RSAConference2017
Abu Dhabi | 7–8 November | Emirates Palace

POWER OF OPPORTUNITY

SESSION ID: SPO1-W04B

Deception for Defeating the Modern Cyberattacker

Ray Kafity
Vice President
Attivo Networks

Defeating the Modern Cyberattacker

Ray Kafity | Vice President

It's Not Enough to Think Like an Attacker

Defeating the Modern Cyber Attacker

1. Know how an attacker attacks
2. Know how to defend and respond

3. Understand the tools and techniques used to move laterally and compromise assets
4. Build an adaptive defense with attack sharing, incident response automations

Stands the Test of Time

Attacker is Surprised → Attacker is Anticipating → Counter-Intelligence

A View Through the Lens of an Attacker's Playbook

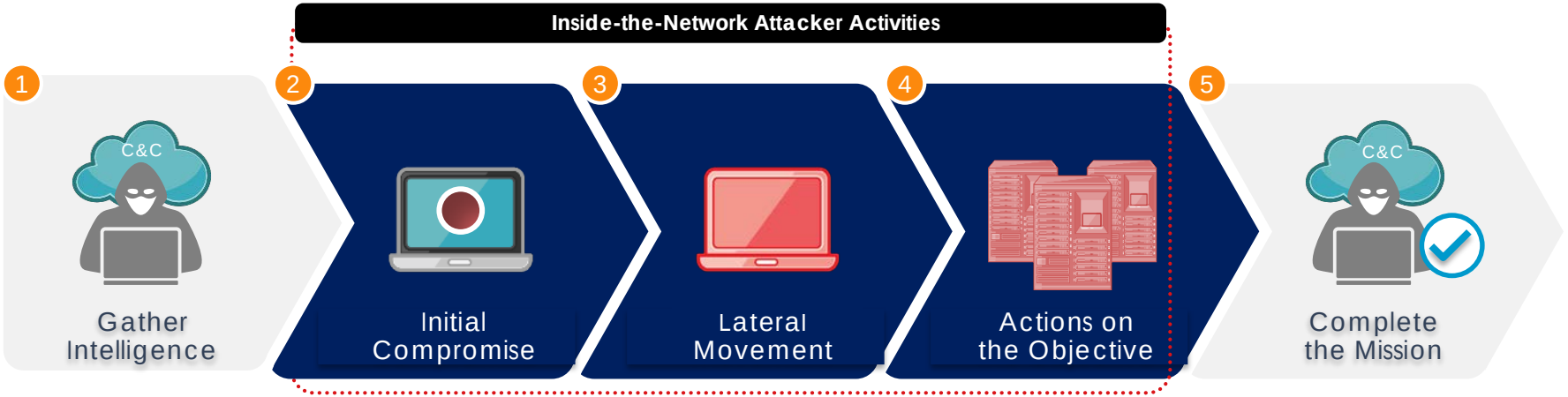
Attacker assumes he has time, has unlimited attempts, and can move slowly through the network to avoid detection

