Attivo NETWORKS®

The Critical Role of Deception in Security Automation

Tony Cole | Chief Technology Officer

Deception Definition

de·cep·tion
dəˈsepSH(ə)n/

noun
1.the action of deceiving someone.
"obtaining property by deception"
- **a thing that deceives.**

"a range of elaborate deceptions"

synonyms:

deceit, deceitfulness, **duplicity**, **double-dealing**, **fraud**, cheating, **trickery**, **chicanery**, deviousness, slyness, wiliness, **guile**, **bluff**, **lying**, **pretense**, **treachery**;

Everyday Deception

Dating

Cinema

Gambling

Magic

Online

Fools Gold

Why Cyber Deception: Preventative Solutions Fail

You Know the Problem (Breakout Time & Dwell Time)

You have on average 4 ½ Hours to stop a breach:

- Before a nation-state attacker moves laterally
- Before they create more beach-heads in your enterprise
- Before they potentially get to their objective

***CrowdStrike 2019 Global Threat Report**

On average, global dwell time is 101 days:

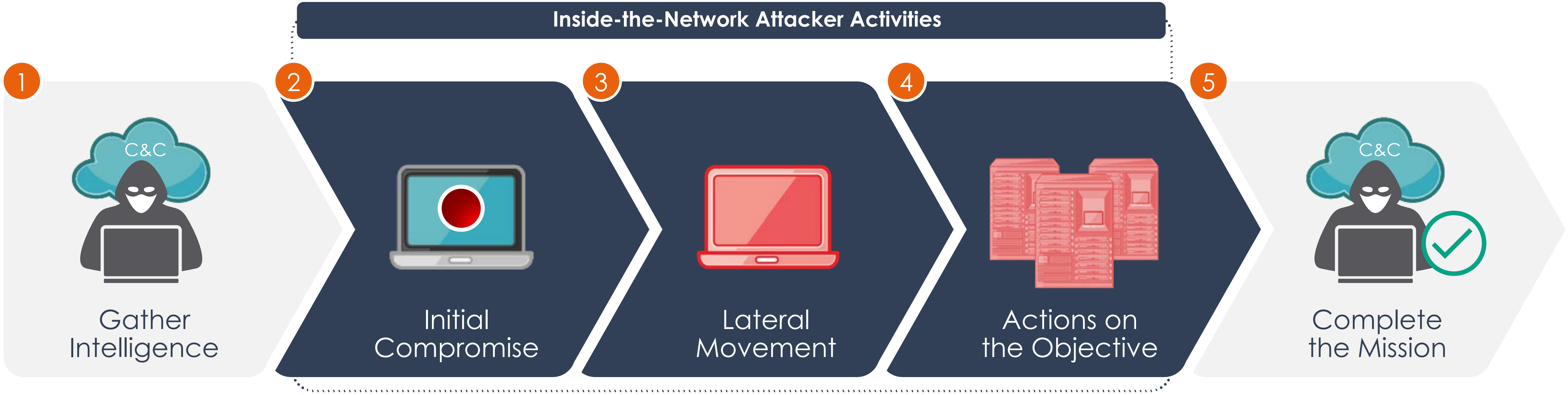
- Before an adversary is detected in an environment
- And much worse in many regions outside North America
- Before Containment of the breach even begins

***FireEye/Mandiant 2018 M-Trends Report**

Key Takeaway: Preventative technology strategies are not working.

Current Detection Gaps

Attackers Are Bypassing Prevention and Evading Detection



Inside-the-Network Attacker Activities

1 C&C Gather Intelligence

2 Initial Compromise

3 Lateral Movement

4 Actions on the Objective

5 C&C Complete the Mission

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

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

Deception

- Steal Data
- Destroy Data
- Ransom
- Sabotage Systems

Security Detection Challenges

Deception Technology: Closes the Detection Deficit

Challenges	Deception-Based Solution
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	SCADA, IOT, POS, SWIFT, Telecom, Router Decoy 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

Defeating Modern Attackers Requires A New Strategy

Arm the Defender

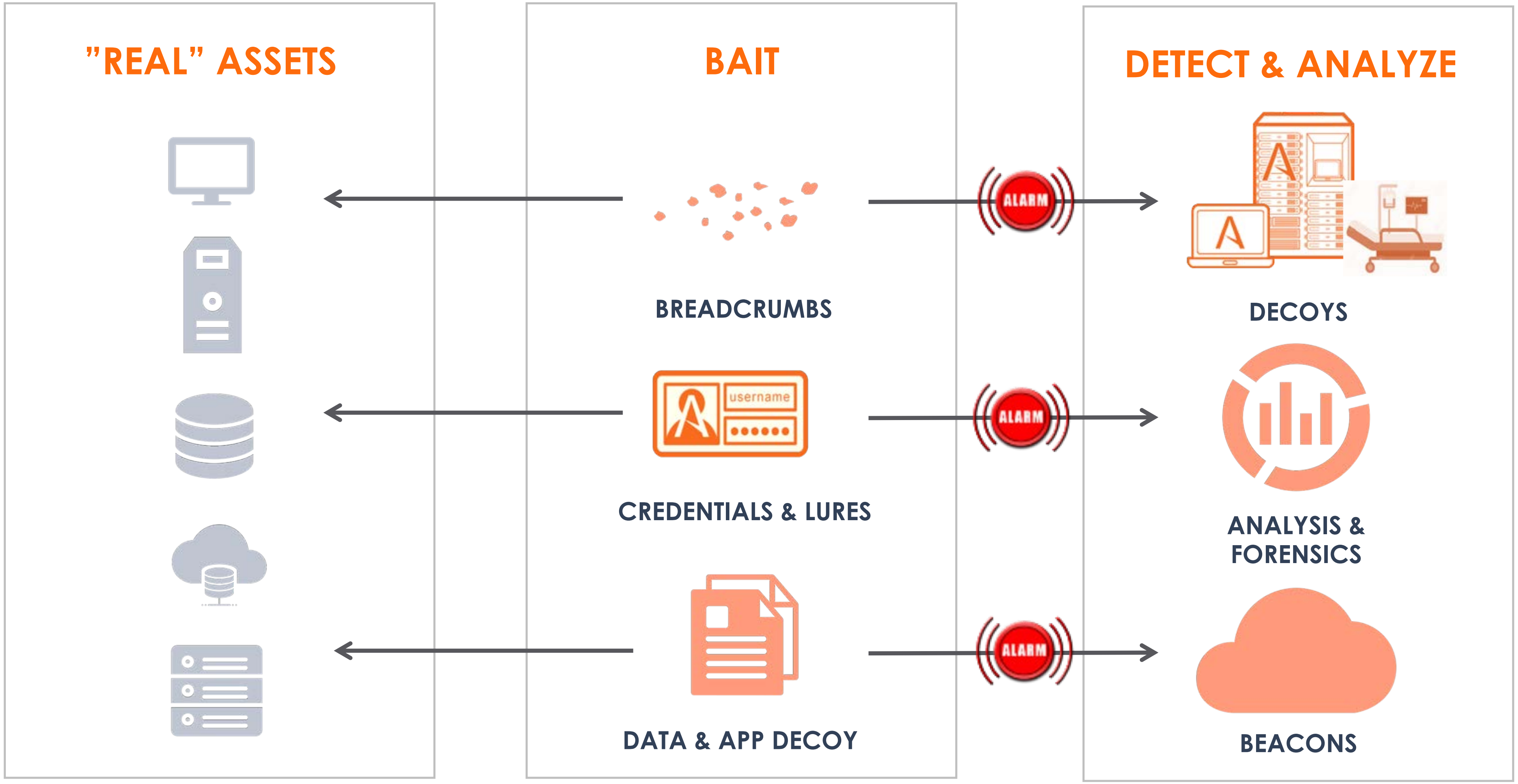
1 Effective regardless of how an attacker attacks

