RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-R02

Using Deception and Forensics to Detect Threats from Within

Joseph R. Salazar

Sales Engineering Manager
Attivo Networks

#RSAC

Who said it?

Appear weak when you are strong,
and strong when you are weak.

About you (I assume…)

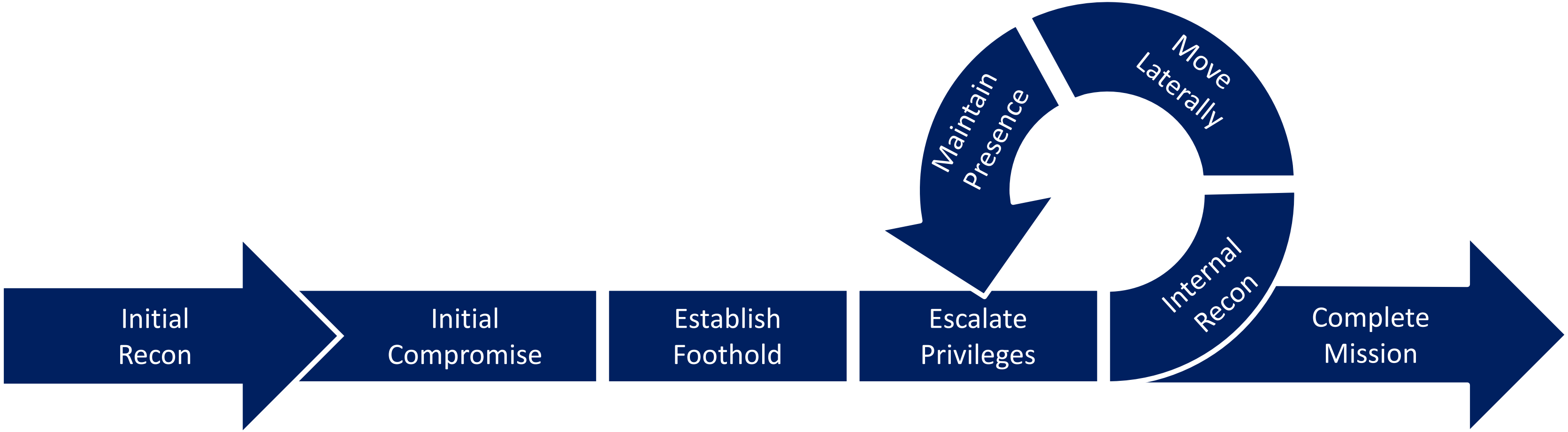
- You are somewhat familiar with current threats
- You have passing familiarity with deception technologies
- You are familiar with forensic technologies
- You want to improve your information security

Objectives

- To understand why breaches are so prevalent
- To show the value of deception technologies
- To explore how forensics can enhance security

