Investigación de Incidentes

Con una profunda comprensión del entorno Azure, Prisma Cloud reduce el tiempo de investigación a segundos. Puede determinar problemas rápidamente, realizar análisis de impacto anterior y posterior, y revisar el historial de cambios a un recurso para una mejor comprensión de la causa raíz de un incidente. Por ejemplo, puede ejecutar una consulta para encontrar todas las bases de datos con comunicación directa en Internet el mes pasado. En el mapa resultante se encontrarán todas estas instancias y se destacarán los recursos potencialmente comprometidos.

Alerta Contextual y Respuesta Adaptativa

Prisma Cloud posibilita que sus equipos puedan responder rápidamente a problemas en base a alertas contextuales. Estas alertas, emitidas a partir de una metodología de puntuación de riesgo con patente en trámite, proveen el contexto de todos los factores de riesgo asociados a un recurso, lo que simplifica la priorización de los problemas más importantes. Usted puede enviar alertas, orquestar las políticas o llevar a cabo reparaciones automáticas. Incluso puede enviar alertas a herramientas como Slack®, Splunk ® y nuestro propio Demisto® para solucionar problemas. En caso de una base de datos riesgosa, Prisma generará una alerta contextual con información sobre los factores de riesgo para habilitar una respuesta automática.

Integración con Azure Security Center

Prisma Cloud se integra con Azure Security Center para proveerle visibilidad centralizada sobre los riesgos de seguridad y de cumplimiento a través de todo su entorno Azure. Con esto, 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 Defensas de Amenazas en la Nube para Microsoft Azure

Prisma Cloud le permite desarrollar un programa de defensa de amenazas en la nube a través de todo su entorno Azure, 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 Azure 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 Amazon Web Services, Microsoft Azure y Google Cloud Platform. 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.