Estudio de caso

MITRE

La tecnología de grafos permite conocer el estado de la ciberseguridad de modo más adaptable, flexible e integral

INDUSTRIA
Ciberseguridad

CASO DE USO
Operaciones de red y TI

OBJETIVO
Crear una herramienta de defensa cibernética que consolide los datos en una visión global

RETO
Los investigadores tenían datos, pero no conocían las relaciones entre ellos y eso dificultaba el análisis del entorno de seguridad

SOLUCIÓN
Usar la tecnología de grafos para conectar datos entre sí, detectar vulnerabilidades, analizar redes y visualizarlo todo

RESULTADOS
- Disponibilidad de capacidades integrales y escalables para visualización y análisis al servicio de organismos gubernamentales
- Visión del entorno de ciberseguridad de los organismos, incluidas las conexiones entre datos que antes se veían aislados
- Aprovechamiento de herramientas, fuentes de datos y normas de seguridad existentes en un entorno centrado en las relaciones entre datos previamente aislados

Los investigadores de MITRE se enfrentaban a innumerables datos de ciberseguridad cuyas relaciones no podían ver, lo que dificultaba la identificación de vulnerabilidades y la ejecución de análisis avanzados. Con Neo4j, MITRE desarrolló CyGraph, una herramienta que consolida los datos (y sus conexiones) en una visión general continua que facilita a los organismos gubernamentales la toma de decisiones y el conocimiento de la situación.

La organización

The MITRE Corporation es una organización estadounidense, con financiación federal y sin ánimo de lucro, que gestiona siete laboratorios nacionales de investigación y desarrollo (entre ellos el Centro de Seguridad Nacional) encargados de abordar cuestiones de ciberseguridad. Fundada en 1958, MITRE trabaja en campos tan diversos como la defensa nacional, la energía, la aviación, la sanidad y la ciberseguridad, con más de 8000 personas empleadas en proyectos de colaboración pública-privada y en un programa de investigación independiente.

El reto

El cambio constante en los entornos de red y su impacto en la seguridad de las entidades gubernamentales del gobierno de los Estados Unidos. Las alertas de intrusión, las advertencias sobre virus e incluso eventos aparentemente inocuos (p. ej. inicios de sesión, conexiones de servicio y acceso a archivos compartidos) podrían estar asociados a actividad malintencionada.

Los investigadores de la ciberseguridad en MITRE no podían limitarse a hacer evaluaciones básicas de la situación de seguridad y la respuesta ante ataques. Era preciso que combinaran datos aislados para crear un nivel superior de información sobre las vulnerabilidades ante posibles ataques a una red y el grado de preparación para afrontar los ataques.

Eso implicaba examinar los incidentes pero también las relaciones entre ellos.

"El problema no es la falta de información, sino la capacidad para recopilar datos dispares con los que crear una visión analítica general que permita conocer la situación, tomar las medidas pertinentes y estar siempre listos para reaccionar", explicaba Steven Noel, ingeniero jefe de ciberseguridad de MITRE.

Steven Noel y su equipo también tenían dificultades para comprender a fondo entornos de seguridad concretos y determinar todas las vulnerabilidades constatadas. Estos objetivos exigían una arquitectura flexible que acomodara análisis avanzados, consultas ad hoc y visualización de grafos, algo de lo que carecían en aquellos momentos.

Para superar esos retos, el equipo de MITRE empezó por crear una herramienta de modelo de grafos preliminares llamada Cauldron. El problema era que esa herramienta no tenía una base de datos subyacente por lo que, al aumentar la envergadura de las consultas de datos conectadas, Cauldron no cumplía el propósito perseguido. Y el equipo de MITRE no tenía tiempo para codificar todas las consultas posibles.

Estudio de caso

"La amplia base de conocimientos de CyGraph cuenta una historia mucho más completa que la de los grafos de ataque básicos o los modelos de dependencias. Incluye relaciones potenciales de patrones de ataque que llenan los vacíos entre las vulnerabilidades conocidas y los indicadores de amenazas".

–Steven Noel, ingeniero jefe de ciberseguridad de MITRE

La solución

Cuando Steven Noel y su equipo descubrieron la base de datos de grafos de Neo4j, aplicaron lo aprendido con la experiencia de Cauldron para desarrollar CyGraph, una herramienta que transforma en conocimientos la información de ciberseguridad.

CyGraph (basada en el modelo de grafos de propiedades implementado en Neo4j) recopila datos y eventos aislados en una visión general continua que facilita la toma de decisiones y el conocimiento de la situación. Según Noel, "en la arquitectura de CyGraph, el esquema del modelo es libre de evolucionar con las fuentes de datos disponibles y los análisis deseados, en lugar de quedar fijado en el momento en que se diseña".

De este modo, CyGraph evoluciona dinámicamente y proporciona contexto para reaccionar adecuadamente a los ataques y proteger los activos más importantes de una red. También incorpora elementos relacionados con ellos, demostrando que los objetivos, las tareas y la información dependen de otros activos cibernéticos.

En particular, su base de conocimientos proporciona un marco bien equipado para explorar toda la pila de entidades y relaciones relevantes para que una organización esté lista para eventualidades.

Usando la tecnología de grafos, CyGraph puede priorizar vulnerabilidades de activos importantes. Al producirse un ataque, correlaciona las alertas de intrusión con las vías de vulnerabilidad conocidas y sugiere medidas. En los exámenes posteriores a un ataque, identifica vías vulnerables que requieren una inspección más exhaustiva.

Los resultados

Actualmente CyGraph proporciona servicios con capacidades analíticas y visuales especializadas (entre ellas dinámica, estratificación, agrupación/filtrado y vistas jerárquicas de grafos) que son más escalables, flexibles y completas.

"La amplia base de conocimientos de CyGraph cuenta una historia mucho más completa que la de los grafos de ataque básicos o los modelos de dependencias", afirma Noel y añade que "incluye relaciones potenciales de patrones de ataque que llenan los vacíos entre las vulnerabilidades conocidas y los indicadores de amenazas".

Una característica clave del diseño de CyGraph es su capacidad para aprovechar las herramientas y fuentes de datos existentes con el fin de rellenar su base de conocimientos. Por ejemplo, CyGraph utiliza el análisis de vulnerabilidades topológicas y las herramienta de MITRE Cyber Command System y Crown Jewels Analysis. Y hace uso de diversos estándares de seguridad, entre ellos Common Vulnerabilidades and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Weaknesses Enumeration (CWE) y Common Platform Enumeration (CPE).

Otra característica destacable es su capacidad de visualizar patrones imprevisibles, lo que permite a los usuarios obtener resultados analíticos e interpretar su entorno.

CyGraph se utiliza en diversas entidades gubernamentales. Los casos de uso incluyen la detección de actividad maliciosa en una red, el modelado y la simulación de ciberataques, el seguimiento de transacciones de Bitcoin y la navegación a través de CAPEC, una compleja taxonomía para la enumeración y clasificación de patrones de ataque comunes. De ese modo, "CyGraph proporciona una visión del impacto que las actividades cibernéticas en una organización", concluye Noel.

¿Tiene preguntas sobre Neo4j?

Contacte con nosotros en todo el mundo:
info@neo4j.com
neo4j.com/contact-us