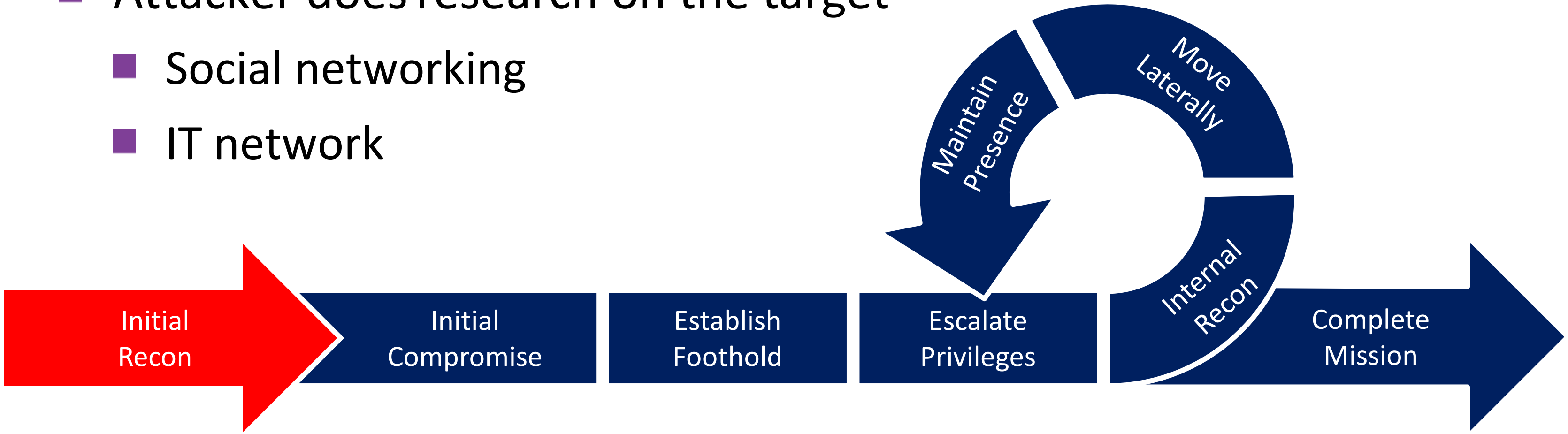
The Cycle of Pain

- Source: Infosecinstitute.org



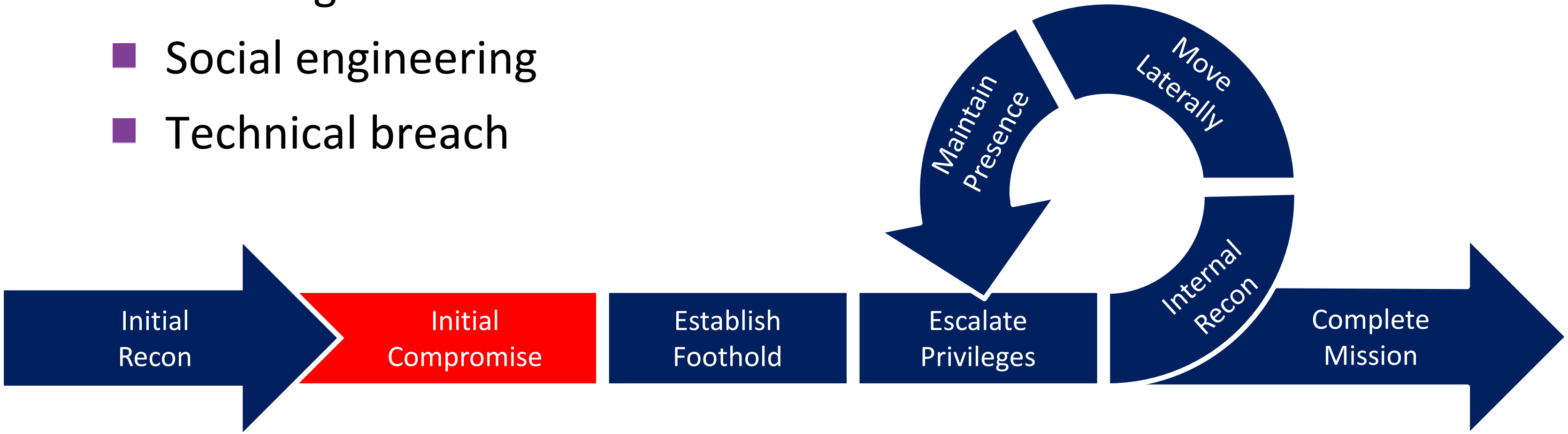
Anatomy of a Data Breach

- Initial Recon
  - Attacker chooses a target
  - Attacker does research on the target
    - Social networking
    - IT network



