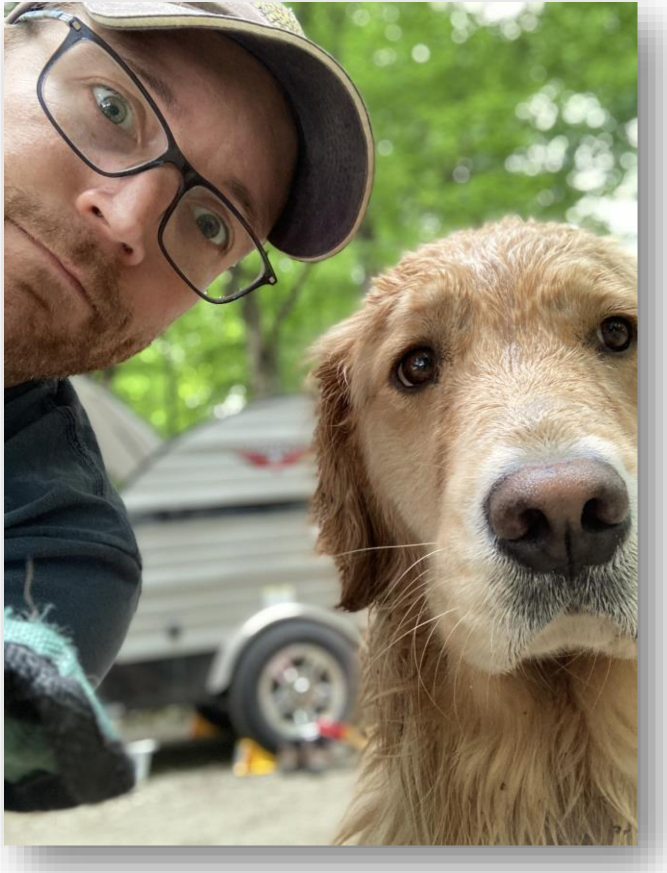
# Graphs for Cyber Security ...*in Action*

Dave Voutila

Senior Sales Engineer, Neo4j

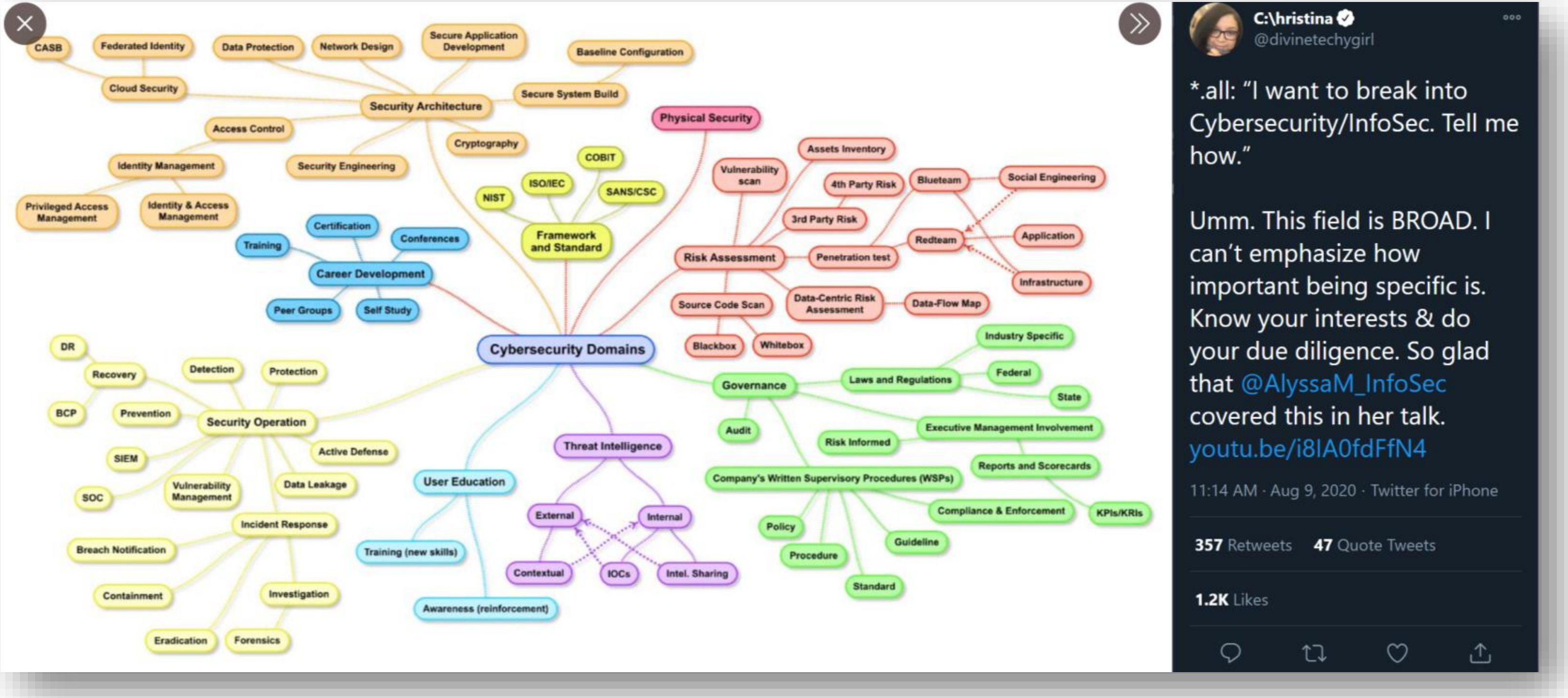
# OHAI!

