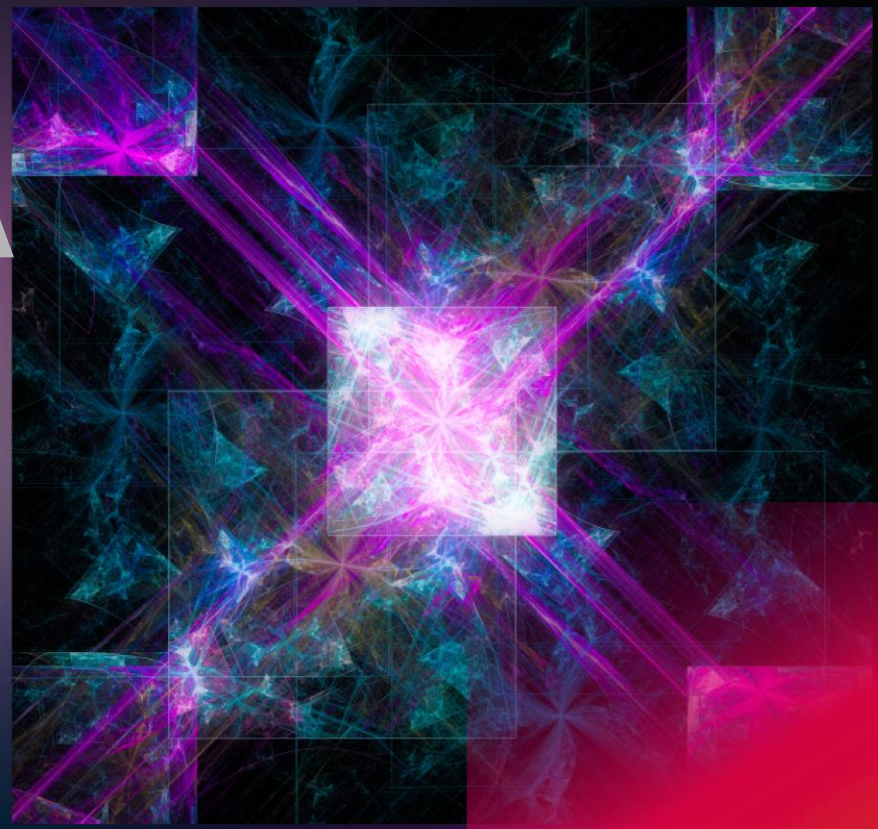
TROOPERS CONFERENCE IN 2024
TROOPERS
JUNE 24TH TO
JUNE 28TH, 2024

semperis

WELCOME

So You Performed A Forest Recovery. How Do You Reconnect Your AD Again With Azure AD? – THE SEQUEL



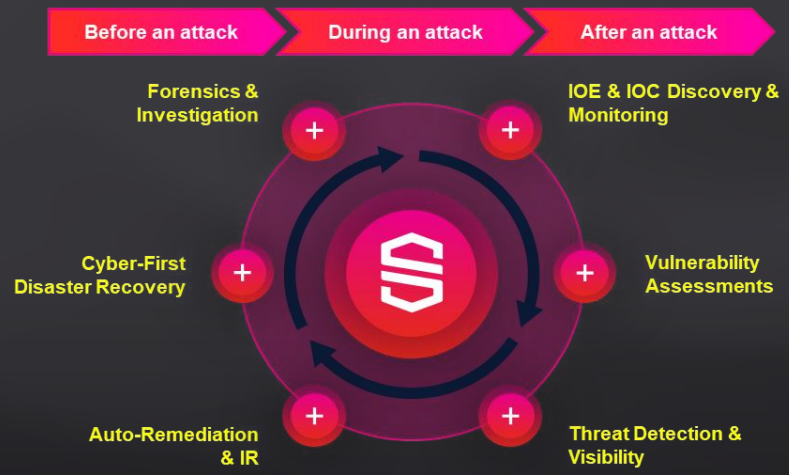
Jorge de Almeida Pinto

Senior Incident Response Lead, SEMPERIS

jorged@semperis.com

Introducing Me, Myself & I! ...And Semperis

semperis



Microsoft MVP Most Valuable Professional

Jorge de Almeida Pinto Senior Incident Response Lead	
LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter
Website	https://www.semperis.com/
Blog	https://www.semperis.com/blog/
Podcast	https://hipconf.libsyn.com/
Contact	jorged@semperis.com

- Architecting, designing, implementing and maintaining secure identity solutions
- Technology Focus: Identity, Security And Recovery
- Product Focus: AD, ADFS, Entra Connect/Cloud Sync, FIM/MIM, Entra (ID) Technologies.

semperis

WHAT ARE WE GOING TO TALK ABOUT?

