Graphing M365

Description

Microsoft 365 (M365) is a complex system that serves multiple needs from end user productivity, customer facilitation, and security. Administrators who need to keep track of the nested layers within M365 lack native tools that reduce the complexity into a comprehendible format. Leveraging the theory of graph database systems, it is possible to reverse engineer the rat's nest and create purpose-built visibility into a M365 tenant and ensure configurations align with intentions.

Objective

Attendees will learn to create customized graph solutions for threat hunting inside Microsoft 365.

Target Audience

Ideal candidates are responsible for M365 administration and security on a regular basis and have basic knowledge in programming, databases, and security principles. Threat hunting teams and security researchers may also find the training useful.

Hardware Required

All attendees should have access to a modern desktop operating system as an administrator. Attendees should stand up a sandbox developer account for Microsoft 365 in advance.

Prerequisite Knowledge

· Programmatic access to Microsoft 365 through PowerShell and Graph API

· Familiarity with M365 security controls

Duration

6 hours, split evenly between two days

Level

Advanced

Course Agenda

Lecture One – Graph Databases what, why, and when.

Graph databases are not a new concept, but their popularity in security applications has seen significant rise in recent years. These powerful data systems help organizations create a mathematical model of their security posture across product stacks and process streams to identify threats to the organization. In this lecture, we will focus on understanding the core concepts of database theories, when you would what to use them, and why.

Lab One – Installing a Graph Database

This lab will focus on the installation of the Neo4j desktop edition. This is a great tool for starting your journey with property graph databases, visualization, and the Cypher query language.

Lecture Two – Guiding Principles for DB Design

With a graph database installed, the initial urge is to start throwing data and see what sticks. This works and we will show key rules that will help streamline your process in the long term. We break down nodes vs edges and how to approach their design to avoid data conflicts down the road.

Lab Two – Implement the Principles

Students will break down Microsoft 365 data structures into distinct edges and nodes and document them.

Lecture Three – Cyphering through the Data

With the theoretical out of the way, students will learn more about the key query commands for adding, removing, selecting, and displaying data within Neo4j.

Lab Three – Ingest data from Lab Two

Using the commands provided in the lecture, build out the database with data identified in Lecture Two.

End of Day 1

Lecture Four – Automating Data Gathering

Now that we have manually designed, modeled, and injected data into the DB, it is time to hand over work to the machines. This lecture covers the highlights of the Analyzing Microsoft 365 with PowerShell Course to refresh and update as appropriate. The focus will be on planning out data collection and breakdown in the script itself.

Lab Four – Unleash the Machines

Building on the models that students generated on day one, create a script to automatically pull the data identified in Lab Two and output the cypher queries required for inserting the data into a new database.

Lecture Five – Hunting for issues

The power in the graph database is that it shows both the individual objects and the relations of those objects. This makes looking for configuration issues easier because we can look at nodes in isolation or in chains depending on our environment. We will break down key examples for querying both individual configuration issues as well as combined configuration issues.

Lab Five – The Game's a Foot

Go forth and implement queries, looking at potential threats in the data set.

Discussion

The discussion on the end will be important as students think about the potential impacts of this beyond just Microsoft 365. Few vendor solutions manage complex models that represent the rat's nests we manage each day within the information security realm. In the closing discussion, we can talk through these unique cases and suggest plans for breaking down the large task ahead.