- Senior {Field, Sales, Solutions} Engineer @ **Neo4j, Inc.**
- **https://sisu.io**
- dave.voutila@neo4j.com
- https://linked.in/dave.voutila
- https://github.com/voutilad
  - *dumb-ws, bolt-proxy, OpenBSD virtualization stuff*



# Let’s talk about Cyber Security

# Cyber cyber cyber cyber cyber?



C:\hristina
@divinetechygirl

*.all: “I want to break into Cybersecurity/InfoSec. Tell me how.”

Umm. This field is BROAD. I can’t emphasize how important being specific is. Know your interests & do your due diligence. So glad that @AlyssaM_InfoSec covered this in her talk. youtu.be/i8IA0fdFfN4

11:14 AM · Aug 9, 2020 · Twitter for iPhone

357 Retweets 47 Quote Tweets

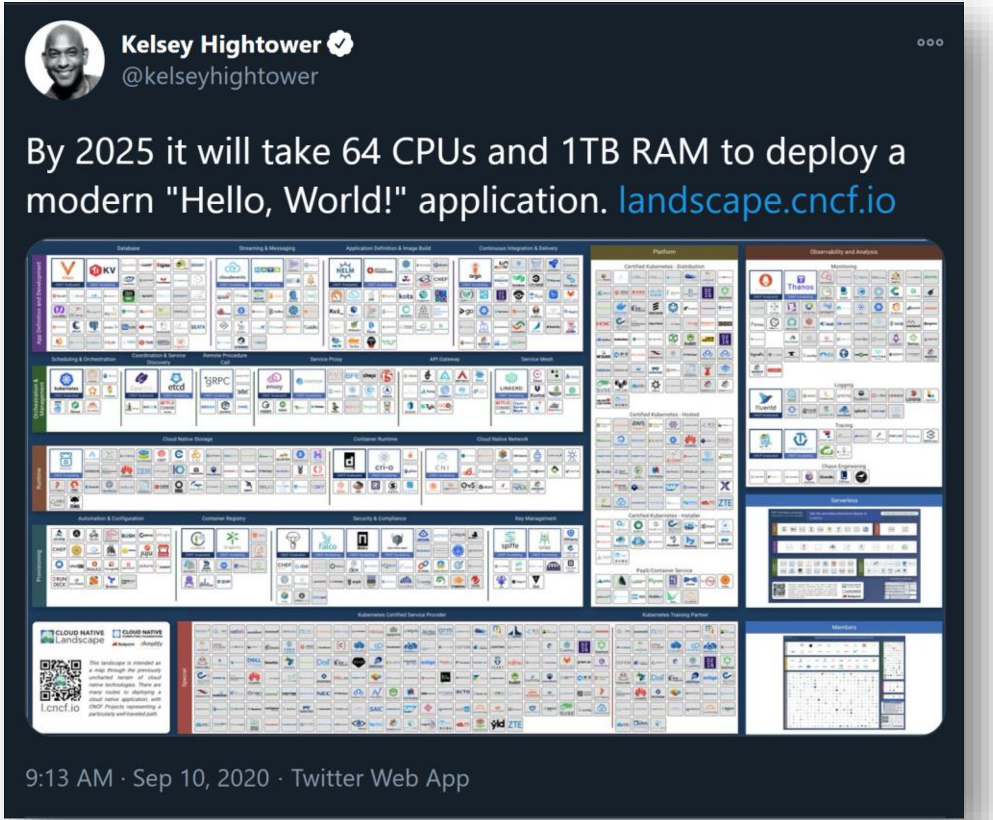
1.2K Likes

# This is not a stock photo of a “hacker”

Andrey Plotnitskiy, who authorities identified as a member of the Russian hacking group Evil Corp. National Crime Agency

