Introduction to Threat Deception for Modern Cyber Warfare

Joseph R. Salazar | Technical Deception Engineer
CISSP, CEH, EnCE

AGENDA

Introduction

Attacker Playbook

The Need for Deception

Deception as Detection

Myths and Realities

root@kali:~# whoami

Joseph R. Salazar

- Information Technology since 1995
- Information Security since 1997
- Major, USAR (retired) with 22 years as a Counterintelligence Agent, Military Intelligence Officer, and Cyber-Security Officer
- CISSP, CEH, EnCE

A Peek at an Attacker's Playbook

Attacker assumes he has time, has unlimited attempts, and can move slowly through the network to avoid detection

Attacker moves laterally inside the network and escalates privileges to reach critical assets

Attacker assumes all information found is real; deceptive data is not expected

Detection Gaps Create Open Doors for Attackers

Most perimeter & end-point security solutions cannot reliably detect the following attack vectors

HTTPS bypasses network security

Zero-day exploitation

Stolen employee credentials

End-point/ BYOD

Active Directory reconnaissance

Breaches can take ***months*** before being detected

Deception as a Method of Detection

The Entire Network Becomes A Trap And A Hall Of Mirrors

Obscures the Attack Surface; Disrupts Attacker

Deception to Divert Attacker's Attention

- Decoy systems to misdirect attacker
- Deception credentials and bait lure attackers

Deception Forces the Attacker to Have to Be Right 100% of the Time.

Deception, for Better Detection Against Better Attackers

VS

Other Detection Methods

- Firewall
  IDS
  Proxy
  AV
- Network
  Anomaly
  Detection
- UEBA
- SIEM
- Hunt
  Teams

