SPECTEROPS

Attack Path Management, the BloodHound Enterprise Way

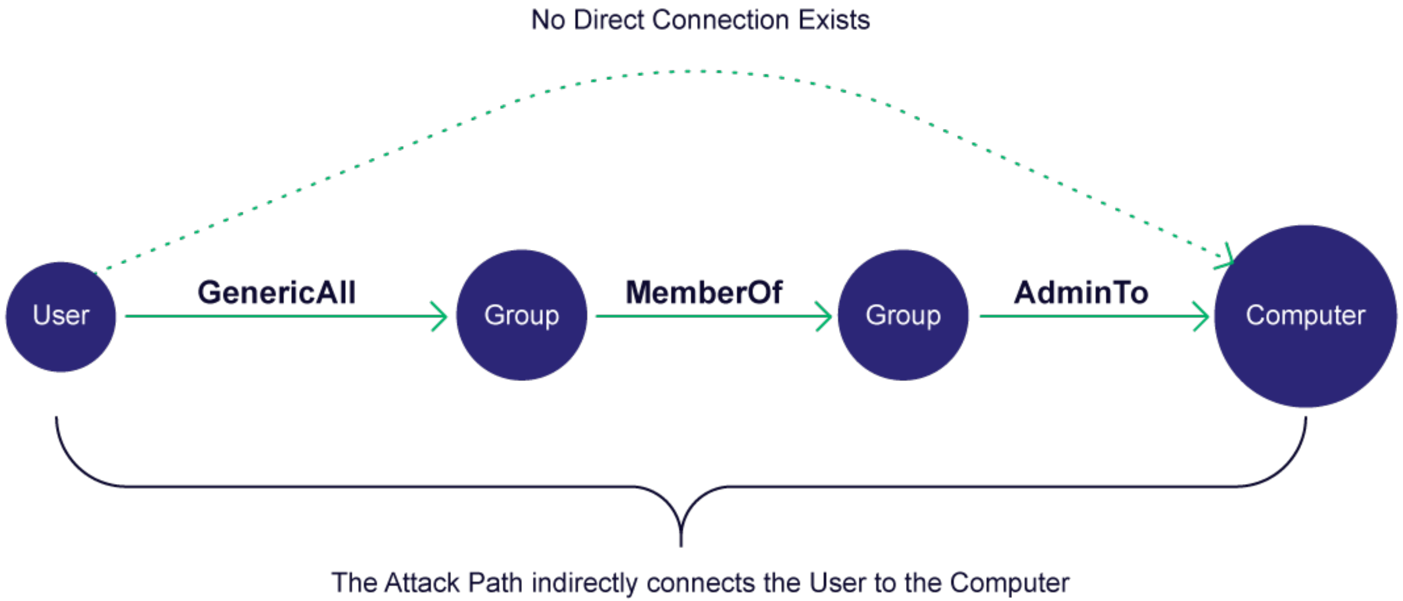
What are we talking about?

- What is an Identity Attack Path?
- Why do I care?
- Attack Path Management and Demo

What is an Identity Attack Path?

What Are Attack Paths?

Attack Paths are the chains of abusable privileges and user behaviors that create direct and indirect connections between computers and users.


No Direct Connection Exists
User
GenericAll
Group
MemberOf
Group
AdminTo
Computer
The Attack Path indirectly connects the User to the Computer

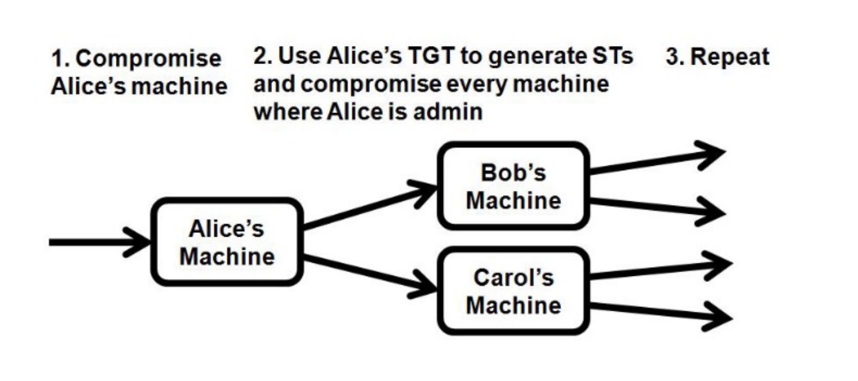
https://posts.specterops.io/the-attack-path-management-manifesto-3a3b117f5e5#4a41