# The Deck is Stacked Against Us

# Old Man Yells At Cloud

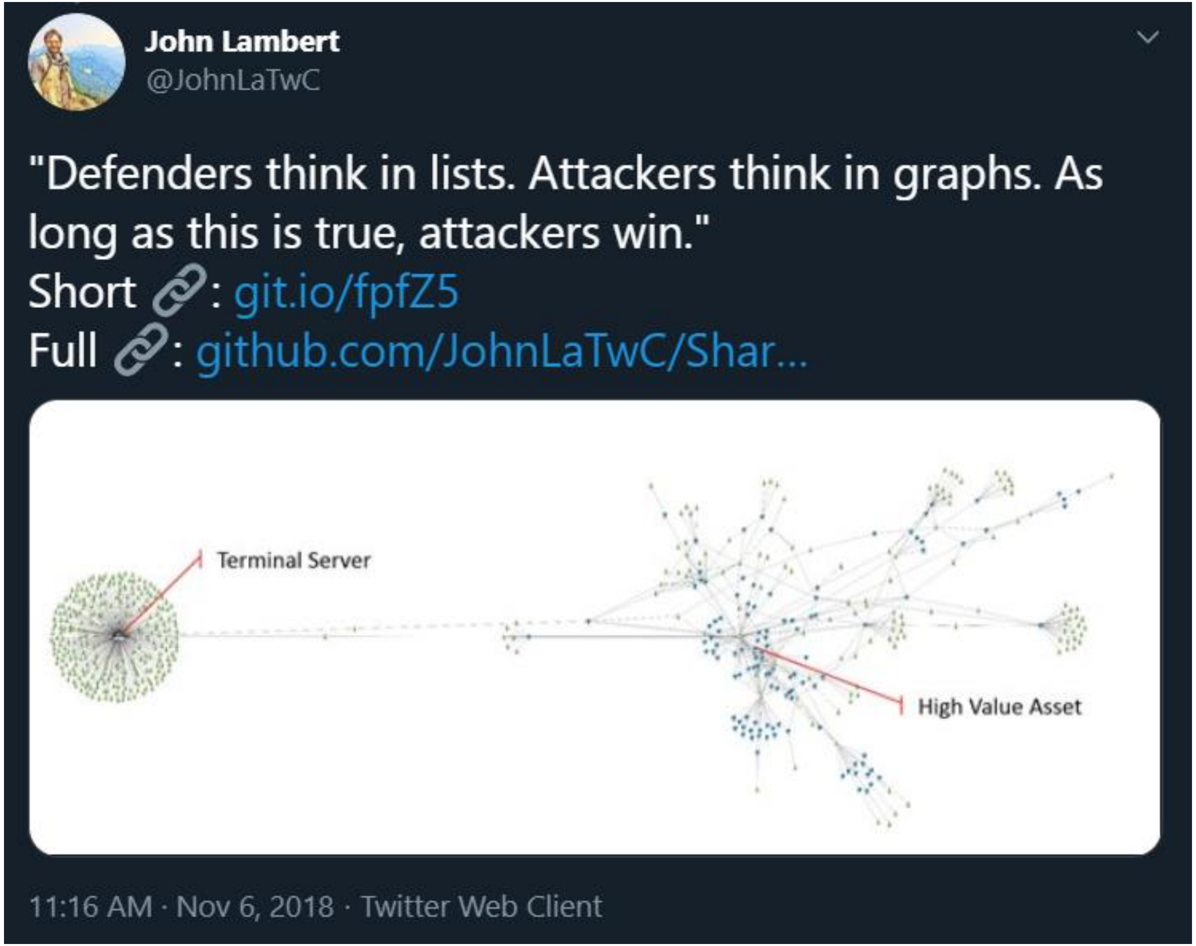


Kelsey Hightower
@kelseyhightower

By 2025 it will take 64 CPUs and 1TB RAM to deploy a modern "Hello, World!" application. landscape.cncf.io

