The Art and Science of Deception

Empowering Response Actions and Threat Intelligence

Attivo NETWORKS®

Don Woodard

November 15th, 2016

Warfare and the Art of Deception

Attacker View

If your enemy is secure at all points, be prepared for him.

If he is in superior strength, evade him.

If your opponent is temperamental, seek to irritate him.

The Art of Deception

Pretend to be weak, that he may grow arrogant.

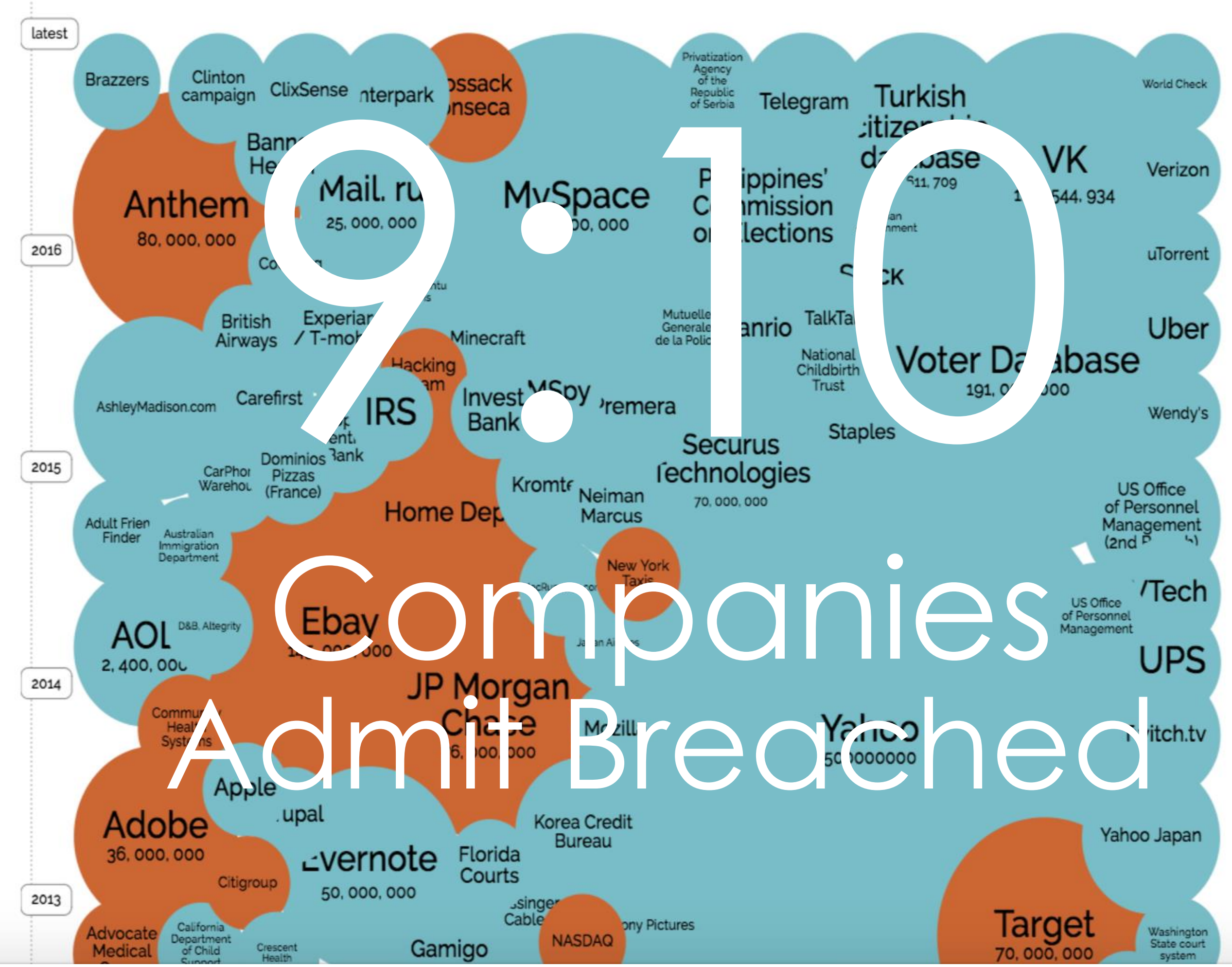
If he is taking his ease, give him no rest.

If his forces are united, separate them.

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

Sun Tzu

From Necessity,
Security Postures Shifting from Prevention to Detection

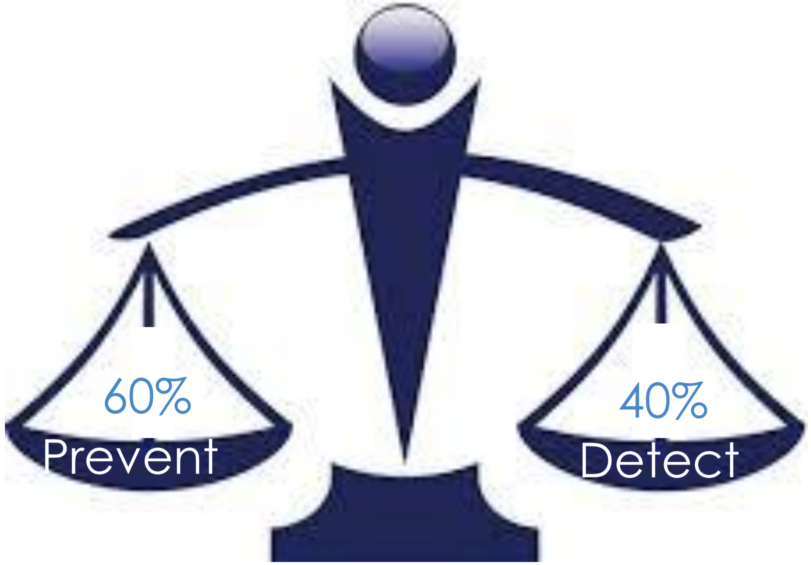


9:10

Companies Admit Breached

Source: FireEye Maginot Revisited: More Real-World Results from Real-World Tests

Enterprise information security budgets will be reallocated to rapid detection and response approaches



