2: Expandir	Etapa 3: Escalar
Huella en la Nube: • Decenas de cargas de trabajo • Pocas cuentas en la nube	**Huella en la Nube:** • Cientos de cargas de trabajo • Muchas cuentas en la nube	**Huella en la Nube:** • Múltiples proveedores de nube • Miles de cargas de trabajo • Decenas de cuentas en la nube
Objetivos: • Garantía de cumplimiento • Control de seguridad	**Objetivos:** • Visibilidad central • Detección de amenazas • Gestión de vulnerabilidades **+ Objetivos de la etapa 1**	**Objetivos:** • Autoreparación • Investigación de incidentes **+ Objetivos de la etapa 1**

Figura 1: Modelo de Madurez de Defensa de Amenazas en la Nube

Prisma Cloud Security Suite

Prisma Cloud brinda visibilidad integral, detección de amenazas y rápida respuesta a través de todo su entorno de nube pública, incluso Google Cloud Platform, Amazon Web Services (AWS®) y Microsoft Azure®. Una combinación única de monitoreo continuo, garantía de cumplimiento y analítica de seguridad permite que los equipos de seguridad respondan más rápidamente a las amenazas más críticas al reemplazar las investigaciones manuales por informes, priorización y solución de amenazas automáticos. Con su enfoque basado en API, Prisma brinda una seguridad superior nativa de la nube.

Prisma Cloud es parte de la Security Operating Platform® de Palo Alto Networks y brinda a las organizaciones un enfoque multidimensional para la seguridad en la nube pública ofrecida a través de tecnologías de protección en línea, basadas en API y hosts, que trabajan juntas para reducir las oportunidades de ataque.

Security Operating Platform extiende la protección a toda su red completa, con protección integral sin importar la ubicación. Sin importar si sus aplicaciones se encuentran en sus instalaciones, fueron virtualizadas y necesitan protección en una nube privada como VMware NSX®, Cisco ACI®, KVM o OpenStack®, se extienden a una nube pública o fueron trasladadas a una aplicación SaaS, podemos protegerlas.

Visite nuestro sitio web para conocer más: www.paloaltonetworks.com.