9:13 AM · Sep 10, 2020 · Twitter Web App

# Graphs Will Save Us
(I hope)

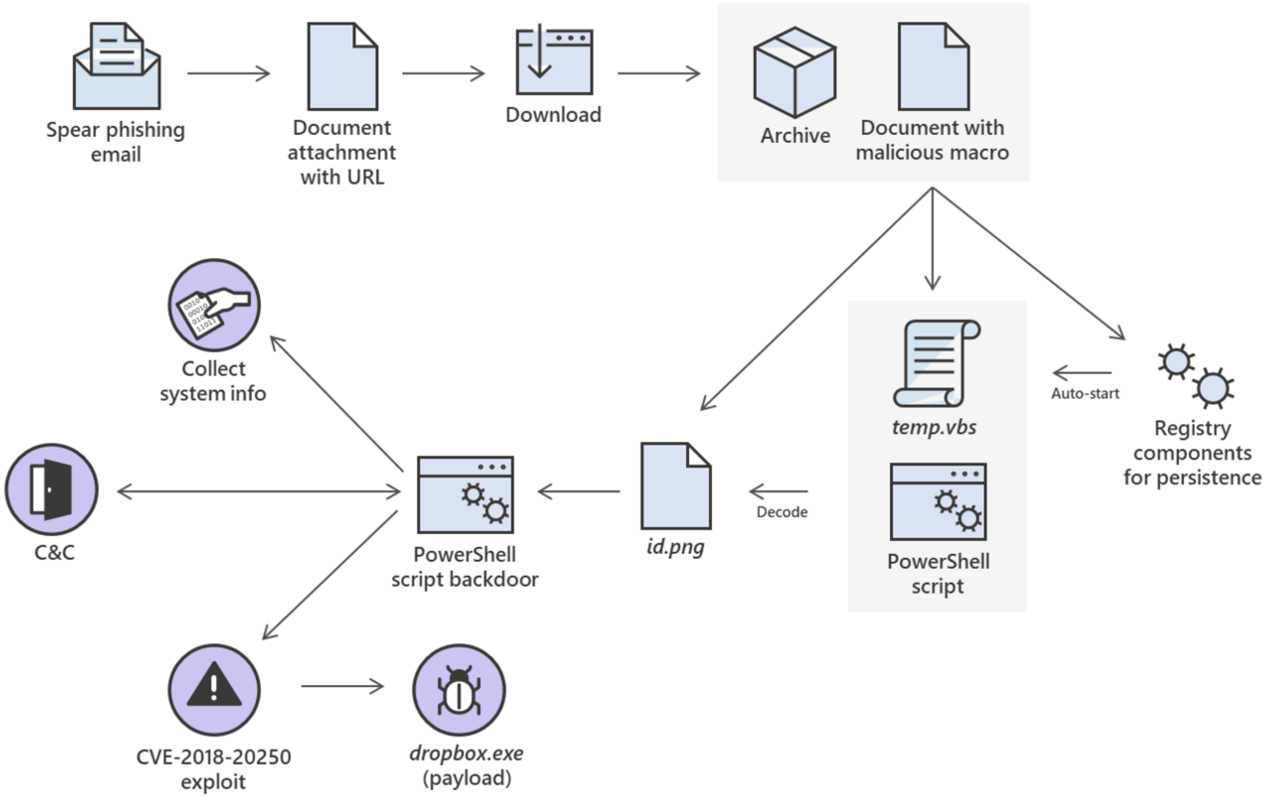


John Lambert
@JohnLaTwC

"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."
Short 🔗: git.io/fpfZ5
Full 🔗: github.com/JohnLaTwC/Shar...

11:16 AM · Nov 6, 2018 · Twitter Web Client

*John Lambert -- Distinguished Engineer, Microsoft Threat Intelligence Center*



***Attack chain that delivered the CVE-2018-20250 exploit (WinRAR RCE)***

https://www.microsoft.com/security/blog/2019/04/10/analysis-of-a-targeted-attack-exploiting-the-winrar-cve-2018-20250-vulnerability/

# 🤔 But, why do YOU need Graphs?

- Your teams need a holistic view of the Enterprise
  - Identify and assess risk to assets and processes