Gartner Predicts: By 2020

Advanced Threat Detection Technology Choices

Analytics: Big Data Learning

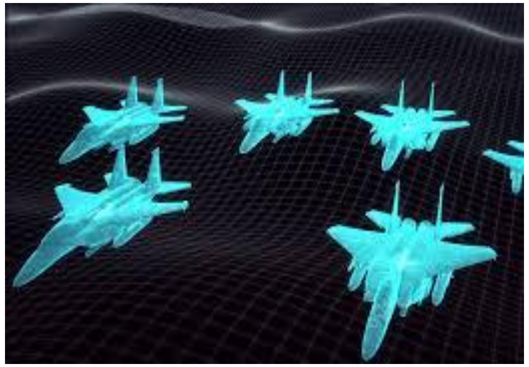
Network Anomaly

SIEM Logs UBA

Investigate Everything: Millions of Logs and Alerts

Deception Technology

Deception Decoy

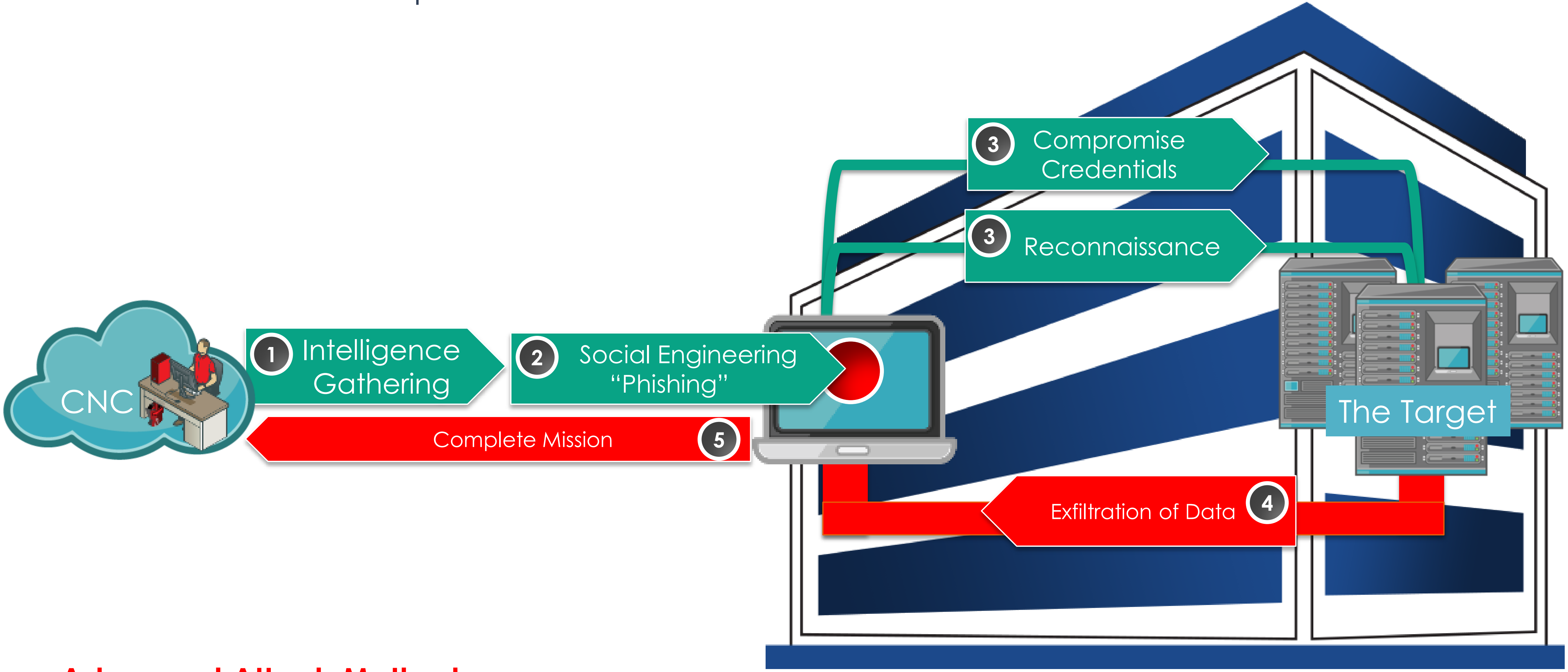


Accurate Visibility

Lures, Traps, and High Fidelity Alerts

Attack Sequence and Methods

Threat Actors are Prepared and Evasive



Advanced Attack Methods:

• HTTPS • Zero-day • Stolen employee credentials • MiTM • End-point/ BYOD • Spear Phishing

Deception: Obscures the Attack Surface and Disrupts Attackers

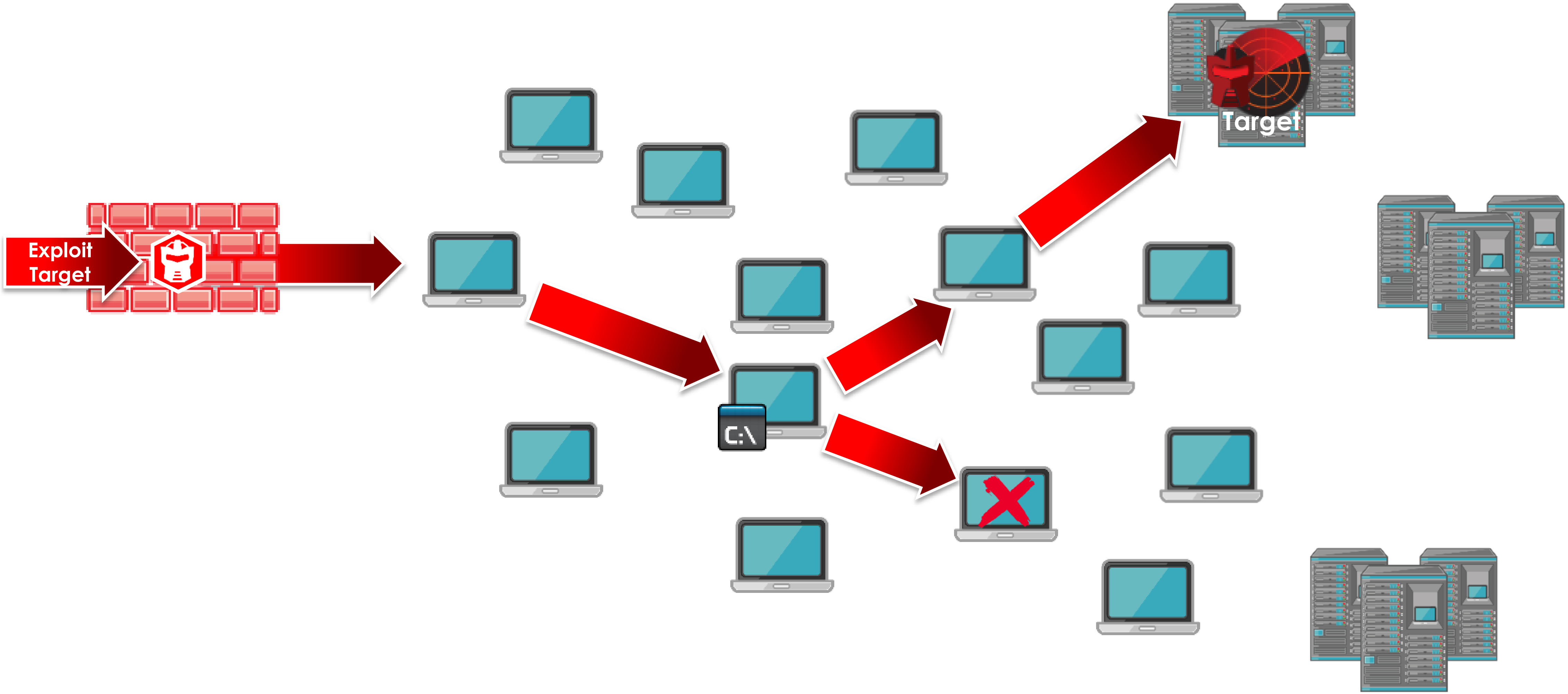
Deception systems turn the network into a ubiquitous trap

- Deception techniques are used to confuse, deceive, and delay attackers by incorporating ambiguity and misdirecting a cyber attacker's operations.
- This provides an early alert system and the much needed time and visibility to thwart the attack and remediate infected systems.