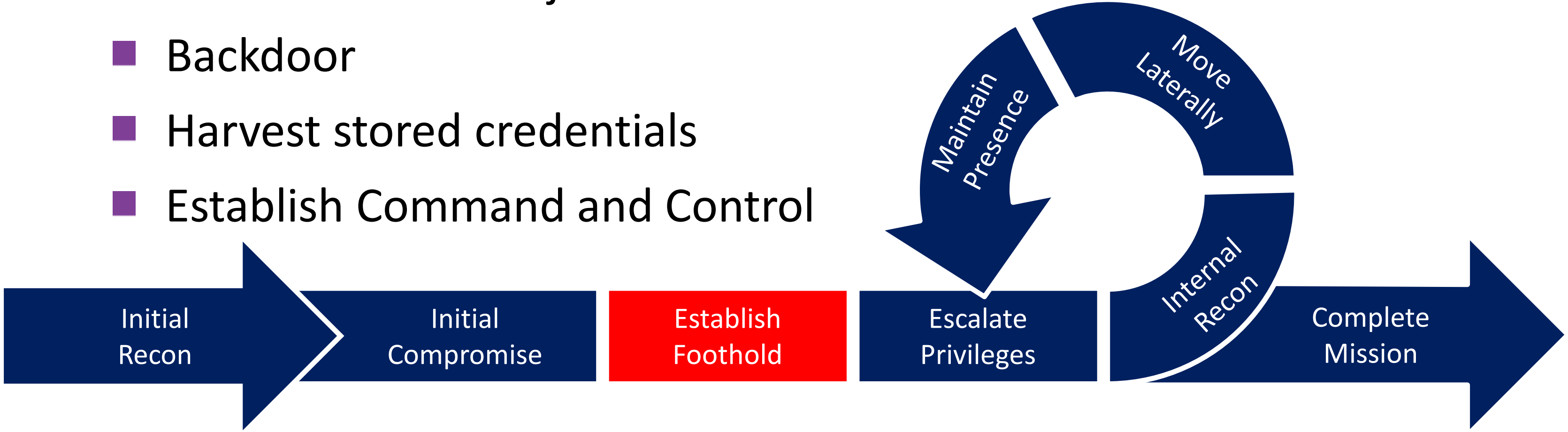
Anatomy of a Data Breach

- Initial compromise
  - Attacker compromises a system
    - Phishing attack
    - Social engineering
    - Technical breach



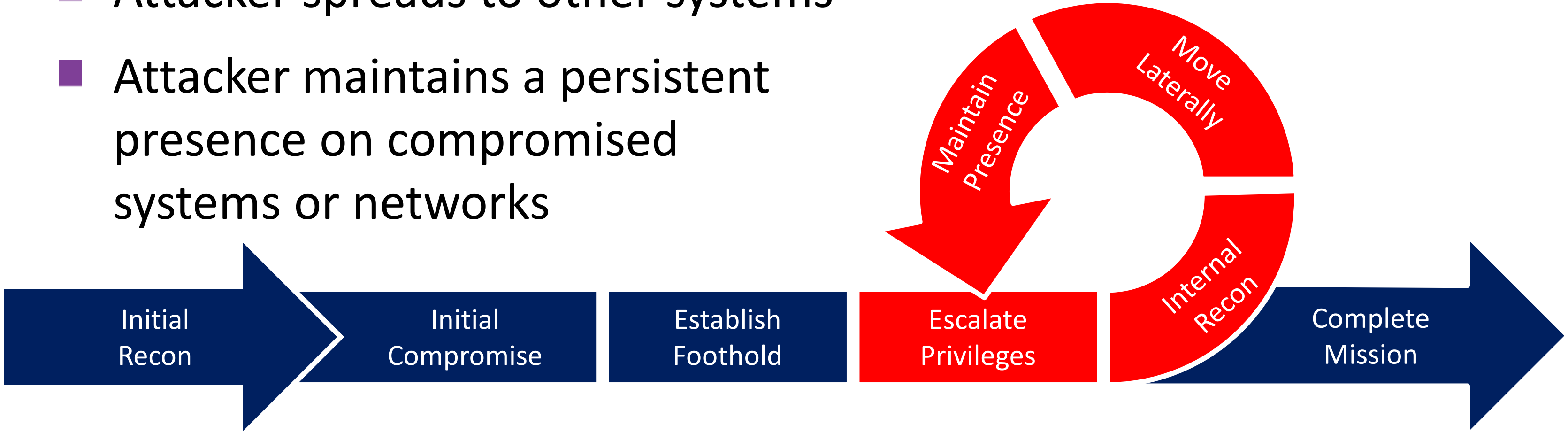
Anatomy of a Data Breach

- Establish a Foothold
  - Attacker installs malware on the compromised system
    - Remote Access Trojan
    - Backdoor
    - Harvest stored credentials
    - Establish Command and Control



