Étude de cas

MITRE

La technologie des graphes renforce la perception de situation en matière de cybersécurité qui est plus évolutive, flexible et complète

SECTEUR
Cybersécurité

CAS D'USAGE
Opérations IT & réseaux

OBJECTIF
Créer un outil de lutte cybernétique qui consolide des données isolées dans une vue d'ensemble

DÉFI
Beaucoup de données Individuelles et une absence de relations entre les incidents rendait difficile l'analyse de l'environnement de sécurité.

SOLUTION
Utiliser la technologie des graphes pour construire un outil qui connecte les points de données, indique les vulnérabilités, analyse les réseaux et visualise tout ce qui précède.

RÉSULTATS
- Offrir aux organisations gouvernementales des capacités d'analyse et de visualisation de plus en plus évolutives et complètes.
- Permettre aux organisations d'obtenir une vue d'ensemble de leur environnement de cybersécurité.
- Tirer profit des outils existants, des sources de données et des standards de sécurité.

Les chercheurs de MITRE ont fait face à un afflux de données sur la cybersécurité sans visibilité sur les relations entre elles et rendant difficile la détection de vulnérabilités et l'exécution d'analyses avancées. Avec Neo4j, MITRE a développé CyGraph, un outil qui consolide des données et leurs connexions en une vue d'ensemble pour l'aide à la décision et l'analyse de situation ; outil destiné aux organismes gouvernementaux.

L'organisation

La société MITRE est une entreprise à but non lucratif, financée par le gouvernement fédéral américain. Elle gère sept laboratoires nationaux de recherche et de développement aux États-Unis, notamment le Centre de Sécurité Nationale, pour répondre aux questions de cybersécurité. Fondée en 1958, MITRE travaille sur des projets dans divers domaines, tels que la défense nationale, l'énergie, l'aviation, les soins de santé et la cybersécurité avec plus de 8 000 employés dans le cadre de ses partenariats public-privé et de son programme de recherche indépendant.

Le défi

Les environnements de réseau changent constamment ce qui impacte la gestion de la sécurité des organismes gouvernementaux des États-Unis. Les alertes d'intrusion, les avertissements antivirus et même des événements en apparence bénins, comme les ouvertures de session, les connexions et l'accès aux partages de fichiers sont tout autant de risques potentiels.

Les chercheurs en cybersécurité chez MITRE avaient besoin d'aller plus loin que les évaluations rudimentaires des dispositifs de sécurité et de réaction aux attaques existants. Pour ce faire, il a fallu consolider des données isolées en une vue compréhensive des vulnérabilités à l'échelle du réseau.

« Le problème n'est pas le manque d'information, mais plutôt la capacité à rassembler des éléments d'information disparates dans une vue analytique globale permettant l'analyse de situations, la mise en place de plans d'action optimaux et le maintien de la préparation aux missions, » a déclaré Steven Noel, ingénieur principal en cybersécurité chez MITRE.

Noel et son équipe ont également eu des difficultés à bien comprendre un environnement de sécurité donné et identifier toutes les vulnérabilités connues. Plus particulièrement, ces objectifs ont nécessité une architecture flexible qui héberge les analyses avancées, les requêtes ad hoc et la visualisation de graphes, tout ce dont ils manquaient jusque-là.

Pour relever ces défis, l'équipe MITRE a commencé à construire un outil de modélisation des graphes préliminaire appelé Cauldron. Celui-ci n'étant pas construit sur une base de données, il n'était donc pas performant or l'équipe MITRE n'avait pas le temps de coder toutes les requêtes au vu du volume.

La solution

Lorsque Noel et son équipe ont découvert la base de données de graphes Neo4j, ils ont utilisé les leçons apprises sur Cauldron pour développer et lancer CyGraph, un outil qui transforme les informations de cybersécurité en connaissance.

