The Art and Science of Deception

Empowering Response Actions and Threat Intelligence

| Attivo Networks | Oct 24, 2016

Why Today’s Security Defenses are Failing

Attackers Still Get In and Once Inside, Can Remain Undetected for Months

Prevention- Based Security

Build a Strong Perimeter

Secure the Entry Points

Monitor Suspicious Behavior

The Gaps

- Insiders, Suppliers, and Zero Day Attacks
- Stolen Credential, Phishing, Human Errors
- Too Much Data and Too Many False Positives
- Lack of Accurate Visibility to In-Network Threats

How Would You Score Your Organization?

Most Organizations Lack Confidence in their Overall Security Posture

1. How reliably does the security program protect the most critical assets (data, systems, people, infrastructure) with the organization?
2. How effective and efficient are security teams at detecting targeted attack activity, understanding severity of threats, and quickly responding to protect critical assets and data?
3. What are the security program gaps and how great is the risk exposure?
4. How prepared is the organization to address a worst case breach scenario?

Changing the Game with In-Network Detection

Protect Your Brand, Improve Operational Efficiency, Mitigate Risk and Costs of Breach

Know What's in the Network

Visibility

- 146 Days Avg. Dwell Time
- <20% Are Self-discovered
- 43% of Data Loss is Insider

Accurately Detect & Analyze Threats

Detection

- 17,000 Alerts/Week
- Only 4% Get Reviewed
- 40% Malware Undetected

Accelerate Incident Response

Response

- 154 Days Avg. to Contain
- $1.3M Annual Cost to Triage Alerts

9 in 10 Companies Have Been Breached with an Avg. Breach Cost of $4M.

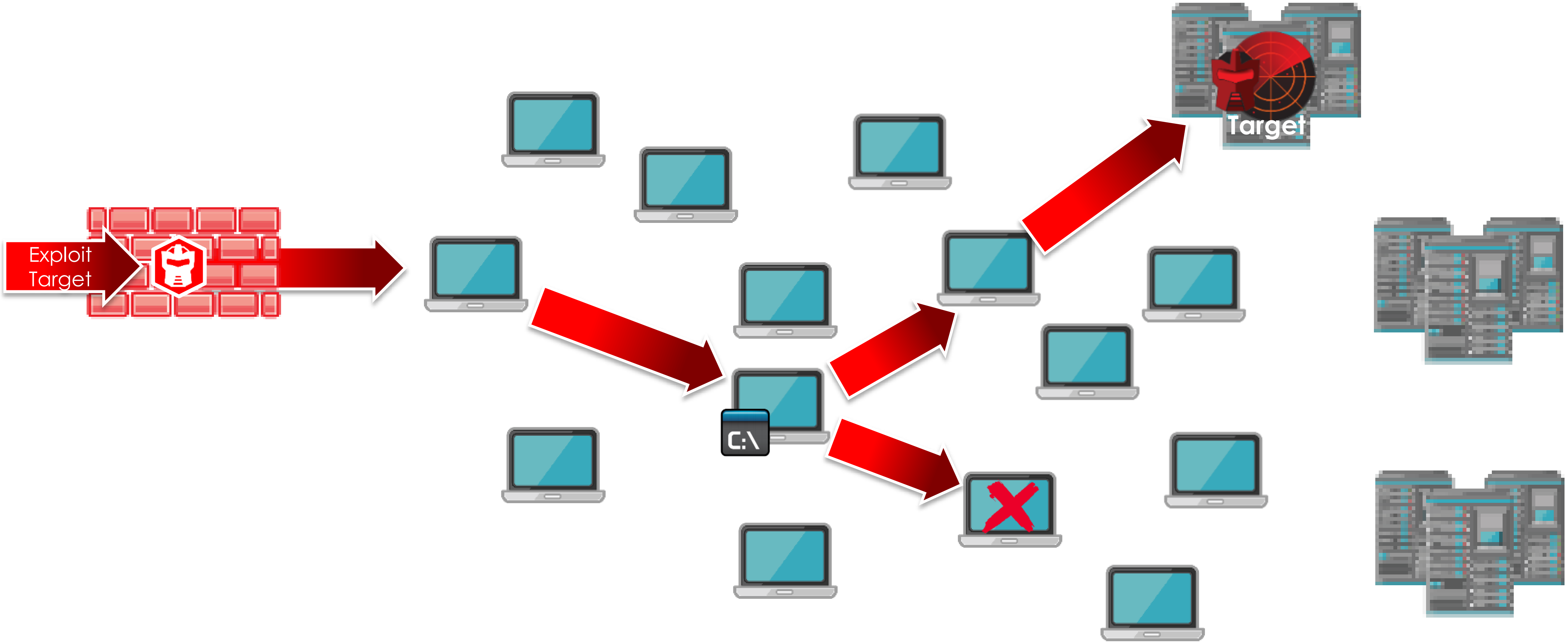
You Don't Want To Be Next.

Attack him where he is unprepared, appear where you are not expected.

Sun Tzu

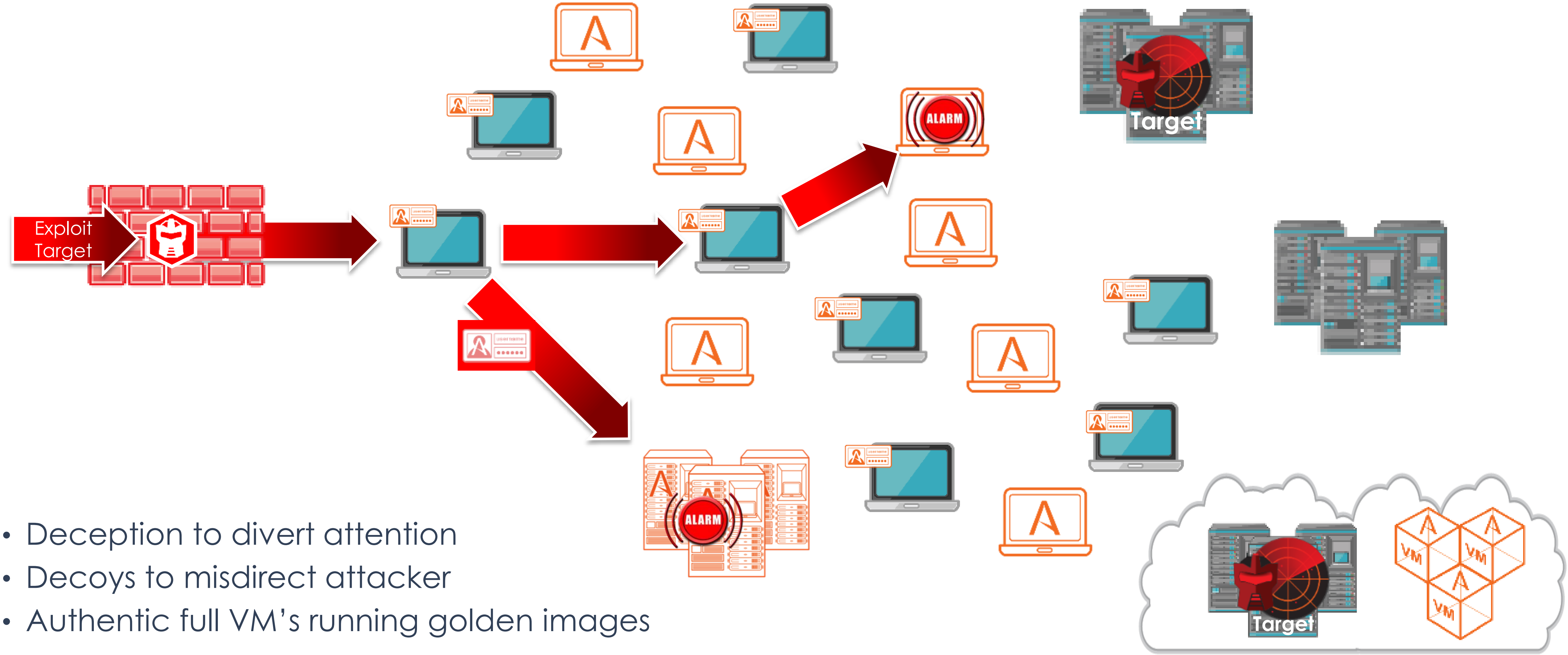
Typical Attack Path Sequence

Once small security gap will present opportunity for attackers



Changing the Game with Deception and Decoys

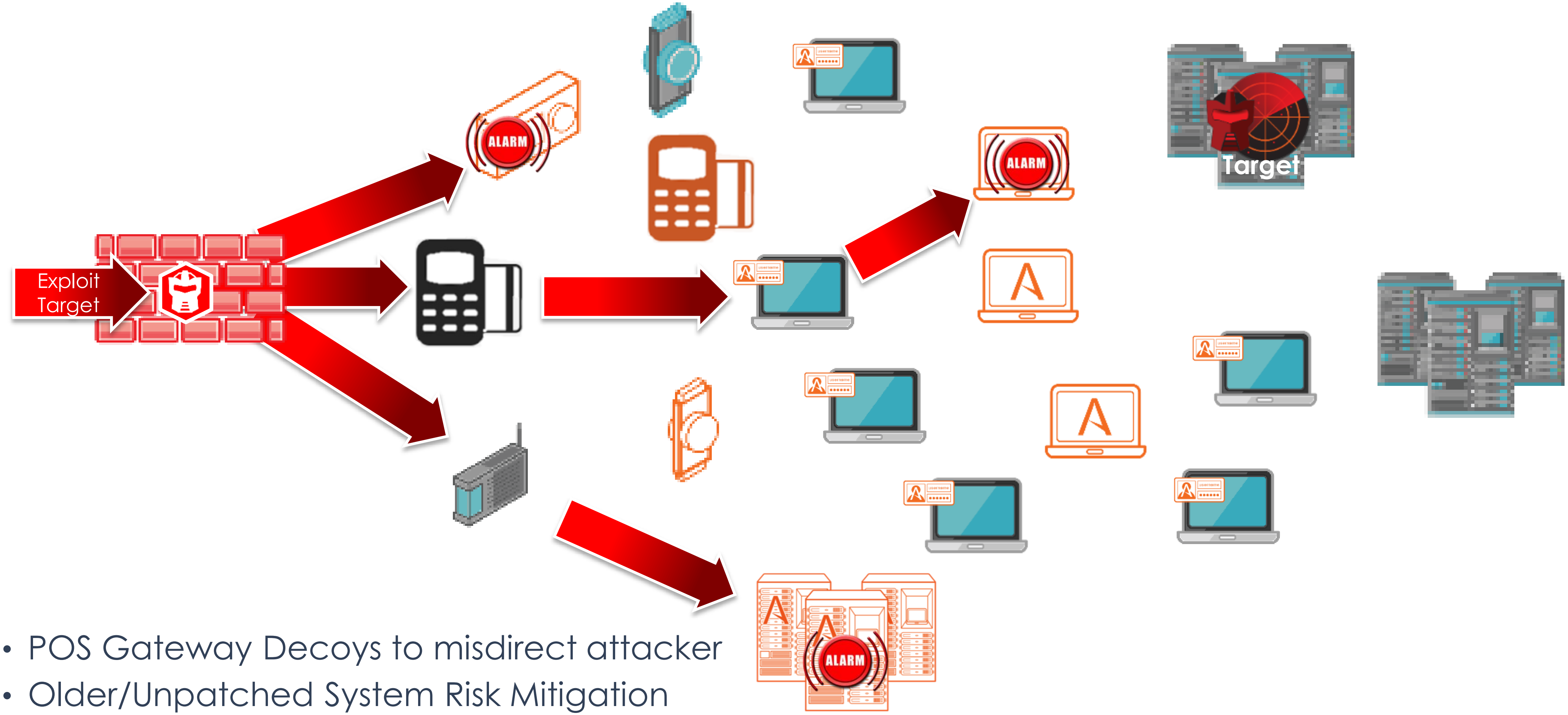
Deception Obscures the Attack Surface and Disrupts Attacks



- Deception to divert attention
- Decoys to misdirect attacker
- Authentic full VM's running golden images

Changing the Game with Deception and Decoys

Accurate Detection of ICS-SCADA, and IoT Network Attacks



- POS Gateway Decoys to misdirect attacker
- Older/Unpatched System Risk Mitigation

Pretend to be weak, that he may grow arrogant.

Authentic Deception Redirects & Detects Attackers

Decoys appear identical to production company servers/devices

Real Operating Systems & Services for Authentic Deception

Authentic

VIRTUAL MACHINES

Run **real** operating systems & services

SERVICES

Fully customizable: golden images & custom applications

SCADA

Dynamic deceptions
Supervisory Control and HMI

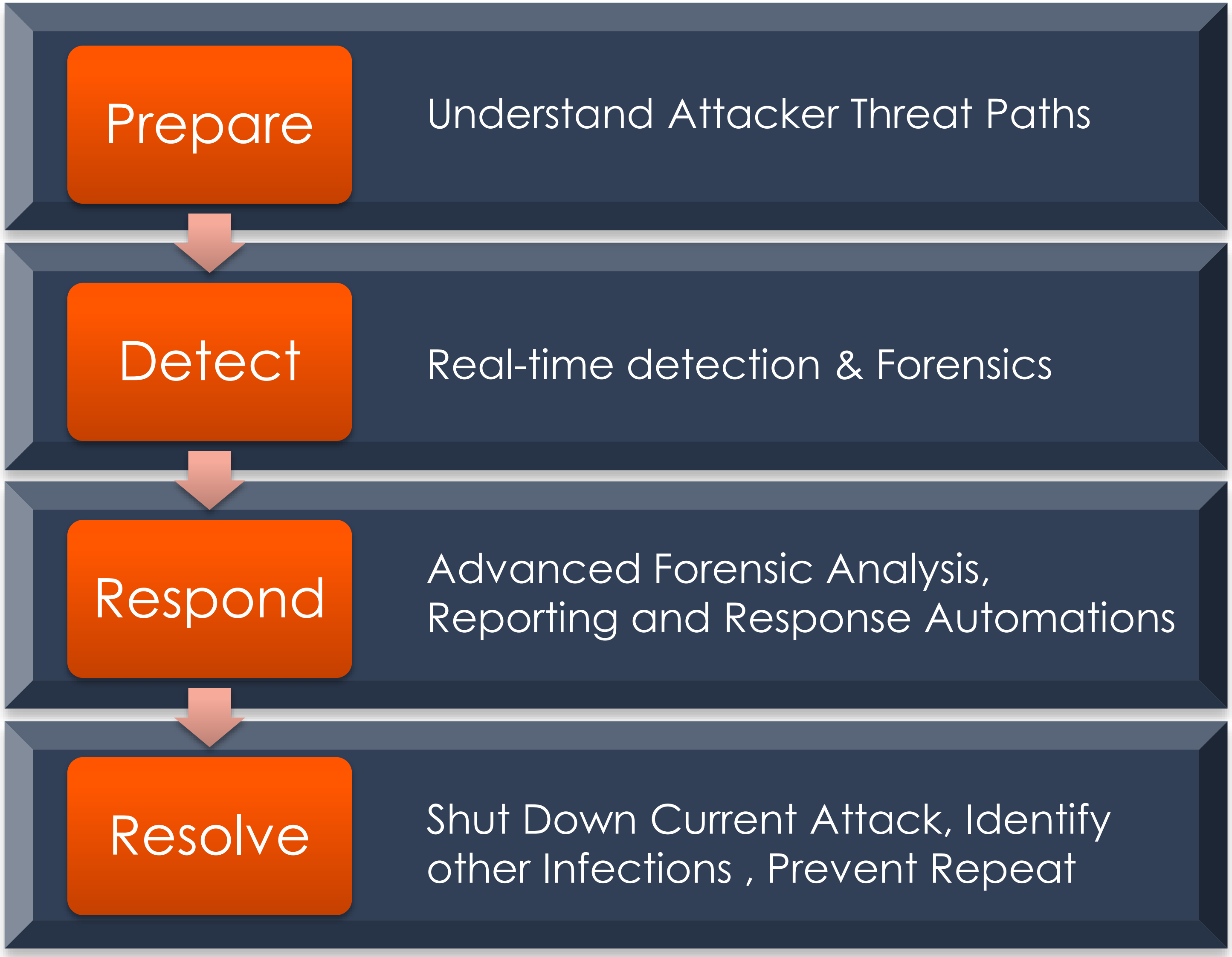
IoT / IoE

Dynamic deceptions
Server and Service Gateways

Advanced Behavior Deception Dynamically Learns & Deploys Credentials, Respins After Attack

If he is taking his ease, give him no rest.
If his forces are united, separate them.

Rapid Detection and Response

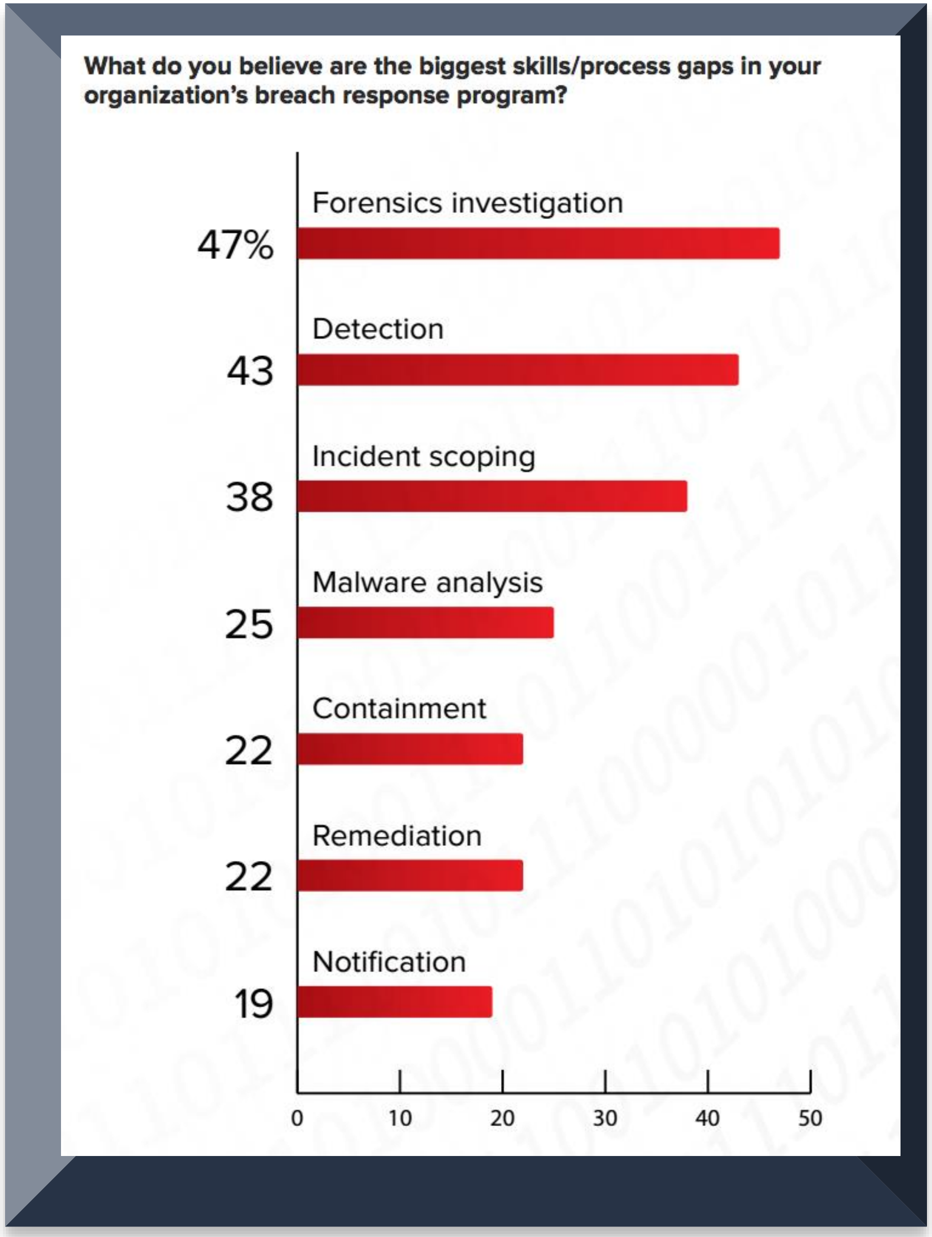


Prepare — Understand Attacker Threat Paths

Detect — Real-time detection & Forensics

Respond — Advanced Forensic Analysis, Reporting and Response Automations

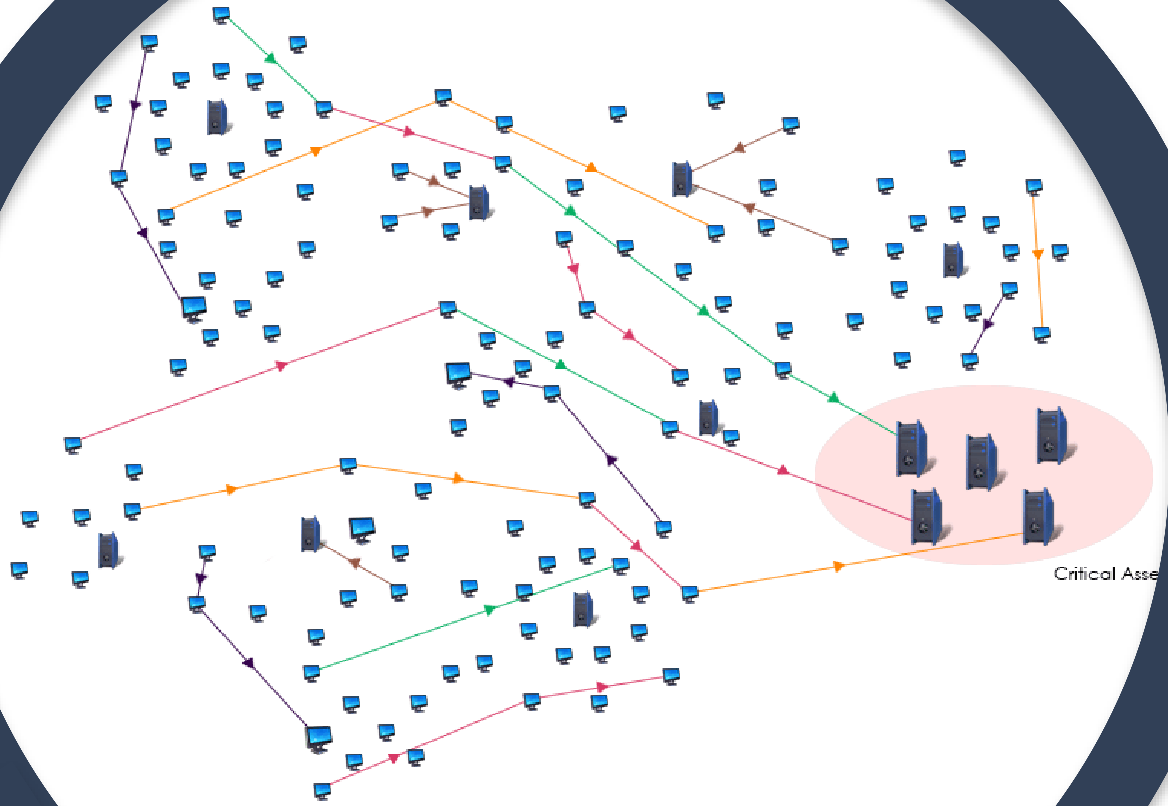
Resolve — Shut Down Current Attack, Identify other Infections , Prevent Repeat



What do you believe are the biggest skills/process gaps in your organization's breach response program?

Understanding Attacker Threat Paths

1. Discovers the paths attacker’s can traverse
2. Provides network map with possible lateral movement paths
3. Provides actionable insights to strengthen policies and prevent lateral movement



- Misconfigurations
- Misused Credentials

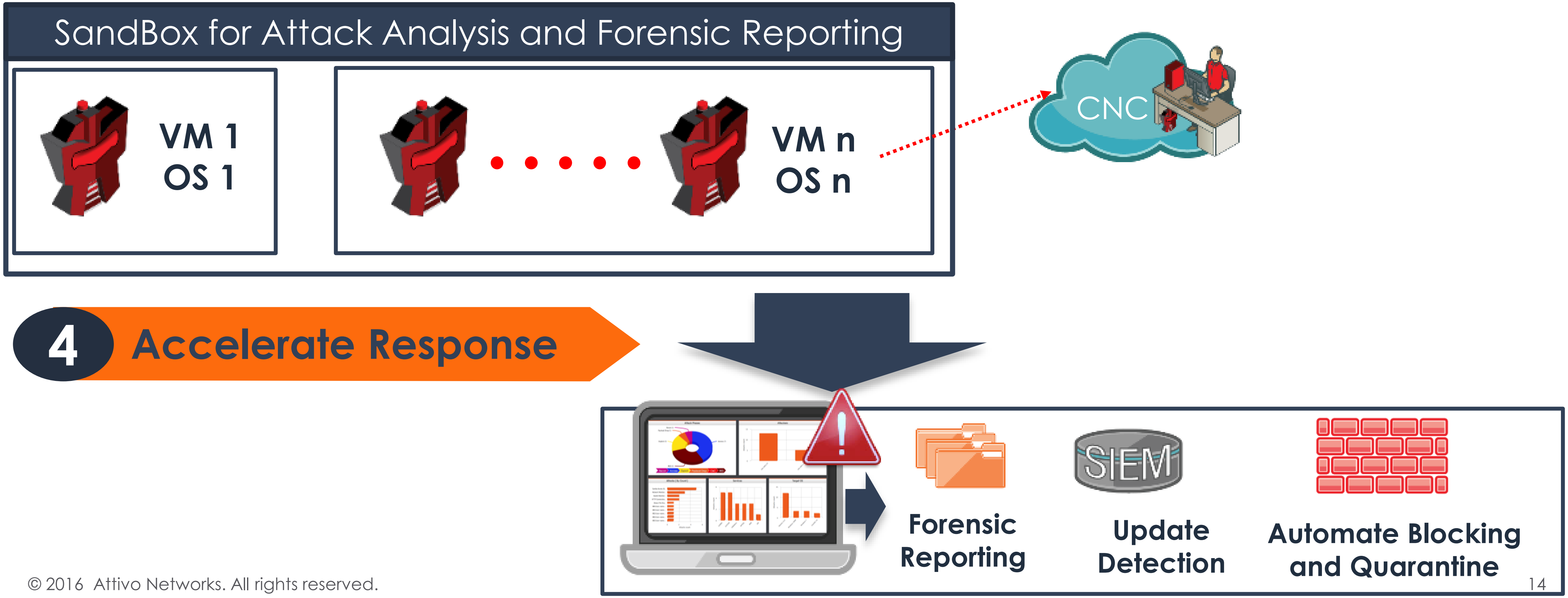
Deception Engagement Server

Engages Attacker and Capture Forensics: Uncovers its Weaknesses

1 ATTACK

2 TRAP and ANALYZE

3 COMMUNICATE



SandBox for Attack Analysis and Forensic Reporting

VM 1
OS 1

VM n
OS n

CNC

4 Accelerate Response

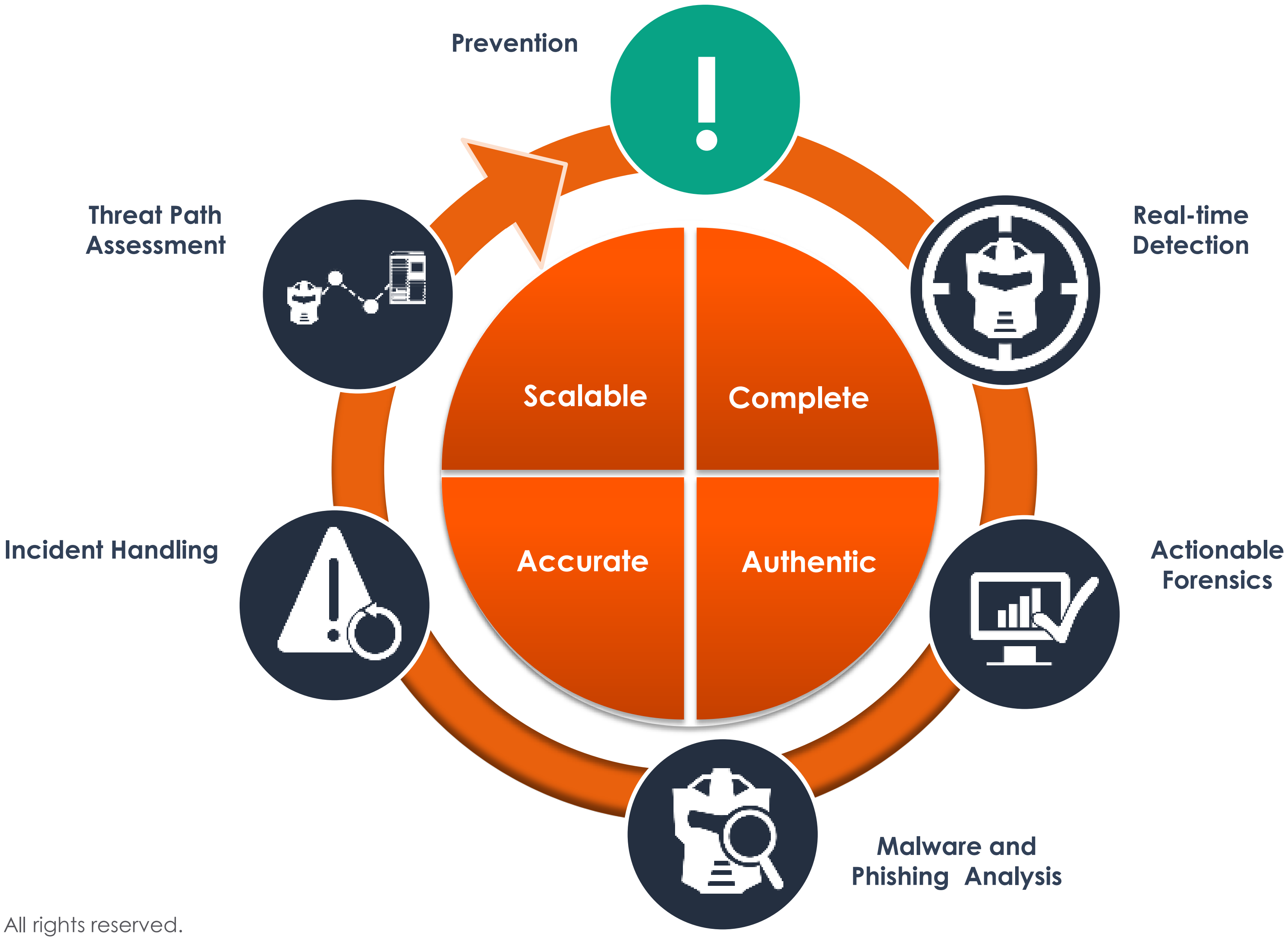
Forensic Reporting

Update Detection

Automate Blocking and Quarantine

A Modern Day Deception and Response Platform

Provides Accurate and Efficient Continuous Threat Management



Deception Technology Derails Ransomware Attack on Regional Healthcare Company

Problem

- Ransomware attack was quickly encrypting their systems and was changing faster than the team could analyze the strains.

Overview

- The customer had the Attivo appliance deployed on their network.

Outcome

- Inoculated their environment by using the attack forensics generated by the Analysis Engine

Customer Value

Successfully stopped the spread of the ransomware attack in their environment.

Aflac, Inc. Uses Deception for Zero-False-Positives Threat Detection

Problem

- The infosec team was unable to keep up with the ever-changing nature of advanced threats.

Overview

- The team had a very mature security posture but wanted to add visibility for zero-day and signatureless attacks.

Outcome

- The team has confidence that they will be able to detect attacks that none of their other security devices will be able to.

Customer Value

Visibility into zero-day and signatureless attacks.

Major Sports Organization Protects Critical Infrastructure With Deception

Problem

- Their SCADA system could be hacked and shut down during an event, causing panic and harm.

Overview

- The small infosec team needed a solution that would require low bandwidth to operate with zero false positives.

Outcome

- The ThreatMatrix platform successfully detected and stopped an attack during a major event.

Customer Value

Successfully detected and stopped an attack during an event.

Major Entertainment Organization Deploys Deception for Insider Threat Visibility

Problem

- This organization was concerned about insider threats and stolen credential attacks.

Overview

- ThreatStrike deceptive credentials drastically increased the odds that stolen credentials could not be used maliciously.

Outcome

- Team shifted the odds in their favor that they will not suffer an attack from insider threats or stolen credentials.

Customer Value

Protect intellectual property from insider and stolen credential attacks.

Attivo Networks Deception Platform for Forensics and Incident Response

Problem

- Vicious malware was spreading aggressively through the customer's network.

Overview

- Customer had a BOTsink appliance installed in a POC stage but not on their full network.

Outcome

- Customer used the Analysis Engine to understand the malware's behavior for accelerated incident response.

Customer Value

Detailed attack forensics and accelerated incident response.

Manufacturer Protects Intellectual Property With ThreatMatrix Platform

Problem

- The team was concerned about advanced threats and stolen credential attacks penetrating their intellectual property.

Overview

- The team had limited visibility into their subnets that contained their most critical assets.

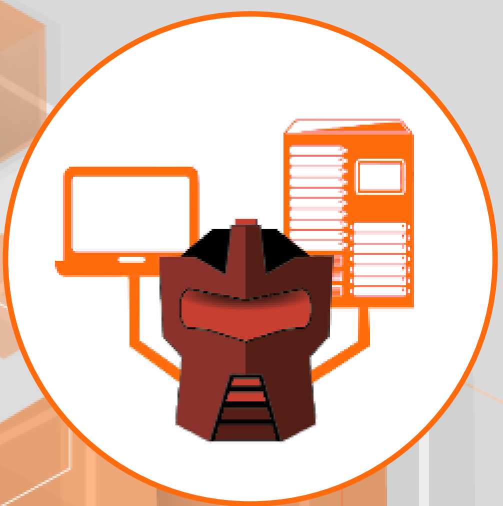
Outcome

- The ThreatMatrix platform gave them unparalleled visibility into their subnets, allowing them to detect malicious activity.

Customer Value

The team has visibility into the subnets that house their most critical data.

Semiconductor Company Implements Deception to Stop Man-in-the-Middle Attacks



Problem

- Organization suffered a man-in-the-middle attack and wanted full visibility in their network to avoid future, similar threats.

Overview

- Team had limited bandwidth for a device that generated false positives and required detailed attention.

Outcome

- With low maintenance and high-fidelity alerts, the team now detects attacks that could not detected before.

Customer Value

The ability to detect threats that have bypassed their other security devices.

Financial Institution Thwarts Penetration Test With Deception

Problem

- Team failed multiple penetration tests and needed to detect advanced, in-network threats.

Overview

- The number of alerts the infosec team receives from other devices almost guarantees that something will go undetected.

Outcome

- The ThreatMatrix platform immediately detected the red team during a penetration test.

Customer Value

Pass penetration tests that they failed with their other security devices.

Analyst 2016 Views

"Global Deception Technology Market to generate revenue over $1B from 2016 to 2020."

Technavio– IT Market Research

"Deception is the most advanced approach for detecting threats within a network."

Peter Firstbrook – Gartner

Gartner identifies top 10 security trends for 2016

Neil McDonald- Gartner

Paradigm shifts in information security

"Block & Detect shifts to Detect & Respond"

"Deception should be a 2016 initiative."

Eric Ouellet- Gartner

Attivo Networks exemplifies a modern-day approach to deception.

Mike Suby – Frost and Sullivan

The Art and Science of Deception

If your opponent is temperamental, seek to irritate him.

Pretend to be weak, that he may grow arrogant.

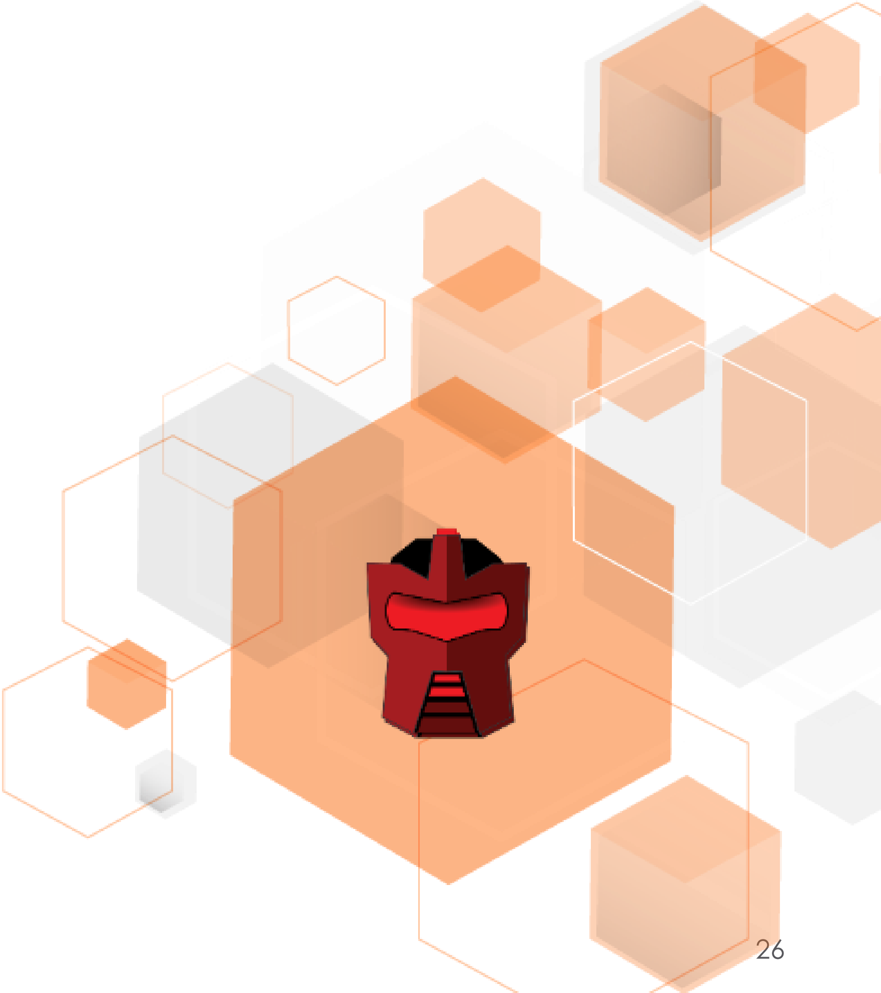
If he is taking his ease, give him no rest.