THREAT DECEPTION: EARLY, ACCURATE, EFFICIENT

ACCURATELY DETECT KNOWN & UNKNOWNS

DETECT ACROSS ALL ATTACK SURFACES

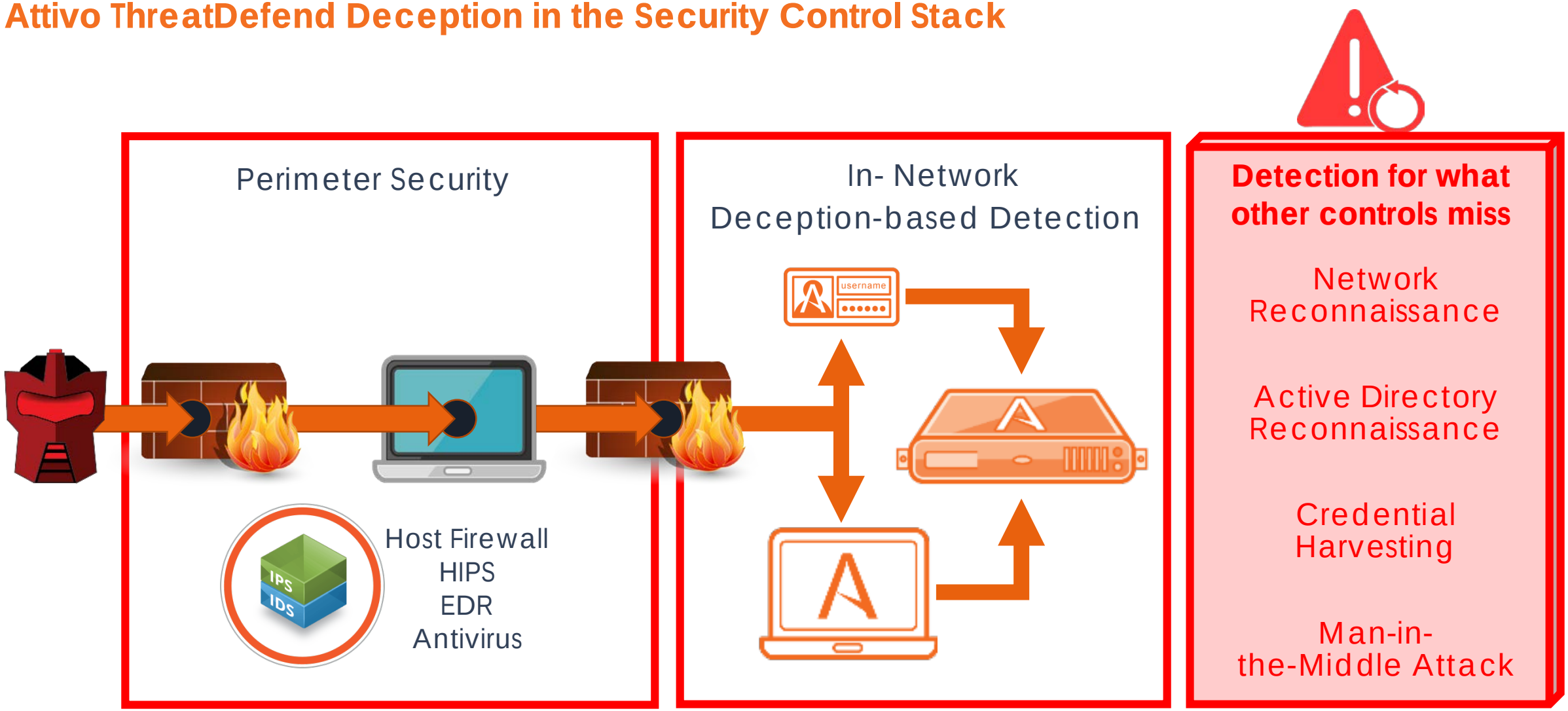
HIGH-FIDELITY ALERTS WITH FORENSICS

EASY, SCALABLE OPERATIONS