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

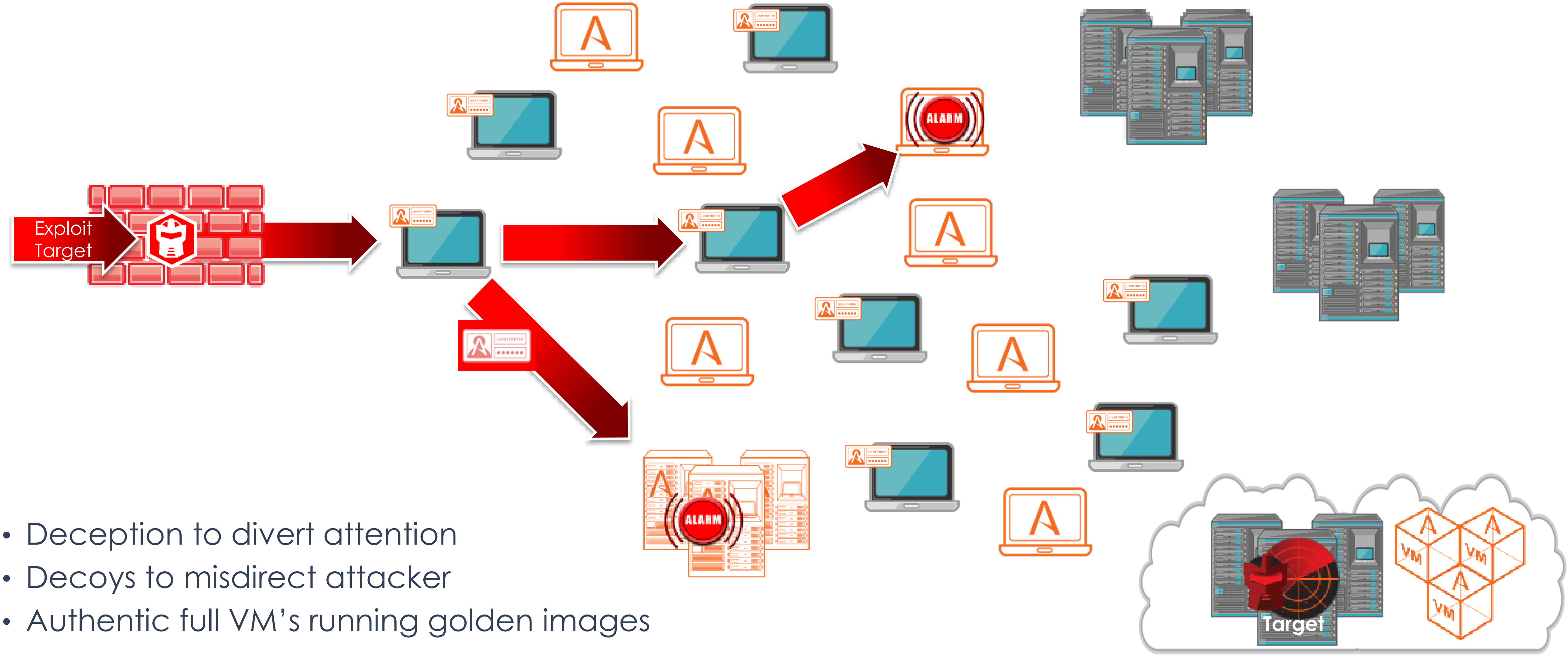
Typical Attack Path Sequence

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

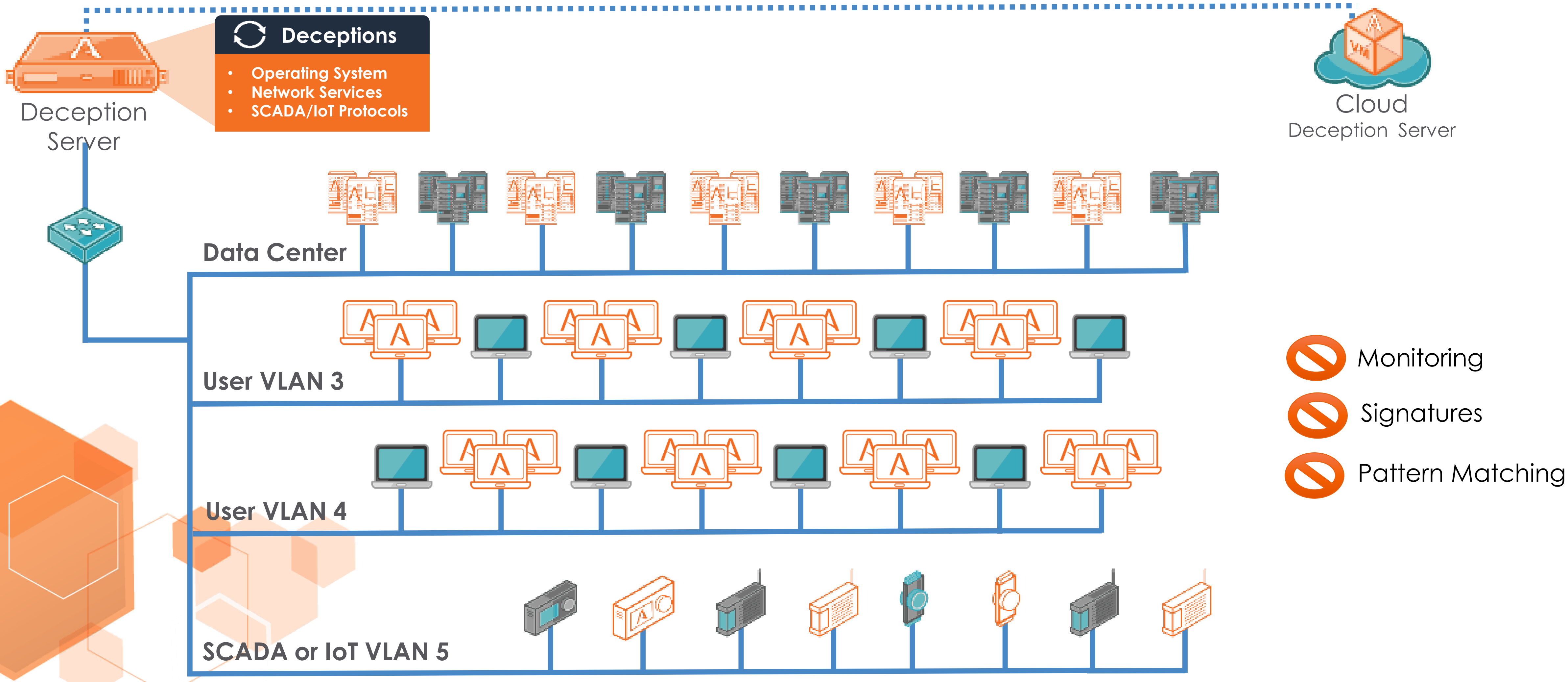
How Secure is Your Defense

The Challenge	Severity	Your Company Score Card
Zero-Day Malware	12 new attack strains per minute	?
Insider Threats	43% of data loss	?
Stolen Credential	2 out of 3 Attacks	?