Étude de cas

« La base de connaissances étendue de CyGraph raconte une histoire bien plus complète que celle de simples graphes d'attaque ou de modèles de dépendance de la mission, » a assuré Noel.
« Elle comprend des schémas de relations possibles entre les attaques qui comblent les écarts entre les vulnérabilités connues et les indicateurs de menace. »

– Steven Noel,
Ingénieur principal en cybersécurité chez MITRE

CyGraph, basé sur un modèle de graphes de propriétés flexible et mis en œuvre dans Neo4j, rassemble des données et des événements isolés dans une vue d'ensemble pour l'aide à la décision et l'analyse de situation.

« Dans l'architecture CyGraph, le modèle est libre d'évoluer avec les sources de données disponibles et les analyses souhaitées, plutôt que d'être figé à des moments prédéfinis, » a affirmé Noel.

De cette manière, l'évolution dynamique de CyGraph fournit un contexte permettant de réagir de façon appropriée aux attaques et de protéger les actifs de réseaux essentiels à la mission. Il intègre également les dépendances de la mission, indiquant ainsi le rapport entre les objectifs, les tâches, les informations et d'autres actifs cybernétiques.

Avec la technologie des graphes, CyGraph est désormais capable de hiérarchiser les vulnérabilités exposées dans un contexte d'actifs essentiels à la mission. Face aux attaques réelles, il met en corrélation les alertes d'intrusion et les accès vulnérables connus, puis suggère les meilleurs plans d'action. Lors des analyses suivant l'attaque, il indique les accès vulnérables méritant une inspection plus approfondie.

Les résultats

CyGraph fourni actuellement des services avec des capacités analytiques et visuelles spécialisées, notamment des dynamiques de graphes, des superpositions, des groupes/filtres et des vues hiérarchiques plus évolutives, flexibles et complètes.

« La base de connaissances étendue de CyGraph raconte une histoire bien plus complète que celle de simples graphes d'attaque ou de modèles de dépendance de la mission, » a assuré Noel. « Elle comprend des schémas de relations possibles entre les attaques qui comblent les écarts entre les vulnérabilités connues et les indicateurs de menace. »

Une caractéristique de conception clé de CyGraph est sa capacité à tirer parti des outils et des sources de données existants pour alimenter sa base de connaissances.

Par exemple, CyGraph a depuis tiré parti de l'analyse de vulnérabilité topologique du gouvernement, ainsi que de l'outil de MITRE Cyber Command System – permettant d'évaluer les répercussions de la mission ou encore de Crown Jewels Analysis - un processus permettant d'identifier les actifs cybernétiques les plus essentiels à la mission. Il tire également profit des différents standards de sécurité, tels que Common Vulnerabilities and Exposures (CVE), un dictionnaire d'informations publiques relatives aux vulnérabilités de sécurité informatique ; Common Vulnerability Scoring System (CVSS), un système d'évaluation standardisé de la criticité des vulnérabilités ; Common Weaknesses Enumeration (CWE), une liste des vulnérabilités que l'on peut rencontrer dans les logiciels et Common Platform Enumeration (CPE), un schéma de nomenclature structuré pour les systèmes informatiques, les plateformes et les packages.

Une autre caractéristique importante est sa capacité à visualiser des comportements imprévisibles, ce qui permet aux utilisateurs d'obtenir un résultat analytique et de comprendre la sémantique de leur environnement.

Aujourd'hui, CyGraph est utilisé dans de nombreuses organisations gouvernementales pour les aider à réaliser leur mission. Les cas d'usage comprennent la détection d'activités de réseau malveillantes, la modélisation et la simulation d'attaques cybernétiques, le suivi de transactions Bitcoin et la navigation dans CAPEC, une taxonomie pour la classification et l'énumération de comportements d'attaques courants.

De cette façon, « CyGraph donne une idée de l'impact des cyberactivités sur la mission, » a conclu Noel.

Des questions sur Neo4j ?

Contactez-nous :
info@neo4j.com
neo4j.com/contact-us