- SLOWS DOWN AND RAISES COST TO ATTACKERS -

Reduce Dwell Time & Close Detection Gaps

Attivo ThreatDefend Deception in the Security Control Stack



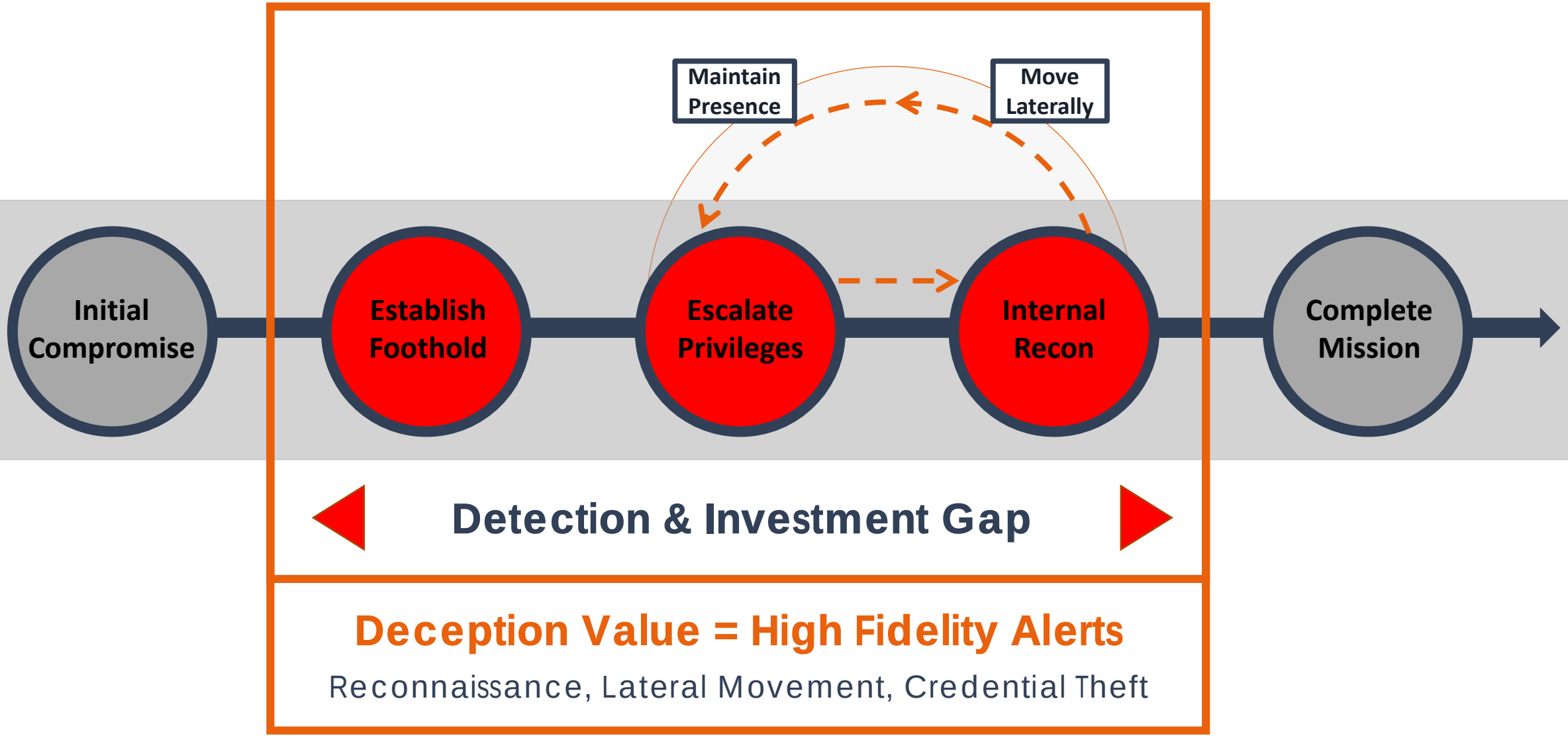
Deception for Closing the Detection Deficit