New….but not really

2009: Identity Snowball Attack Research

Heat-ray: Combating Identity Snowball Attacks Using Machine Learning, Combinatorial Optimization and Attack Graphs

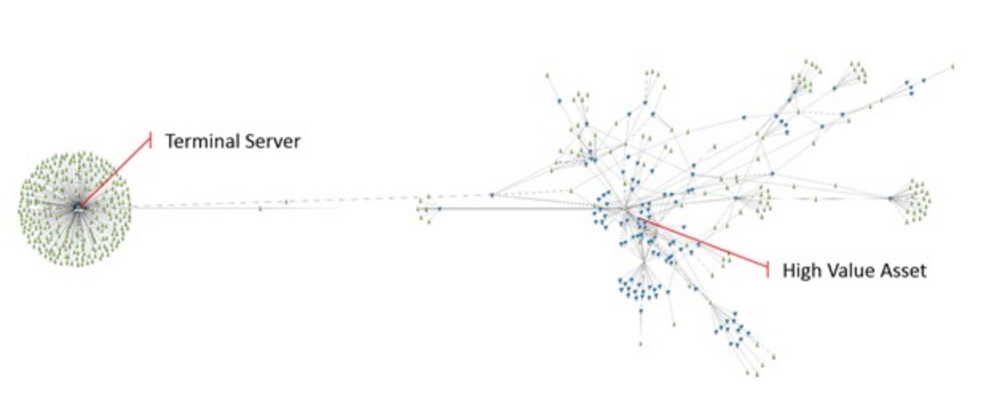
https://www.microsoft.com/en-us/research/wp-content/uploads/2009/01/sosp2009-heatray-10pt.pdf


1. Compromise Alice's machine
2. Use Alice's TGT to generate STs and compromise every machine where Alice is admin
3. Repeat
Alice's Machine
Bob's Machine
Carol's Machine

2015: John Lambert TWC Blog

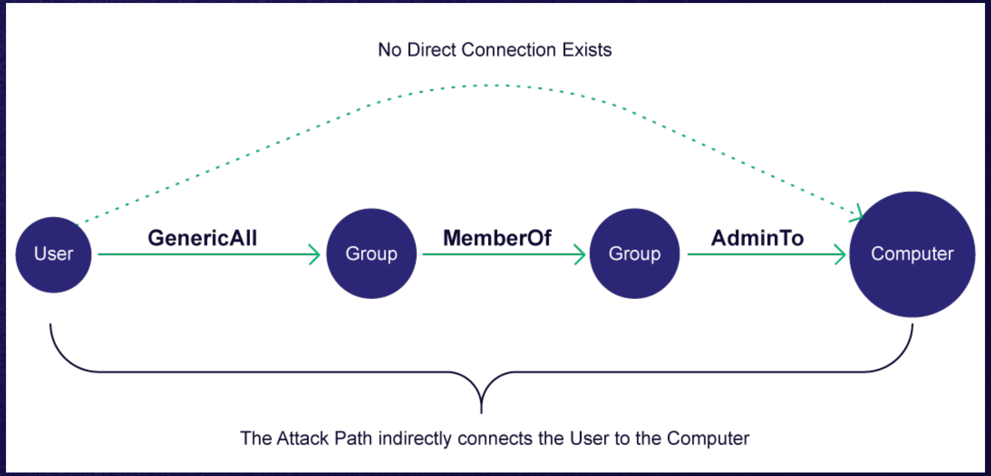
"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

https://github.com/JohnLaTwC/Shared/blob/master/Defenders%20think%20in%20lists.%20Attackers%20think%20in%20graphs.%20As%20long%20as%20this%20is%20true%2C%20attackers%20win.md?trk=article-ssr-frontend-pulse_little-text-block



A more powerful attack

- Attackers appear legitimate
- Subverts many existing controls
- “Functioning as intended”

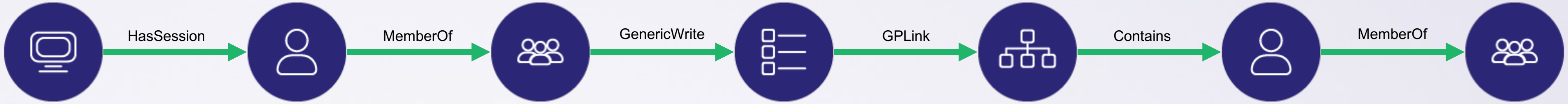

No Direct Connection Exists
User
GenericAll
Group
MemberOf
Group
AdminTo
Computer
The Attack Path indirectly connects the User to the Computer

