Attivo NETWORKS

Using Deception Technology to Close Your Detection Gaps

Joseph R. Salazar, CISSP, CEH, EnCE

Technical Deception Engineer, Attivo Networks

October 28, 2019

root@kali:~# whoami

Secret Squirrel Stuff

Joseph R. Salazar

- CISSP, CEH, EnCE
- IT since 1995, InfoSec since 1997
- Major, USAR (retired) with 22 years as a Counterintelligence Agent, Military Intelligence Officer, and Cybersecurity Officer
- 19 years of private and public sector experience in Incident Response, Cybersecurity, and Computer Forensics
- Co-author, *Deception-Based Threat Detection – Shifting Power to the Defenders*

Company Background

Innovation that Shifts Power to the Defender

Innovator in Detection, Leader in Deception Technology

Shipping Since 2014: Customer Proven at Scale

#31 on the Deloitte Fast 500™

Customers Across All Major Verticals & Sizes Including 50%+ midmarket and multiple within the Fortune 10

Global Operations & Customer Success Programs

Attivo NETWORKS®

Deception

In-Network Detection

Actionable Response

Active Defense

Deceive. Detect. Defend.

5 million apps, 6 billion connected people, 26 billion devices
3 million shortfall in InfoSec…

The Attacker Mindset

How do I:

- get in?
- conduct reconnaissance undetected?
- install remote controlled backdoors?
- increase my access level?
- jump to different systems undetected?
- monitor, steal, change, or destroy data?

The Defender Mindset

Can I:

- prevent them?
- detect them?
- stop him?
- learn anything about them?

The Battle Has Moved Inside the Network

And the Adversary Has the Advantage

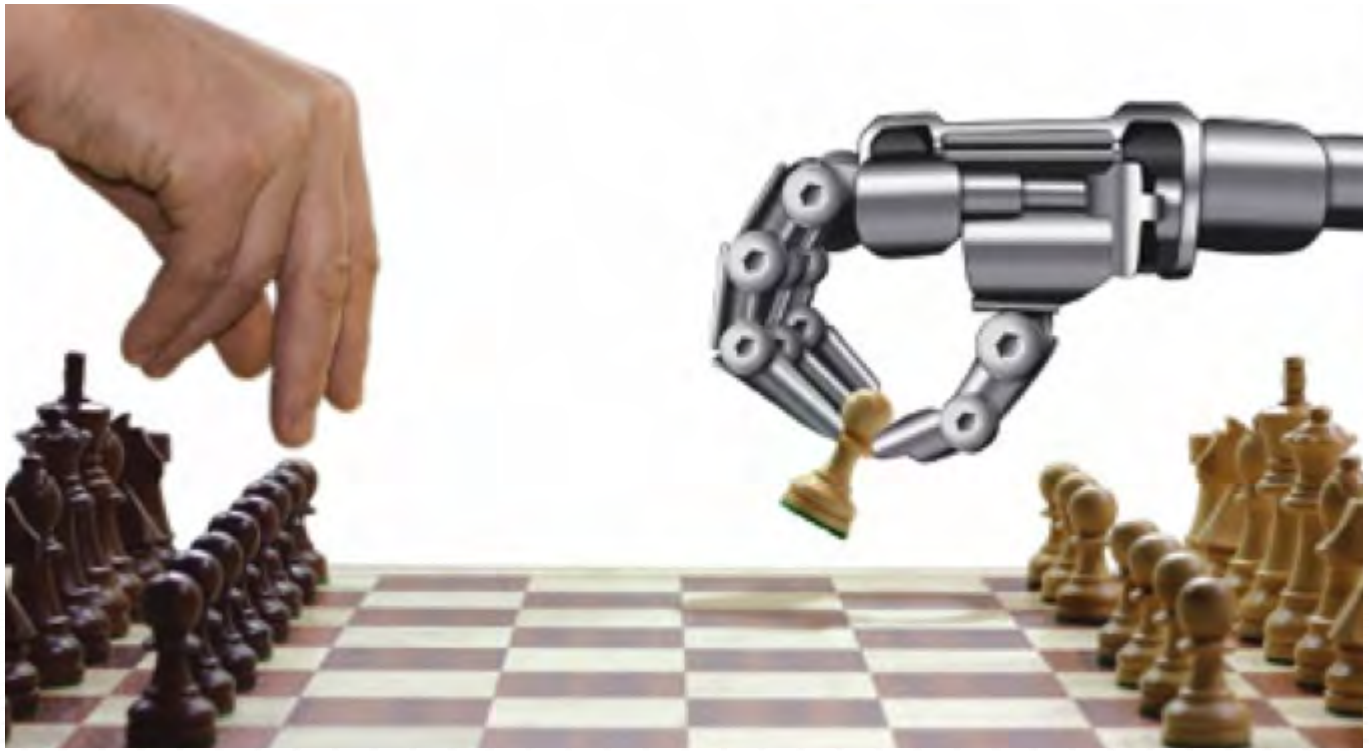
<5 Hours to Infiltrate
15 Hours to Exfiltrate
78 Days to Find

4.5 Hours to Break Out
60% Move Laterally
64% Will Return

Advantage of Time
Element of Surprise
Access to Information

Comprehensive Detection	Dwell Time Reduction	Actionable Intelligence

Our thinking and approach must evolve.



How Do You Defend Against Better Attackers?

Step 1: Remove the easy ways in!

- Education
- Pass phrases, password vaults, no defaults
- Separation and segmentation
- 2/Multi-factor authentication, OOB (not SMS)

Step 2: Accept that you don’t have a perimeter

- Laptops, iPhones, IoT took control away
- Computer No. 1 on your network is compromised
- 2018’s NGIPS/UBA/NGFW won’t help
- Reactive, static defenses won’t work

What Assets Do You Have?