Efficient, Scalable, In-network Threat Detection that changes Asymmetry of Attack

Challenges	Deception-Based Solution to Close the Gap
Lateral Movement Threat Detection	In-network: Recon, Credential Harvest; Slowing of Attack
Credential Theft Based Attack	Detect Endpoint & Domain Credential Theft; Attack Path Visibility
Ransomware	Detection, Analysis, Interaction to Slow Attack
Evolving Attack Surface	User Networks, Datacenters, Specialized (SCADA, IoT, POS, SWIFT, Telecom, Router Decoys), Cloud (AWS, Azure, OpenStack)
Compliance, Breach Investigation, M&A Visibility	Compliance and Forensics; Pen Test, Evaluate Latent Threats
Skills Shortage and Ability to Respond to Incident	Easy to Deploy and Operationalize Automated Attack Analysis and Incident Response

Closes the Detection Gap with Accurate Detection and Threat Visibility

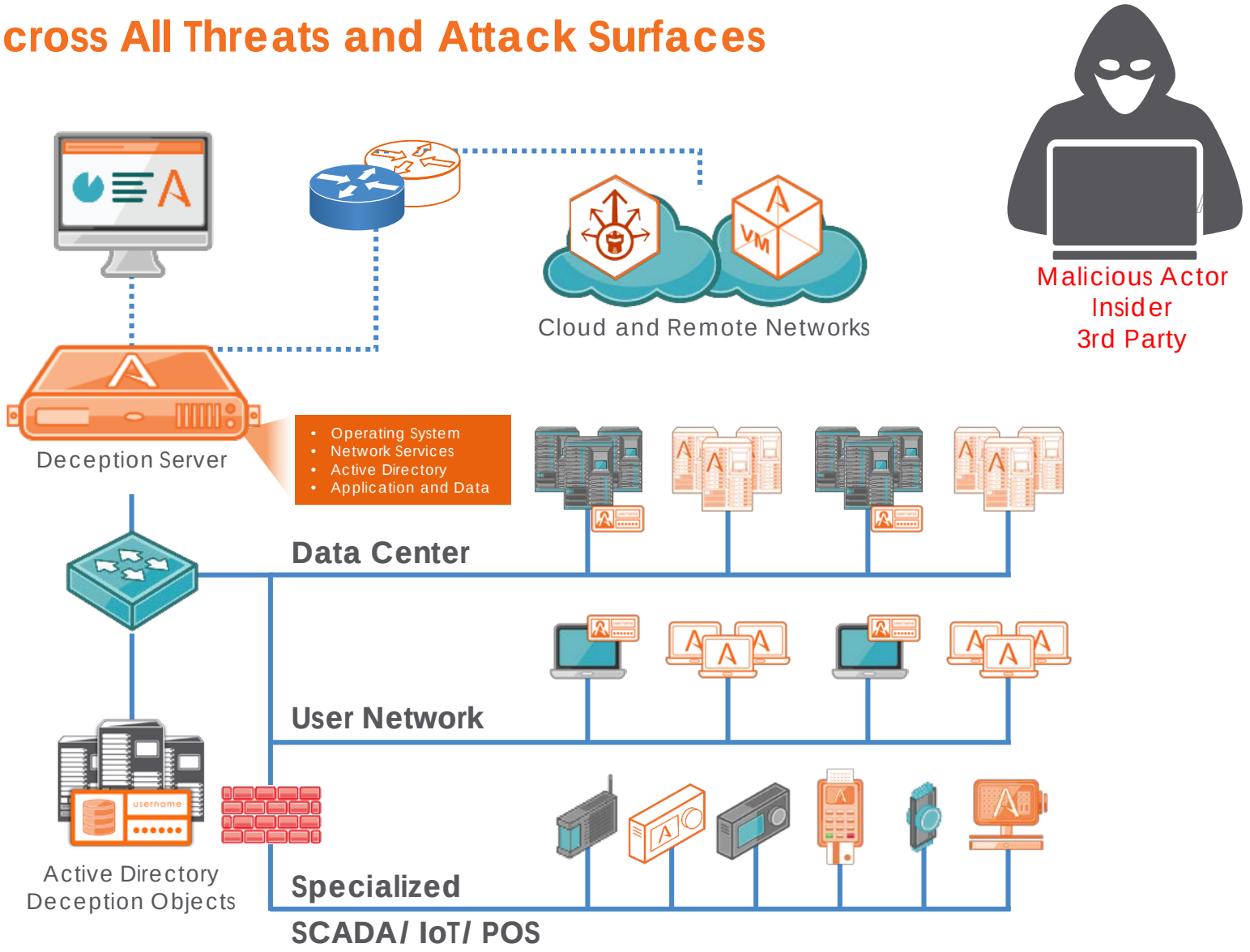
Deception in the Attack Life Cycle



Deception-based Detection for Evolving Attack Surfaces

Entire Network Becomes a Trap Across All Threats and Attack Surfaces

1. Lateral Movement
2. Credential Theft
3. Ransomware
4. Active Directory Recon



Myth 1

100% Security is Achievable.

Reality 1

A Shift to Detection as a Security Control is Critical.

Detection for the Modern Day Attacker

Evolving Threats

Reconnaissance

Stolen Credential

Active Directory

Man-in-the-Middle

Evolving Attack Surface

Endpoint

Network & Campus

Data Center & Cloud

IoT, ICS, POS, SWIFT …

Myth 2

Deception is Just a Honeypot.

Reality 2

Only if you believe a horse and buggy is the same as a Tesla Model S.

