BloodHound:

Attack Graphs Practically Applied to Active Directory

HELLO!

I am Andy Robbins

Adversary Resilience Lead at SpecterOps

BloodHound co-creator and developer, Red Teamer

You can find me at @_wald0

HELLO!

I am Rohan Vazarkar

Adversary Resilience Senior Operator at SpecterOps

BloodHound co-creator and developer, Red Teamer

You can find me at @CptJesus

Agenda

- The Problem
- The Solution
- Conclusion

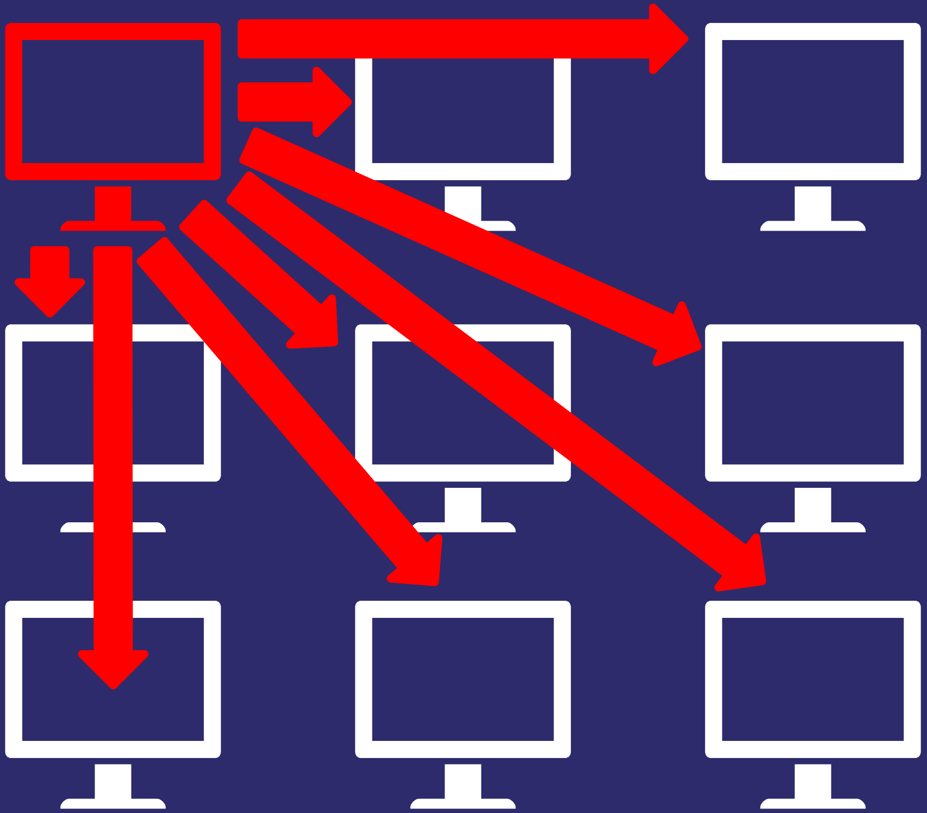
Purpose

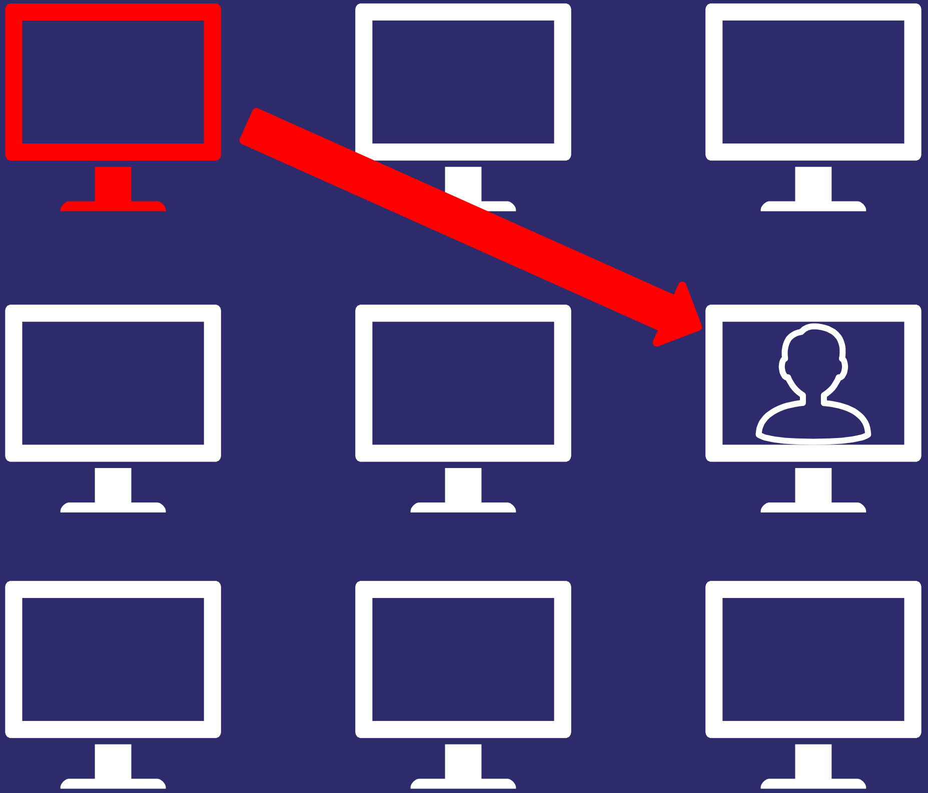
We want to demonstrate how **graphs** can be an **elegant and practical solution** to incredibly **complex problems**, and inspire **you** to consider using **graphs** for problems you face

