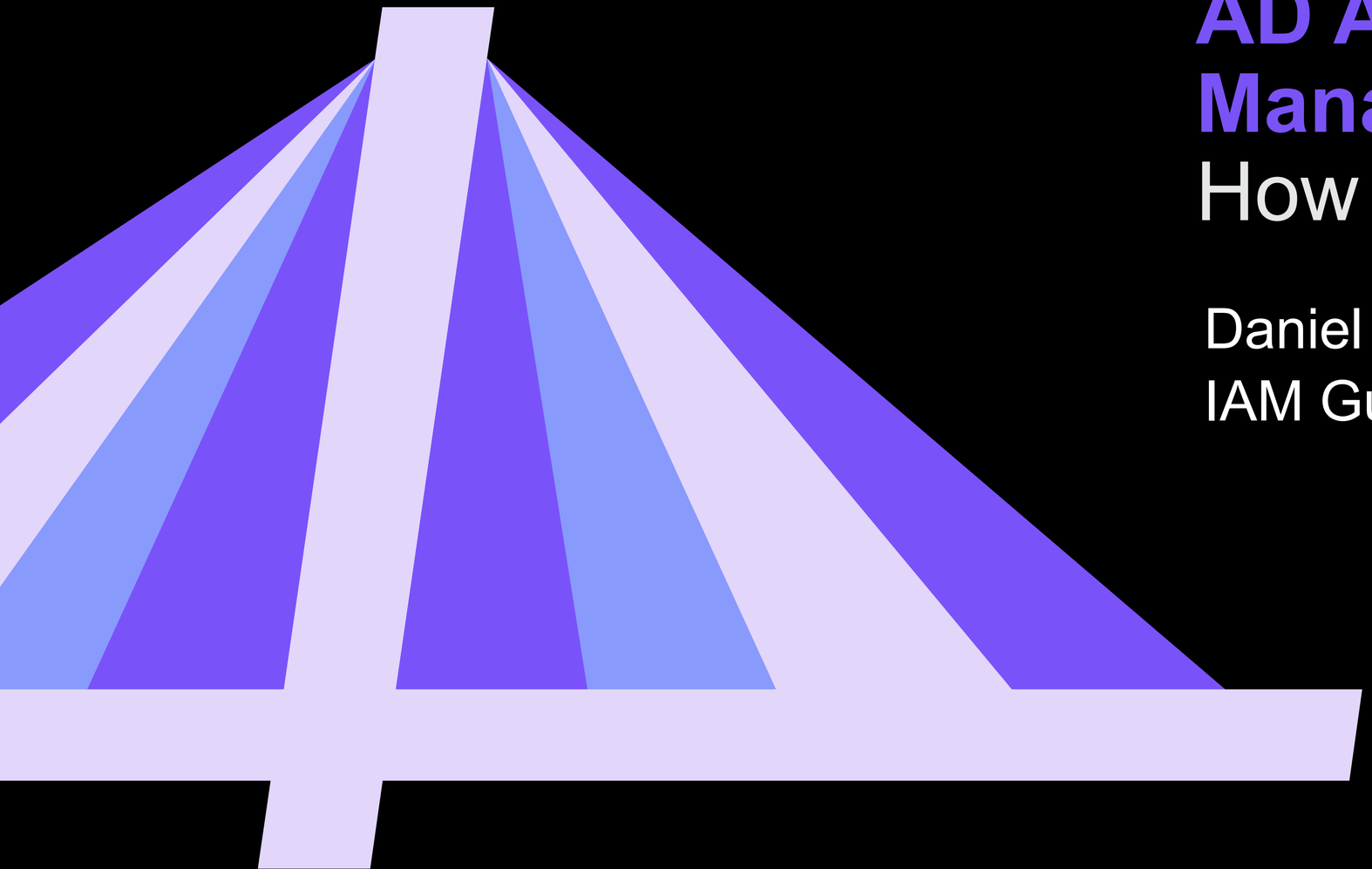
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