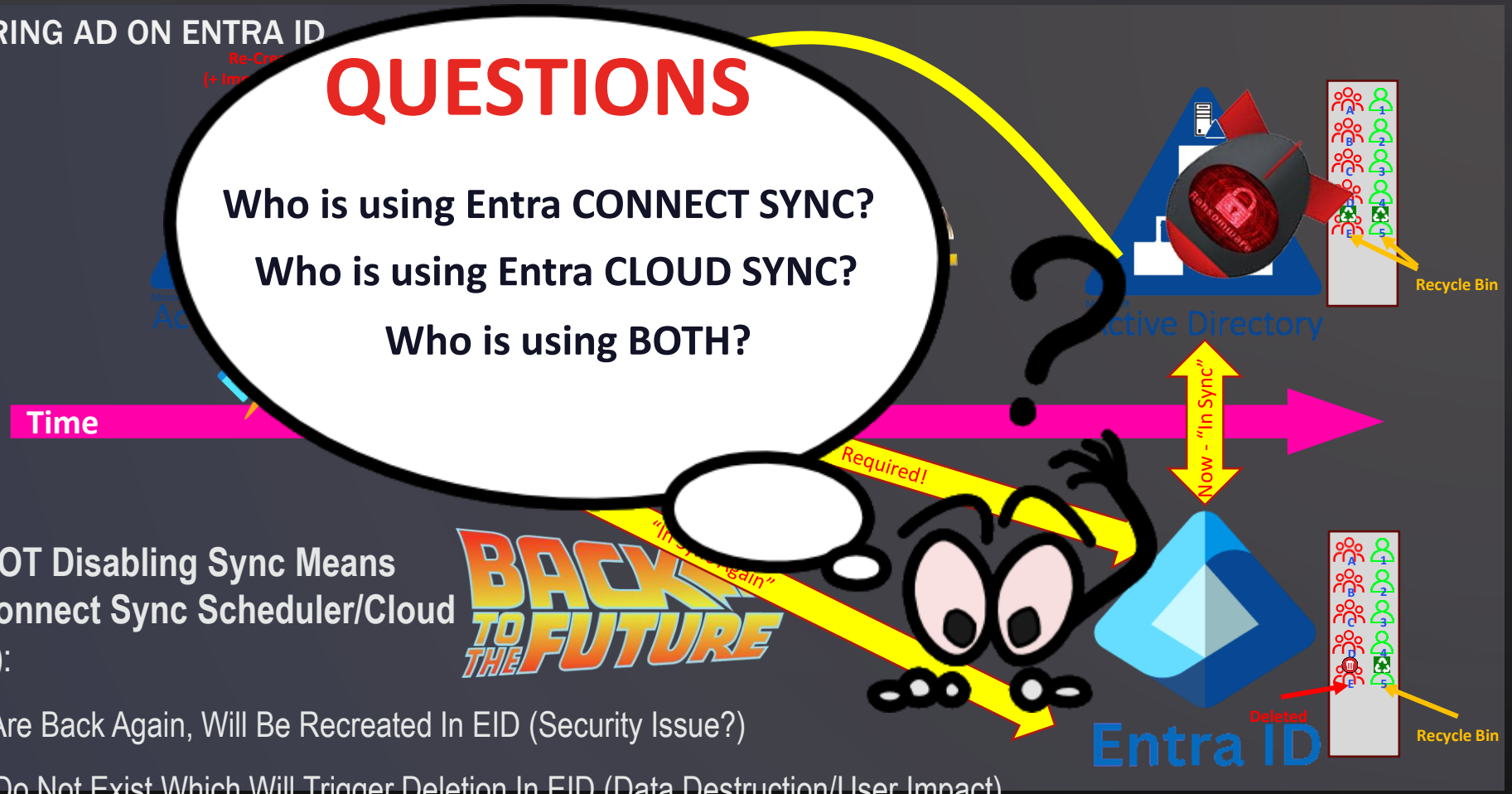
Agenda

1. Introduction / Recap
2. The Process In Steps
3. Details To Be Aware Of
4. Demo Setup
5. The Real Thing – DEMO!

Introduction / Recap
> *The Facts*

semperis

IMPACT OF RECOVERING AD ON ENTRA ID



JUST Reenabling Sync OR NOT Disabling Sync Means (REMARK: Assumed Entra Connect Sync Scheduler/Cloud Sync Config Is Still Enabled!):

- Previously DELETED Objects Are Back Again, Will Be Recreated In EID (Security Issue?)
- Previously CREATED Objects Do Not Exist Which Will Trigger Deletion In EID (Data Destruction/User Impact)
- Members re-added (security issue?)/removed (loss of functionality?) from synched groups

THEREFORE: Disable Sync (Connect Sync) Or Disable Configuration (Cloud Sync) Before Forest Recovery!