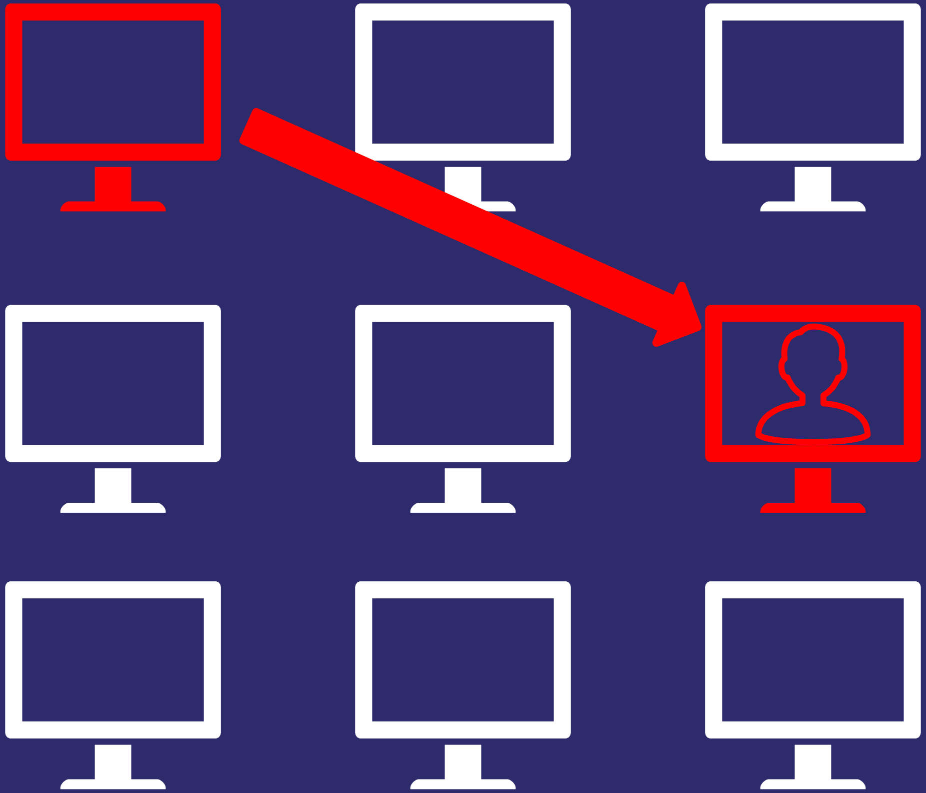
The Problem

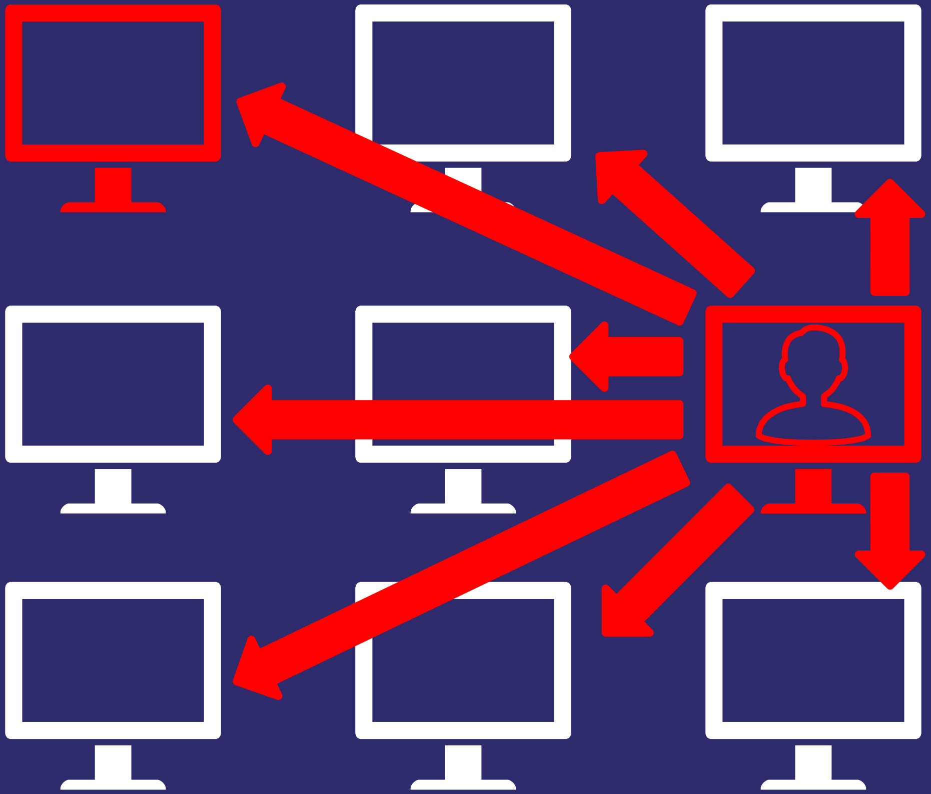
Pushed Into a Corner, circa 2014-2015

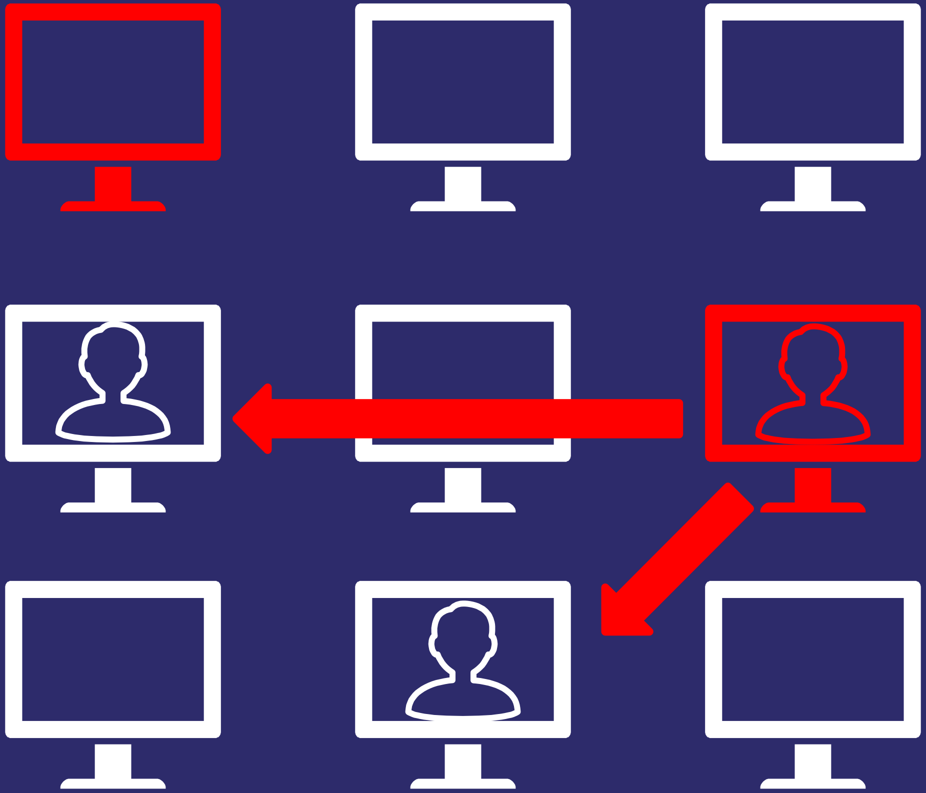
- Remote Code Execution (RCE) flaws in Windows become increasingly rare and risky to exploit
- Maturing vulnerability management programs ensure ephemerality of RCE in the enterprise
- A common methodology appeared…