AD Attack Path Management: How to Stop the Insanity

Daniel Stefaniak
IAM Guy @ JPMC

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

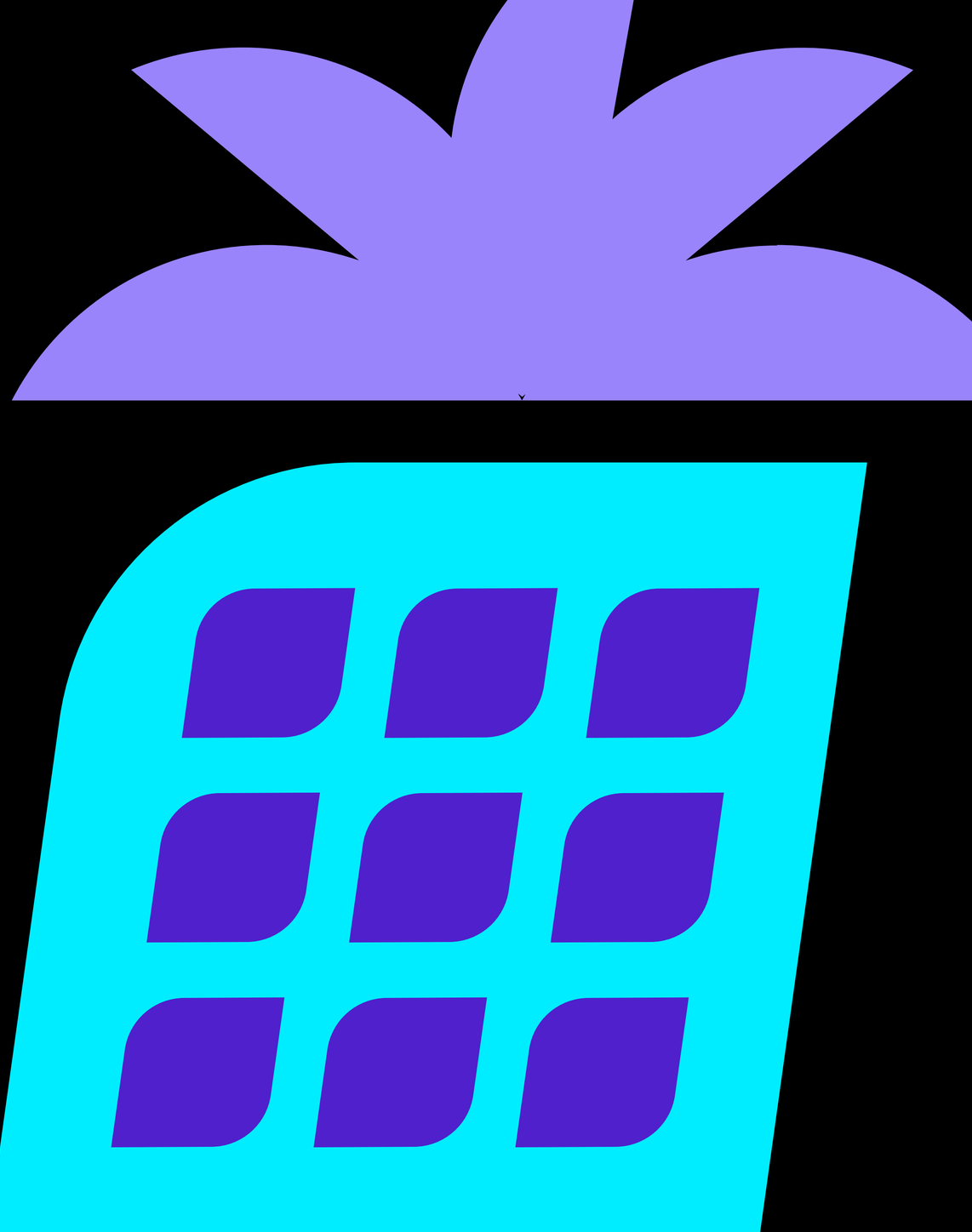
Daniel Stefaniak

IAM Guy, JPMC

Experienced IT Architect, Consultant, Security Engineer and Technical Program Manager specializing in Active Directory, ADFS and Entra ID.

Agenda

- Attack paths 101
- Assumptions vs Reality
- Selecting a tool
- Should I bother?
- How not to go insane? NUMBER!
- Process
- Saying “no”
- What did we learn?
- Call to action



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Attack paths 101

- Account takeover
- Variety of escalation techniques
  - Simple example: Helpdesk resets password of Enterprise Admin
  - More complex: Memory dump of a terminal server that Domain Admin is logged on to
- Attack path management is mostly preventative

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

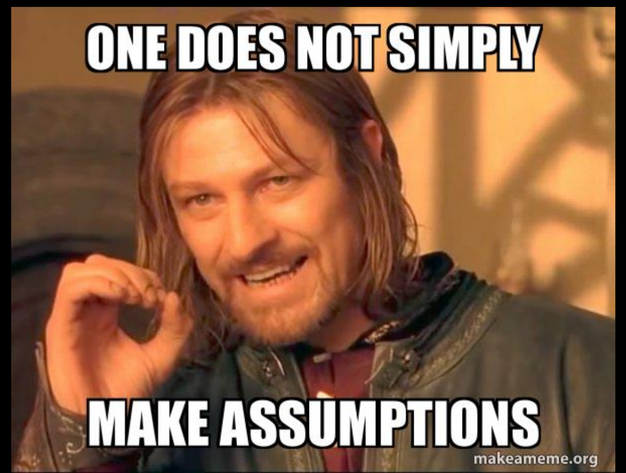
Assumption vs reality

Assumptions:

- I can secure all escalation paths
- Zero Trust FTW
- I can do this as part of my regular duties
- I can do it with Tool X/Y/Z

Reality:

- You need to run on the side of acceptable risk and have detection for paths that are there for BAU
- Tiering model is orthogonal here. Deepen the Moat
- It is a difficult problem – you need to staff an entire team
- Cleanup is a process problem especially if you have never been pwnd (RedTeam does not count ☺)