Why Honey Pots are Not the Same as Deception

BOTs and Brute Force Attacker ⟵ Designed for ⟶ the Human Attacker

Myth 3

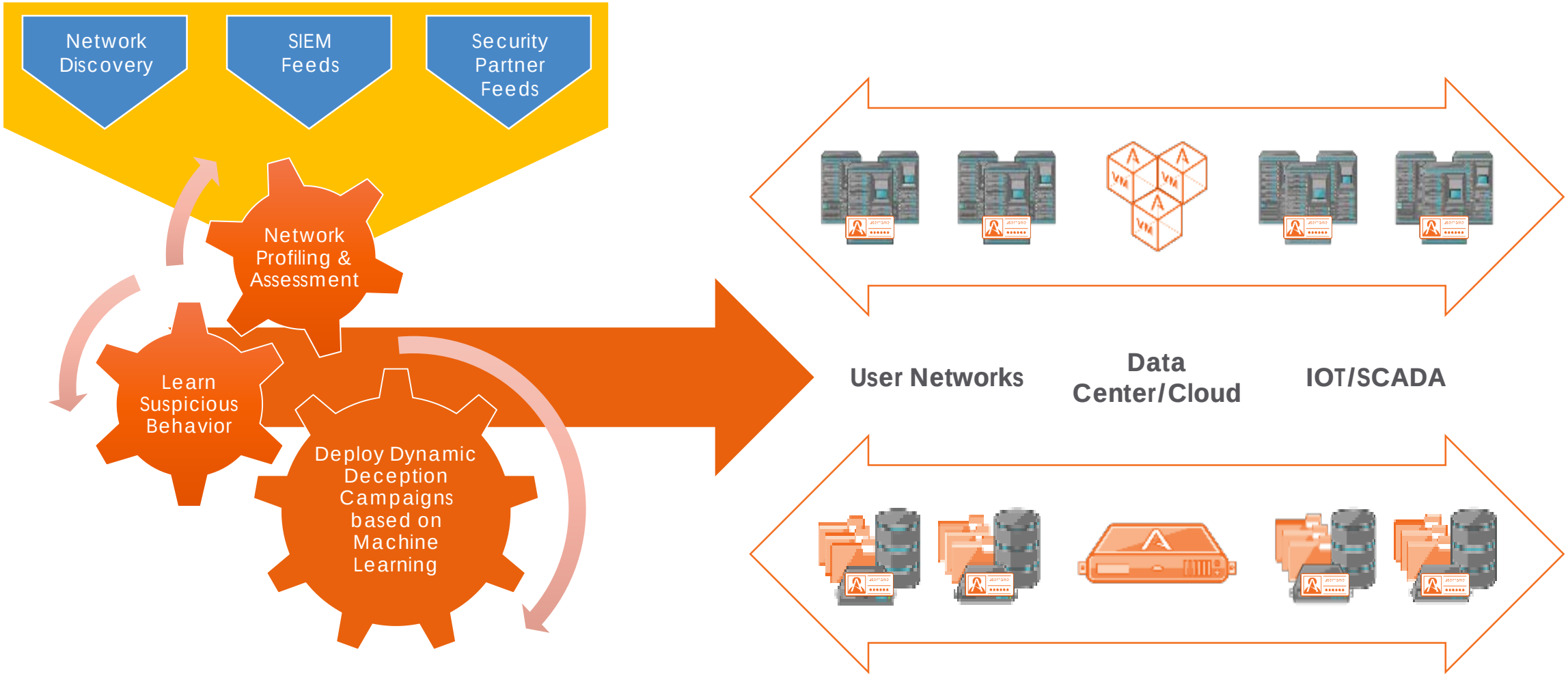
Deception is Hard to Deploy.

Reality 3

Machine learning and ubiquitous computing make deployment easy.

Adaptive Deception Campaign Deployment

Scalability and On Demand Ability to Change the Game Board on Attackers



1 Manual 2 Auto-Propose 3 Auto-Deploy

Myth 4

All Deception is Created Equal.

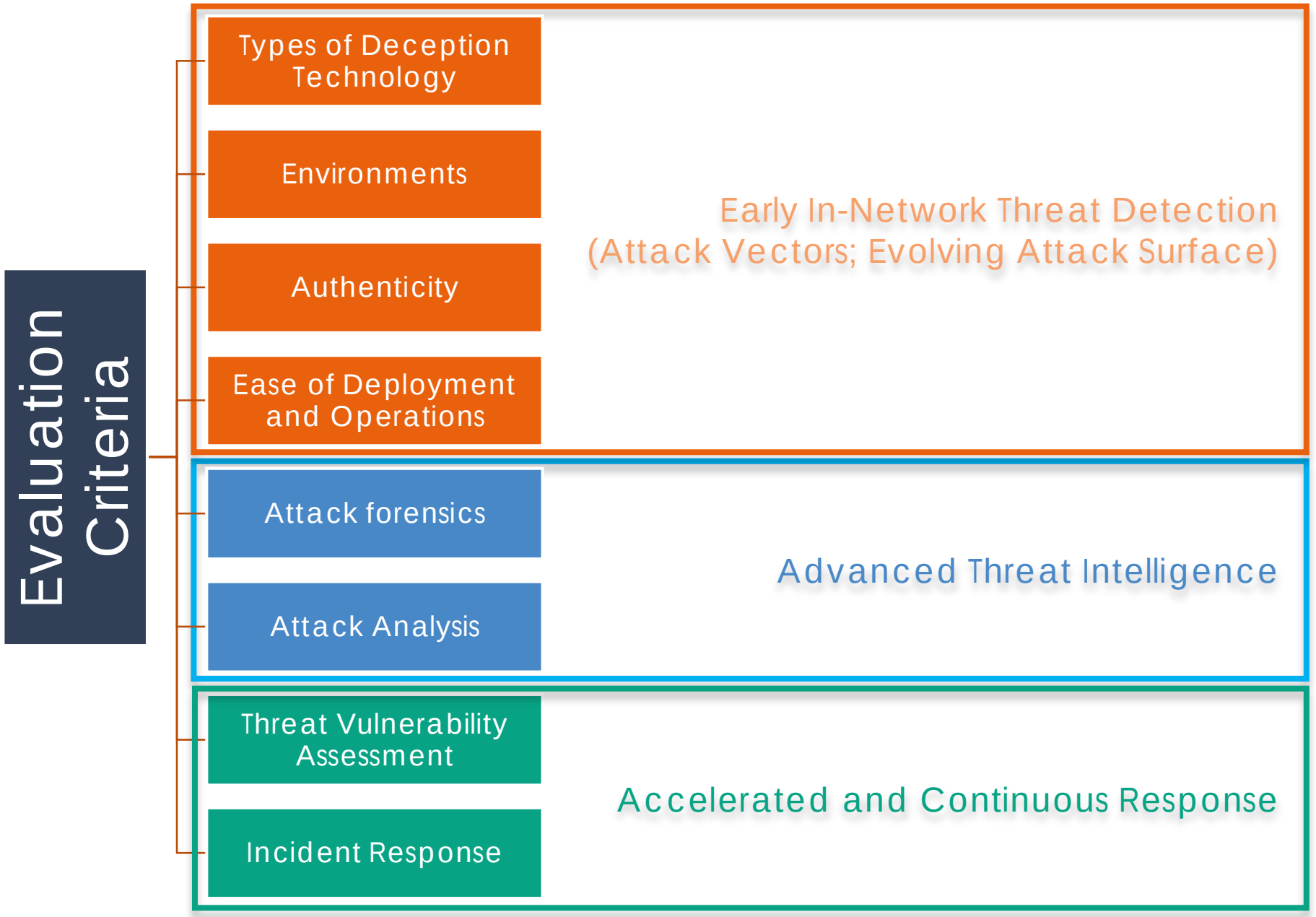
Reality 4

Solutions vary widely based on comprehensiveness, authenticity, attack analysis, and ability to improve incident response.

Not All Deception Technology Provides an Active Defense

	Enterprise Grade	Limited Functionality
Depth of Deception	Network, Endpoint, Application, Data	Only Network or EP
Authenticity	Real OS, Apps, Services, high interaction, Dynamic	Low interaction, emulated, static
Evolving Attack Surface	Network, DC, Cloud, Specialty IOT, ICS, POS, and more	Limited environments
Ease to Operationalize	Not inline; Agentless	Inline, reliant on agents
Attack Threat and Malware Analysis	Full sandbox and forensic reporting	Limited forensics and analysis
Simplifies Incident Response	Integrations for automated blocking, quarantine, hunting	No or limited automation
Attack Simulation & Threat Assessment	Attack path and replay visual maps, simulators	Partial assessment tools
	Built for the anticipating attacker	**Relies on the element of surprise**

Evaluating Deception Technology and Providers



Myth 5

It’s a “nice to have,” not a “need to have.”

Reality 5

Deception is customer proven to close the detection gap with early and accurate detection.

Organization Discovers Insider Threat

Concern

- The customer was concerned about internal risks to the network and sensitive client information.

Overview

- After installing the deception solution, security saw SMB share connections to multiple endpoints followed by recon scans.
- Network administrator with credentials had infected endpoints as zombies to scan network.

Outcome

- Only the deception solution efficiently and accurately detected the recon activity.
- Network administrator was terminated by customer and legal action are pending.

Value

The customer was able to monitor for insider threats and collect the necessary evidence to support legal action.

Mergers & Acquisitions Security Concerns

Concern

- The organization wanted visibility into the networks of recently acquired companies.
- They suspected the networks were compromised, had no dedicated security team, and lacked a mature security infrastructure.

Overview

- They deployed the deception solutions to the subsidiary networks for visibility, and a central manager in the cloud for reporting and alerting.

Outcome

- They were able to assess the network security infrastructure remotely, and validated their visibility by running Red Team tests in the acquired networks that they detected with the deception solutions.

Value

The organization assessed the security readiness of the acquired networks and resolved issues before connecting them to the corporate network.

Annual Penetration Testing for Compliance Validation

Concern

- Customer wanted to validate their network resiliency to meet annual security compliance requirements.
- The team had failed multiple penetration tests because of their inability to detect advanced, in-network threats.

Overview

- Customer installed deception solution for pen test.
- Pen tester compromised an endpoint, stole deceptive credentials, and engaged with deception solution decoy, thinking it was a real system.

Outcome

- The deception solution immediately detected when the pen tester used stolen credentials during the penetration test.
- The InfoSec team was able to track their every move.

Value

The customer successfully validated their security infrastructure resiliency for annual compliance requirements.

Myth 6

Deception Won’t Work Against Real Attackers.

Reality 6

Accurate, realistic, and authentic Deception can fool even the most experience attackers.

"From an environment perspective, looking at it from the network and Active Directory, everything looked legitimate. That's where most people will be coming from. It's likely they won't be able to decipher what is real and what is not, like I couldn't."

- Senior Penetration Tester
Pen-testing Attivo Deception

Compromised AD/Network Incident Response and Cleanup

Concern

- Attackers had been inside customer's network for years.
- Attackers compromised numerous servers including AD and the gift card portal with stolen credentials,
- Attackers created AD accounts to maintain access.

Overview

- Customer stealthily installed deception solution for network visibility and IR.
- Professional services engaged to help triage, respond, and remediate attacker presence across numerous environments.

Outcome

- The deception solution detected attacks to the Citrix environment, identified fraudulent AD accounts, and identified credentials used to steal gift card information.
- Final cleanup is ongoing with deception solution providing visibility.

Value

The customer used the deception solution for unparalleled network visibility to clean up the persistent presence without alerting the attacker.