2 Early & scalable detection across all attack surfaces

3 Delivers intelligence on origin, tools, techniques, and attacker motives

4 Arms defender to respond decisively, automate response, build active defenses

DECEPTION ARCHITECTURE



”REAL” ASSETS

BAIT

BREADCRUMBS

CREDENTIALS & LURES

DATA & APP DECOY

DETECT & ANALYZE

DECOYS

ANALYSIS & FORENSICS

BEACONS

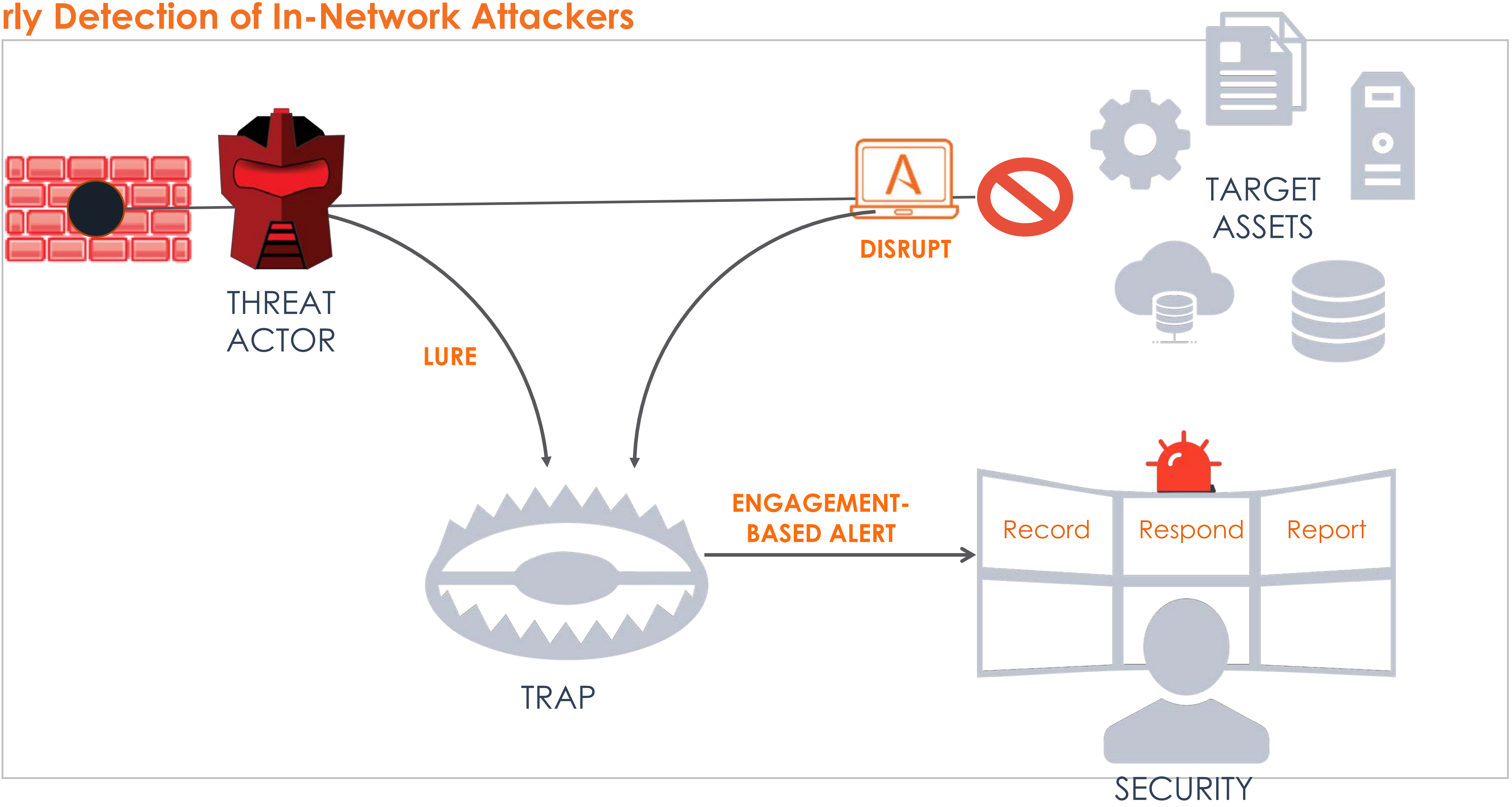
REDUCE
Dwell Time

REDUCE
Response Time

GAIN
Counterintelligence

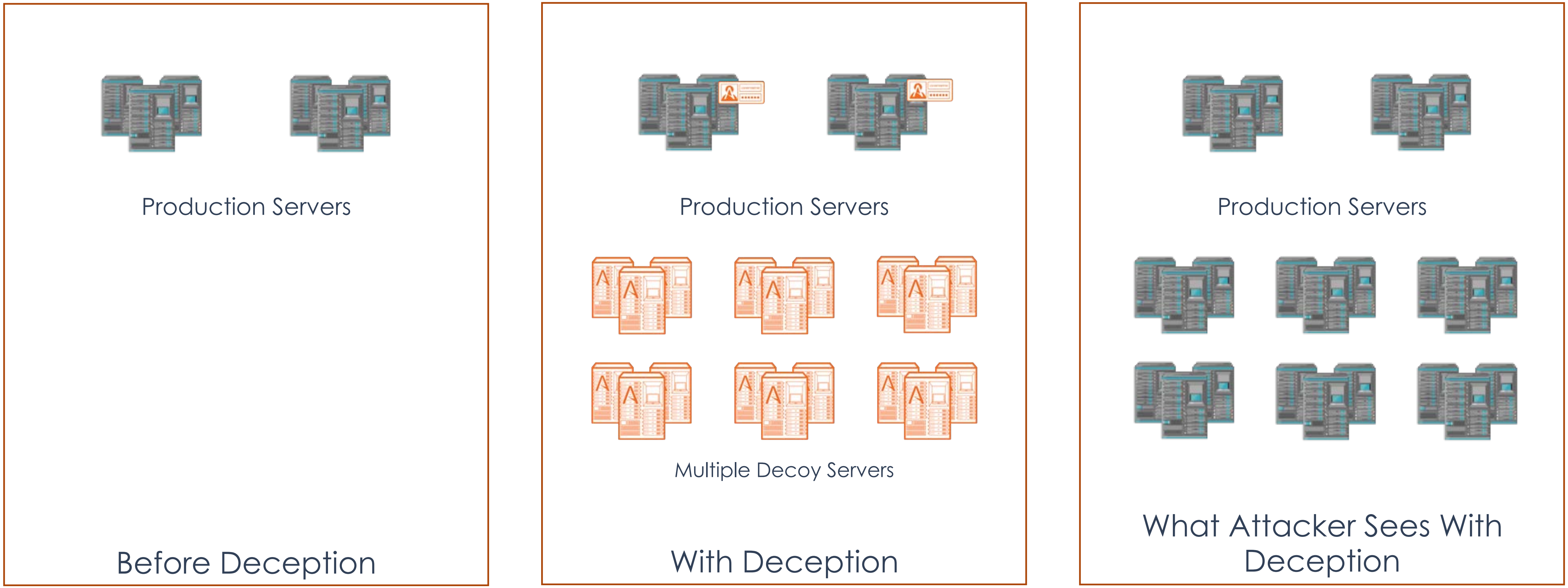
How Deception for Threat Detection Works