Steals credentials from the endpoint, moves laterally, escalates privileges

Assumes all information found is real; deceptive data is not expected

Attack Sequence and Methods: Detection Gaps

Attackers Are Bypassing Prevention and Evading Detection



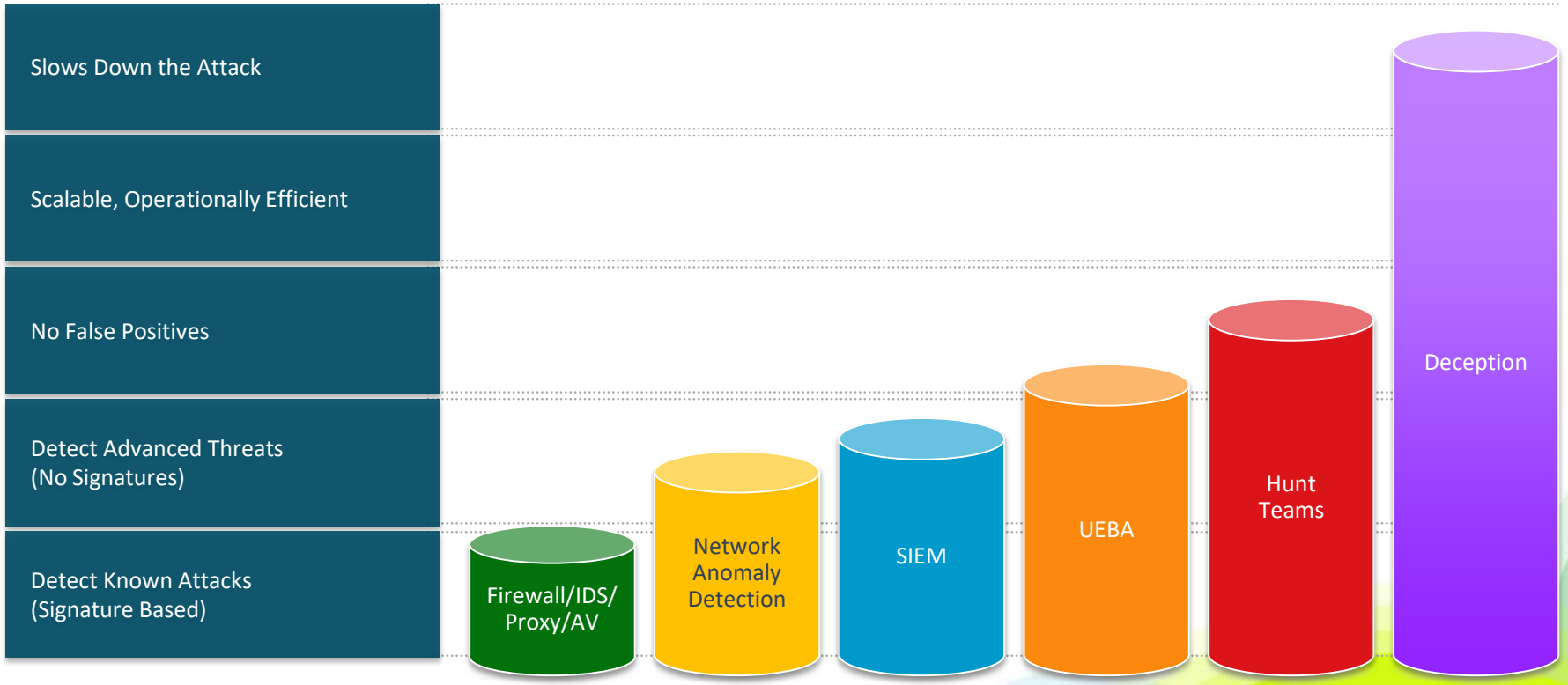
- Phishing
- Zero-day Exploit
- Unpatched Systems
- Stolen Credentials
- End-point/BYOD
- Website Downloads

- Network Recon
- Harvest Credentials
- Man-in-the-Middle
- Active Directory Recon

- Steal Data
- Destroy Data
- Ransom
- Sabotage Systems

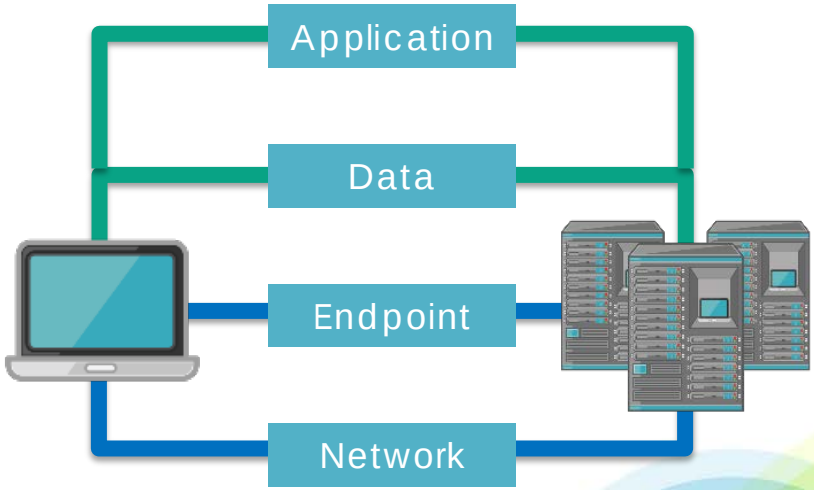
Choices in Closing the Detection Blind Spot

Deception: Detecting Attackers Better and Detecting Better Attackers



What is Deception?

Deception is an active countermeasure used to overpower the cognitive processes of the adversary to induce errors in their thinking that a defender can exploit.



Not All Deception is Created Equal

Evolving Attack Surface

- Datacenter
- User Networks
- Cloud
- IOT/SCADA

Attractiveness/ Authenticity

- Full Operating Systems
- Applications
- Data

Attack analysis/ forensics

- IOCs
- Disk activity
- Network PCAPs
- Memory

Accelerated Incident Response

- Blocking
- Quarantine
- Investigation
- Remediation

Ease of Operations and Scalability

Major Energy Company Protects Critical Infrastructure

Problem

- Protection of critical infrastructure and business networks to prevent incidents from tampering or sabotage of field fuel sensor and refinery controls.

Overview

- The team had a mature security posture, but lacked visibility into attacker lateral movement within their industrial control networks.

Outcome

- Deception engagement servers and SCADA decoys provide real-time visibility into lateral movement inside their network and high fidelity alerts on intrusions.

Customer Value

Real-time detection and accurate alerting to industrial control network intrusions.

Wrapping It Up

What should you take away from this?

Summary

- Attacker's perspective
- In-Network Detection
- Deception

Conclusions

- Attackers will get in
- Early detection is key
- Attackers are forced to be on the defensive
- Deception for the evolving threat landscape

Questions?

Let's Keep in Touch

Ray Kafity

ray@attivonetworks.com