Where are they?

Can you patch them?

Can they run AV?

Can they generate logs?

Step 3: Get eyes inside your world!

- Know where your assets are
- Understand attack paths and techniques
- Implement internal visibility mechanisms
- Apply deceptive, asymmetric defensive technology

Adversaries WILL Get In (if they aren't already there)

We can't stop them.

The question is simple…

HOW will you know,
WHEN will you know, and
WHAT are you going to do about it?

Detection Must Be Universal

How well can you defend your attack surface?

Why Deception?

This is what an attacker has encountered until this point...

This is what companies NEED...

Deception, A Page Out of an Attacker's Playbook

Exploit Their Trust, Create Uncertainty, Slow the Attack, Change The Game!

Threat Deception

Can't Tell Real From Fake

Make Mistakes

Increase Attacker Costs

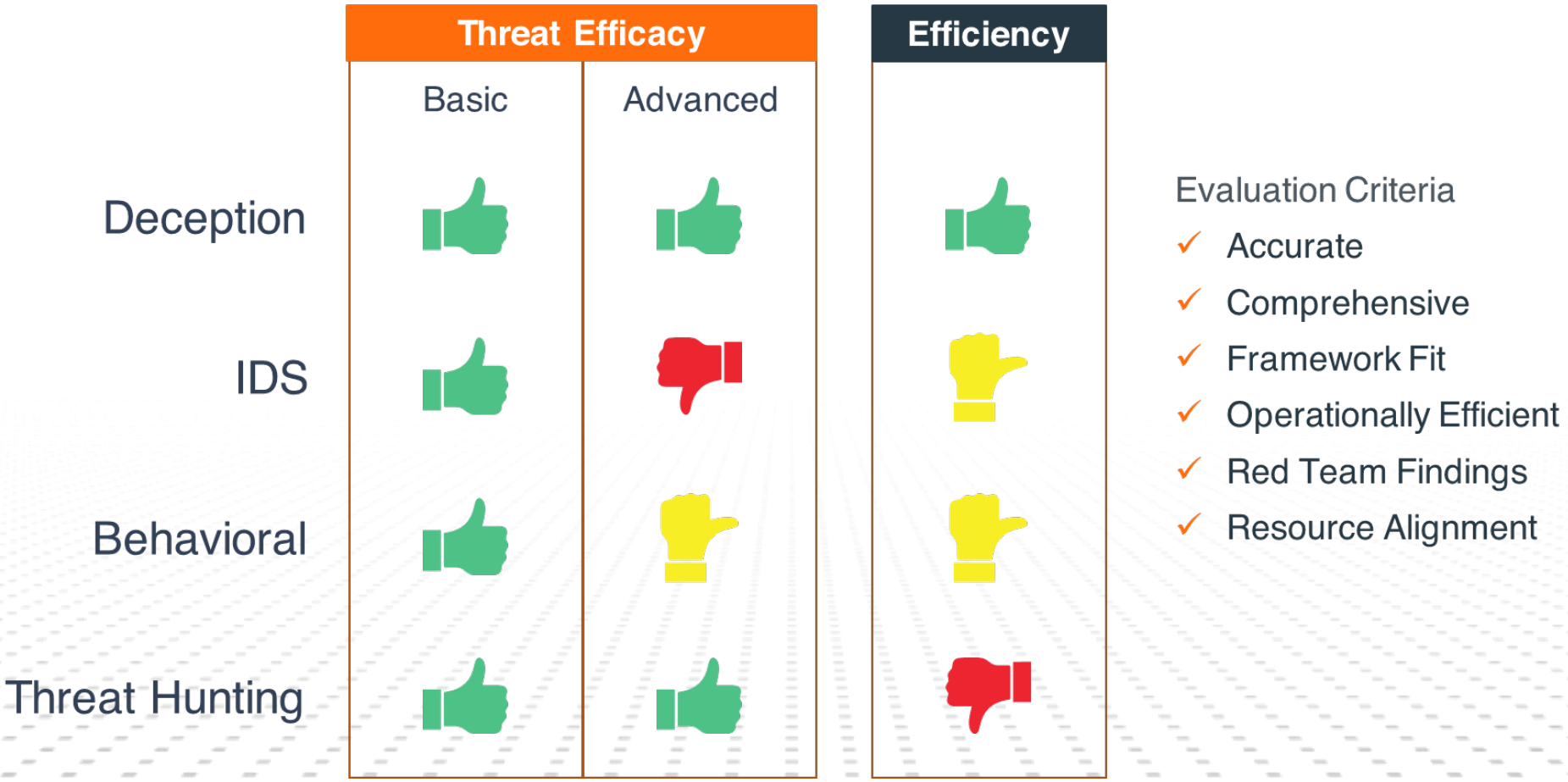
Spend More Time / Start Over

Make Economics Undesirable

Seeks an Easier Target

Which Detection Option is Best for You?