Early Detection of In-Network Attackers



Obscuring Your Infrastructure

Confuse and Misdirect to Make the Attacker's Job Harder



Production Servers

Before Deception

Production Servers

Multiple Decoy Servers

With Deception

Production Servers

What Attacker Sees With Deception

Deception Platform: Believability

High-interaction decoys appear identical to production company assets

50+ campaigns

USER DATA

- Memory credentials
- Active connections
- Credential lures
- SMB shares lures
- Browser credentials, history, shortcuts
- Application credentials
- Vulnerable data in SMB Shares
- PC, Mac, Linux deceptive credentials

APPLICATIONS | *CUSTOMIZE WITH YOUR OWN GOLDEN IMAGE*

- FTP/SFTP
- HTTP/HTTPS
- Print
- SMB
- NBNS
- SSH
- SMTP
- SWIFT Messaging
- SNMP
- Telnet
- RDP
- GIT
- mDNS
- MySQL
- Apache
- Tomcat
- Jboss
- SVN/CVS
- VPN
- Mongo DB, ES, Redis
- WinRM
- AD
- MSSQL

ICS/SCADA

- Modbus
- BACnet
- Siemens S7comm
- IPMI
- Common Industrial Protocol (CIP)

IoT/IoE

- MQTT
- CoAP
- XMPP
- Health Level-7
- Digital Imaging & Comms in Medicine (DICOM)

OPERATING SYSTEMS

Windows XP 7 2008 2016 8 10 2012

ubuntu 12.04 & later

CentOS

redhat 6.5

Cisco IOS SOFTWARE

PLATFORM

amazon web services

Microsoft Azure

openstack.

ORACLE CLOUD

Microsoft Hyper-v

vmware

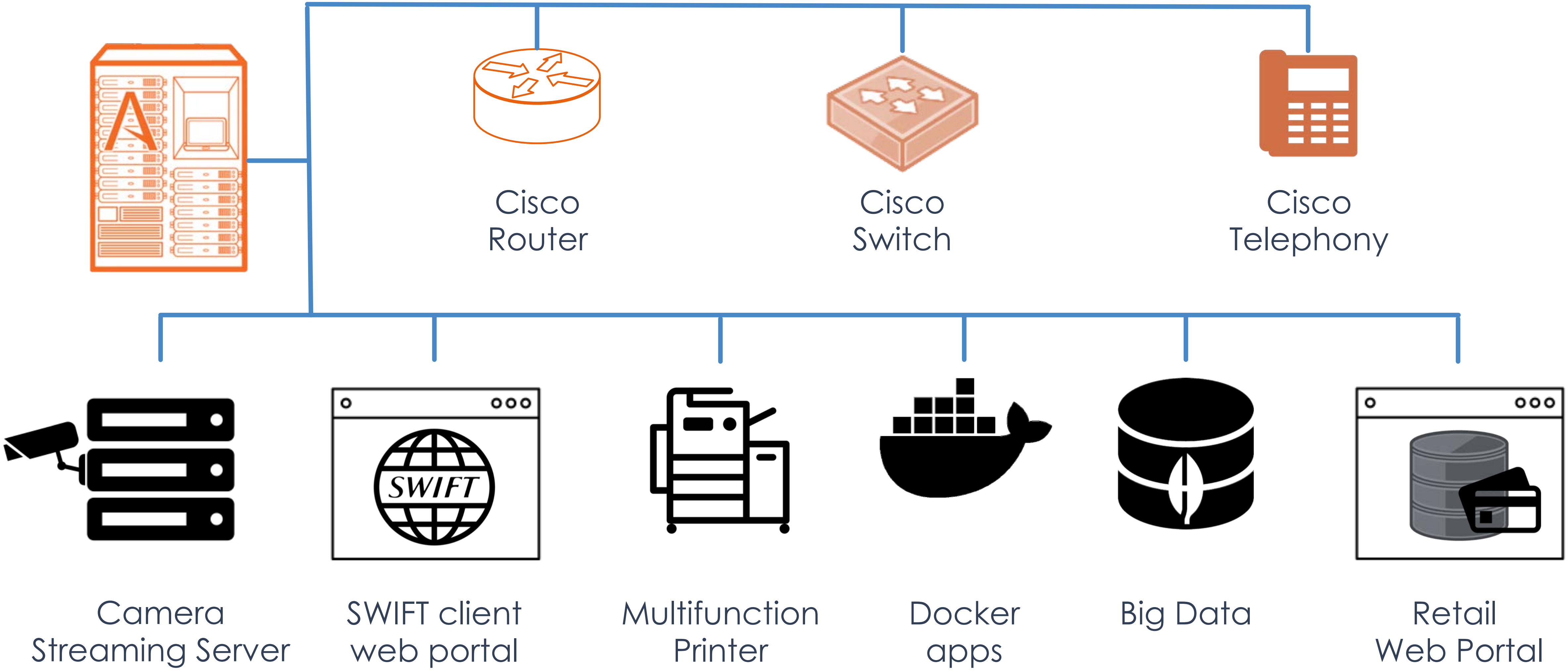
Google Cloud Platform

Appliance

The BOTsink Addresses Evolving Attack Surface with Authentic and Attractive Deception