Summary and Conclusions

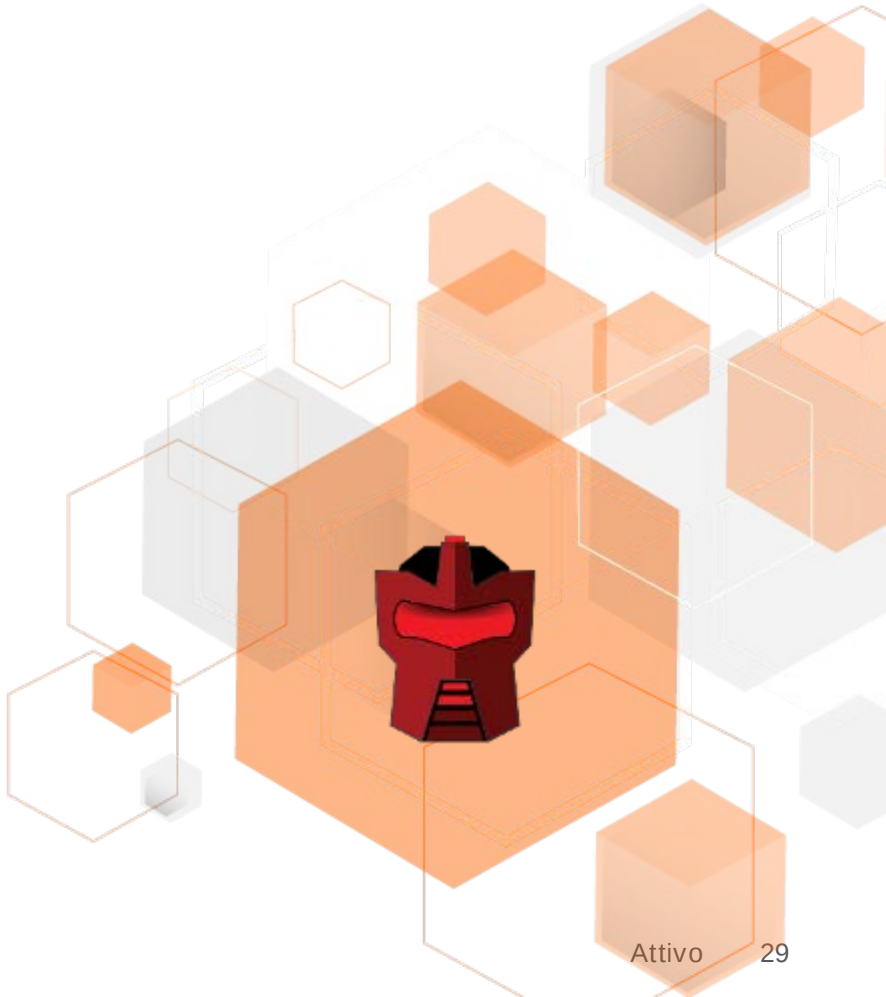
Summary

- Deception for Internal Threat Detection
- Myths and Realities
- Evaluating Deception Technology Differences
- Value of Deception

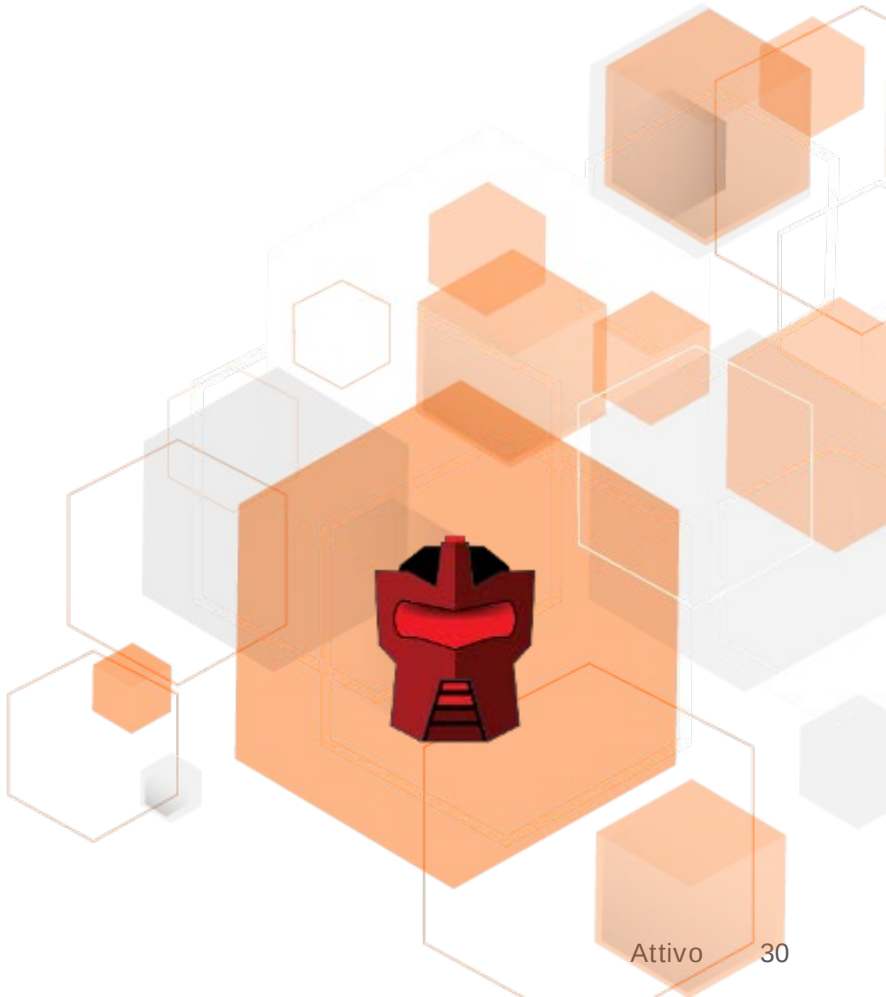
Conclusion

- Detection Efficiently Closes the Detection Deficit
- Deception Platforms are Not Created Equal
- Deception is a need-to-have technology that provides immediate and long-term value

Questions?



Let’s Keep in Touch!



Deceive. Detect. Defend.