Introduction / Recap
> *The Facts*

semperis

THE PREFERRED BACKUP – WHICH ONE AND WHY?

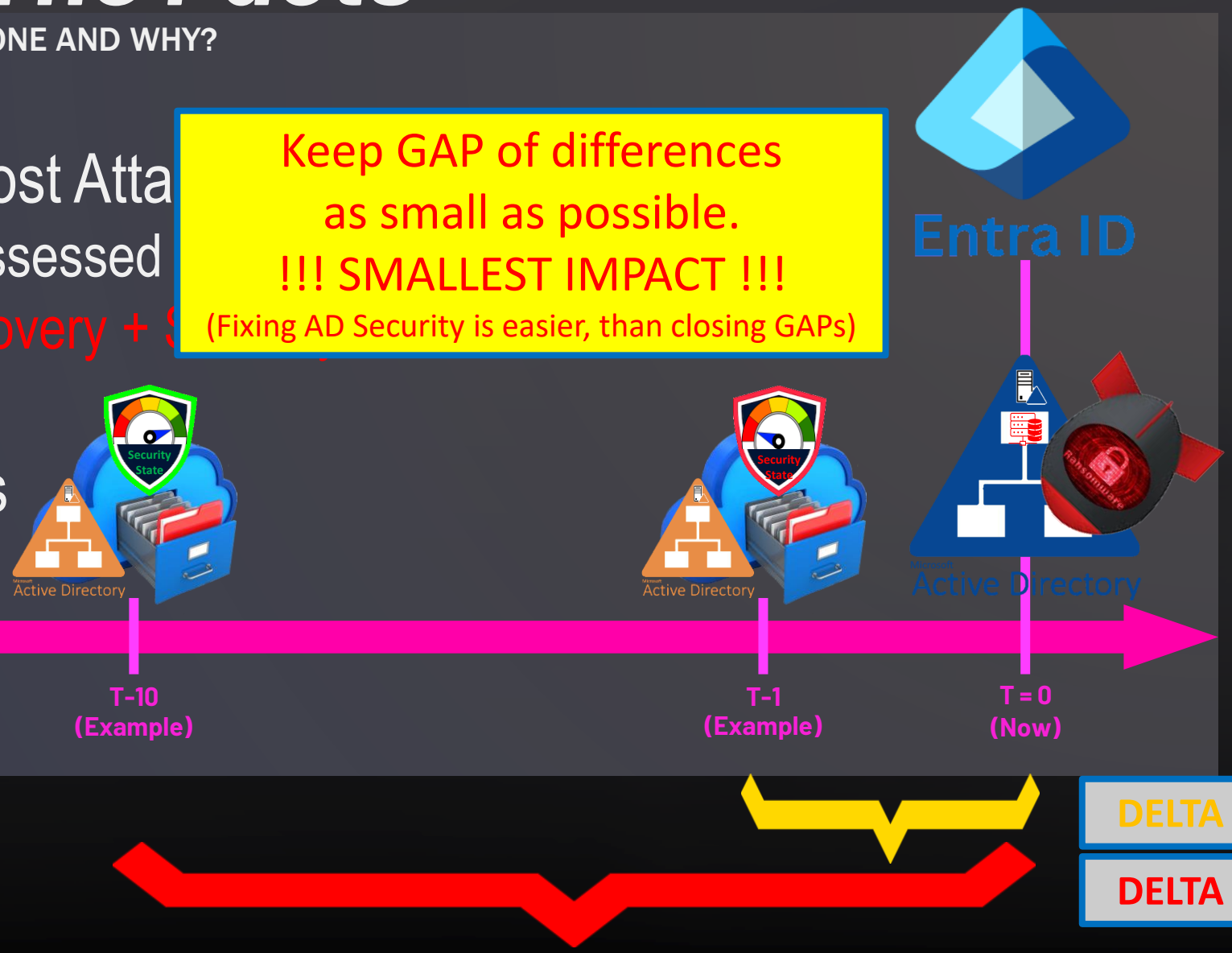
- Any Chosen Backup – Post Atta
  - AD Security MUST BE Assessed

