VIAVI Solutions

Folleto

Gestión de la Exposición a Amenazas para Amazon Web Services (AWS)

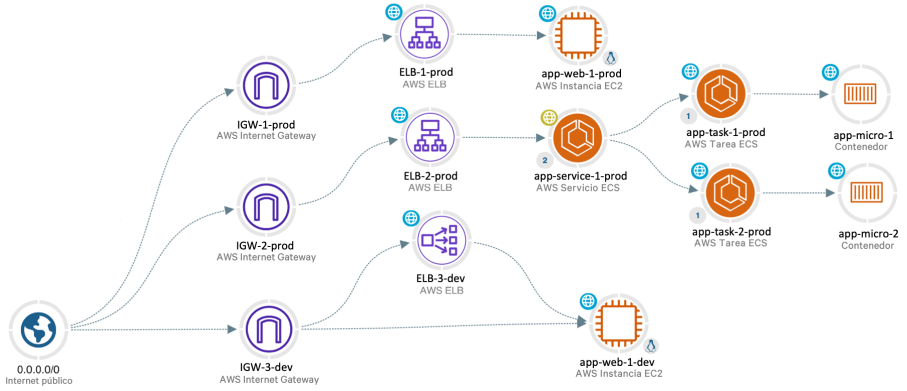
Observer Sentry le permite ver su entorno desde la perspectiva del atacante

El Desafío

En un esfuerzo por mejorar y expandir continuamente la prestación de servicios y aprovechar al máximo los avances tecnológicos, las arquitecturas de prestación de servicios basadas en la nube cambian constantemente. Las presiones comerciales y competitivas obligan a muchas organizaciones a reaccionar con rapidez, a menudo implementando cambios lo más rápido posible. ¿Cuáles son las consecuencias? Identidades de nube demasiado permisivas, aplicaciones de contenedores de terceros con vulnerabilidades de seguridad y activos críticos que quedan expuestos externamente. Estos problemas generalizados se han traducido en un crecimiento radical de los casos de explotación de la nube y de brechas de datos.

Solución

La Solución Observer Sentry de VIAVI (SaaS) proporciona una gestión de la exposición a amenazas, lo que proporciona a los arquitectos de servicios en la nube, de operaciones, de desarrollo o de seguridad, la visibilidad de las amenazas que tanto se necesita en los entornos cambiantes de AWS.



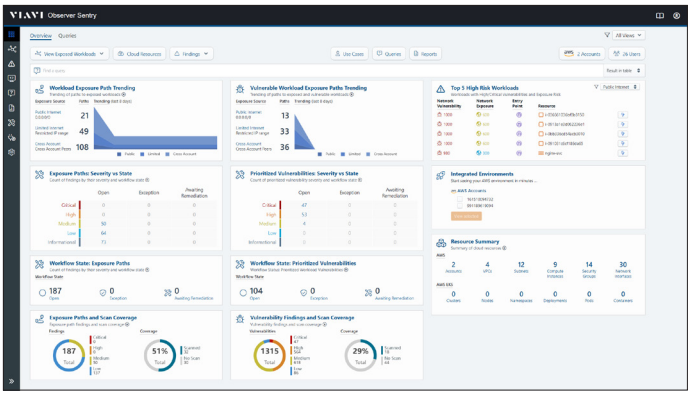
"Los defensores piensan en listas. Los atacantes piensan en gráficos. Mientras esto sea así, los atacantes ganan".
John Lambert, Microsoft Threat Intelligence Center

Al descubrir y combinar rutas de ataque internas con análisis de superficies de ataque externas específicos, Observer Sentry identifica exposiciones de la seguridad, analiza las consecuencias comerciales y contribuye a priorizar operaciones de remediación. Por medio de la integración de AWS, los detalles de la configuración y los datos de tráfico proporcionados, los usuarios pueden ver dos perspectivas de radical importancia: lo que la configuración puede permitir (aquello que es posible) y lo que está ocurriendo en realidad. De esta manera, se pone de manifiesto si los ciberdelincuentes han comprometido los recursos expuestos o si han aprovechado vulnerabilidades conocidas.

Gestión de superficies de ataque y rutas de ataque

Observer Sentry crea un inventario detallado de sus activos basados en la nube y, después, realiza un análisis para determinar su superficie de ataque, su exposición y sus riesgos. Este análisis se puede aplicar también de forma colectiva a agrupaciones lógicas de activos para componer aplicaciones y cargas de trabajo específicas. Estas agrupaciones se pueden rastrear en sistemas de calificación de riesgos y visualizar en mapas de superficies de ataque.

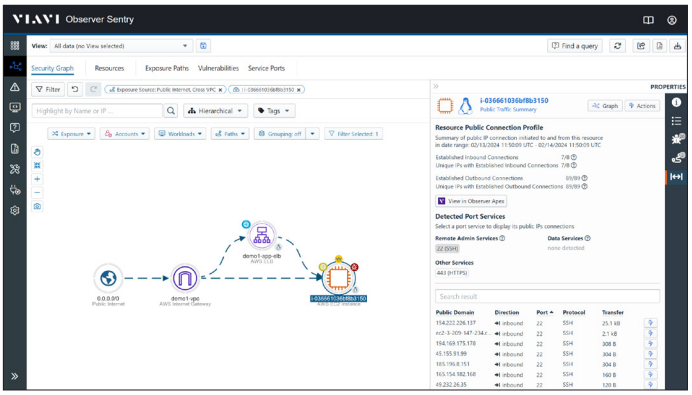
Las rutas de ataque son la peligrosa combinación de exposición, vulnerabilidades de red aprovechables y configuraciones en riesgo que proporcionan rutas con la menor resistencia a recursos de alto valor dentro de su entorno. La gestión de rutas de ataque proporciona un contexto viable para sus problemas más críticos, de modo que sus equipos pueden mejorar su posición de seguridad en la nube de manera proactiva y continuada.



Identifique exposiciones no intencionadas y priorice las cargas de trabajo de alto riesgo solo de un vistazo.

Integración de los datos de tráfico

Cuando se identifican exposiciones no intencionadas o vulnerabilidades sin solucionar, no basta con comprender qué podría pasar o qué podría haber pasado ya: es necesario saber qué ha pasado en realidad. A través de la integración de los datos de tráfico que proporcionan los registros de flujo de VPC de AWS, los usuarios de Sentry obtienen visibilidad en cuanto a los intentos de conexión entrantes y salientes y las conexiones establecidas por puerto y protocolo, junto con el volumen de datos asociado a una conexión. Los usuarios pueden entonces pasar de Observer Sentry a Observer Apex para realizar análisis forenses detallados del tráfico de conversaciones de interés o relacionados con posibles problemas.



Los equipos de seguridad obtienen información necesaria sobre exposiciones de alta prioridad al integrar los detalles del tráfico y el historial de las conversaciones.

Observer Sentry responde a estas preguntas:

¿Cómo ven los atacantes mi entorno de AWS?
¿Dónde hay configuraciones incorrectas?
¿Qué rutas pueden explotar los atacantes?
¿Dónde hay riesgos para mis activos de la nube?
¿Dónde hay configuraciones demasiado permisivas?
¿Cómo debo priorizar la mitigación de riesgos?
¿Se han comprometido recursos expuestos?
¿Se han explotado vulnerabilidades conocidas?

Observabilidad en AWS y Priorización basada en riesgos.

Conéctese a su entorno de AWS, a Elastic Kubernetes Services (EKS) y a los clústeres de Elastic Container Service (ECS) en cuestión de minutos. Observer Sentry escanea continuamente sus entornos de AWS y genera diagramas altamente intuitivos de diversos entornos que le ayudan a identificar rápidamente configuraciones incorrectas, configuraciones demasiado permisivas y exposiciones no intencionadas.

Observer Sentry prioriza los riesgos críticos basándose en el análisis de configuraciones incorrectas, la exposición de la red, vulnerabilidades y otros factores para proporcionar una vista priorizada de los riesgos de su entorno basado en la nube.

Aprenda más: viavisolutions.com/es-es/node/113528

Pruebe el servicio Observer Sentry, sin riesgos, en su entorno. La activación de la cuenta y la configuración inicial requieren menos de 15 minutos.

VIAVI Solutions

Contáctenos +34 91 383 9801
+1 954 688 5660

Para localizar la oficina VIAVI más cercana, por favor visítenos en viavisolutions.es/contactenos

observer-sentry-br-ec-es
30193967 901 0224