Alert Noise and Limited Resources	Industry avg. 14 alerts per hour	?
Attacker Dwell Time	146 Days	?
Attack Time to Respond	154 Days to contain when detected by external party	?

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

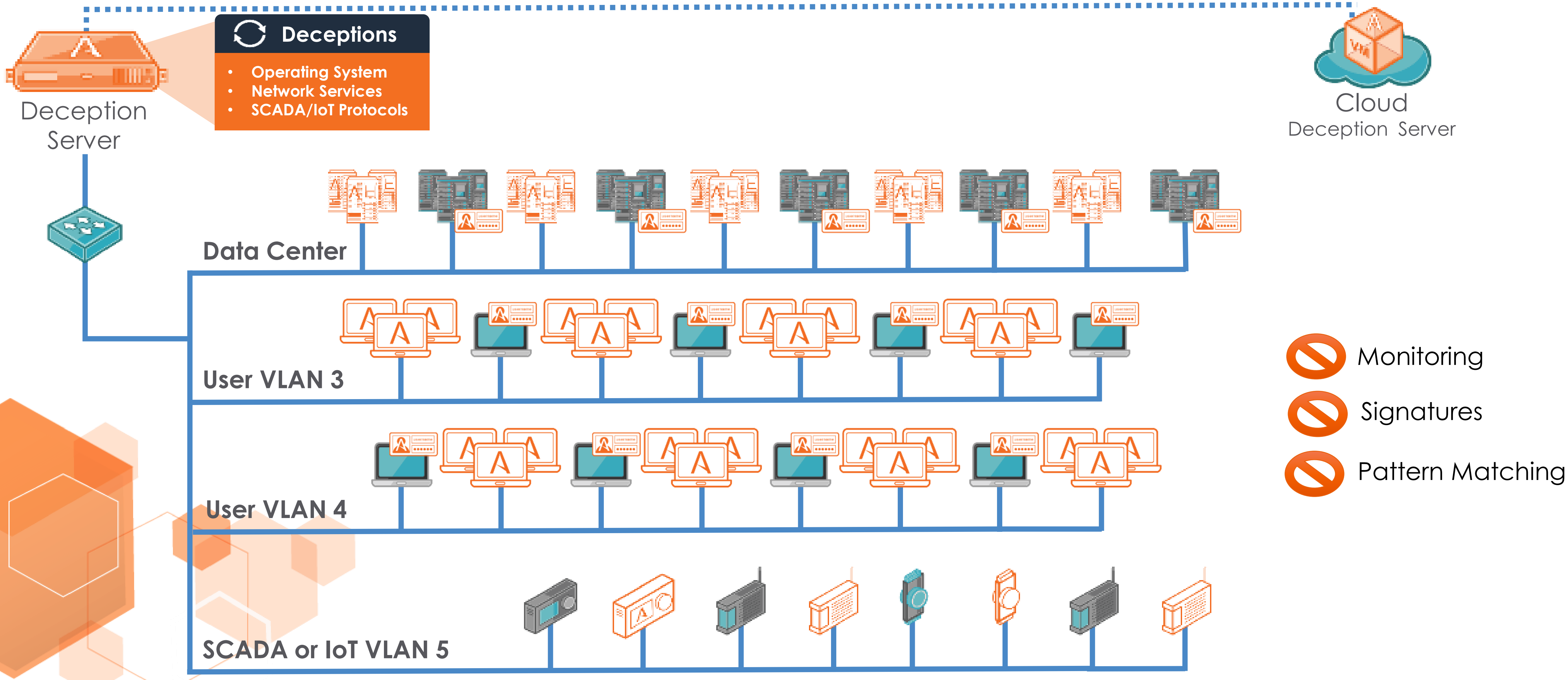
In-Network Deception: Hide in Plain Site

Adding in Deception



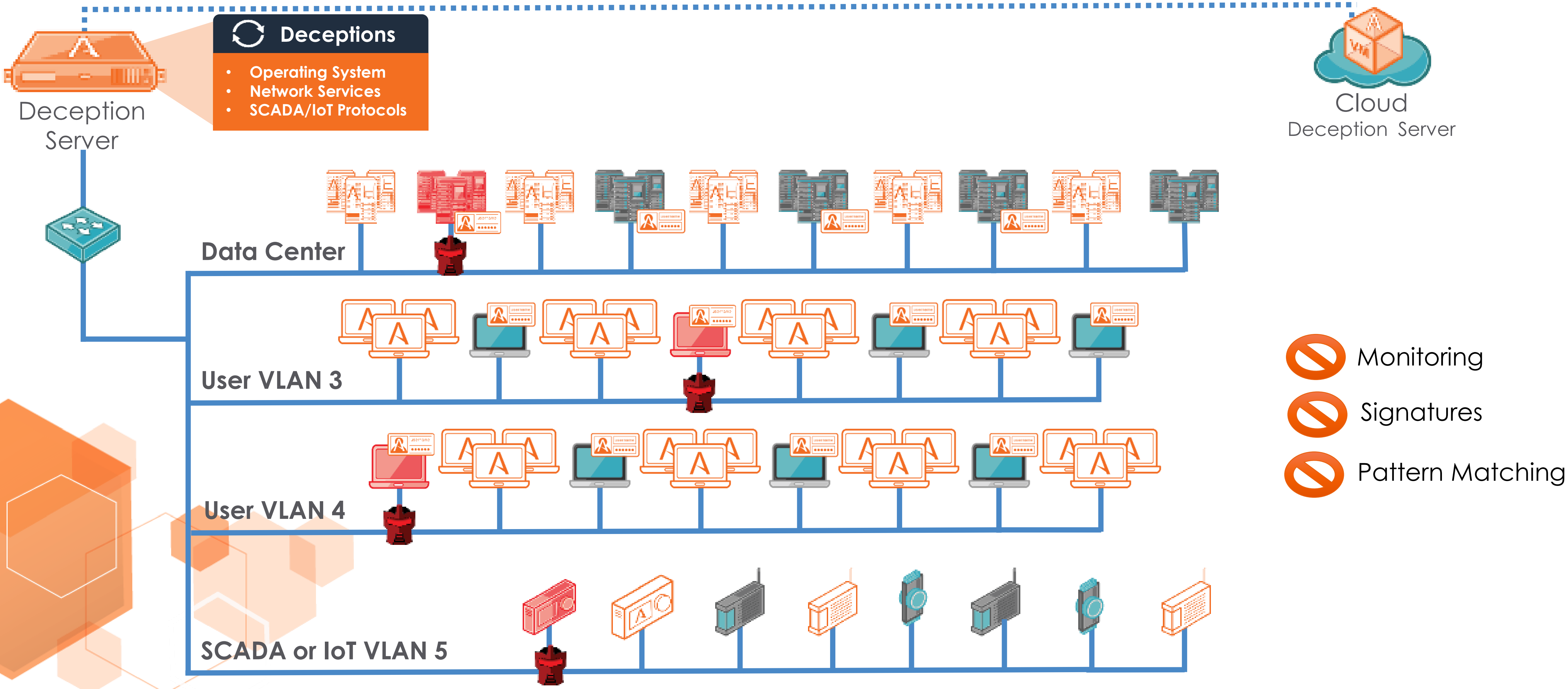
In-Network Deception: Hide in Plain Site