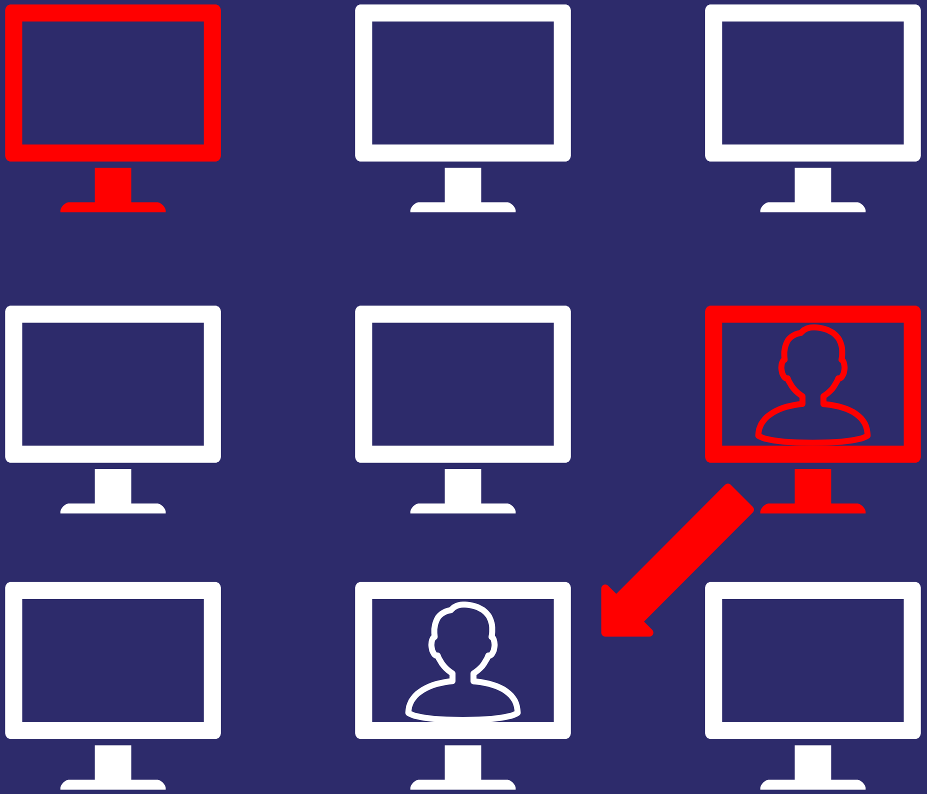


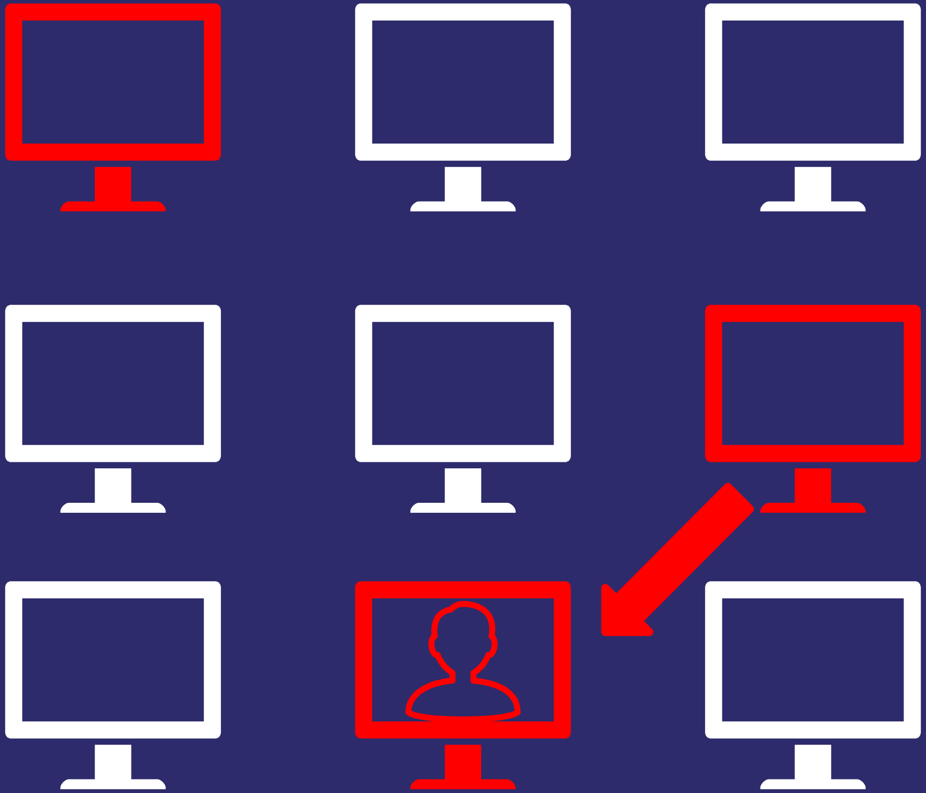


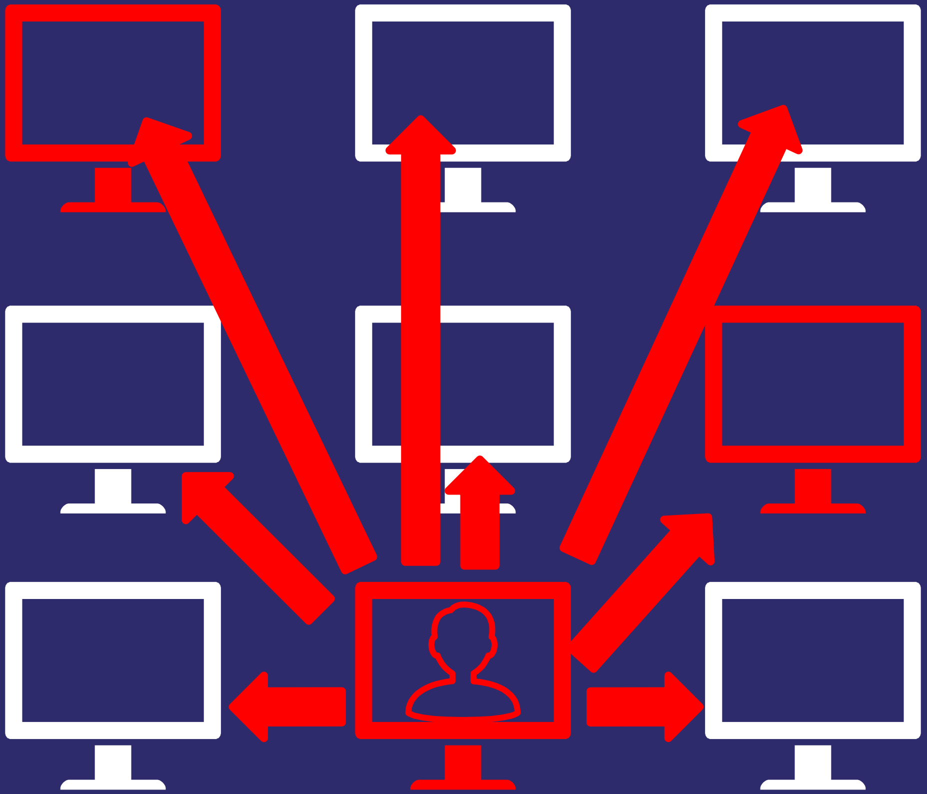