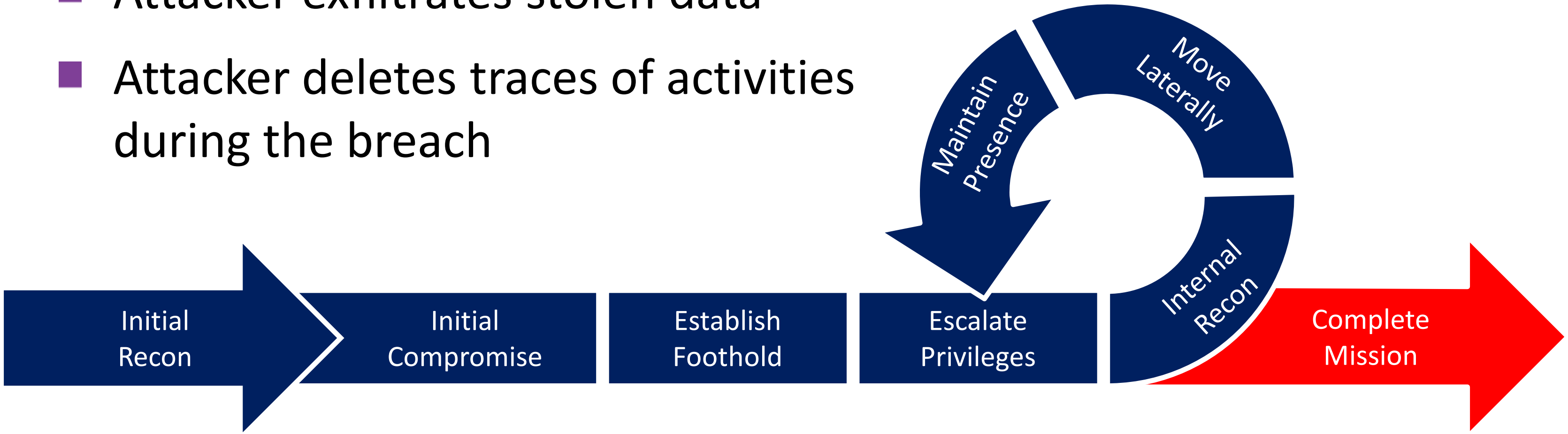
Anatomy of a Data Breach

- The Persistence Cycle
  - Attacker escalates privileges on the compromised system
  - Attacker spreads to other systems
  - Attacker maintains a persistent presence on compromised systems or networks



Anatomy of a Data Breach

- Complete mission
  - Attacker packages files for theft
  - Attacker exfiltrates stolen data
  - Attacker deletes traces of activities during the breach



Why are breaches so prevalent?

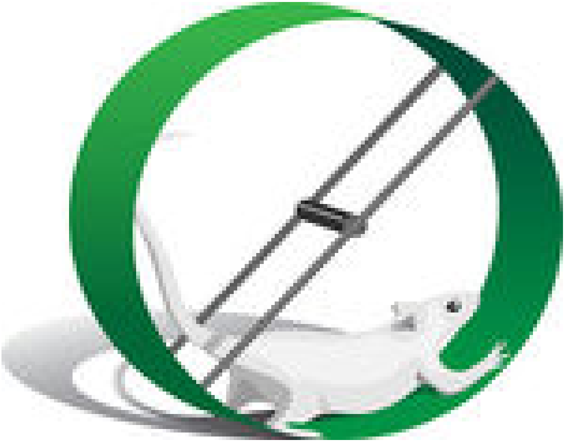
- Users are bad at security
- AV can’t keep up with new malware
- Unpatched vulnerabilities
- Distributed workforce and the porous perimeter

Users – the Weakest Link

- Bromium Survey – January 2015
  - end users are the biggest security headache
- Ponemon Institute Survey – 2015
  - more security incidents are caused by unintentional mistakes than by intentional and/or malicious acts

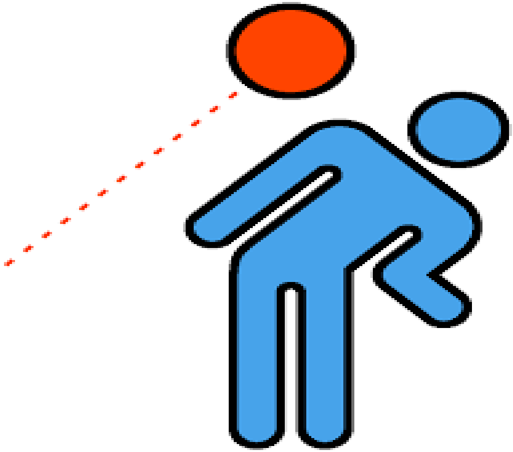
AV (in)effectiveness

- Imperva Hacker Intel monthly trend report #14, 2012
- Damballa research findings, October 2014
- Lastline labs report, May 2014, and April 2015



Malware Detection

- AV detection
  - Signature
    - File byte sequence
    - File hash
  - Heuristics
- Malware sandbox



Malware Detection Evasion

- Evading AV
  - Compression
  - Packaging and encoding
  - Encryption
  - Targeting
  - File-less execution

- Evading sandbox analysis
  - Delayed Onset
  - Sandbox hypervisor detection
  - Human Pulse detection

Vulnerabilities and the porous perimeter

- Complex software has undisclosed vulnerabilities
  - Zero days
  - Malware economy
- Distributed workforce
  - “free” wi-fi

Discussion No. 1

If an attacker succeeded today, would you know?