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Tool Selection

- Try them all
- None will work 100%
- Think of scale (double your DC sizing)
- Do you care about cloud?
- Do you care about SAML/Oauth IdPs?
- Do you need one? Maybe you can script with your eyes closed ☺
- LLMs’ capability to hallucinate is disqualifying for the problem

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

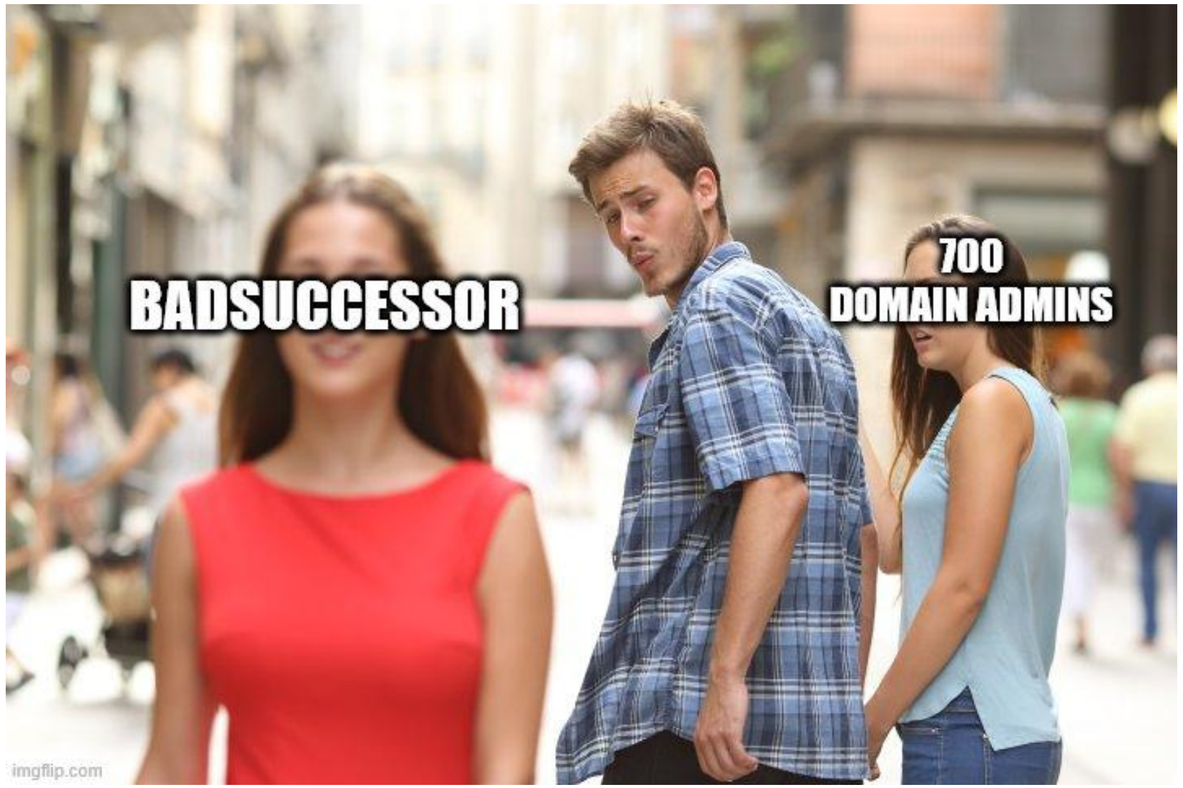
Should I/we bother?

- Hygiene
- What happens in Tier0 stays in Tier0

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

How to stay sane?

- Choose a number that corresponds closest to your version of risk
  - Paths By Account
  - Exposure
  - Impact
  - Something else?
- Do not get distracted by cool new stuff
- Have a number goal in mind
  - Measure what matters (e.g., OKR of lowering number by X% every Y)
  - IT WILL NEVER BE 0
- Understand what's controlled/secured in your organization



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Process

- I can take a while (multiple quarters) to find The NUMBER
- Start with “big uglies” – taking care of some outliers will make your discovery and cleanup tasks easier
- If you have nobody on your team that has AD expertise (300+ level), hire up!
- Do not “call baby ugly”
- Document everything
- Eventually you should develop into a Program
- Add things to Tier0 if they are “controlled”
- Scope out “cloud” at the start

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Saying “no”

- Your/your team’s job is to lower The NUMBER
- There are plenty of weaknesses and exploits
  - Unless they contribute to your KR: backlog

- Add things to a backlog
- Fundamentals are…FUNDAMENTAL
- Splitting hair between classes of escalation paths is very often not worth it

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

What did we learn?

- Dedicated team
  - Redundancy is nice
- Understand “normal”/BAU of how business uses and manages AD
- It will never end
- Nothing is urgent frfr no cap
- You need a PM
- Keep detections in your back pocket as a valuable mitigation

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Call to action

- Today: Scan for attack paths
- Next week: Fix one “big ugly”
- Next month: Pick a number
- Next quarter: Lower that number

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Special thanks

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON