Case Study

MITRE

Graph Technology Powers Cybersecurity Situational Awareness That's More Scalable, Flexible & Comprehensive

INDUSTRY
Cybersecurity

USE CASE
Network & IT Operations

GOAL
Create a cyber warfare tool that consolidates data into a comprehensive picture

CHALLENGE
Researchers had data, but lacked relationships, making it difficult to analyze the security environment

SOLUTION
Used graph technology to connect data points, show vulnerabilities, analyze networks and visualize all of the above

RESULTS
- Provided government agencies with scalable, comprehensive analytic and visualization capabilities
- Allowed agencies to capture a picture of their cybersecurity environment that connects previously isolated data points
- Leveraged existing tools, data sources and security standardsenvironment that focuses on relationships between previously isolated data points

MITRE's researchers faced an influx of cybersecurity data without visibility into its relationships, making it difficult to map vulnerabilities and execute advanced analytics. With Neo4j, MITRE developed CyGraph, a tool that consolidates data – and its connections – into an ongoing overall picture for decision support and situational awareness for government agencies.

The Organization

The MITRE Corporation is a federally-funded, not-for-profit company that manages seven national research and development laboratories around the United States – including the Center for National Security – to address issues of cybersecurity. Founded in 1958, MITRE works on projects in fields as diverse as national defense, energy, aviation, healthcare and cybersecurity, among others, with over 8,000 employees in both its public-private partnerships and its independent research program.

The Challenge

Network environments constantly change, impacting the security posture of U.S. government agencies. Intrusion alerts, anti-virus warnings and even outwardly benign events like logins, service connections and file share access are all potentially associated with adversary activity.

Cybersecurity researchers at MITRE needed to go beyond rudimentary assessments of security posture and attack response. Doing so required merging isolated data into higher-level knowledge of network-wide attack vulnerabilities and mission readiness.

This involved not only looking at incidents themselves, but also at the relationships between them.

"The problem is not lack of information, but rather the ability to assemble disparate pieces of information into an overall analytic picture for situational awareness, optimal courses of action and maintaining mission readiness," said Steven Noel, Principal Cybersecurity Engineer at MITRE.

Noel and his team also struggled with fully comprehending a given security environment and mapping all known vulnerabilities. Specifically, these goals demanded a flexible architecture that accommodated advanced analytics, ad hoc queries and graph visualization, all of which they then lacked.

To overcome these challenges, the MITRE team started by constructing a preliminary graph model tool called Cauldron. However, Cauldron wasn't built on a database. So, as connected-data queries became increasingly extensive, Cauldron wasn't performant, and the MITRE team didn't have time to code every possible query.

Case Study

"CyGraph's comprehensive knowledge base tells a much more complete story than that of basic attack graphs or mission dependency models. [It] includes potential attack-pattern relationships that fill in gaps between known vulnerabilities and threat indicators."

–Steven Noel,
Principal Cybersecurity Engineer,
MITRE

The Solution

When Noel and his team discovered the Neo4j graph database, they used their lessons learned from Cauldron to develop CyGraph, a tool that transforms cybersecurity information into knowledge.

CyGraph – which is based on the property graph model implemented in Neo4j – brings together isolated data and events into an ongoing big picture for decision support and situational awareness. "In the CyGraph architecture, the model schema is free to evolve with the available data sources and desired analytics, rather than being fixed at design time," Noel said.

In this way, the dynamically evolving CyGraph provides context for reacting appropriately to attacks and protecting mission-critical network assets. It also incorporates mission dependencies, showing how objectives, tasks and information all depend on other cyber assets.

Particularly, its knowledge base provides a rich framework for exploring the full stack of entities and relationships relevant to an agency's mission readiness.

With graph technology, CyGraph is able to prioritize exposed vulnerabilities in mission-critical assets. In the face of attacks, it correlates intrusion alerts to known vulnerability paths and suggests courses of action. For post-attack forensics, it shows vulnerable paths that warrant deeper inspection.

The Results

CyGraph currently provides services with specialized analytic and visual capabilities – including graph dynamics, layering, grouping/filtering and hierarchical views – that are more scalable, flexible and comprehensive.

"CyGraph's comprehensive knowledge base tells a much more complete story than that of basic attack graphs or mission dependency models," Noel said. "[It] includes potential attack-pattern relationships that fill in gaps between known vulnerabilities and threat indicators."

A key CyGraph design feature is its ability to leverage existing tools and data sources to populate its knowledge base. For example, CyGraph uses Topological Vulnerability Analysis, as well as MITRE's Cyber Command System and Crown Jewels Analysis. It leverages various security standards such as Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Weaknesses Enumeration (CWE) and Common Platform Enumeration (CPE).

Another significant feature is its ability to visualize unpredictable patterns, which allows users to obtain analytic results and comprehend the semantics of their environment.

CyGraph is used by multiple government agencies to help them achieve their mission. Use cases include detecting malicious network activity, modeling and simulation of cyberattacks, tracking Bitcoin transactions and navigating through CAPEC, a taxonomy for common attack pattern enumeration and classification that is laborious to traverse. In these ways, "CyGraph provides insight into the mission impact of cyber activities," Noel concluded.

Questions about Neo4j?

Contact us across the globe:
info@neo4j.com
neo4j.com/contact-us