Considerations

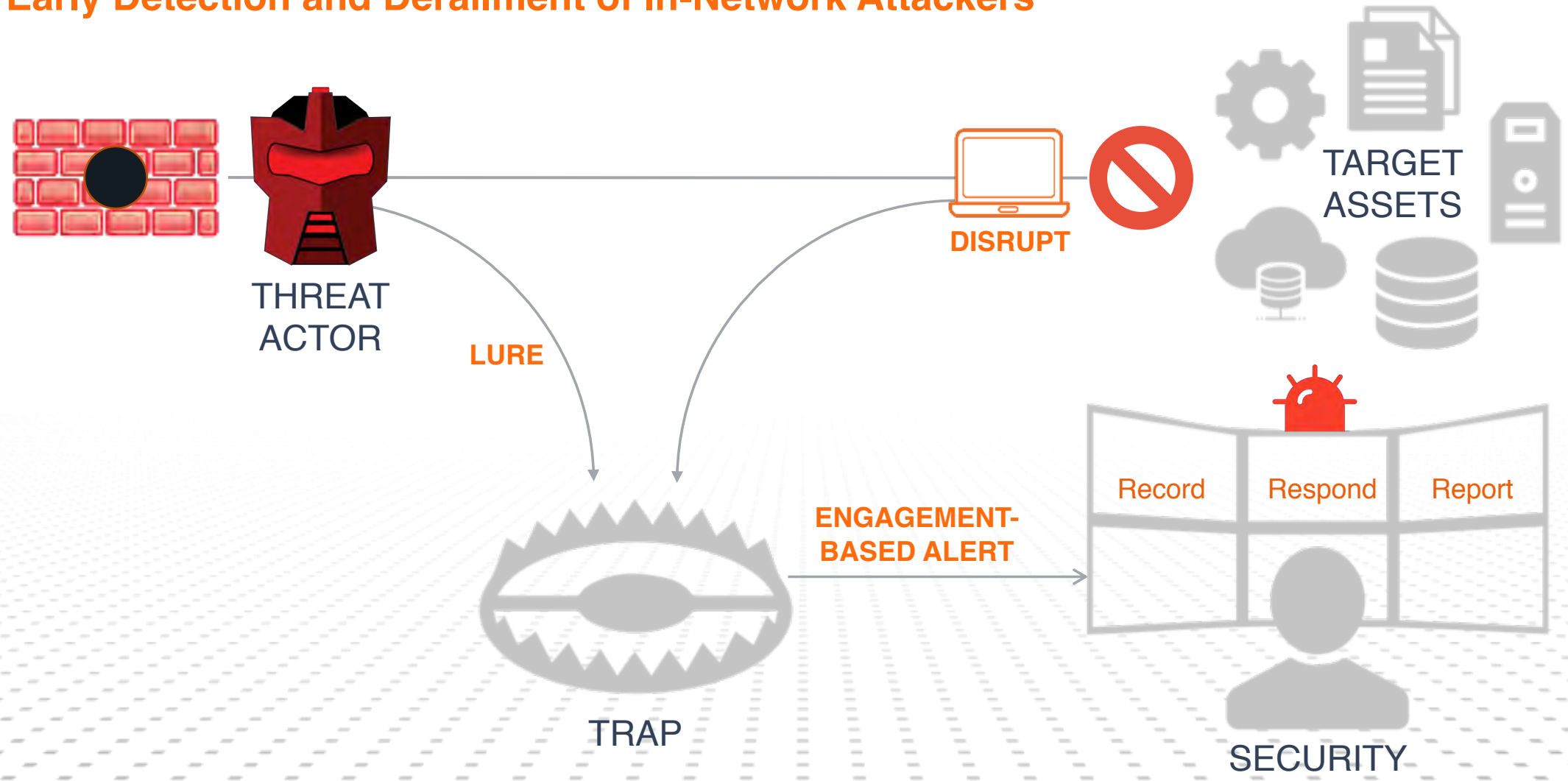


Evaluation Criteria

- ✓ Accurate
- ✓ Comprehensive
- ✓ Framework Fit
- ✓ Operationally Efficient
- ✓ Red Team Findings
- ✓ Resource Alignment

How Deception for Threat Detection Works

Early Detection and Derailment of In-Network Attackers



Why Honeypots are Not the Same as Deception

Honeypots

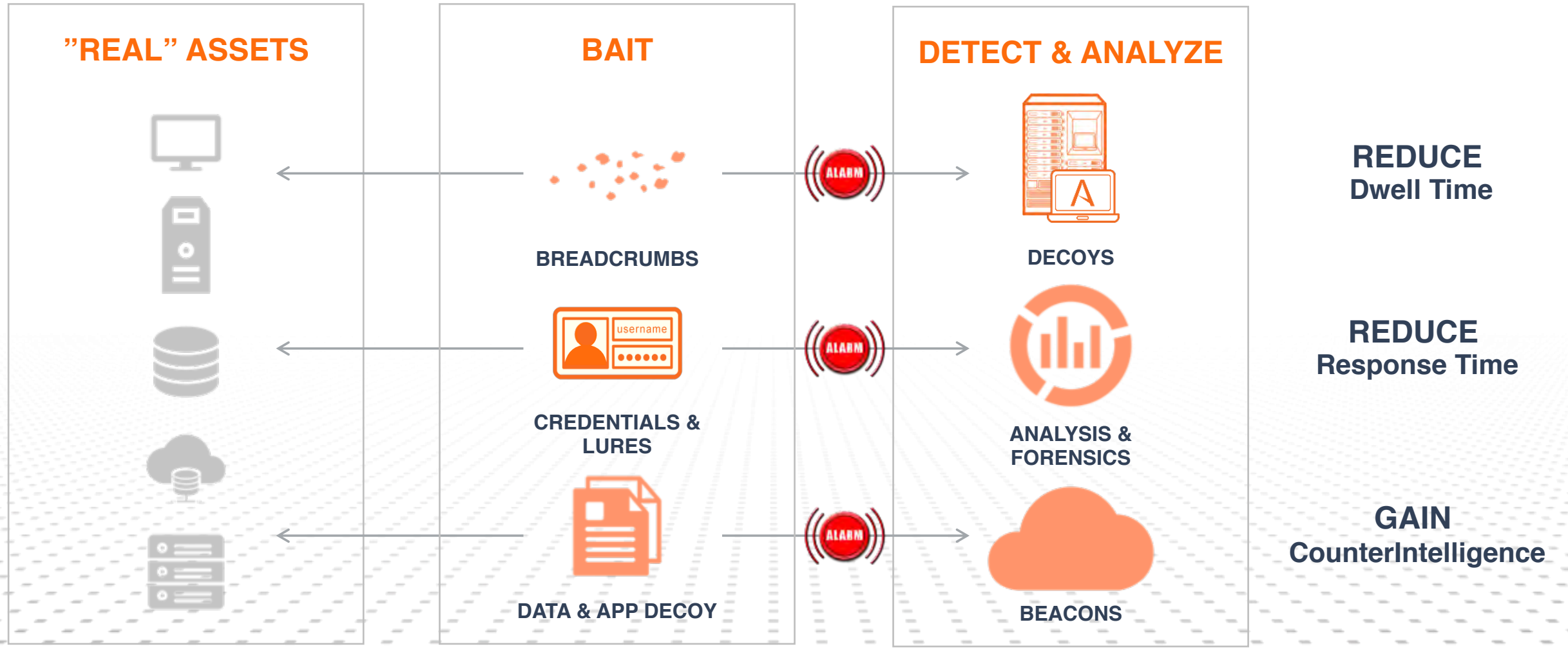
- Research
- Low Interaction
- Emulated
- Outside the Network