  Going To Production = Recovery + S

- Fix Changes/Mismatches In Restored AD Between "Today" And…
  - Most Recent AD Backup

  Or
  - 10 days Old AD Backup

Keep GAP of differences
as small as possible.
!!! SMALLEST IMPACT !!!
(Fixing AD Security is easier, than closing GAPs)



The Process In Steps
> *Detailed Steps - Start 2 End*

semperis

semperis

Details To Be Aware Of
> *The Facts*

- Forest Recovery (FR) → AD goes back in time
- AD is authoritative, but due to FR, EID knows more than AD itself
- Identity data needs to be "fixed" in AD
- Possible impact of not doing this → absence of objects in AD causes the deletion of objects in EID
- EID Recycle Bin: Users ONLY! Still impacts user productivity
- WHEN to start THIS process? → FR? Start getting the data from EID!

semperis

Details To Be Aware Of > *"Fixing Data" (1)*

- Main Goal:
  - Prevent deletion of objects In Entra ID
  - Prevent deletion (and addition?) of relations (memberships) in Entra ID
  - NOT to restore object IN FULL in AD! → Enrich with IdM/IAM System!

semperis

Details To Be Aware Of > *"Fixing Data" (2)*

- Recreating missing objects, populating synched attribute data, reestablishing relationships between objects (e.g. group memberships)
  - "immutable ID" needed to relink recreated objects from AD to EID
    - MSFT Graph exposes immutable ID (sourceAnchor) for USERS, but NOT for CONTACTS, GROUPS, DEVICES
    - DirSync API exposes the immutable ID (sourceAnchor) for USERS, CONTACTS, GROUPS, DEVICES.
  - DirSync API → Used as main source for almost all attributes
  - Enriched by MSFT Graph API data for reference attributes
  - Non-Synched Attribute Data → Enrich with IdM/IAM System!

semperis

Details To Be Aware Of
> *Points Of Attention (1)*

- “Contact” in EID can be a “contact” or “user” in AD
- “User” in EID can be a “user” or “inetorgperson” in AD
- Multiple AD domain forest? For users, groups & computers possible to determine AD domain. Not possible for contacts (No SID and/or DN)
- Synching groups from AD to EID? EID can’t tell what the group scope was (Universal, Domain Local, or Global) (Hint: membership rules!)
- Fixing group memberships? Adding members is OK. Removing members is tricky! (Hint: EID only knows about synched members!)

semperis

Details To Be Aware Of
> *Points Of Attention (2)*

- UPN in EID may not be UPN in AD. For when using alternate logon ID
- Using synched Directory Extensions? Where is the data being sourced from? System owned attribute or writable attribute? → Check the name of the Directory Extension → Know your data model (i.e. sync rules)
- After fixing the data:
  - Enable data sync
  - Do not enable PHS → First SSPR + Writeback, then enable PHS
- Assumption: 1 AD forest ←→ 1 Entra tenant!

Demo Setup
> *Environment*

- Single AD domain forest (No exchange) + Entra Tenant (Basic/Free)
- CLOUD Sync: 1 OU in AD with 25 cnts/25 usrs/25 grps/refs
- CNNCT Sync: 1 OU in AD with 25 cnts/25 usrs/25 grps/2 cmps/refs
- PHS is used, no PTA, no fed. (does not matter for data, completeness)
- Immutable ID is ttribute)
- Cloud/Connect d EID.
- Connect Sync only: fixed/updated multiple sync rules

There is NO overlap!

Data is predictable/recognizable to be able to catch anomalies
(# of total & processed objects, memberships, etc)

Demo Setup
> *Components Used (1)*

- AAD INTERNALS (THANK YOU Nestori Syynimaa, a.k.a. @DrAzureAD)
  - Get required data from DirSync API
  - Considered malware by e.g. Windows Defender (and probably others)
- Solution:
  - Copied required functions into separate script (needs to be prettyfied!), fixed bugs in functions and added additional functions to support work
- Additionally
  - MSFT Graph used to get data for references between objects

semperis

Demo Setup
> *Components Used (2)*

- Storing the data from EID - Requirements:
  - Get it only once as it can take some time (do it right after decision of FR!)
  - Export to CSV, XML, JSON: too cumbersome to manage
  - Needed DB-like solution for queries/updates, taking lots of data into account. SQL = too heavy → Something more lightweight!
- Possible Light Weight Solution(s):
  - LiteDB (LiteDB, LiteDB.Studio, PSLiteDB) ← Used in THIS session/demo!
  - SQLite (SQLite, SQLiteBrowser, PSSQLite)