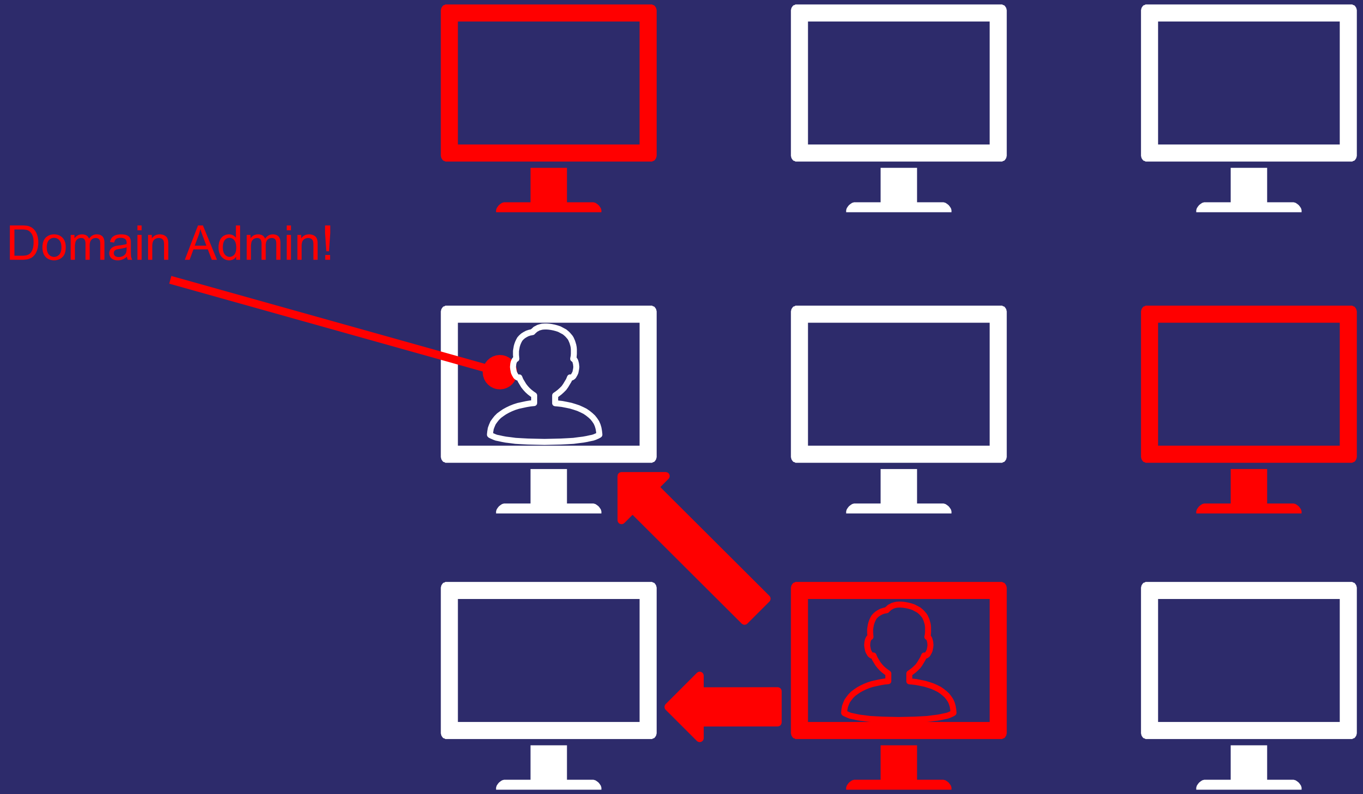


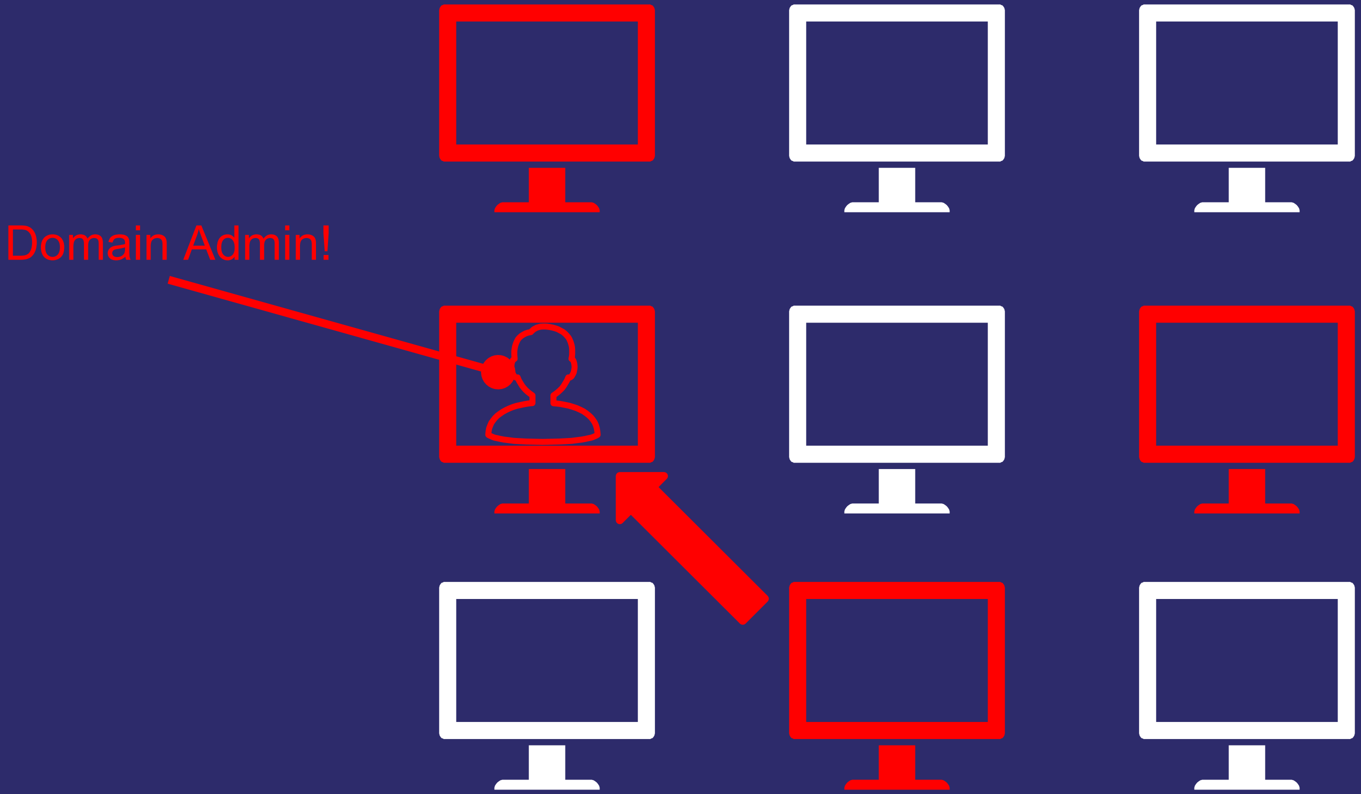









Domain Admin!

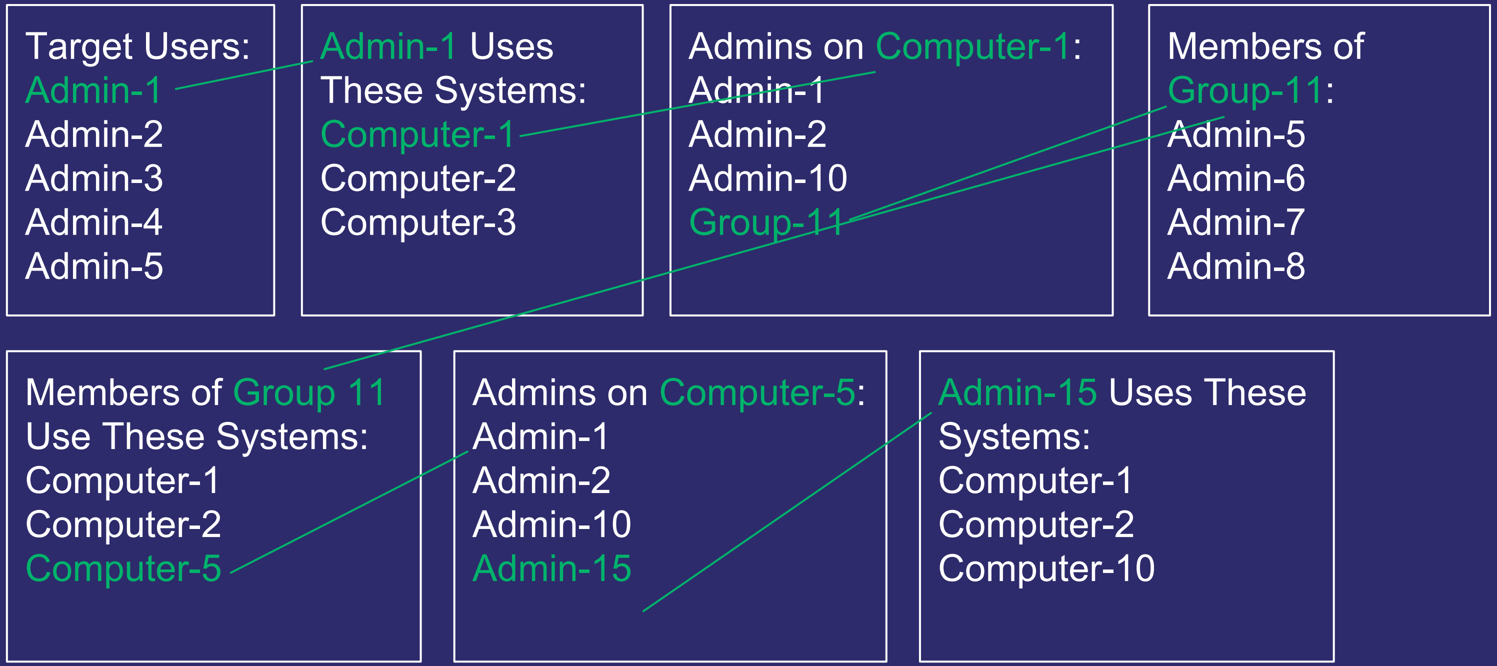

Domain Admin!

The Data is RIGHT… THERE!

- Question: Where are users logged on?
- *Answer: NetSessionEnum*
- Question: Who are local admins on a system?
- *Answer: NetLocalGroupGetMembers*
- Question: Who belongs to what security group?
- *Answer: Basic LDAP queries*

By default, all data is accessible by any domain authenticated principal on systems before Windows 10 Anniversary (1607)

An effective, albeit tedious and naive approach...



Target Users:
Admin-1
Admin-2
Admin-3
Admin-4
Admin-5

Admin-1 Uses These Systems:
Computer-1
Computer-2
Computer-3

Admins on Computer-1:
Admin-1
Admin-2
Admin-10
Group-11

Members of Group-11:
Admin-5
Admin-6
Admin-7
Admin-8

Members of Group 11 Use These Systems:
Computer-1
Computer-2
Computer-5

Admins on Computer-5:
Admin-1
Admin-2
Admin-10
Admin-15

Admin-15 Uses These Systems:
Computer-1
Computer-2
Computer-10

The Problem, In Short

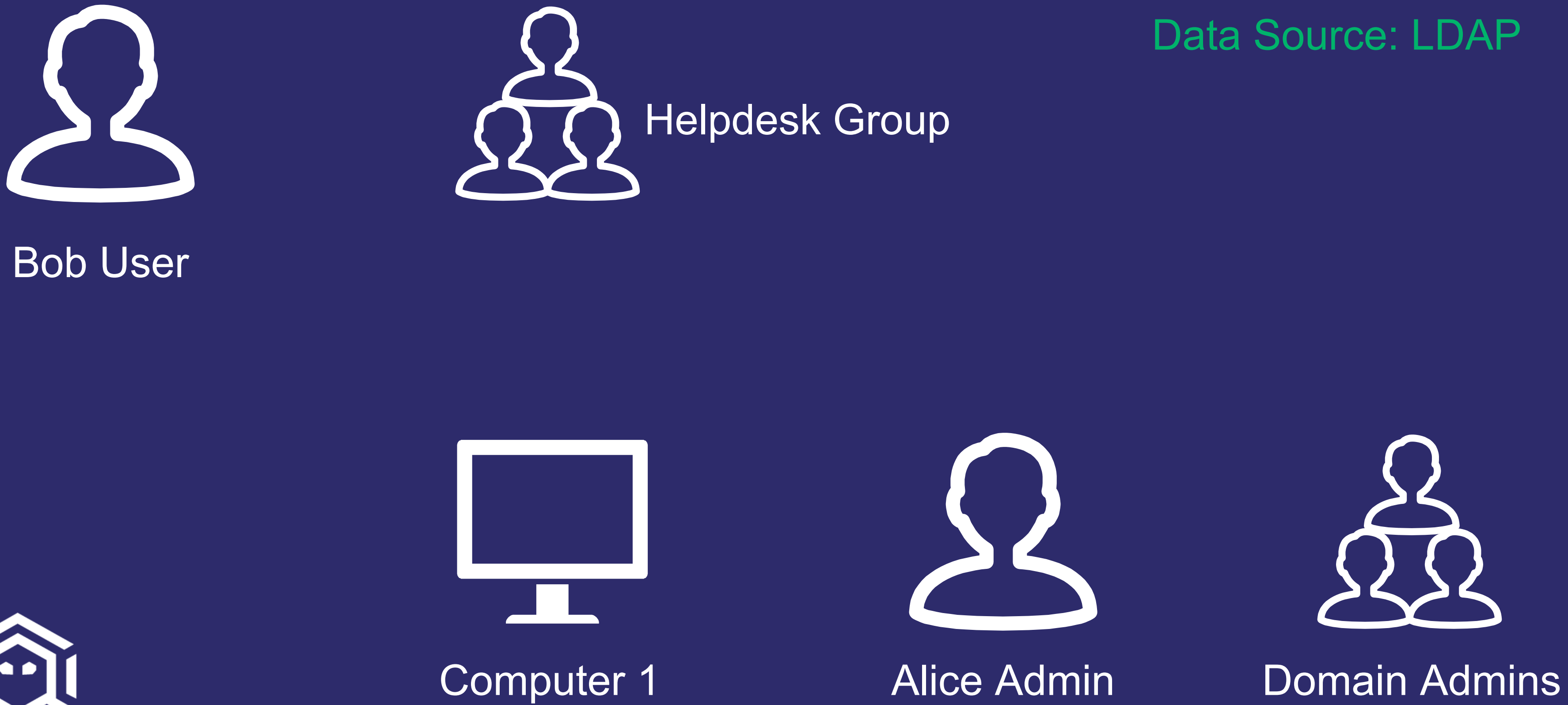
- We have a reliable, proven methodology for escalating rights in almost any Active Directory deployment
- That methodology is enhanced by data which, by default, anyone in a domain can access
- The data is way too complicated to analyze by hand

The Solution

It’s a graph, dummy!

- Every principal (user, group, computer) is a node
- Every privilege (and group membership) is a relationship
- Graphs are phenomenally fast at finding paths between disparate nodes

Data Source: LDAP



Bob User

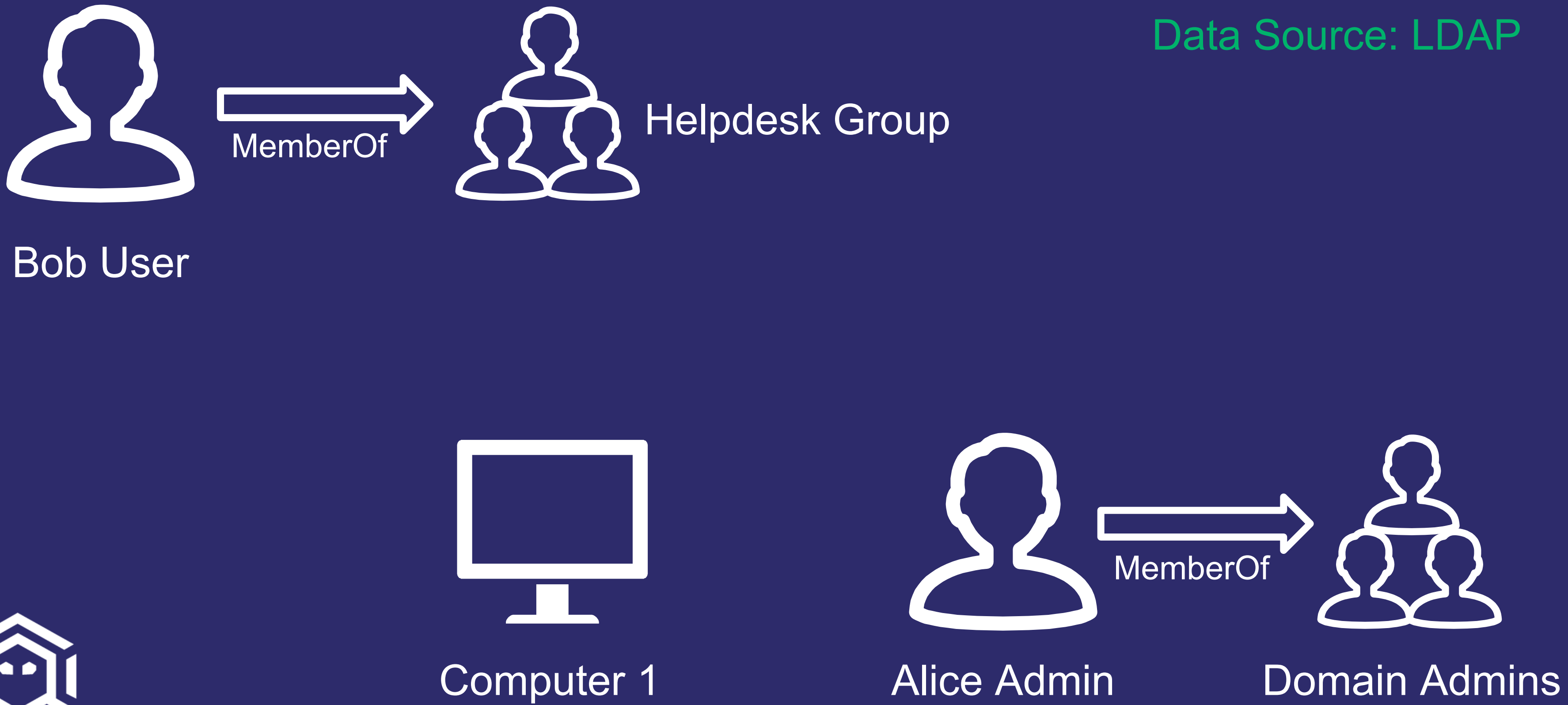
Helpdesk Group

Computer 1

Alice Admin

Domain Admins

Data Source: LDAP



Bob User

MemberOf

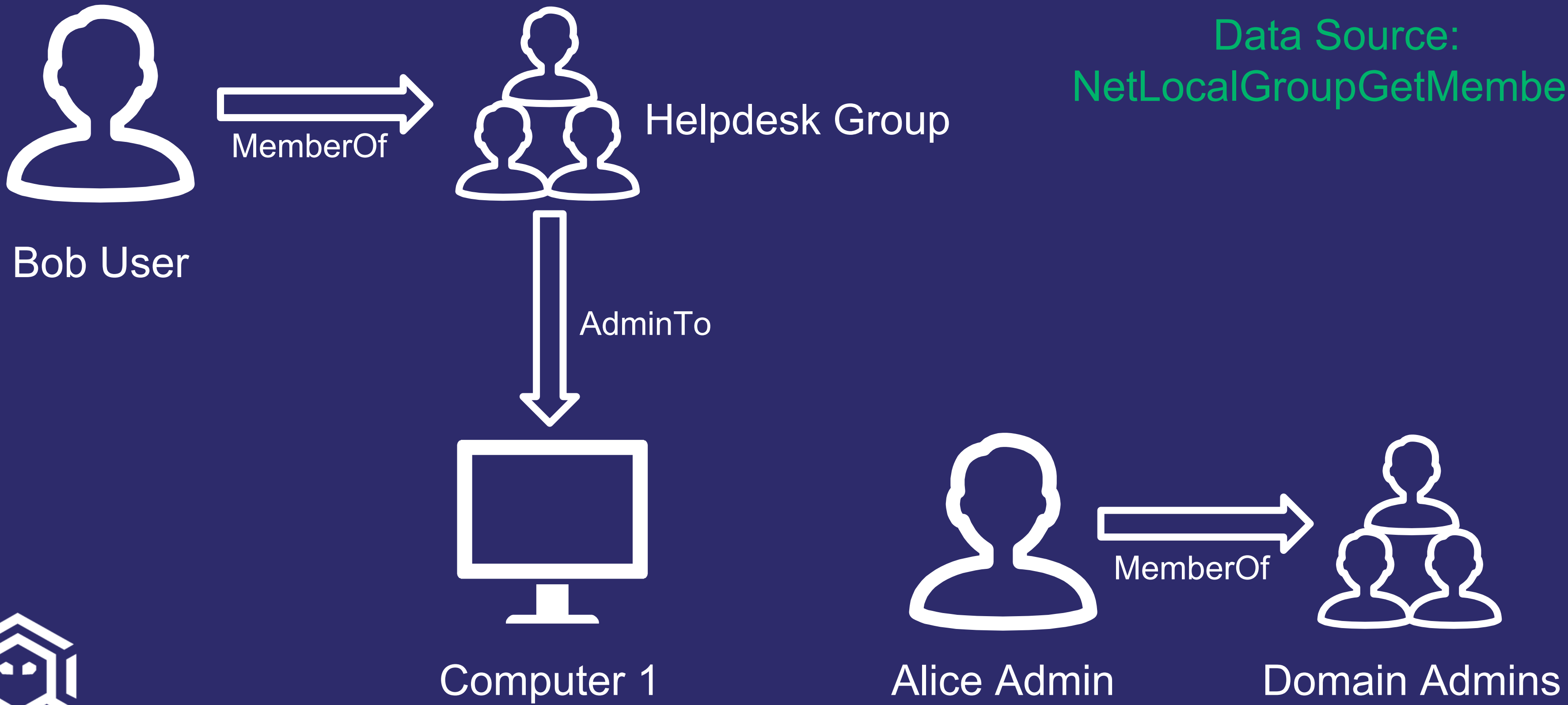
Helpdesk Group

Computer 1

Alice Admin

MemberOf

Domain Admins



Bob User

MemberOf

Helpdesk Group

AdminTo

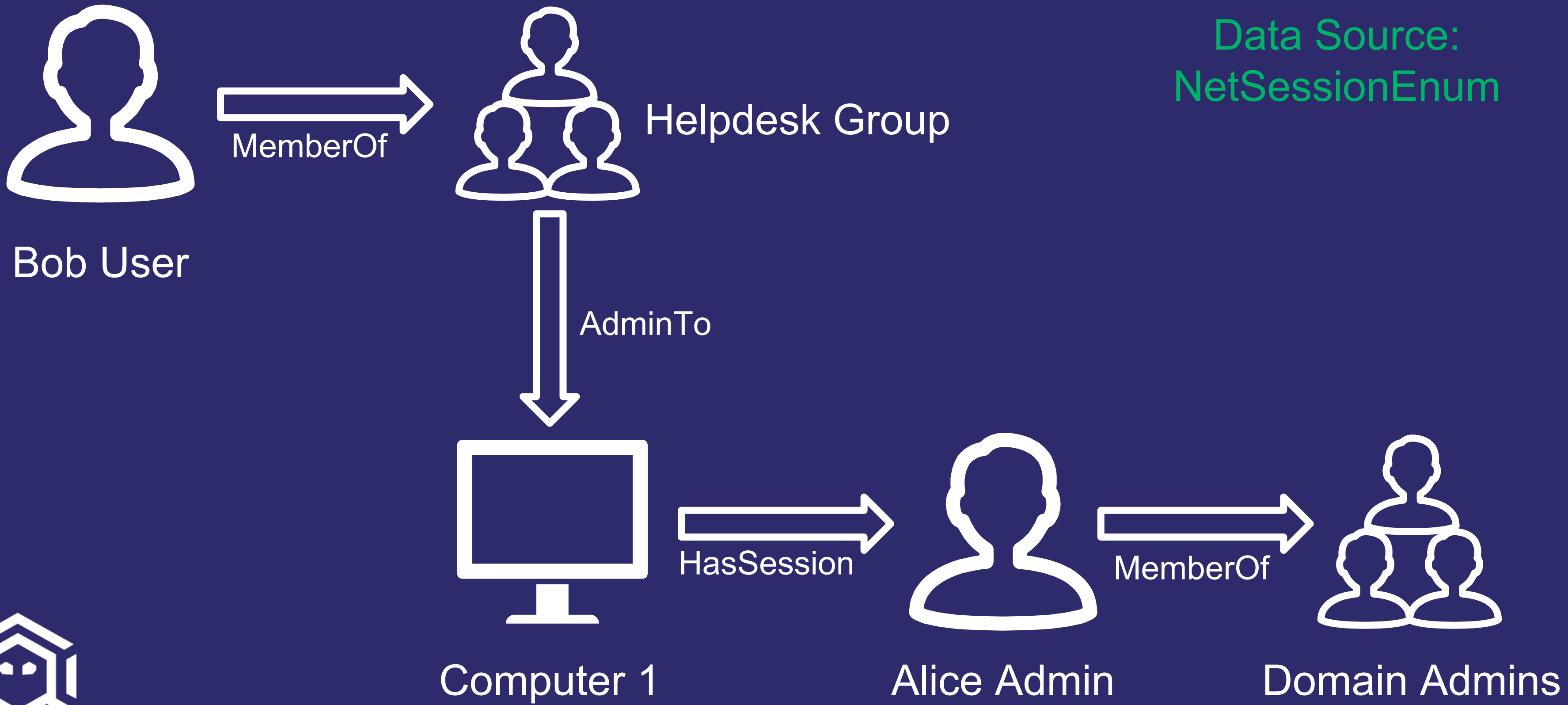
Computer 1

Alice Admin

MemberOf

Domain Admins

Data Source:
NetLocalGroupGetMembers

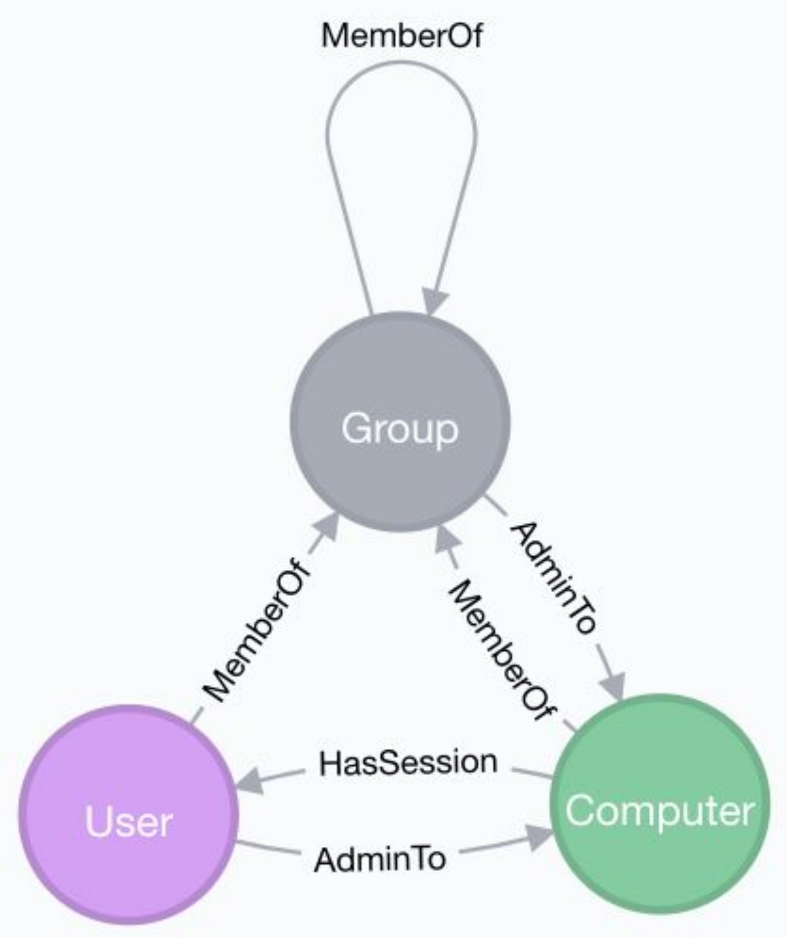


Data Source:
NetSessionEnum

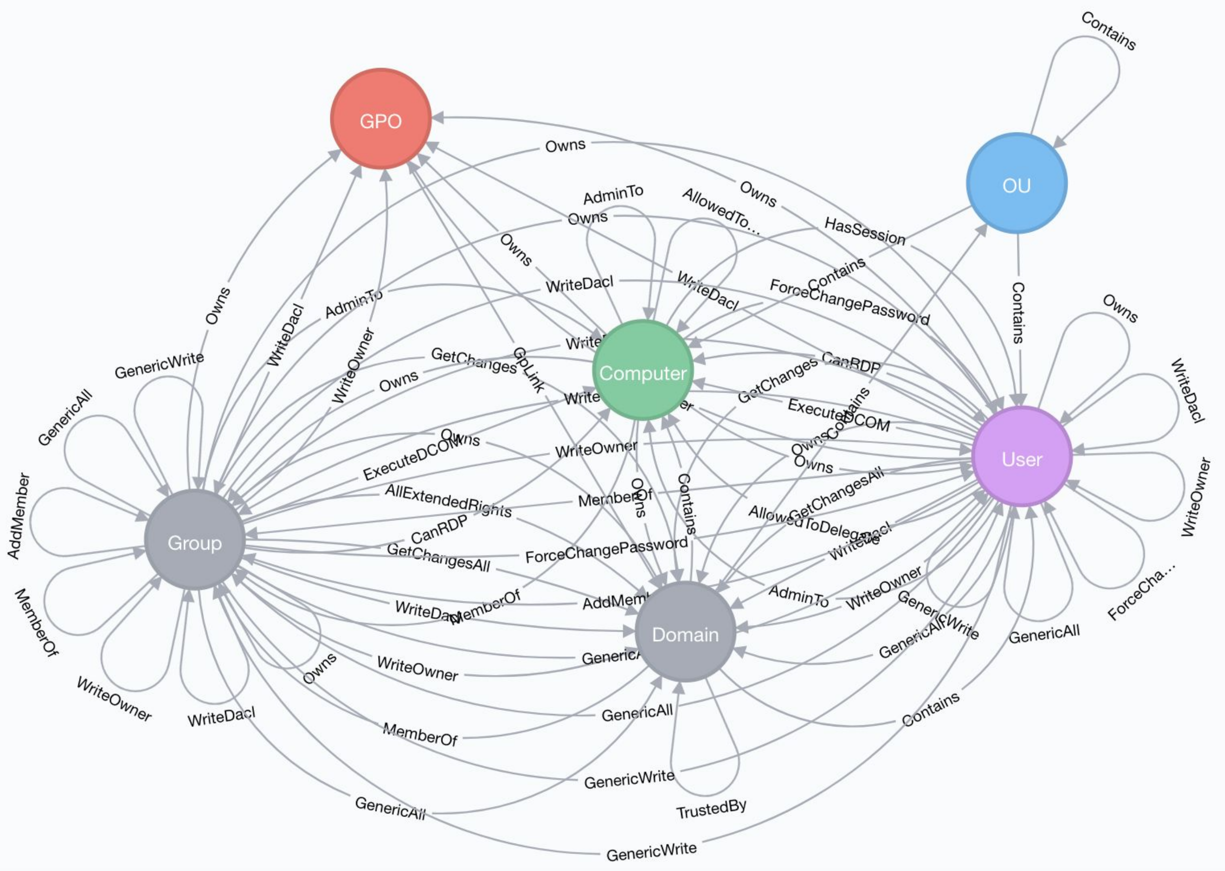
Now You’re Thinking With Graphs

- Manual “derivative local admin” takes days to months
- Data collection, graph analysis, and attack path execution takes minutes to hours

BloodHound 1.0 Schema



BloodHound 2.0 Schema



Conclusion

Three Problems Graphs Solved

- Complexity - Analyzing thousands of paths became possible
- Readability - Presenting concepts to non-technical audiences became easier
- Accessibility - Opened up the methodology to both the defensive and offensive side

Three Exciting Defensive Applications

- Easier, more effective, more accurate permission auditing
- Attack path identification and mitigation/elimination
- Empirical key terrain identification

If There’s One Thing to Take Away From this Talk

- Graphs are **not the solution to every problem**; however, they allow you to look at problems in a **unique way** and **solve complex problems** that otherwise would be **insanely difficult** to visualize, compute, or solve

Acknowledgements and Prior Work

http://alicezheng.org/papers/sosp2009-heatray-10pt.pdf

https://www.sixdub.net/?p=591

https://bitbucket.org/iwseclabs/bta

https://github.com/ANSSI-FR/AD-control-paths

https://powersploit.readthedocs.io/en/latest/Recon/

Thank you!

QUESTIONS?

You can find us at:

- specterops.io
- @SpecterOps
- @_wald0
- @CptJesus
- BloodHound: https://bit.ly/GetBloodHound
- BloodHound Slack: https://bloodhoundgang.herokuapp.com

SPECTEROPS