  - Protect systems, services, and crown jewels 👑
  - Detect anomalies
  - Respond rapidly with confidence to minimize impact
  - Recover quickly in the event of incidents

- A Holistic view → Connected Data

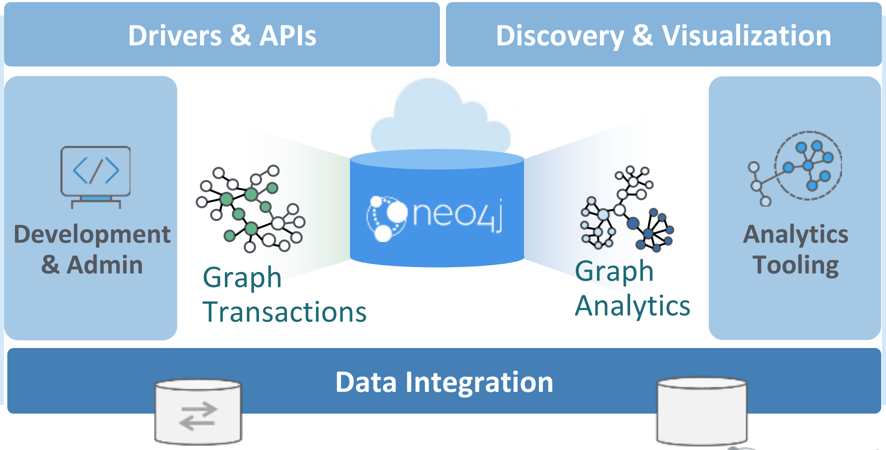
# Native Graph Technology

Neo4j is an ***enterprise-grade native graph database and tools***:

- Store, reveal and query data relationships
- Traverse and analyze any levels of depth in real-time
- Add context and connect data to support emerging AI applications

## Designed, built and tested natively for graphs from the start for:

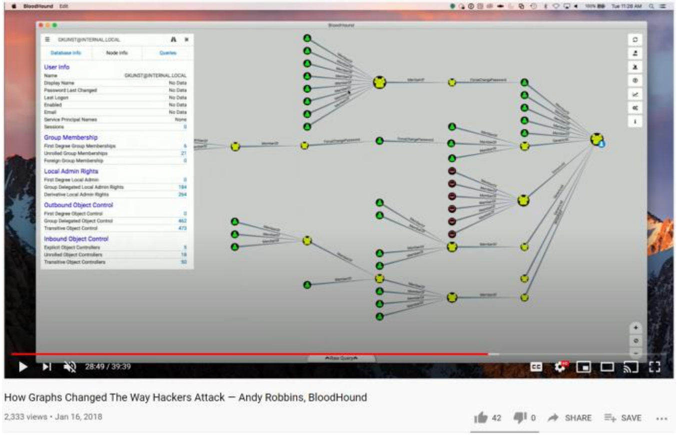
- Performance
- ACID Transactions
- Schema-free Agility
- Graph Algorithms
- Developer Productivity
- Hardware Efficiency
- Global Scale
- Graph Adoption



# Some examples of Neo4j "In the Wild"

BLOODHOUND

Cartography



BloodHound Edit

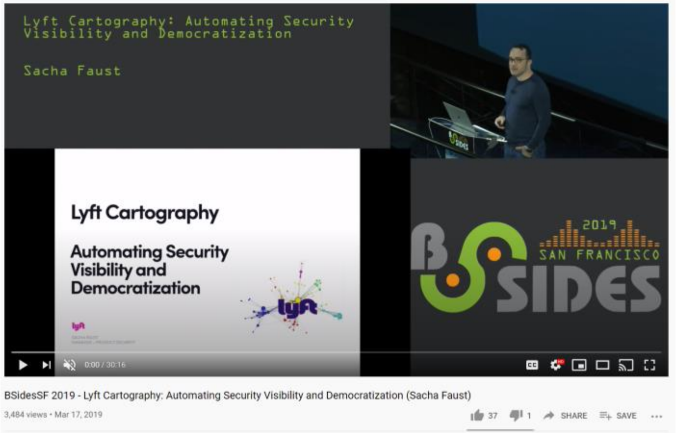
GKUNST@INTERNAL.LOCAL

Database Info | Node Info | Queries

| User Info | |
|---|---|
| Name | GKUNST@INTERNAL.LOCAL |
| Display Name | No Data |
| Password Last Changed | No Data |
| Last Logon | No Data |
| Enabled | No Data |
| Email | No Data |
| Service Principal Names | None |
| Sessions | 0 |
| **Group Membership** | |
| First Degree Group Memberships | 6 |
| Unrolled Group Memberships | 21 |
| Foreign Group Membership | 0 |
| **Local Admin Rights** | |
| First Degree Local Admin | 0 |
| Group Delegated Local Admin Rights | 184 |
| Derivative Local Admin Rights | 294 |
| **Outbound Object Control** | |
| First Degree Object Control | 0 |
| Group Delegated Object Control | 462 |
| Transitive Object Control | 473 |
| **Inbound Object Control** | |
| Explicit Object Controllers | 5 |
| Unrolled Object Controllers | 18 |
| Transitive Object Controllers | 50 |

How Graphs Changed The Way Hackers Attack — Andy Robbins, BloodHound

2,333 views • Jan 16, 2018



Lyft Cartography: Automating Security Visibility and Democratization

Sacha Faust

Lyft Cartography

Automating Security Visibility and Democratization

BSidesSF 2019 - Lyft Cartography: Automating Security Visibility and Democratization (Sacha Faust)