Deception Platforms

- Global Scale
- IR Automation
- Easy Operation
- Dynamic Deception
- Real OS, Services
- Network, Credential
- Inside the Network

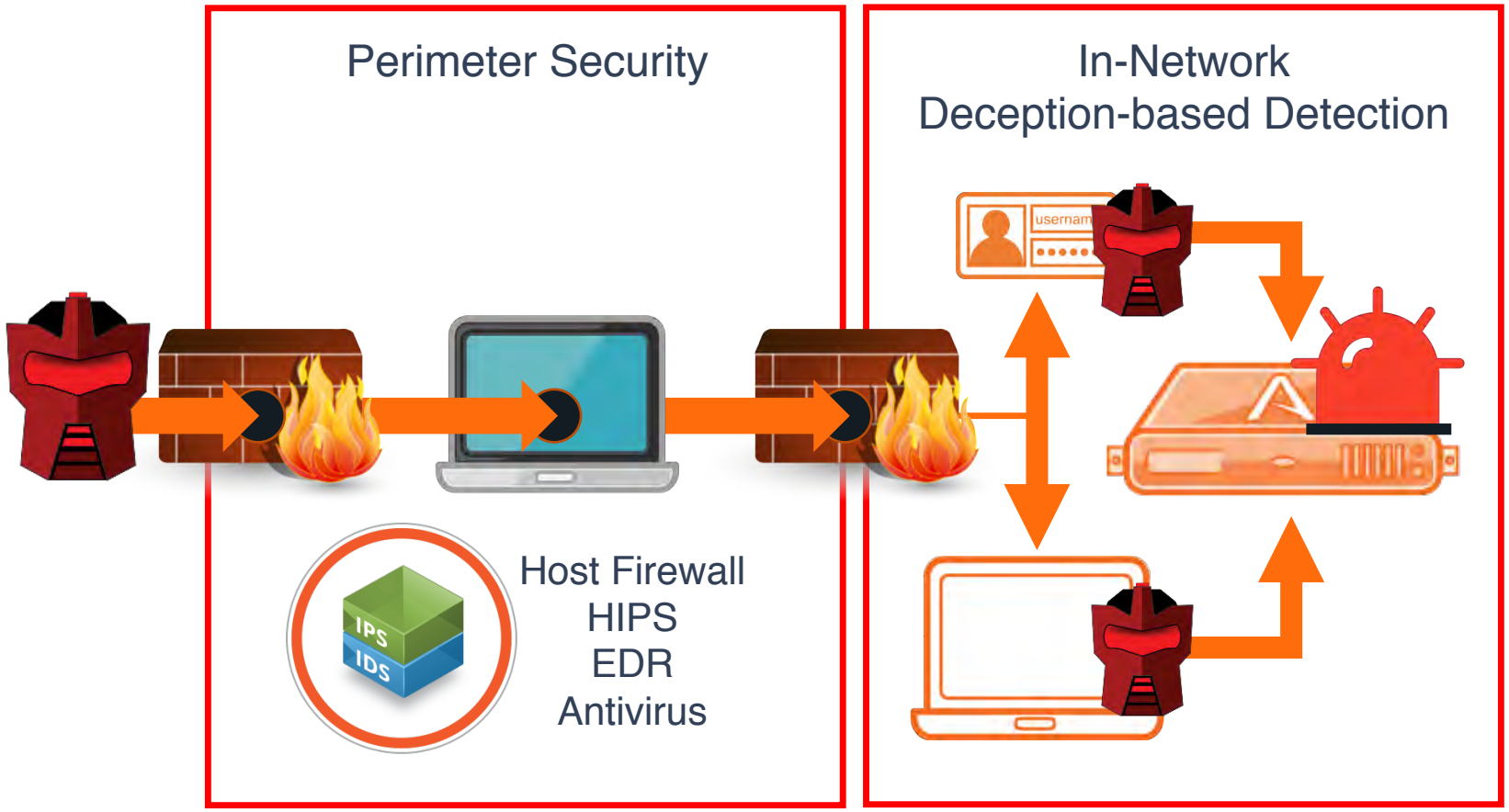
BOTs and Brute Force Attacker ⟵ Designed for ⟶ the Human Attacker

Deception Architecture



Deception in the Security Control Stack

In-Network Detection Closes Gaps and Reduces Dwell Time



Accurately alerts on what other controls miss

Network Reconnaissance

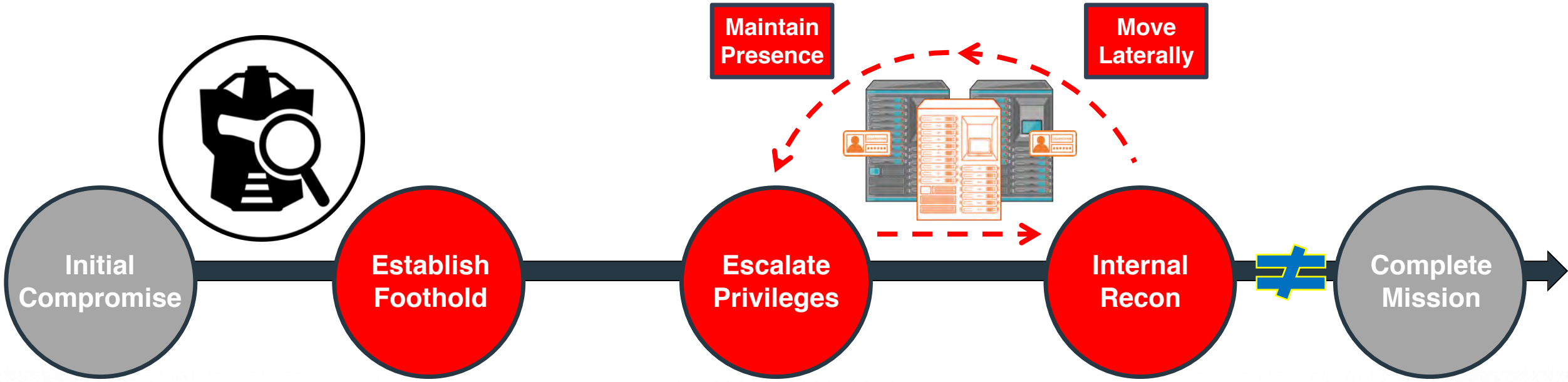
Active Directory Reconnaissance

Credential Harvesting

Man-in-the-Middle Attack

Early alerting when attackers bypass security

Deception's Role: Detect and Disrupt

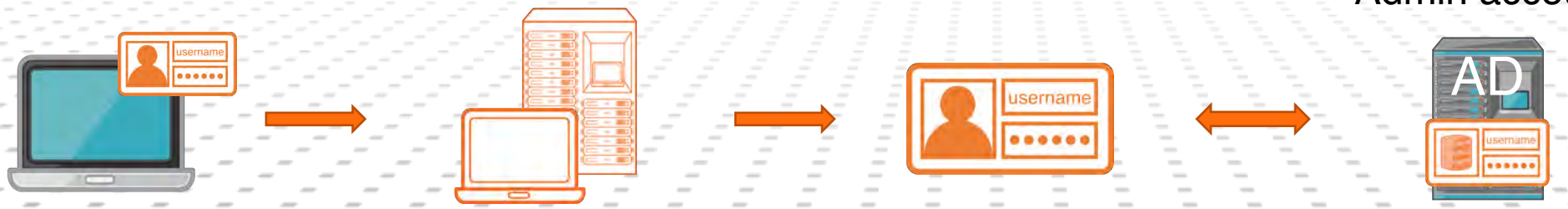


- Find next system
- Move across shares
- Steal credentials

- Install back doors
- Establish C2 connections

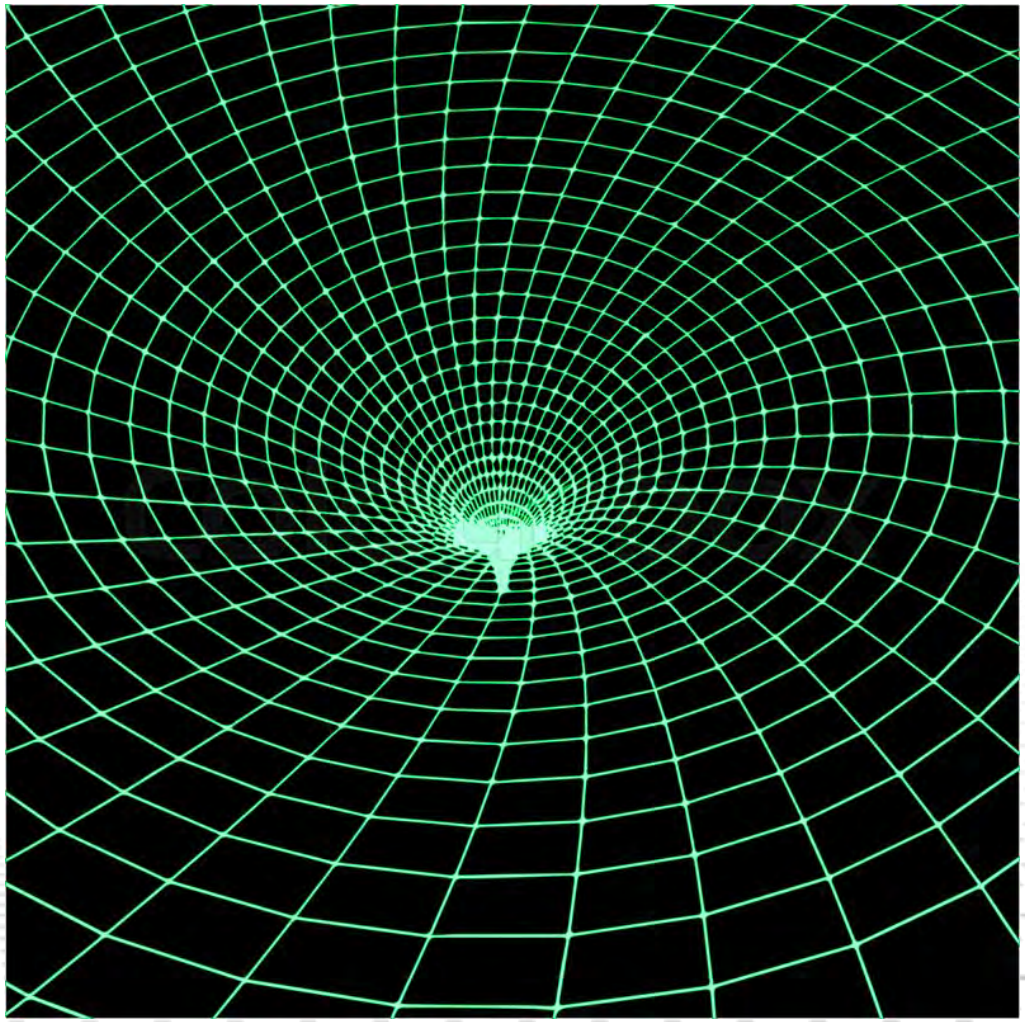
- Obtain passwords to privileged accounts
- Crack stored hashes

- Find critical systems
- Find target data
- Identify AD Domain Admin accounts



How Do I Deploy It?

1. Add SMB shares
2. Add Credentials
3. Use Known Adversary Intelligence (Prior TTPs & Intent)
4. Map Attack Paths
5. Place Lures and Decoy Landmines
6. Add AD deceptions and endpoint redirection technologies
7. Pen-Test/Red/Purple Team
8. Refine and Expand



Efficient Investigations and Operations

High-Fidelity Alerts – Reduce Response Time to Minutes

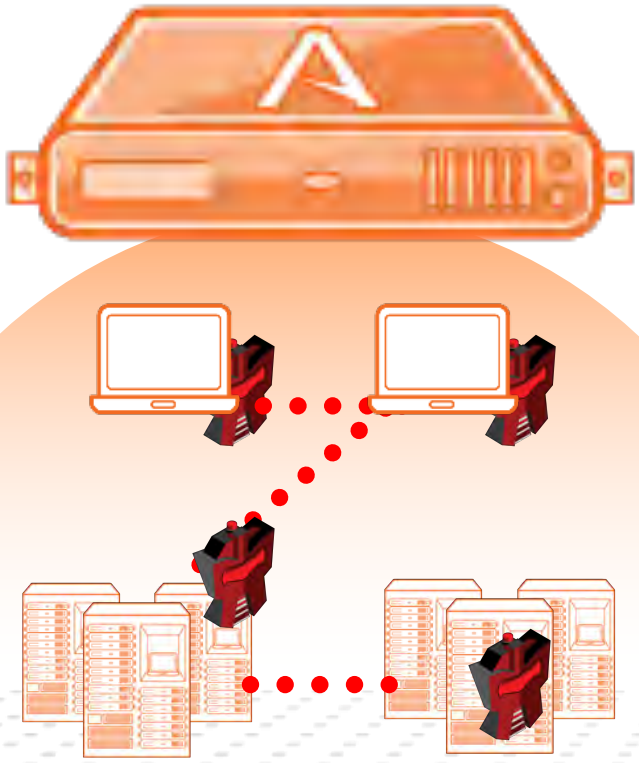
- Substantiated, engagement-based alerts
- Collection of forensics and automated analysis
- Integrations for information sharing and automated response
- Visibility to exposed attack paths

Simple and Easy Operations

- Machine-learning to prepare, deploy and maintain deceptions
- Non-disruptive out-of-band deployment & agentless endpoints
- Manage all environments, including multi-cloud, ubiquitously
- Basic and advanced dashboards; on premise or in the cloud
- Effective for malicious threats, policy violations, misconfigurations

Deception Forensics and Intelligence Capabilities

Engagement-Based Collection



Study and Correlate

Correlate attacker activity
Develop TTPs

Capture forensic artifacts
Document IOCs

Track deceptive data
Counterintelligence

SIEM integration and
attacker behavior analysis

3rd Party integrations with
automated response

Attack Detection Example

Exploitation detected

Summary

File\URL Name	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\SPOOLSV.EXE
Submitted FileName	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\SPOOLSV.EXE
Submission Type	Exploited Process
OS	Windows 7-64
SHA1	3ECAE0D7DE04F08E911FD6041386907C9B9291D8
MD5	85DAA09A98C9286D4EA2BA8D0E644377
Submitter	PayLoadDrop
User	Windows7-64

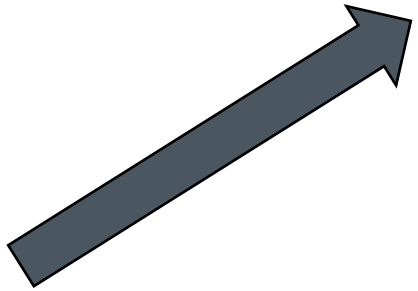
Behavior(s)

Severity	Description
High	A process executed API call from the non Image section. This is usually an indication of the exploited process executing the attacker controlled code.
Low	Used Microsoft Crypto APIs for possibly encrypting the data

Alerts

212	Medium	Access	[redacted]	[redacted]	SMB	CentOS70	[redacted]	CentOS 7.0	4	**SMB** authentication failure (user: [redacted] check_ntlm_password: Authentication for user [redacted] -> [redacted] [redacted] FAILED with error NT_STATUS_NO_SUCH_USER)
213	Medium	Access	[redacted]	[redacted]	SMB	CentOS70	[redacted]	CentOS 7.0	4	**SMB** authentication failure (user: [redacted] Dec 27 05:23:35 **CentOS70** smbd[2449]: check_ntlm_password: Authentication for user [redacted] -> [redacted] FAILED with error NT_STATUS_NO_SUCH_USER)
214	Medium	Access	[redacted]	[redacted]	SMB	CentOS70	[redacted]	CentOS 7.0	4	**SMB** Access (user: **nobody**: Dec 26 10:03:50 **CentOS70** smbd_audit: User:nobody | SrcIP:**172.16.26.34** | Share:**Home** | SrcOS:Vista | SrcName [redacted] Directory:/ | **pread** | **ok** | **middleware/fos-web-service-1.0.2.zip**)

Deception collects forensics for faster investigation



Memory Forensics Behavior

Severity	Description
High	Commands were executed on the system using Windows Management Instrumentation (WMI).
High	Connection was established to the BOTSink Engagement VM.
High	Credentials stealing tool Mimikatz found running on the system.
High	One or more malicious artefacts found in the memory while scanning running processes.
Medium	Commands were executed on the system using Windows Powershell.
Medium	One or more process(es) found running on the system that had open process handle to lsass.exe. A process can open a handle to lsass.exe with the intent of reading memory and potentially stealing stored credentials

Memory Forensics Behavior Detail

High: Commands were executed on the system using Windows Management Instrumentation (WMI).

Commands Executed
SYSACCOUNT

High: Connection was established to the BOTSink Engagement VM.

Dest Host	Dest Port	Src Host	Src Port	PID	Process Name
10.16.6.155	3389	10.16.129.16	49511	1596	mstsc.exe
10.16.7.209	445	10.16.129.16	49507	4	System

High: Credentials stealing tool Mimikatz found running on the system.

Commands Executed
privilege::debug
sekurlsa::logonpasswords

High: One or more malicious artefacts found in the memory while scanning running processes.

Process Name	PID	Detection
wce.exe	1632	Windows Credential Editor was found running on the system
PsExec.exe	3952	PSEXEC found running on the system.

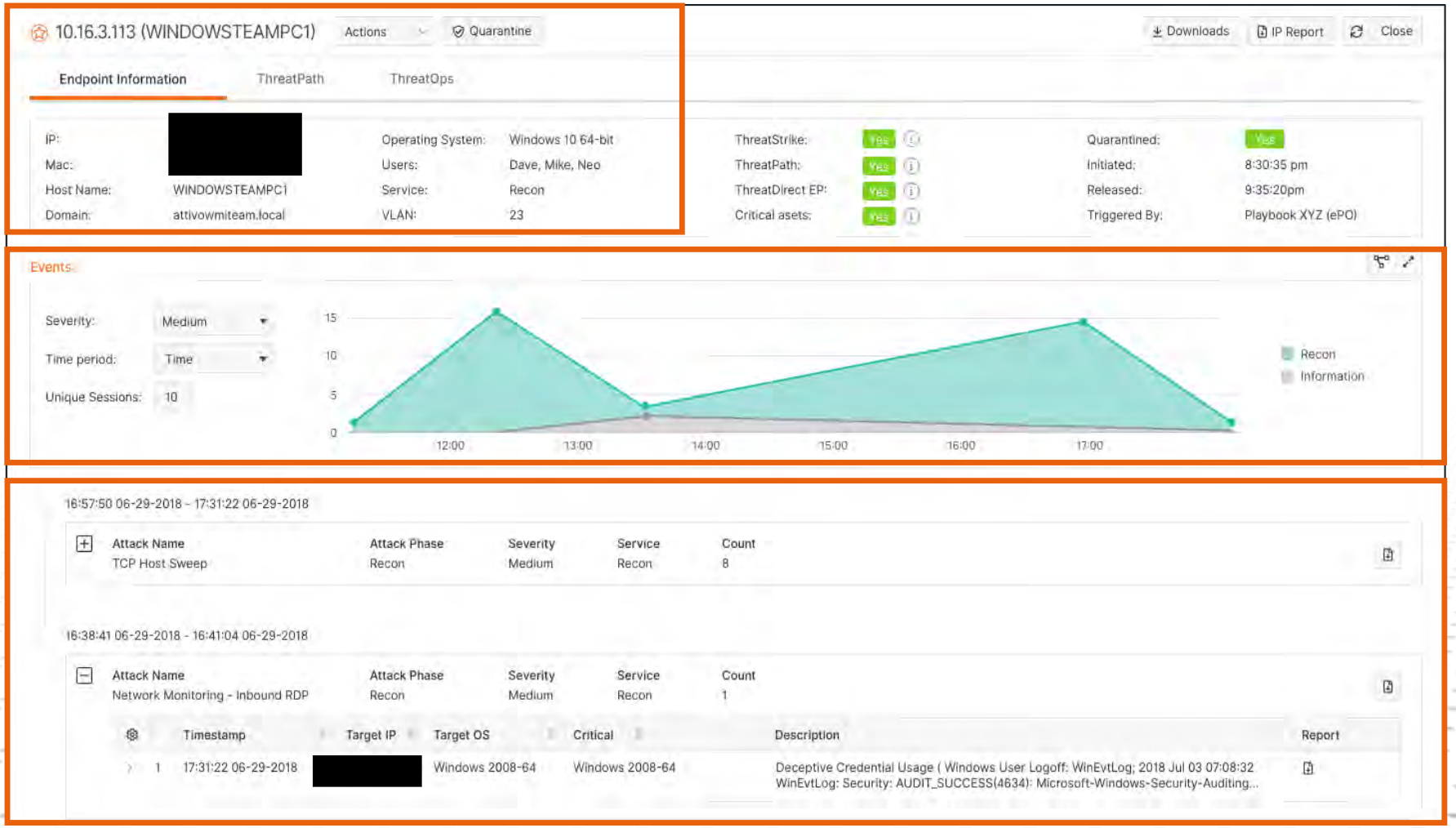
Medium: Commands were executed on the system using Windows Powershell.