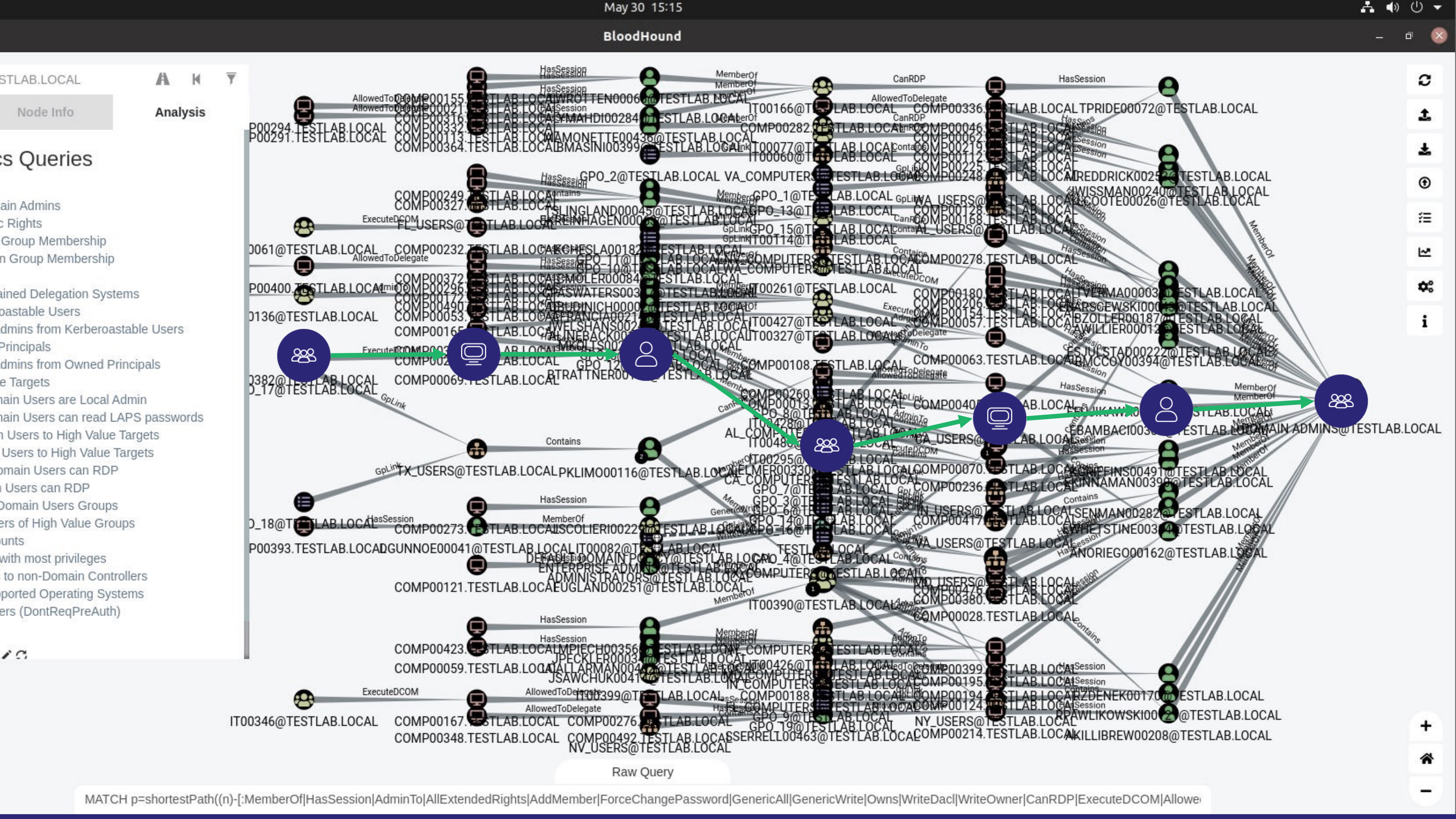
Why do I care?

Real-World Exploitation of Identity Attack Paths

- 2019: APT 10 observed invoking Mimikatz / BloodHound via Powershell
    - https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf
- 2020: Ryuk observed invoking SharpHound
    - https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack
- 2021: Use of ADFind and BloodHound observed in ransomware campaigns
    - https://www.trendmicro.com/vinfo/ie/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021
- 2022: Black Basta infiltrates networks via QAKBOT, utilizes SharpHound
    - https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html
- 2023: CISA Lockbit advisory regarding use of ADFind, Mimikatz, BloodHound
    - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
- 2024: Midnight Blizzard nation-state Attack on Microsoft Graph privileges
    - https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Simple (ish) Identity Attack Path in Active Directory



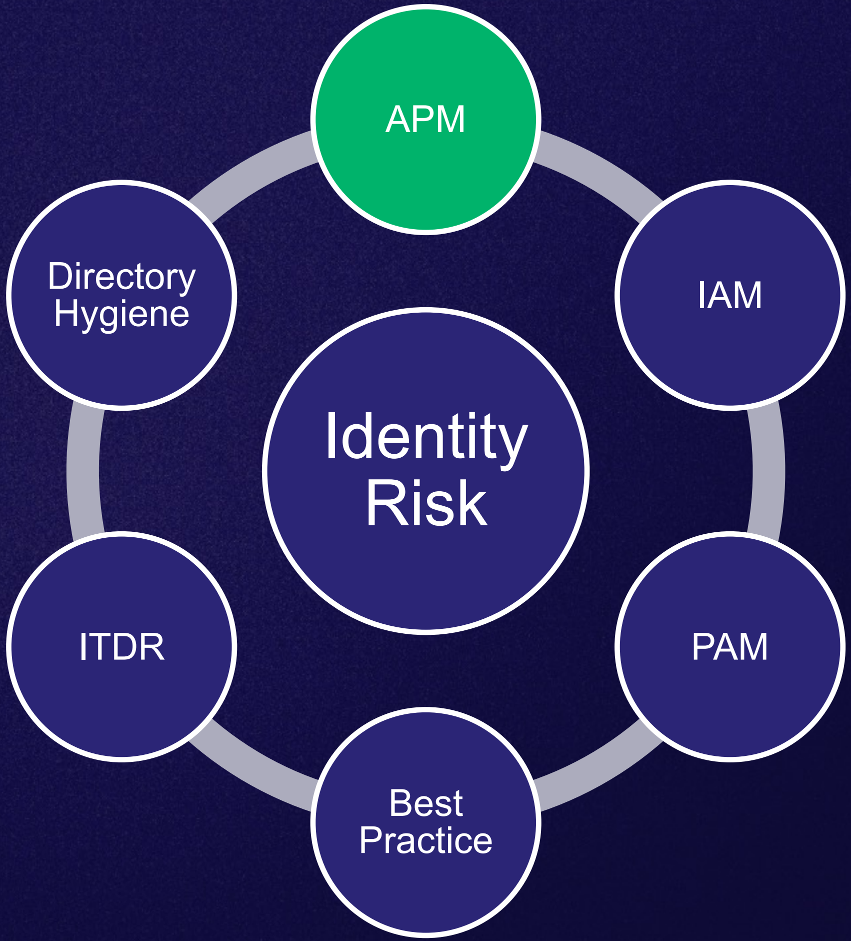


```
MATCH p=shortestPath((n)-[:MemberOf|HasSession|AdminTo|AllExtendedRights|AddMember|ForceChangePassword|GenericAll|GenericWrite|Owns|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|Allowe
```