What is Deception?

- **Military deception** refers to attempts to mislead enemy forces during warfare, usually by creating or amplifying an artificial fog of war through disinformation and other methods.
  - Wikipedia

Deception in Information Security

- The assumption: No one should legitimately be communicating with your deception assets
- Deceive and detect
- Deception mechanisms
  - Honeypots
  - Honeynets
  - Honeytokens

Honeypots

- Types
  - Production
  - Research
- Categories
  - Low-interaction
  - High-interaction
  - Pure

Honeynets

- "A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated."
  - Lance Spitzner, founder of the Honeynet Project, in his 1999 paper "To Build a Honeypot“.

Honeytokens

- Non-production pieces of data
- No prevention of data tampering
- Indicates that data integrity has been compromised

Discussion No. 2

Who here is
using deception in
their networks
right now?

Traditional Deception as Network Security

- Distracts attackers from sensitive production assets
- Decreases likelihood of attacker finding a legitimate production asset
- Increases likelihood of detecting internal scans
- Understand what data was breached

Modern Deception for Intelligence

- Provides threat intelligence and insight
  - Tactics/techniques/procedures
  - Targets/motives
- Integration with security devices

What is computer forensics?

- **Computer forensics** (sometimes known as **computer forensic science**) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media.
  - Wikipedia

Discussion No. 3

Who here uses forensics on a regular basis?

Forensics and malware incident response

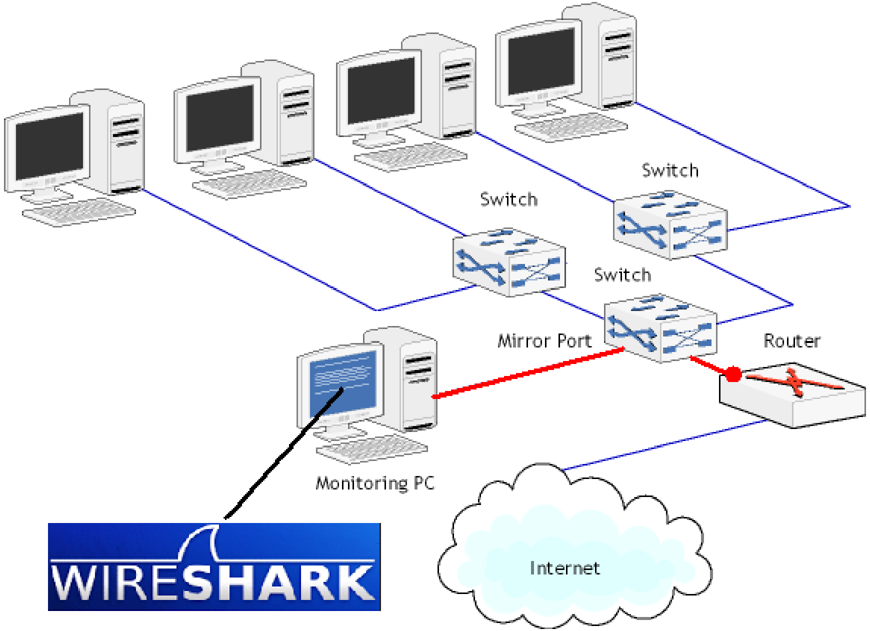
- Positive identification of infected systems
- Post infection malware analysis
- Identify affected data

What about network forensics?

- **Network forensics** is a sub-branch of digital **forensics** relating to the monitoring and analysis of computer **network** traffic for the purposes of information gathering, legal evidence, or intrusion detection.
  - Wikipedia

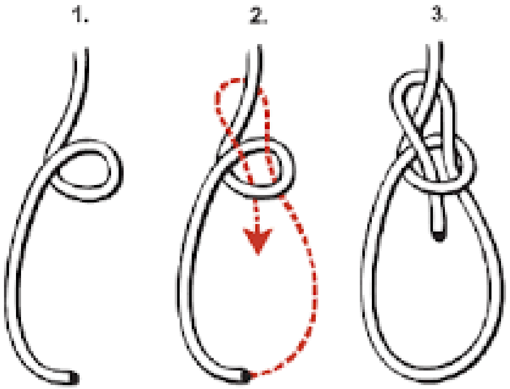
Discussion No. 4

Who here currently has network forensics capabilities?



