Google anunció el miércoles la versión 0.1 Beta de GUAC (Graph for Understanding Artifact Composition) para que los organizadores aseguren sus cadenas de suministro de software.

Con ese fin, la Google pone a disposición el marco de código abierto como una API para que los desarrolladores integren sus propias herramientas y motores de políticas.

GUAC tiene como objetivo agregar metadatos de seguridad de software de distintas fuentes en una base de datos geográfica que mapea las relaciones entre el software, ayudando a las organizaciones a determinar cómo una pieza de software afecta a otra

> *«El gráfico para comprender la composición de artefactos (GUAC) le brinda información organizada y procesable sobre la posición de seguridad de su cadena de suministro de software»,* dice Google en su documentación.

> *«GUAC ingiere metadatos de seguridad de software, como SBOM, y mapea la relación entre el software para que pueda comprender completamente su posición de seguridad de software».*

En otras palabras, está diseñado para reunir documentos de lista de materiales de software (SBOM), atestaciones de SLSA, fuentes de vulnerabilidad OSV, información de deps.dev y metadatos privados internos de una empresa para ayudar a crear una mejor imagen de perfil de riesgo y visualizar las relaciones entre artefactos, paquetes y repositorios.

Con una configuración de este tipo, el objetivo es hacer frente a ataques de cadena de suministro de alto perfil, generar un plan de parches y responder rápidamente a los compromisos de seguridad.

> *«Por ejemplo, GUAC se puede utilizar para certificar que un constructor está*

> *comprometido (por ejemplo, a través de la fuga de credenciales o la ingestión de malware) y después consultar los artefactos afectados»,* dijo Google.

> *«Esto permite que el [director de seguridad de la información] cree fácilmente una política para prohibir el uso de cualquier software dentro del radio de la explosión».*