3,484 views • Mar 17, 2019

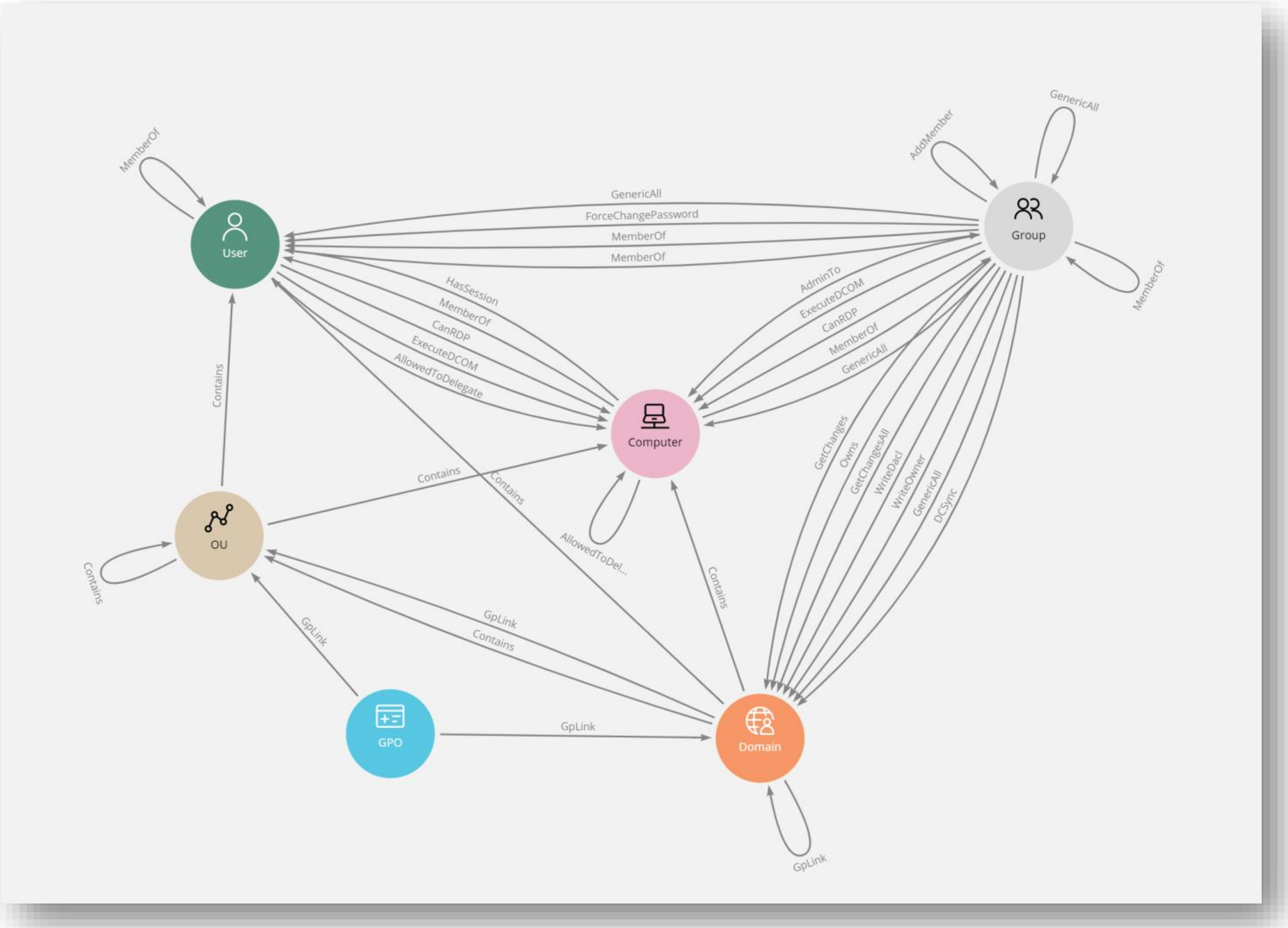
https://youtu.be/cT4xEhssz0U

https://youtu.be/ZukUmZSKSek

# Demo time!

# Let’s take a particular use case

- **Windows Domain Auditing!**
  - How are graphs a natural fit?
  - Where are our critical/weak points?
  - How can we use *Graph Data Science* techniques to assess exposure/risk?


User
Group
Computer
OU
GPO
Domain
MemberOf
GenericAll
ForceChangePassword
MemberOf
MemberOf
AddMember
GenericAll
MemberOf
HasSession
MemberOf
CanRDP
ExecuteDCOM
AllowedToDelegate
AdminTo
ExecuteDCOM
CanRDP
MemberOf
GenericAll
Contains
Contains
Contains
AllowedToDel...
GetChanges
Owns
GetChangesAll
WriteDacl
WriteOwner
GenericAll
DCSync
Contains
Contains
GpLink
GpLink
Contains
GpLink
GpLink

# End of Demo Time!

# Thanks!

## Dave Voutila

Senior Sales Engineer
dave.voutila@neo4j.com

*Demo Materials available at:*
**https://github.com/voutilad/neo4j-connections-cyber-2021**

neo4j