Adding in End-point Deception



In-Network Deception: Hide in Plain Site

Deception to Make the Entire Network a Trap for Real-Time Threat Detection



Deceptions

- Operating System
- Network Services
- SCADA/IoT Protocols

🚫 Monitoring

🚫 Signatures

🚫 Pattern Matching

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

OPERATING SYSTEMS

VM

- CentOS: 6.5, Red Hat*
- ubuntu: 12.04, 13.1
- Windows: XP*, 7, 8*, 10*, 2008, 2012*

Run **real** operating systems & services

SERVICES

FTP/SFTP	SNMP	Tomcat
HTTP/HTTPS	Telnet	Jboss
Print	RDP	SVN/CVS
SMB	GIT	Active Directory
NBNS	mDNS	Trac
SSH	MySQL	Radius
SMTP	Apache	NetBios

Fully customizable: golden images & custom applications

SCADA

Modbus | ASHRAE BACnet

Common Industrial Protocol (CIP)

Siemen's S7 PLC

IPMI | SNMP | MIB

Veedor-Root Tank software

Dynamic deceptions
Supervisory Control and HMI

IoT / IoE

XMPP | CoAP

MQTT.ORG

DICOM based PACS

POS | GE Simplicity

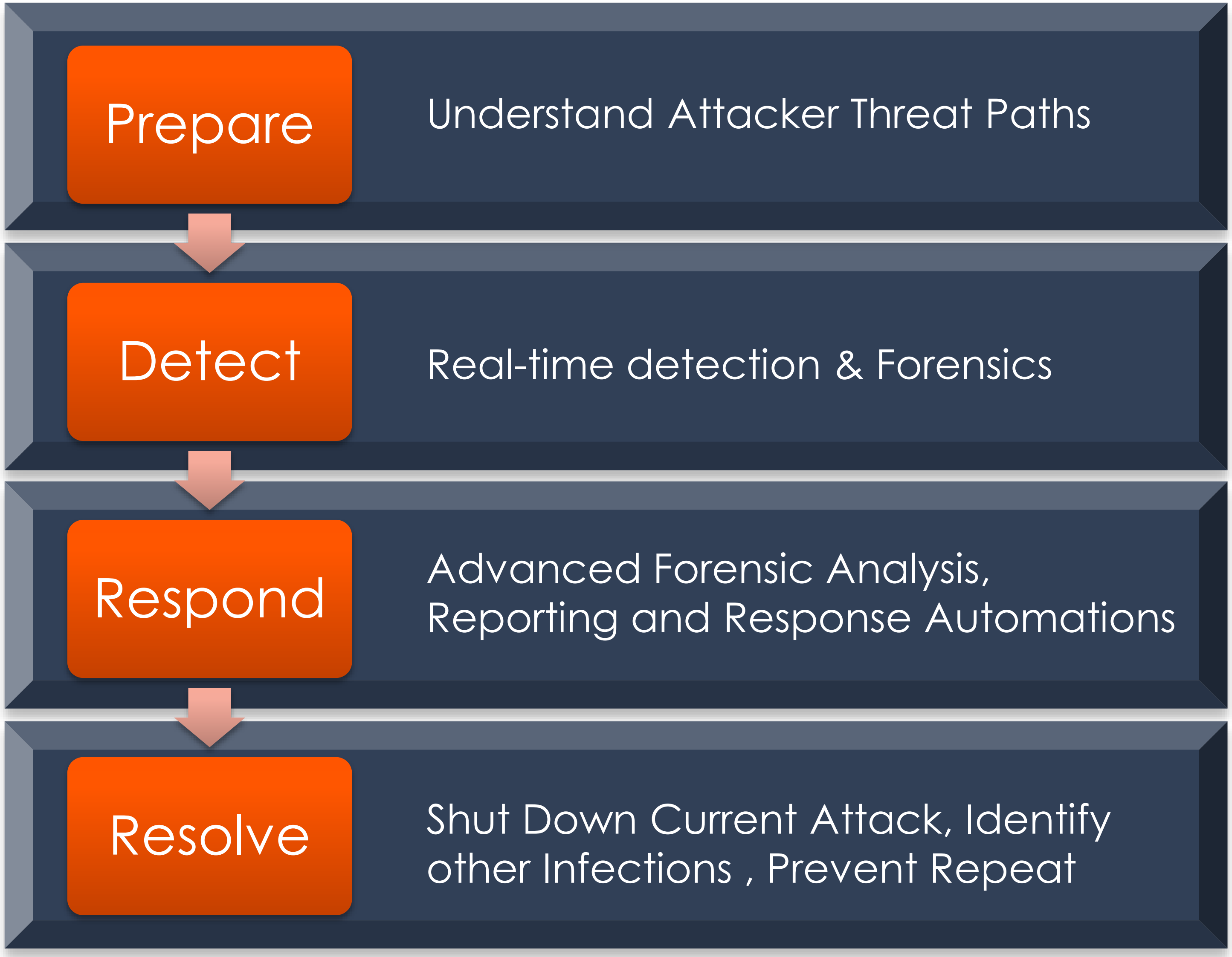
Hospital Supply Chain Management

Dynamic deceptions
Server and Service Gateways

Customers choose: Out-of-the-box setup with default settings or can be customized

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

Rapid Detection and Response

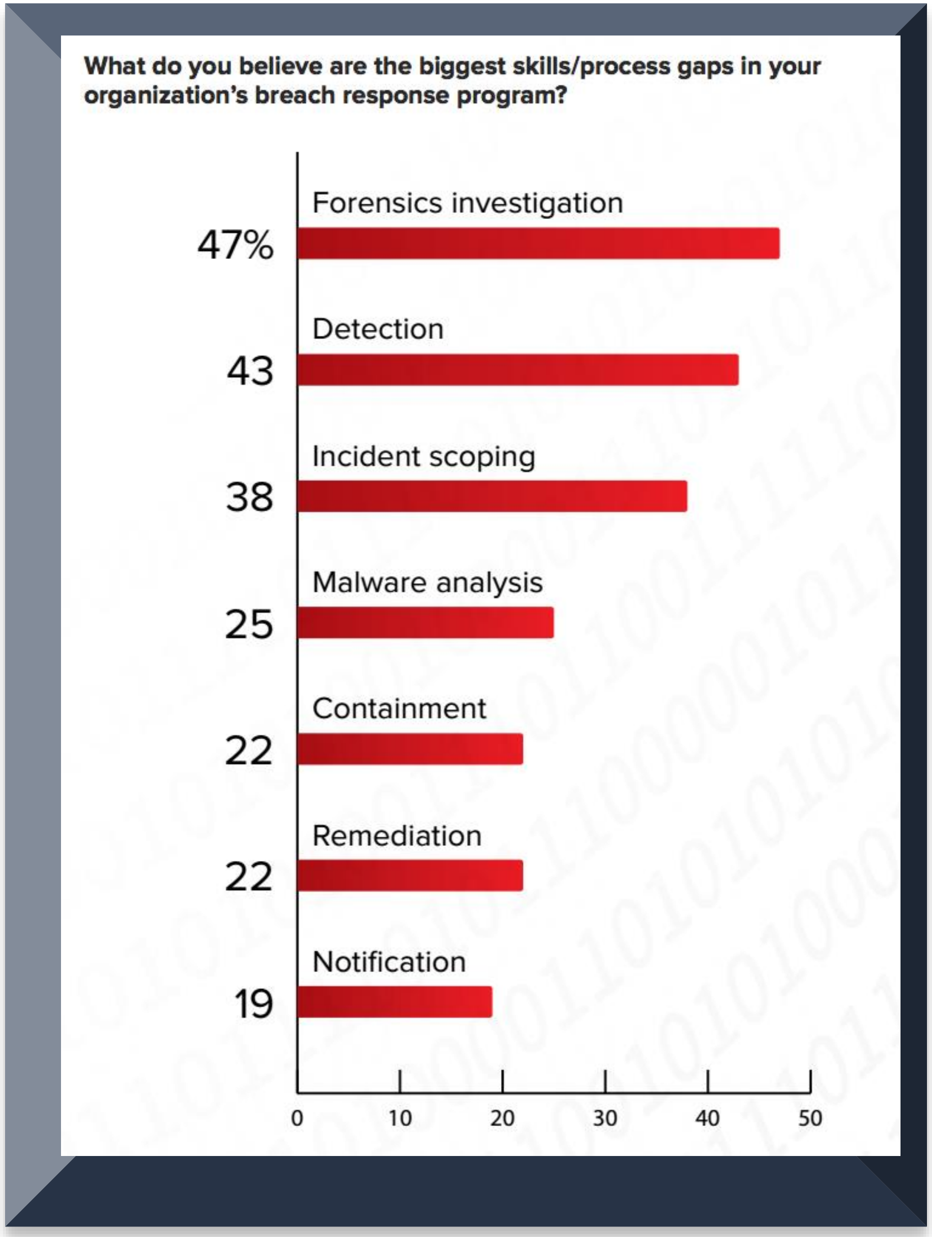


Prepare – Understand Attacker Threat Paths

Detect – Real-time detection & Forensics

Respond – Advanced Forensic Analysis, Reporting and Response Automations

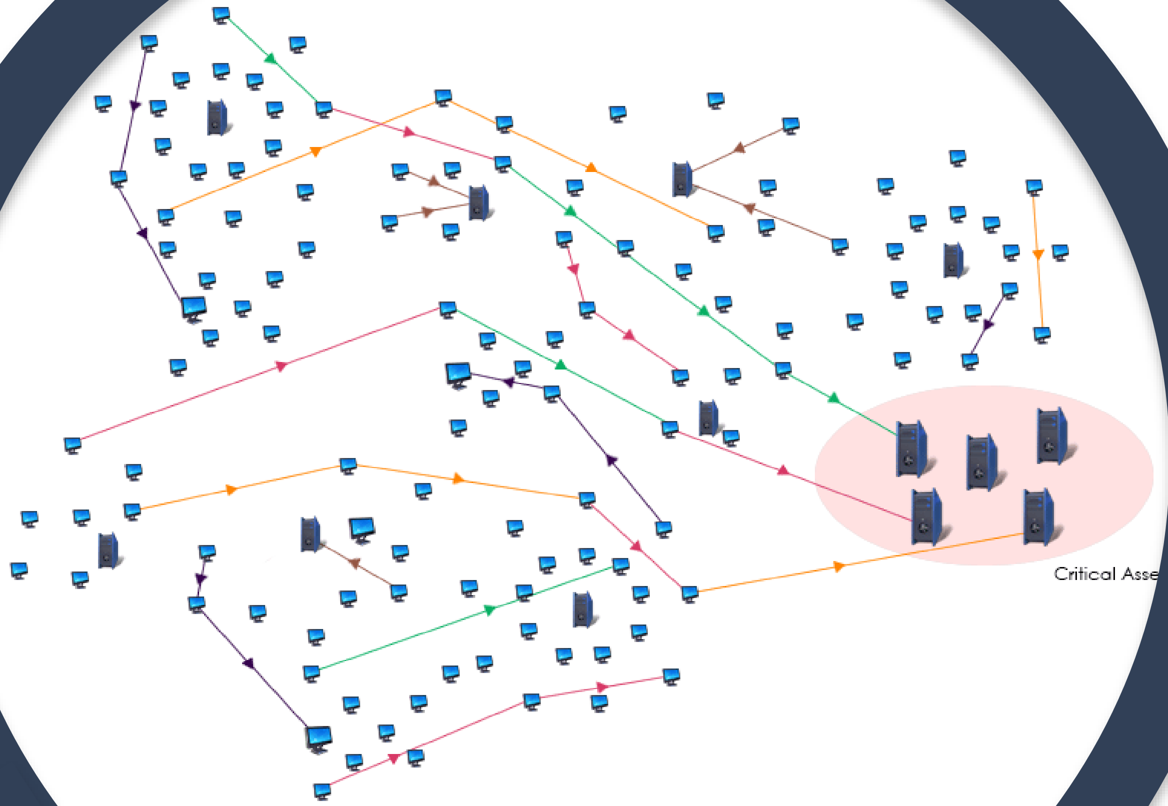
Resolve – Shut Down Current Attack, Identify other Infections , Prevent Repeat



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

Understanding Attacker Threat Paths

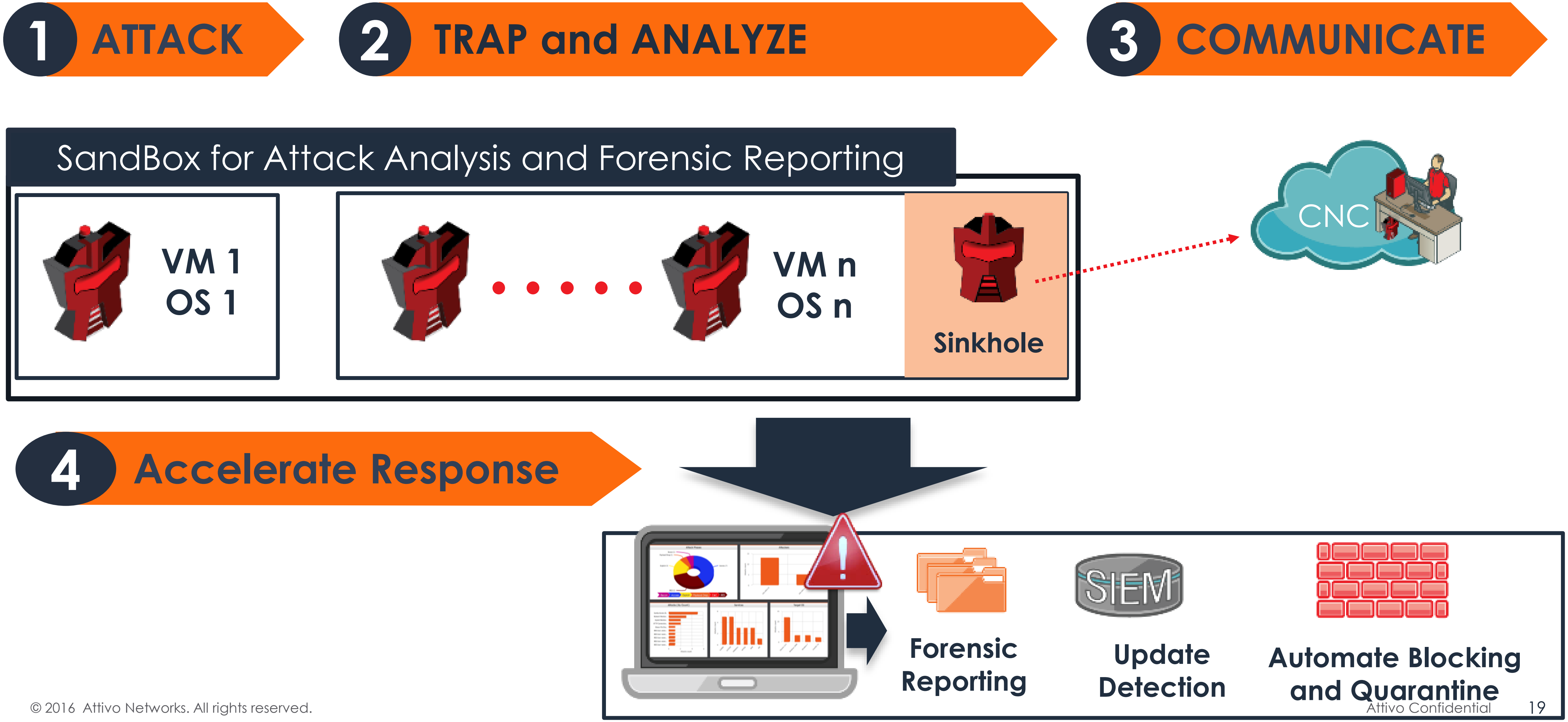
1. Discovers the paths attacker's can traverse
2. Provides network map with possible lateral movement paths
3. Provides actionable insights to strengthen policies and prevent lateral movement



- 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

Sinkhole

4 Accelerate Response

Forensic Reporting

Update Detection

Automate Blocking and Quarantine

Deception for Threat Intelligence

Attack Visibility

- All deception server activity, from kernel to network
- Attacker methods, targets, and communication paths

Threat Intelligence

- **Network level**
  - Command and Control traffic
  - Attack IPs/Ports/ Protocols and methods
  - Network forensics

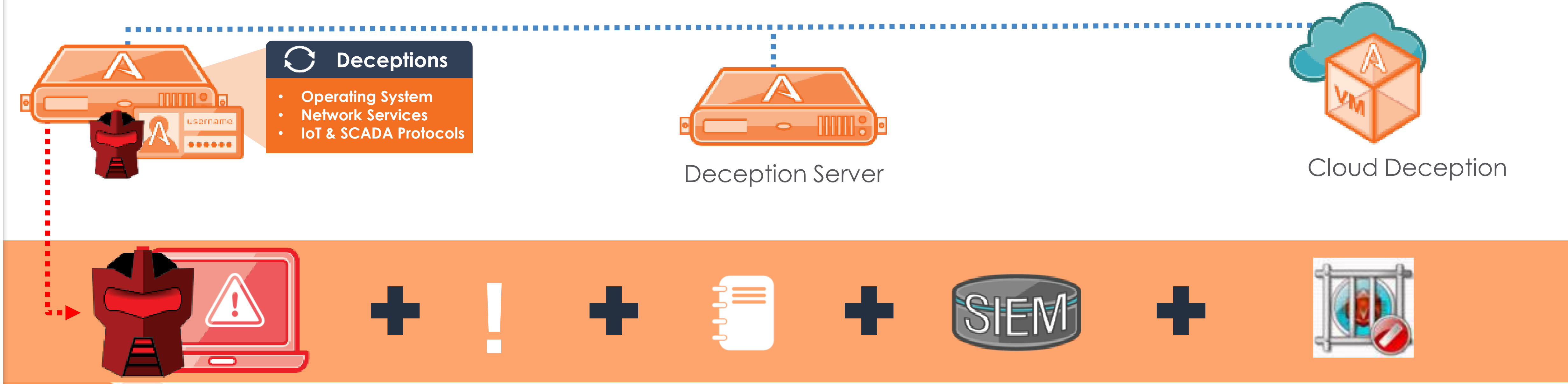
Threat Intelligence

- **Host level**
  - Payloads
  - Stolen data repositories
  - Registry/ permission/ policy changes
  - Disc Forensics
  - Memory forensics