If his forces are united, separate them.

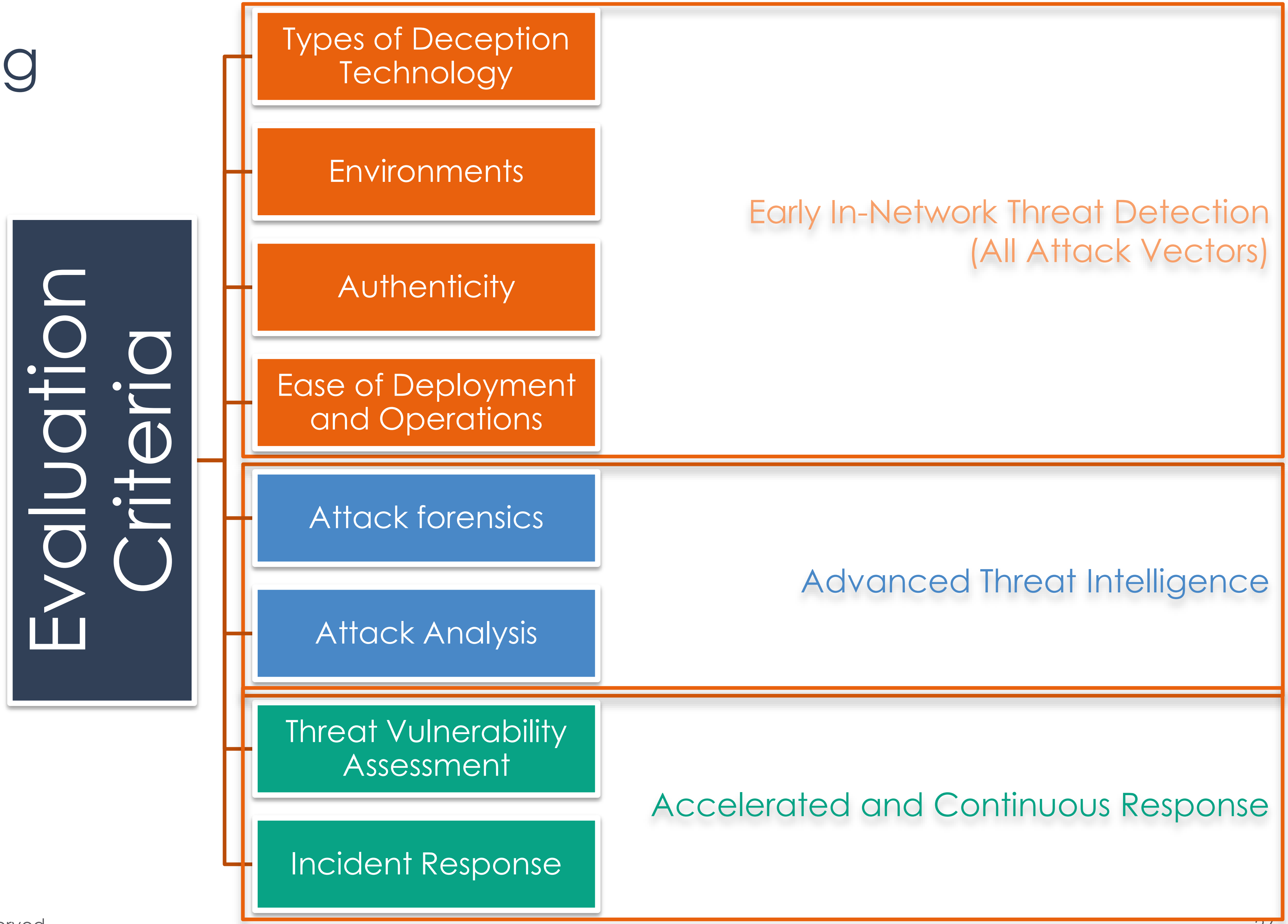
Attack him where he is unprepared, appear where you are not expected.

Sun Tzu

Thank you.



Incorporating Deception Technology



Evaluation Criteria

Types of Deception Technology

Environments

Authenticity

Ease of Deployment and Operations

Early In-Network Threat Detection
(All Attack Vectors)

Attack forensics

Attack Analysis

Advanced Threat Intelligence

Threat Vulnerability Assessment

Incident Response

Accelerated and Continuous Response