SecTalks Canberra
10/09/2019

Twitter/Github/Instagram: @joflixen

Maltego

WHO WHEN WHAT WHERE HOW WHY

Malt-WHO-ego?

- Paterva
- South African (Based in Pretoria)
- Started by Roelof Temmingh
- Make Maltego Software itself
- Trainerising using Maltego
- Solutioneering with Maltego

Malt-WHEN-ego?

...did it come about

- Originally released as Paterva Evolution
- Renamed Maltego in July 2007 due to Novell Trademark
- Commercial Version 2.0 released May 2008
- CE released with BackTrack 3.0 in June 2008
- Transform Distribution Server launched August 2010
- CaseFile is released with version 3.1 in 2012
- Transform Hub introduced in 2015
- Maltego eXtra Large released in 2016
- Unified Client released October 2017

Malt-WHAT-ego?

…is it this thing

- Maltego Client
  - Maltego Community Edition — Free as in Beer
    - 12 results per transform, 10K entity limit
  - Maltego Classic — $999US ($499US/year)
    - 10K results per transform, 10K entity limit
  - Maltego eXtra Large — $1999US ($999US/year)
    - 64K results per transform, 1,000K entity limit
- Server Editions — Start from $40,000

Malt-WHAT-ego?

…does it do for me

- Maal Tee Goh
- Data Visualisation Tool
- Directed Graph Representation
- Search from an object type:
  - Local Transforms
  - Remote Transforms
- Import & Export Data (MTZ, Table, Image, XML)
- Cross-Platform, Java based (yeah sorry)

Malt-WHERE-ego?

...does it get used

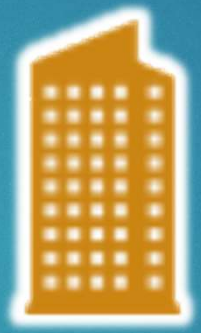
- Open Source Intelligence
  - Ingest public sources of information
  - People, Infrastructure, Organisations, etc...
- Tracking Artefacts & Information Forensics
  - Tracking Unique System Objects
  - Activists/Terrorism/Drugs/Crime
- Presenting Entity Relationships
  - Simple Hieratical Datasets (One-Way)
  - Compound and Complex Datasets (Two-Way)

Malt-WHERE-ego?

…are the pen-testing tools

- Red Canari v3 – Transform Prototyping tool
  - https://github.com/redcanari/canari3
- Sploitego – Query local Nmap, Metasploit, Nessus, etc
  - https://github.com/allfro/sploitego
- msploitego – Metasploit, Nikko, Enum4Linux, DNS scan
  - https://github.com/shizzz477/msploitego
- HackerTarget – Uses HackerTarget API (200 req/day)
  - https://github.com/peter-hackertarget/maltego_transforms
- Maltego Teeth - Installed in Kali by default

Malt-HOW-ego



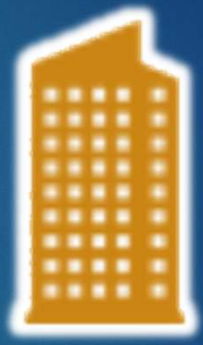
Company

SecTalks Canberra
10/09/2019

Twitter/Github/Instagram: @joflixen

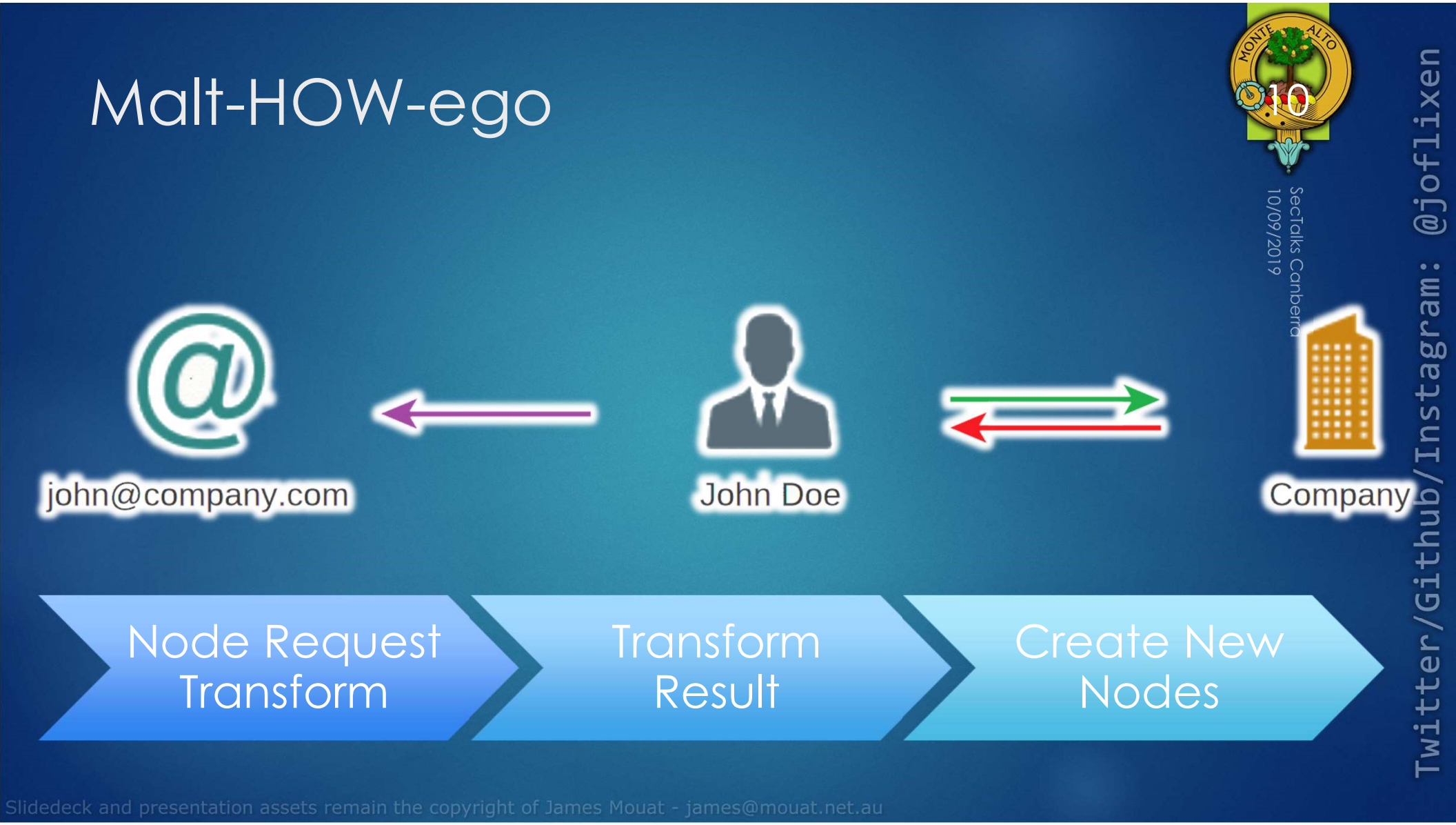
Malt-HOW-ego

John Doe



Company

Malt-HOW-ego



SecTalks Canberra
10/09/2019

Twitter/Github/Instagram: @joflixen

Malt-WHY-ego?

...why are you talking

- Get to the Demo...
- ...because...
- ...everyone loves a demo