Unconventional Attack Surface Deceptions

Expanded Decoy and Deception Portfolio

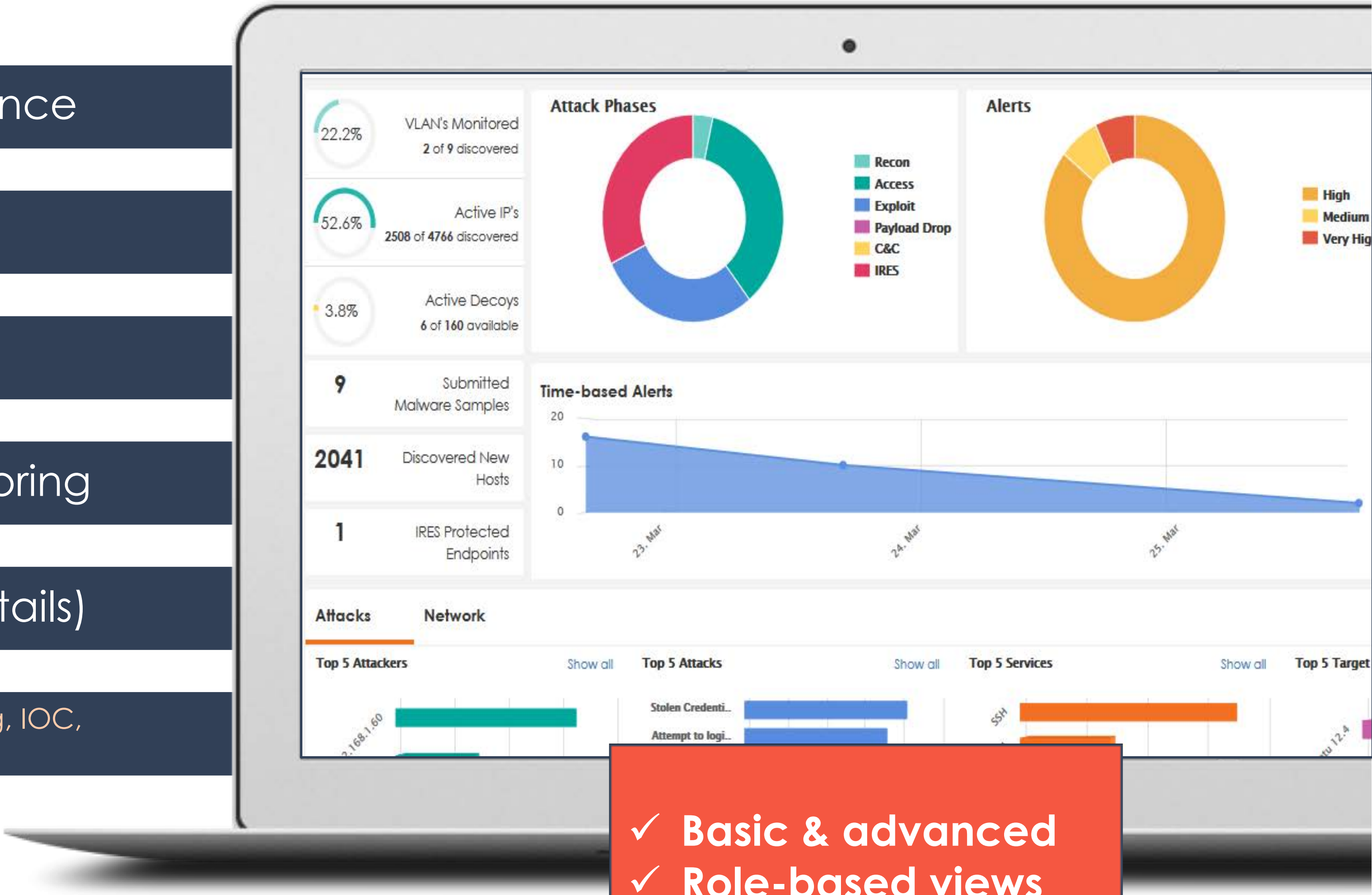


Comprehensive Threat Intelligence

Threat Visibility With Actionable Dashboards

Reporting and Analysis

- Centralized Threat Intelligence
- Kill Chain Attack Analysis
- Attack TTP Information
- VM Management & Monitoring
- Network Visibility (VLAN details)
- Reporting UI, PCAP files, Syslog, IOC, and CSV formats



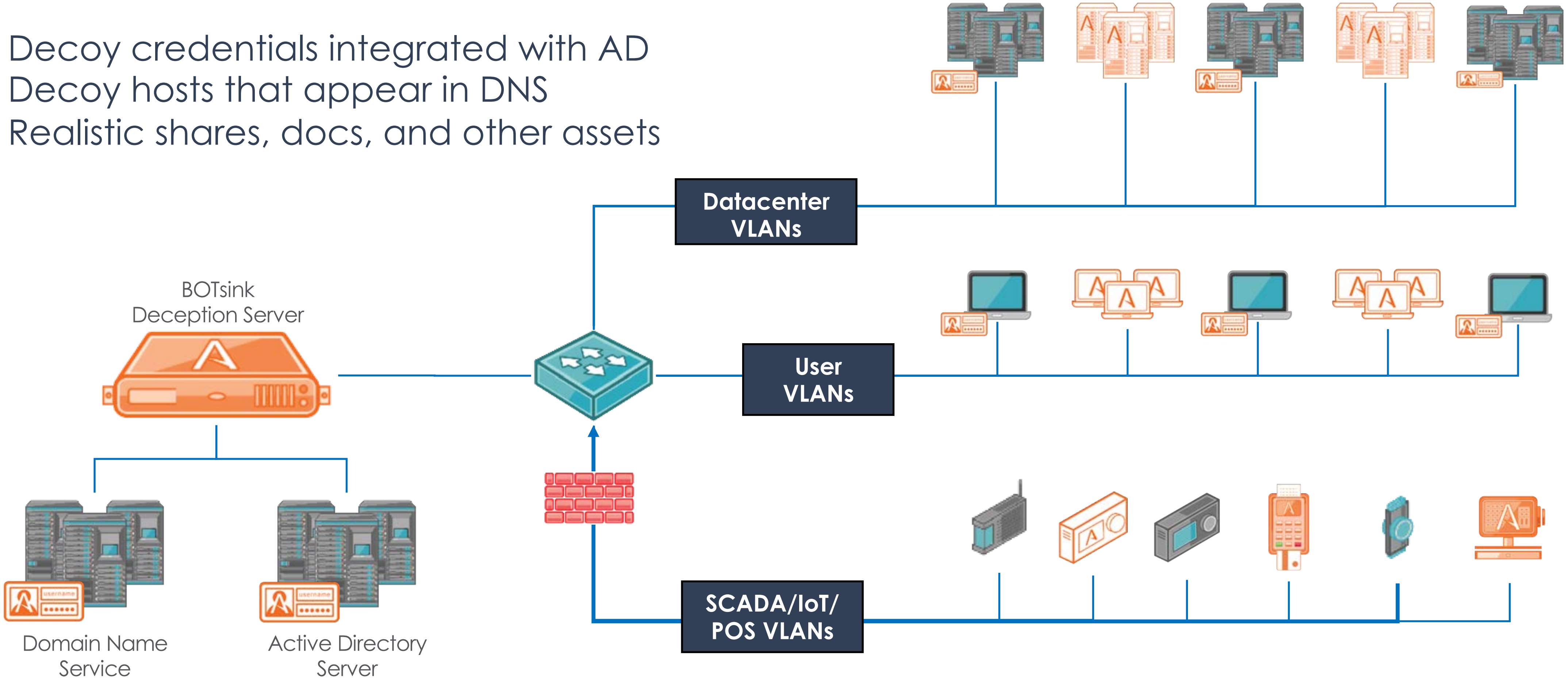
- ✓ Basic & advanced
- ✓ Role-based views

Automatic Deployment

Identify the Threat Space, Adapt, then Automatically Deploy Decoys and Lures

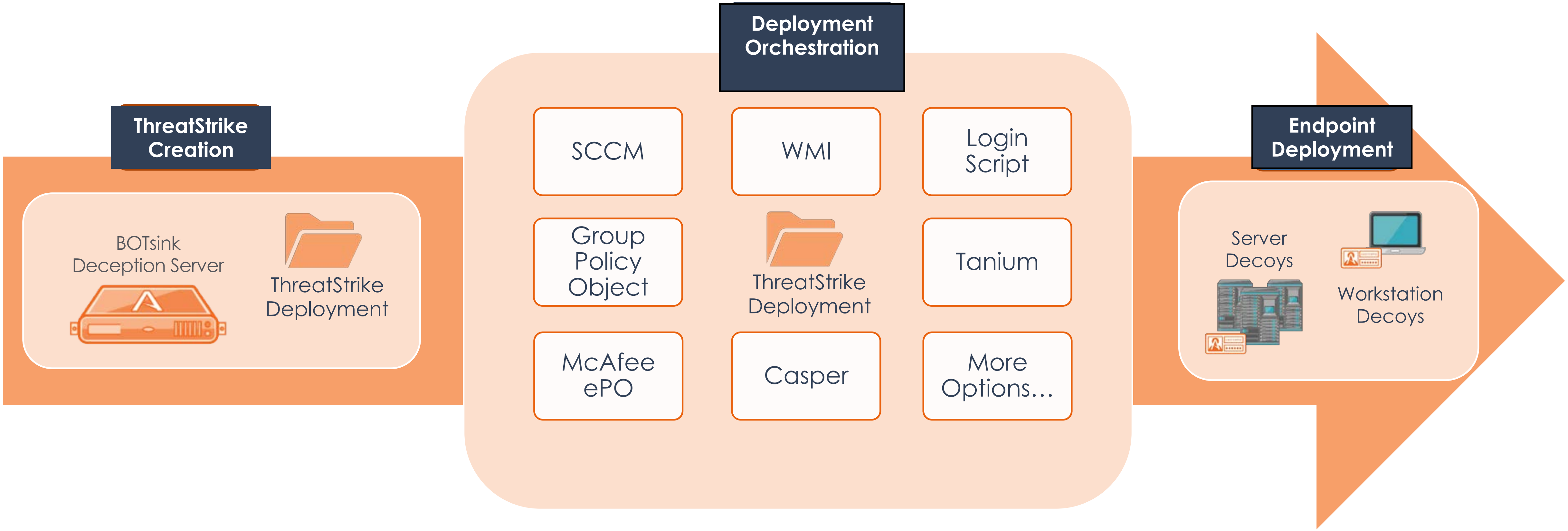
Realistic credentials and assets

- Decoy credentials integrated with AD
- Decoy hosts that appear in DNS
- Realistic shares, docs, and other assets



ThreatStrike™ Deployment Flexibility

Supports Multiple Deployment Methods



QuickDeploy
Self-Learning Deployment

Machine learn and auto-deploy based on existing environment

Deception Creation

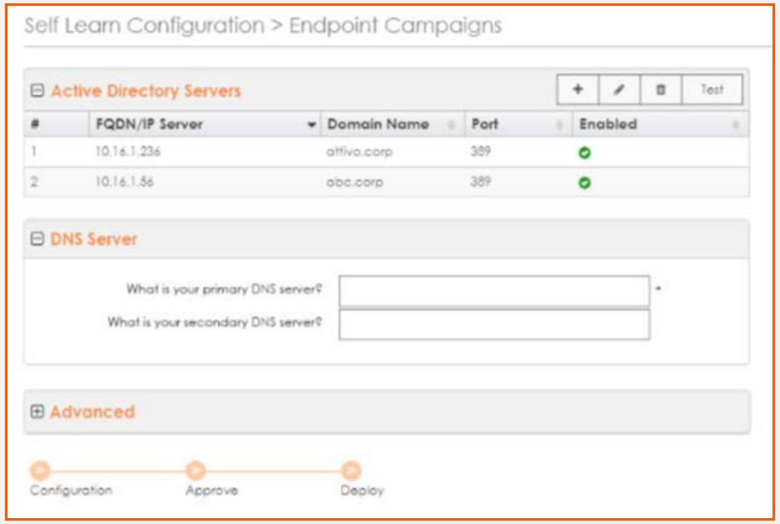
1. Select options for automated creation

2. Initiate learning

3. Review proposed deceptive content

4. Auto deploy

Automatically created & customized:



Self Learn Configuration > Endpoint Campaigns

⊟ Active Directory Servers

#	FQDN/IP Server	Domain Name	Port	Enabled
1	10.16.1.236	attivo.corp	389	✓
2	10.16.1.56	abc.corp	389	✓

⊟ DNS Server

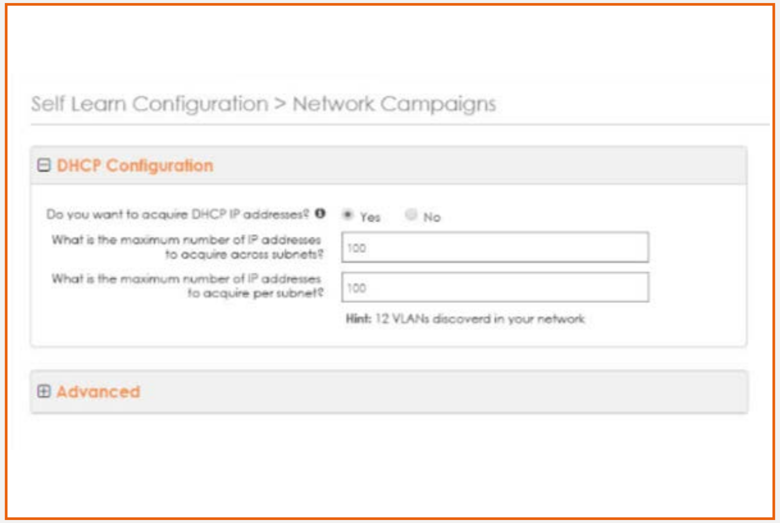
What is your primary DNS server? *

What is your secondary DNS server?

⊞ Advanced

Endpoint credentials - Agentless

- Lures & decoy campaign families
- Services
- Domains & hostnames
- MAC addresses



Self Learn Configuration > Network Campaigns

⊟ DHCP Configuration

Do you want to acquire DHCP IP addresses? ● Yes ○ No

What is the maximum number of IP addresses to acquire across subnets? 100

What is the maximum number of IP addresses to acquire per subnet? 100

Hint: 12 VLANs discoverd in your network

⊞ Advanced

Decoys

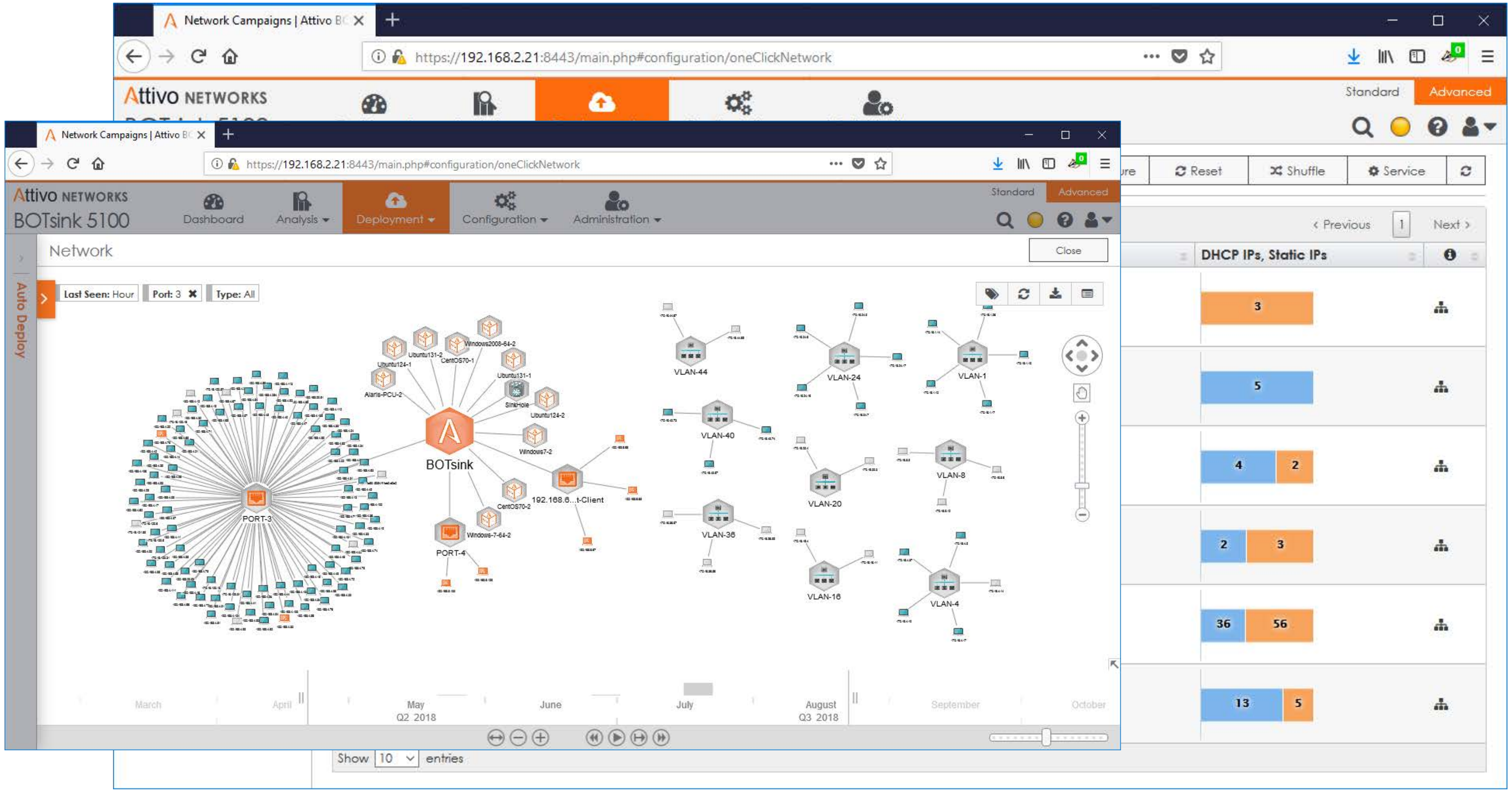
- Deploys decoy campaigns
- Engages services relevant to each network
- Domains & hostnames
- MAC addresses

Automatic Deployment

Identify the Threat Space, Adapt, then Automatically Deploy Decoys and Lures

Easy Network Deployment

- Automatic VLAN ID
- Automatic subnet ID
- Automatic Service ID
- Automatic OS ID

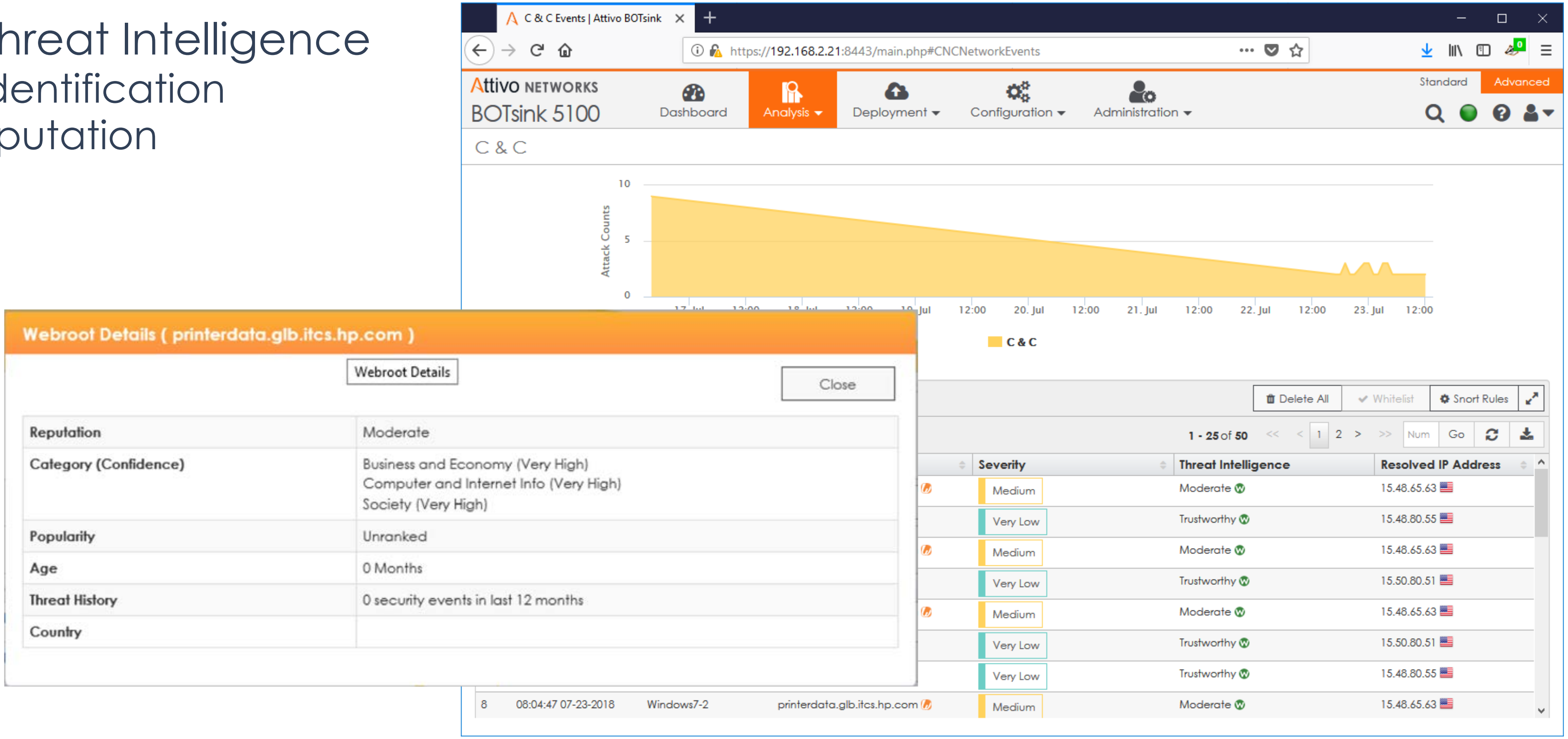


New: Comprehensive Threat Intelligence

Threat Intelligence from Multiple Feeds

Multiple options for Threat Intelligence

- Included Malware identification
- Included Domain reputation
- Partner integrations:
  - Webroot
  - ThreatConnect
  - DXL
  - VirusTotal
  - ReversingLabs
    - Q4



				Severity	Threat Intelligence	Resolved IP Address
				Medium	Moderate	15.48.65.63
				Very Low	Trustworthy	15.48.80.55
				Medium	Moderate	15.48.65.63
				Very Low	Trustworthy	15.50.80.51
				Medium	Moderate	15.48.65.63
				Very Low	Trustworthy	15.50.80.51
				Very Low	Trustworthy	15.48.80.55
8	08:04:47 07-23-2018	Windows7-2	printerdata.glb.itcs.hp.com	Medium	Moderate	15.48.65.63

Webroot Details (printerdata.glb.itcs.hp.com)

Reputation	Moderate
Category (Confidence)	Business and Economy (Very High) Computer and Internet Info (Very High) Society (Very High)
Popularity	Unranked
Age	0 Months
Threat History	0 security events in last 12 months
Country	

New: Comprehensive Threat Intelligence

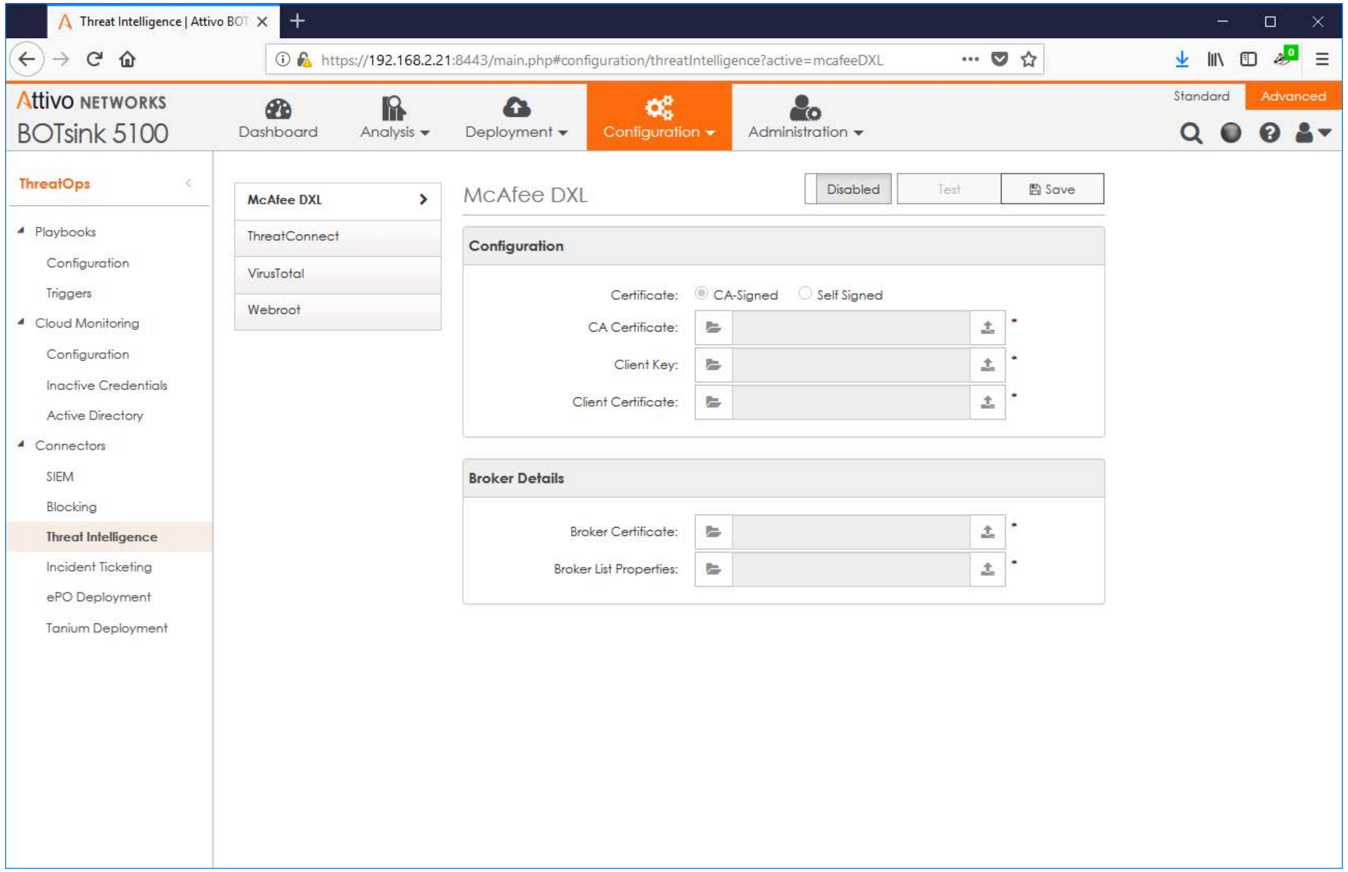
Optional Integrations

Integration with McAfee DXL

- Pass event information
- Exchange IoC’s with partners
- Get the reputation of any dropped payload with DXL

Benefits

- Accelerates IR
- Efficient Threat Intelligence sharing
- Eliminates manual workflow
- Facilitates Threat Hunting



McAfee DXL

Configuration

Certificate: ● CA-Signed ○ Self Signed

CA Certificate: *

Client Key: *

Client Certificate: *

Broker Details

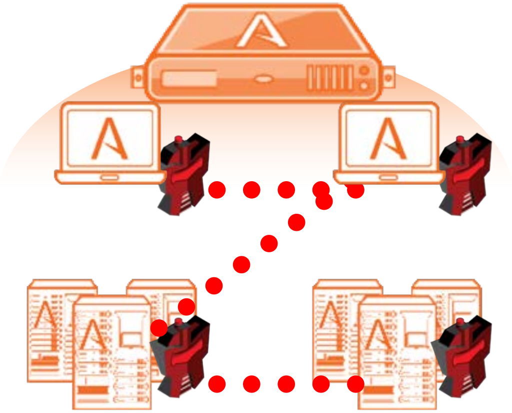
Broker Certificate: *

Broker List Properties: *

Multi-Dimensional Forensics Capabilities

For Faster Remediation and Hunting

Data Collection and Analysis



Capture forensic artifacts

Capture and analyze attacker memory

New

Assemble and report full TTP

Polymorphic attack tracking and signatures

New: Counterintelligence with DecoyDocs

Data Loss Tracking (DLT)

Data Sharing and Actioning

SIEM

SIEM integration and attacker behavior analysis

3rd Party integrations with automated response

Repeatable Processes

Repeatable playbooks based on company’s security infrastructure and policies

Attivo Networks: Native Partner Integrations

Integrations and Playbooks for Automated Incident Response

Distribution

McAfee™

TANIUM™

Endpoint management solutions such as SCCM, WMI, Casper, and others

Investigation / Analysis & Hunting

IBM QRadar

splunk>

LogRhythm™

ForeScout™

THREATCONNECT™

McAfee™

TANIUM™

Carbon Black.

MICRO FOCUS®

virustotal

Ticketing

servicenow

Traffic Redirection

McAfee™

Contain / Network Blocking

Check Point® SOFTWARE TECHNOLOGIES LTD.

JUNIPer® NETWORKS

FORTINET®

Symantec.

BLUE COAT

CISCO™

paloalto NETWORKS®

Contain / Endpoint Quarantine

Carbon Black.

CISCO™

CounterTack®

aruba a Hewlett Packard Enterprise company

TANIUM™

McAfee™

ForeScout®

Cloud Monitoring

Google™ Drive

box

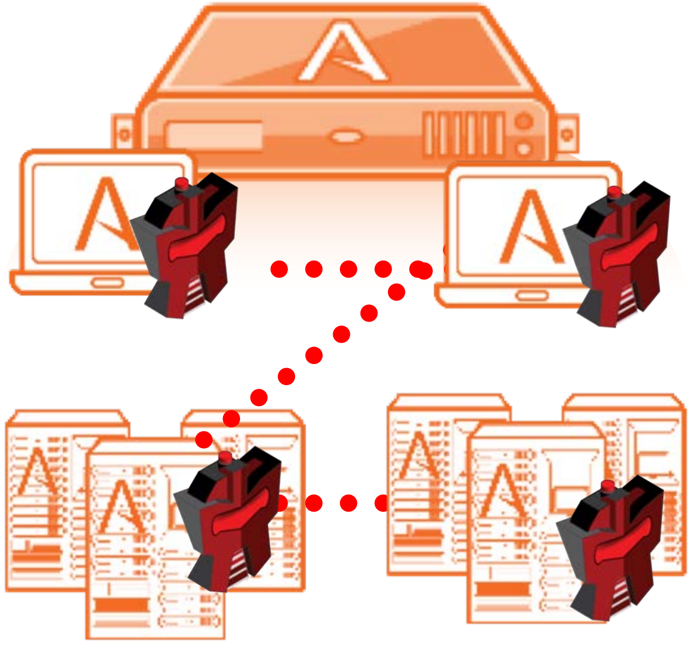
salesforce

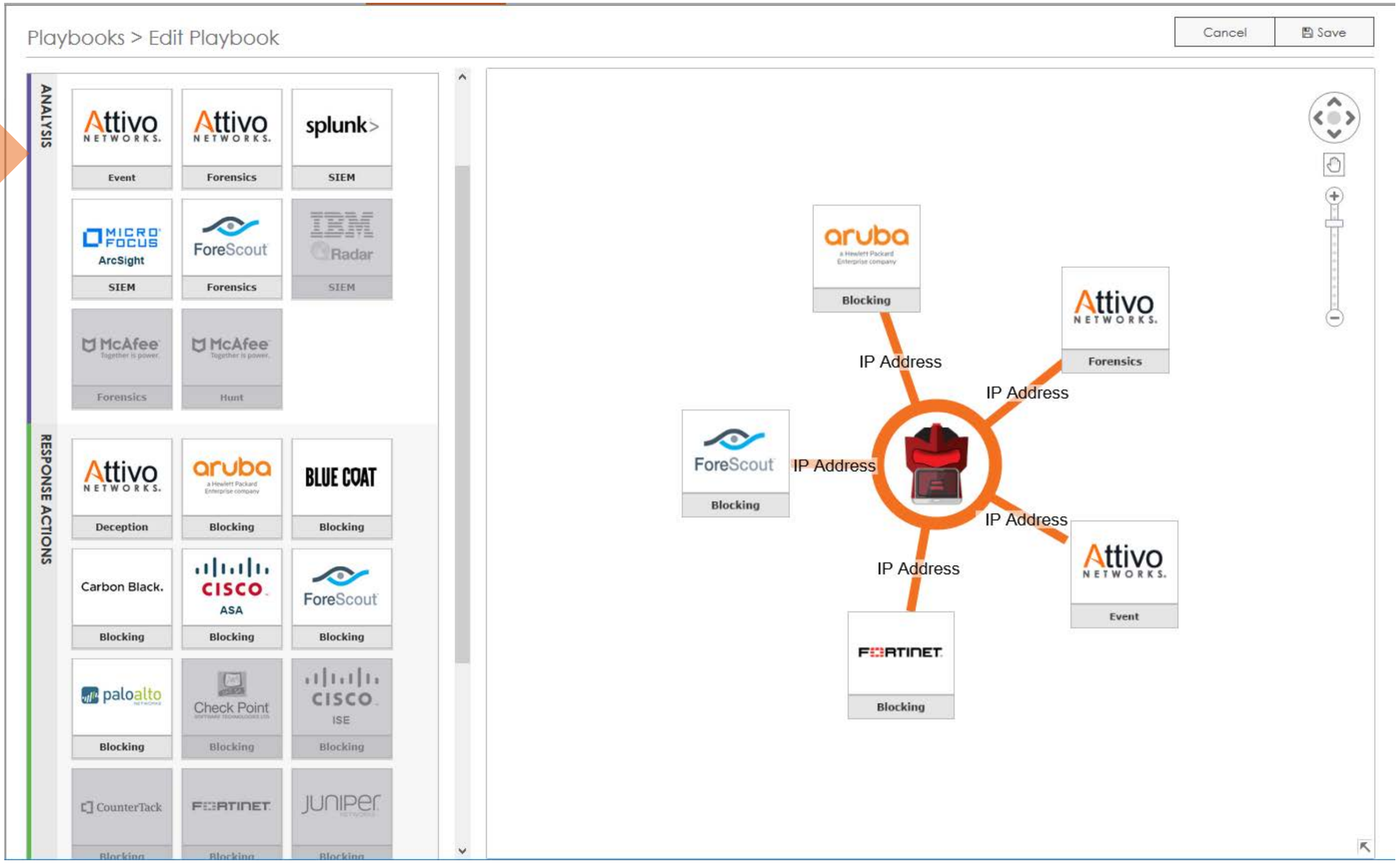
Orchestration

DEMISTO

Automated Incident Response & Playbooks

Automated Data Collection and Analysis





Substantiated Alerts

- Alerts only on engagement
- Collects Forensics adversary Intelligence
- Reduce response time: hours to minutes
- Detects criminal activity, policy violations, misconfig's

Scalable Operations

- Manage all your deception environments ubiquitously
- Centralized attack data and action
- Automated sharing amongst security controls

Ease of Management

- Machine-learning to prepare, deploy and maintain deceptions
- Non-disruptive out of band deployment &agentless on the endpoint
- Basic and advanced dashboards on prem or in the cloud

Deception Platform Savings & Benefits

Security teams will save time correlating, understanding, and responding given the high-fidelity of deception alerts.

Myths and Realities of Deception

It is Easy to Detect	**False:** Real OS/Golden Images, dynamic deception, Active Directory integration match production assets; Pen Testers consistently deceived.
It is Resource Intensive	**False:** Alerts are engagement based and automated attack analysis simplifies incident handling and response.
It is Hard to Operate and Not Scalable	**Depends:** Non-inline designs are Friction-less to deploy and provide Cloud and Data Center Scalability; End-point deployment depends on approach.
It Creates a Dirty Network	**Depends:** Understand how decoys are deployed; see what tools they provide to whitelist and not interfere with other tools.
No Incremental Value	**False:** Achieves early detection at the end-point and in-network. DDP’s also provide the automations and integrations for simplified response.
There is Legal Risk	**False:** Unless counter hacking, deception is viewed in line with typical security defense controls.

Impact

What do deception users say?

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.

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 Effective In-network Threat Detection
- Role of Deception Tech
- Evaluating Deception Technology Differences
- Customer Value

Conclusion

- Deception plays a critical role in the security stack
- Deception arms the defender with a lifeline for early detection and accelerated response
- Deception is not limited to organizations with a mature security program
- Deception platforms are not Created equal

Use a Page Out of an Attacker's Playbook. Use Deception.

Detect them Quickly, Exploit Their Trust, Create Uncertainty, Change The Game!

Can't Tell Real From Fake

Make Mistakes

Increase Attacker Costs

Spend More Time/ Start Over

Make Economics Undesirable

Find an Easier Target

Questions?

Tony Cole
tony@attivonetworks.com
Twitter: @nohackn

Deceive. Detect. Defend.

Company Background

Innovation that Shifts Power to the Defender

Leader in Deception-based Threat Detection & Response

Shipping Since 2014: Customer Proven Globally

#31 on the Deloitte Fast 500™

Hundreds of Customers Across All Major Verticals & Sizes Including multiple within the Fortune 10

Global Operations & Customer Success Programs

Attivo NETWORKS®

Deception

In-Network Detection

Actionable Response

Active Defense

Deceive. Detect. Defend.