Demo Setup
> *Blog Post & The Code*

semperis

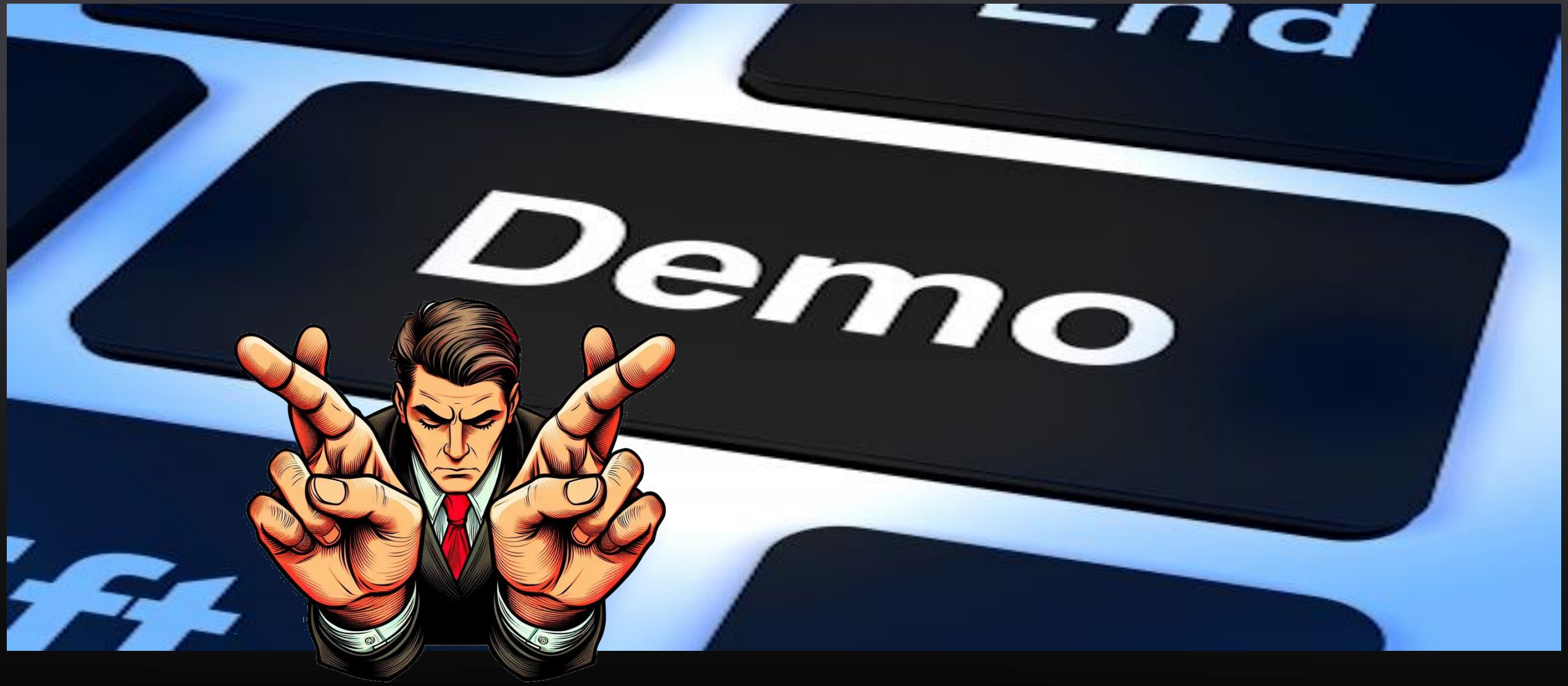
← Blog Post Will Be Available Through:

https://jorgequestforknowledge.wordpress.com/

Get The DEMO Code From: →
https://github.com/zjorz/Public-EID-AD-GAPAndFix

semperis

The Real Thing
> *DEMO!*



semperis

ANY QUESTIONS?

THANK YOU!

Jorge de Almeida Pinto Senior Incident Response Lead	
LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter
Website	https://www.semperis.com/
Blog	https://www.semperis.com/blog/
Podcast	https://hipconf.libsyn.com/
Contact	jorged@semperis.com