CONTROL YOUR FUTURE

TANIUM CONVERGE 17

Offensive Cyber Hunting: Deploying Deceptive Tools And Tactics

Gregory Pothier

Offensive Cyber Hunting

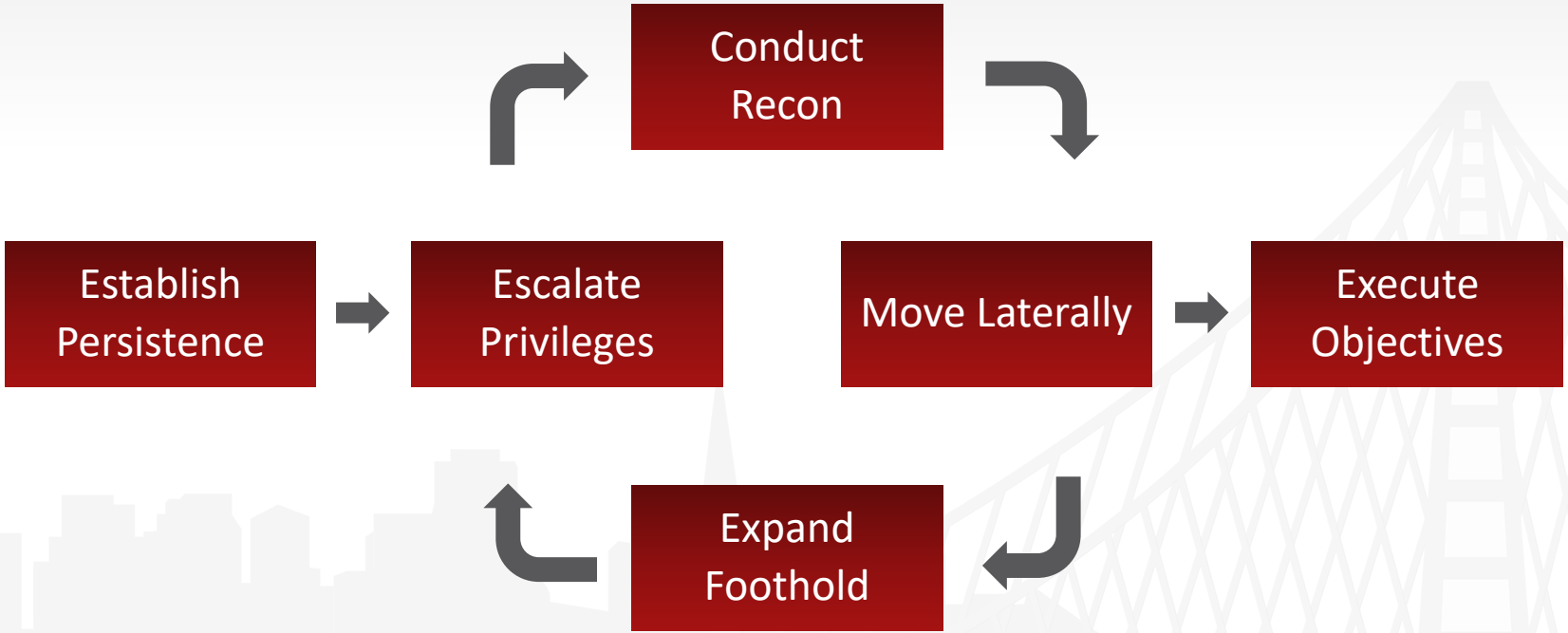
- About me

TANIUM

Objectives

- Introduction to Deception Tools and Tactics
- Overview of Cyber Attack Kill Chain
- Identify deployment and management of Deceptive Tokens
- Enjoy making life as difficult as possible for attackers

Cyber Attack Kill Chain



Trap Tokens

- Deploy and Manage Deception documents across the enterprise in seconds.
- Multiple layers of deception to snare attackers and insider threats:
  - Opening the document alerts via webhook
  - Set Traps within the Trap
  - Leverage Tanium Integrity Monitor and Trace

Trap Tokens

- Demo

TANIUM

Credential Memory Injection

- Insert Credentials into memory across the enterprise in seconds.
- Turn the tables on Mimikatz!

Credential Memory Injection

- Demo

TANIUM

NetBIOS-NS and LLMNR spoofing

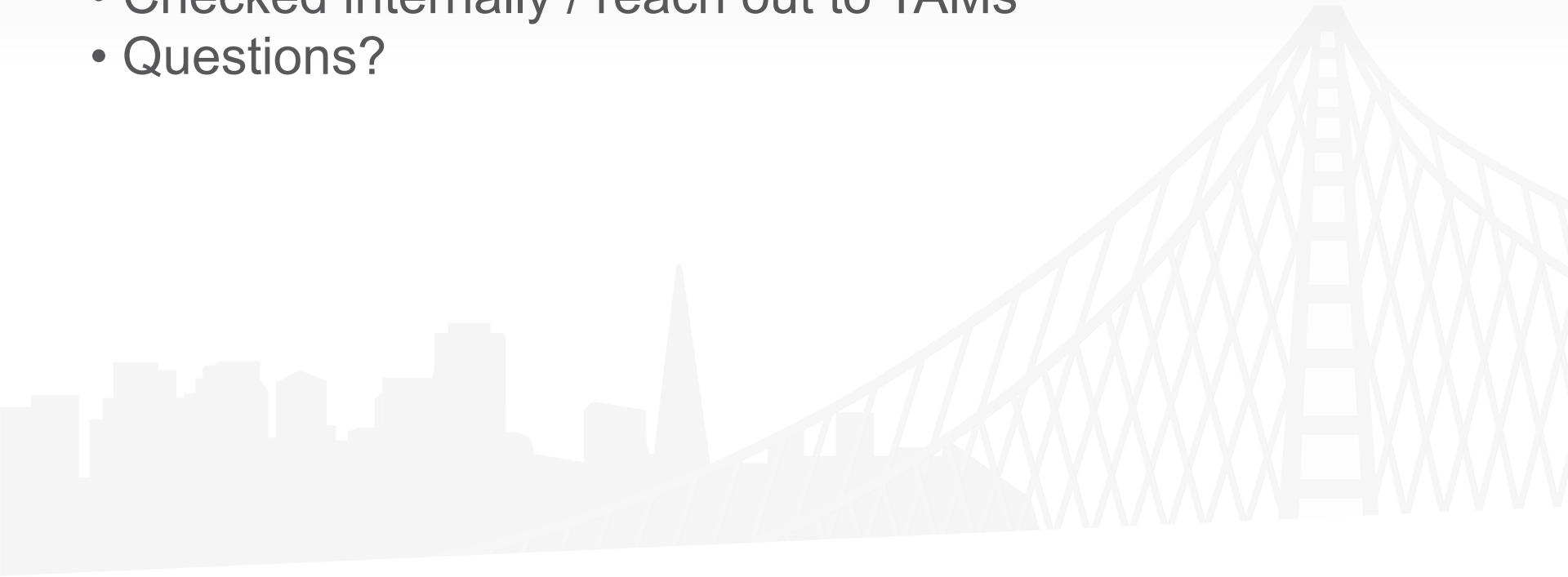
- NetBios-NS and LLMNR Spoofing is too easy
- Deploy to Trap requests to every broadcast domain

NetBIOS-NS and LLMNR spoofing

- Demo

Summary

- Checked internally / reach out to TAMs
- Questions?



TANIUM

CONTROL YOUR FUTURE

TANIUM

CONVERGE 17

Thank you for your time!