Tying forensics with deception

- Host forensics on a deception asset
- Network forensics on networked deception assets
- Threat intelligence
  - Host change tracking
  - IOCs
  - PCAPs



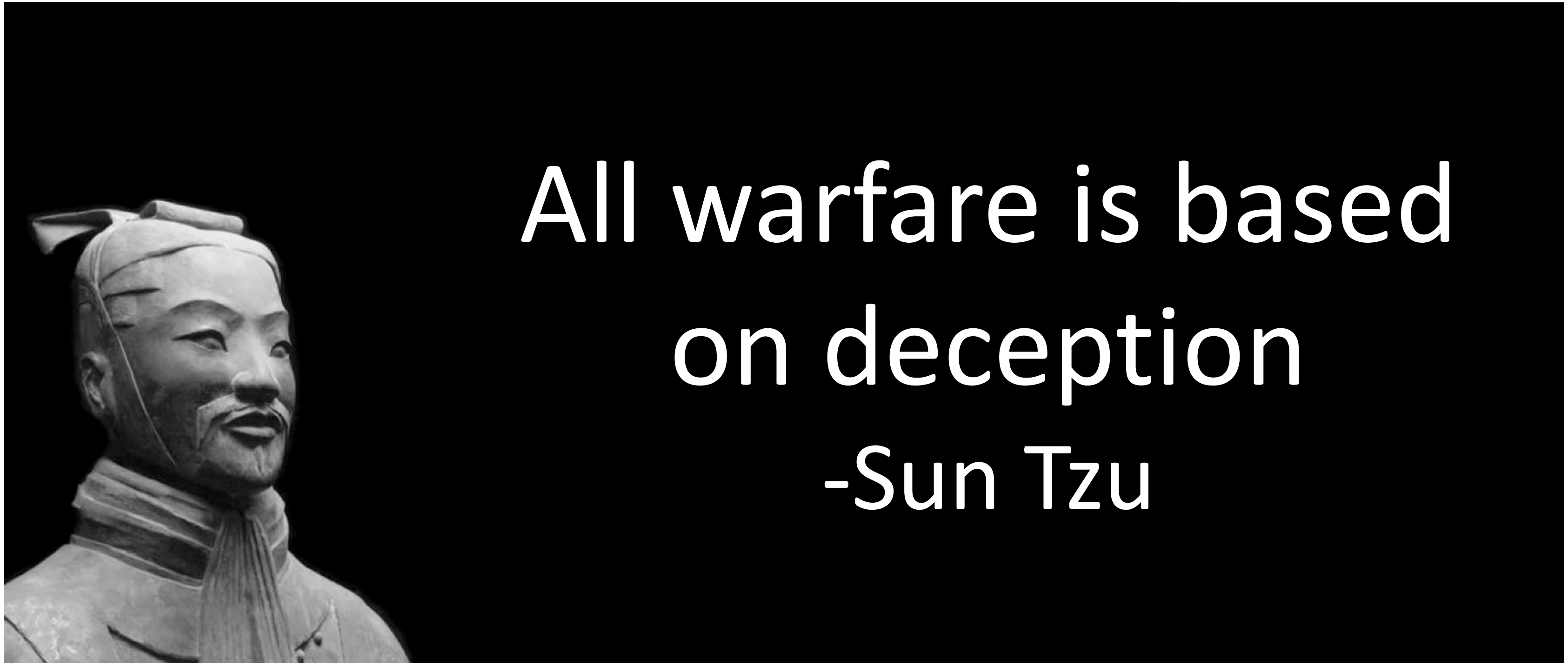
Wrapping it up (the quiz at the end)

- Why are breaches so prevalent?
- What can deception do for you?
- What can forensics give you?

Applying this back home

- Next week you should:
  - Identify gaps in your internal visibility and threat intelligence
- In the first three months following this presentation, you should:
  - Evaluate deception and forensics solutions to bridge those gaps
- Within six months to a year, you should:
  - Deploy deception and forensic solutions that meet your requirements

Parting Shot



All warfare is based on deception

-Sun Tzu

Questions?

Joseph R. Salazar
Sales Engineering Manager
Attivo Networks

jsalazar@attivonetworks.com