Deception for a Continuous Threat Response Platform

Detect, Respond, Resolve

Continuous Threat Response

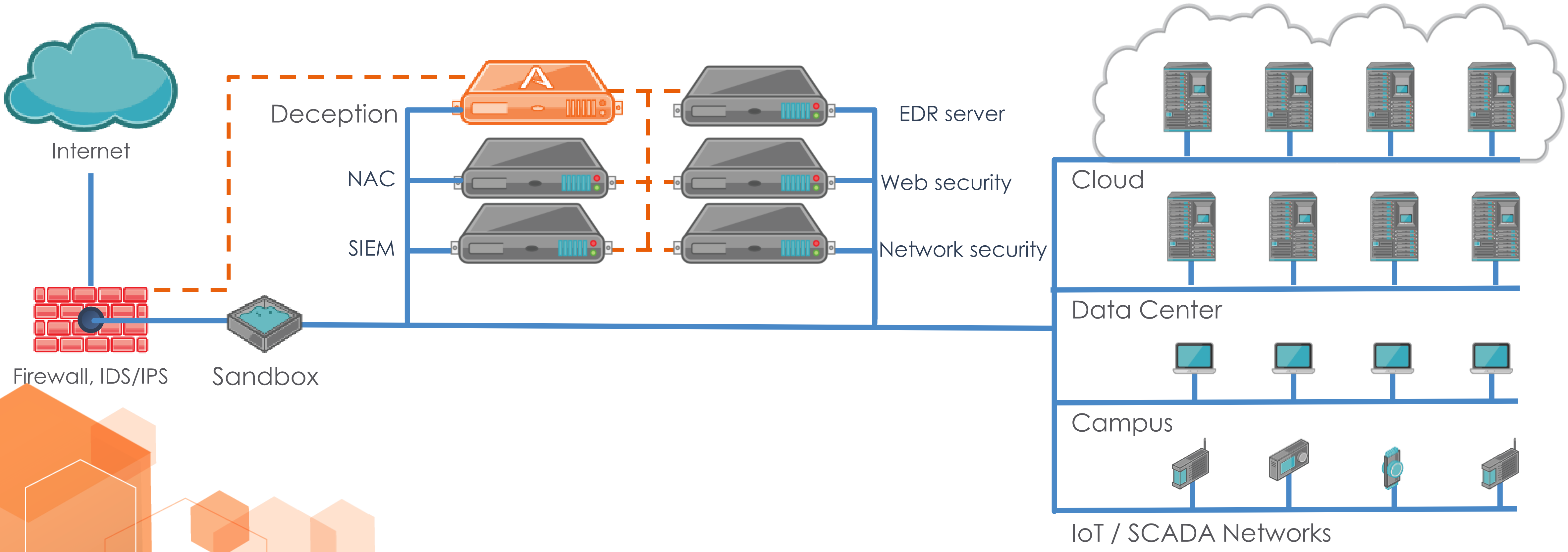


Deceptions

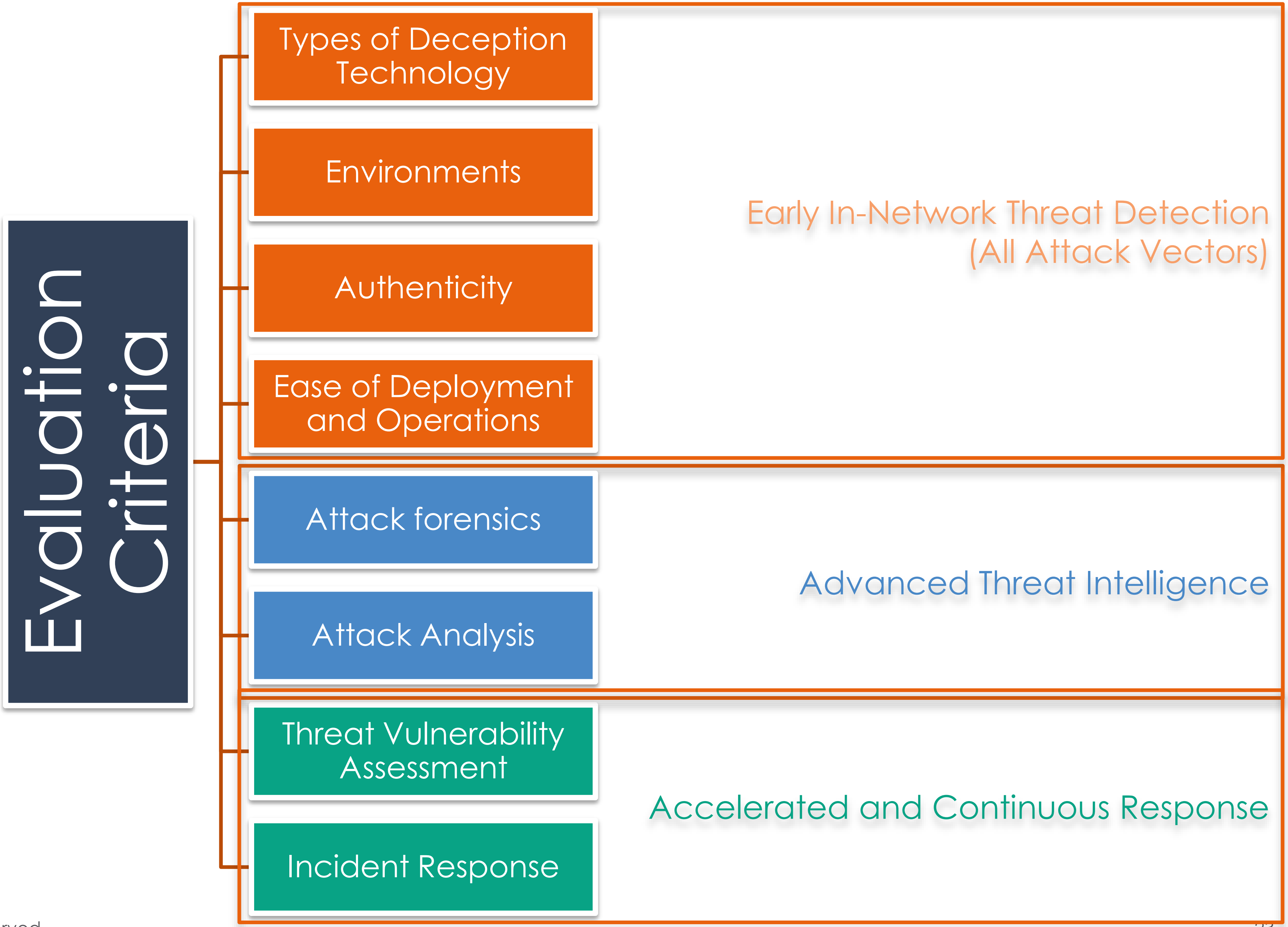
- Operating System
- Network Services
- IoT & SCADA Protocols

Real-Time Detection and Attack Analysis + Substantiated Actionable Alert + Actionable Forensics + Network Visibility + 3rd Party Response Action Integrations

Adaptive Defense for Continuous Threat Response



Guide to Evaluating Deception Technology and Providers



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

"All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."

Sun Tzu

Thank you.