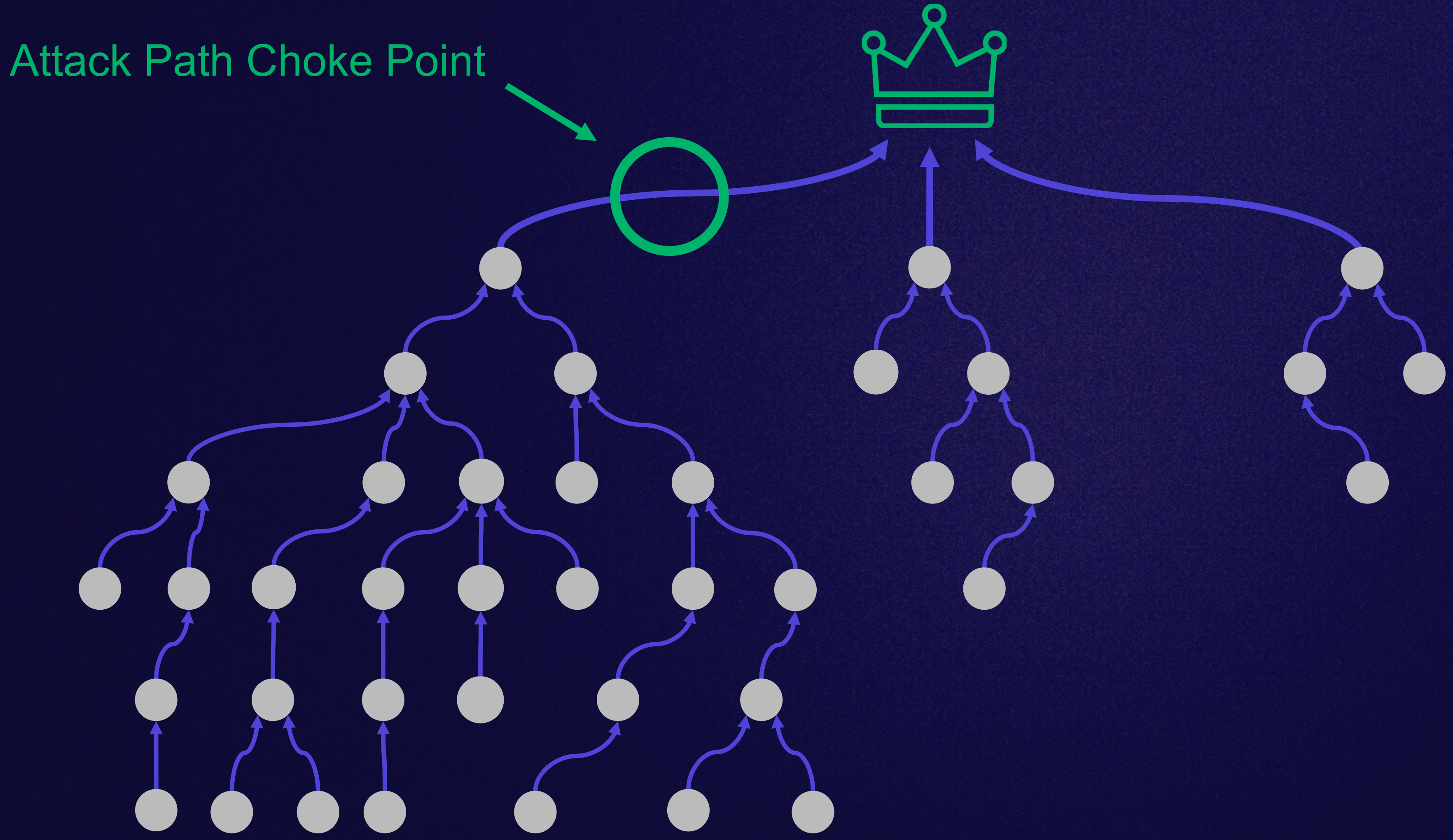
Attack Path Management

Attack Path Management

is the continuous discovery, mapping, and risk assessment of Attack Path Choke Points.

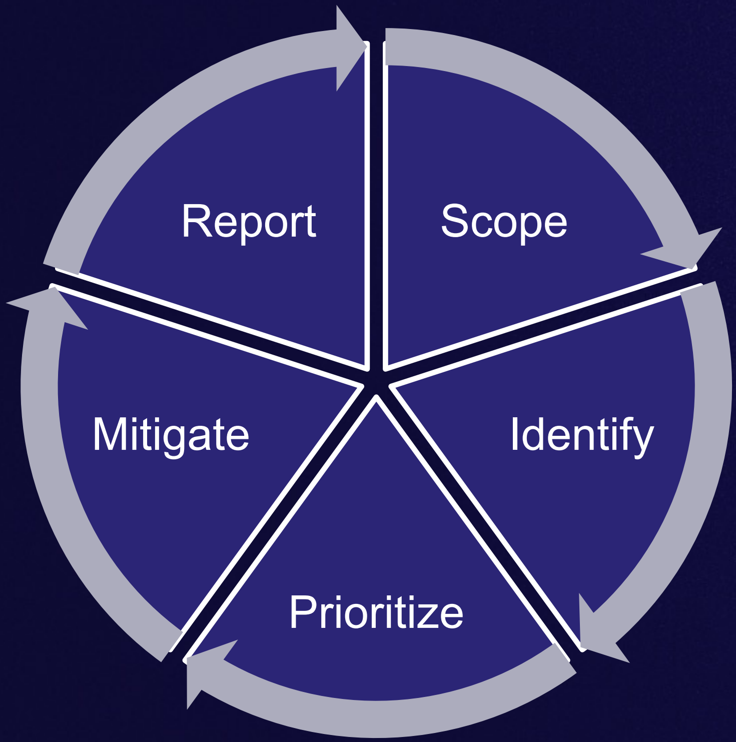


https://posts.specterops.io/the-attack-path-management-manifesto-3a3b117f5e5



Attack Path Choke Point

APM Process and benefits



- ✓ Proactive, comprehensive visibility
- ✓ Single fixes to sever multiple Attack Paths
- ✓ Prioritized by exposure and impact
- ✓ Step-by-step remediations
- ✓ Measurable progress and trend reporting

Demo