Commands Executed
ipconfig
Get-Help Copy-Item
Write-Host "Test cmd"

Consolidated and Correlated Attack Info

Accelerated Investigation and Response

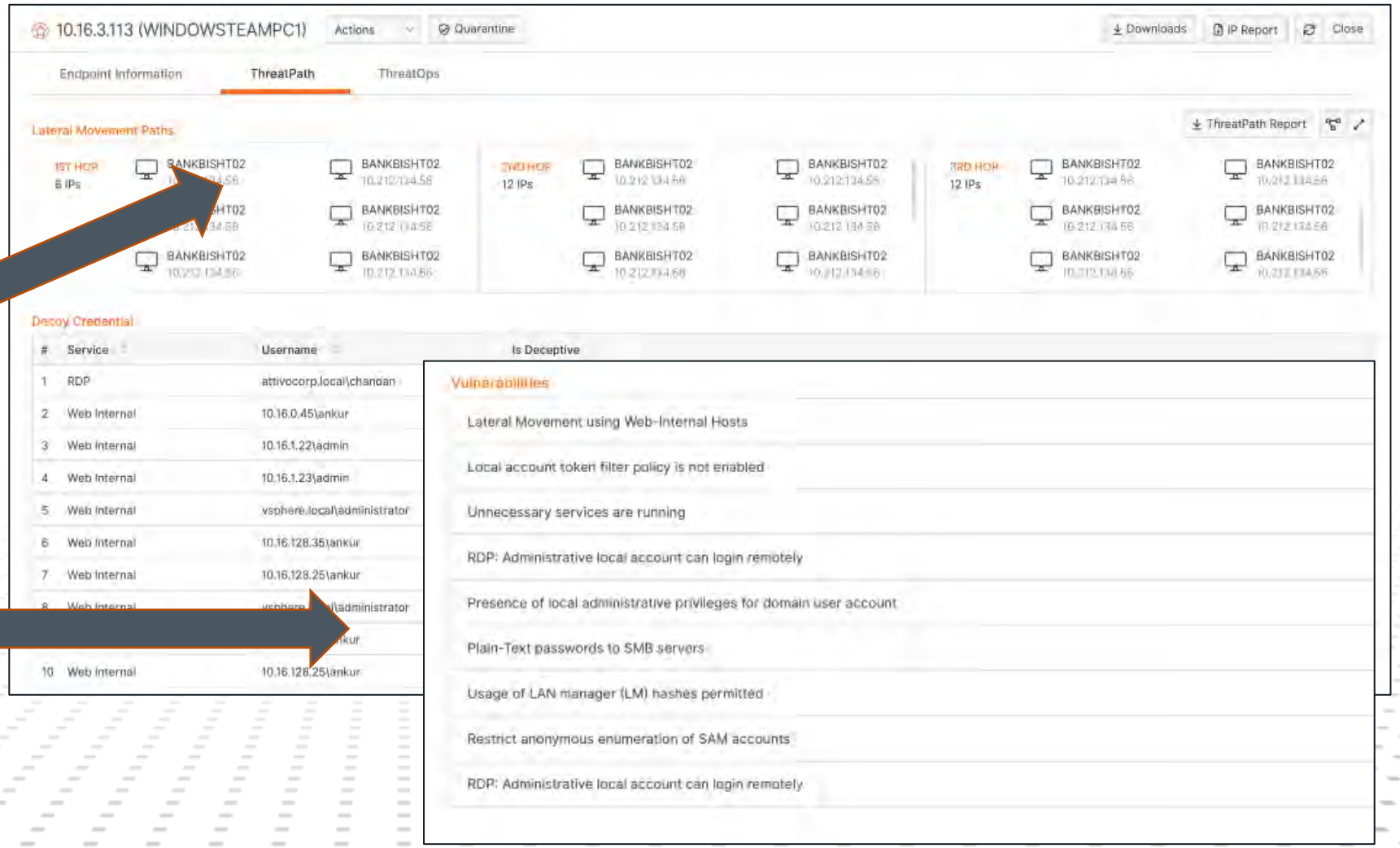
- Endpoint information for attack source
- Timeline view to retrace attack activity
- Event details for streamlined investigations



Lateral Movement Paths: 1st, 2nd, 3rd Hops

Visibility

- Stored Credentials attackers can use for lateral movement
- Endpoint vulnerabilities attackers can compromise



Deception for Risk Mitigation and Compliance

High-fidelity Detection, Arming the Defender, Reducing Risk

1. Reduces Risk: Early In-network Threat Detection
2. Ongoing Assessment of Security Control Reliability
3. Attack Forensics for Evidence-backed Investigations
4. Analysis, Reporting, & Tracking of Cyber Incidents
5. Incident Response, Containment, Eradication
6. Return Adversary Mitigation
7. Asset and Credential Vulnerability Visibility

Effective for external adversaries, internal, and supplier threats.

Support for Security Frameworks

ISO 27001

ISO/IEC 2700 and 27002

Some deception platforms meets or supports 27 of the framework control requirements

NIST Cybersecurity Framework

Some deception platforms meet 32 of the reference subcategories in the framework

In June 2019, NIST issued draft security guidelines that formally include deploying deception technology.

Draft NIST Special Publication 800-171B

Chapter 3, p.30, paragraph 3.13.3e

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Enhanced Security Requirements for Critical Programs and High Value Assets

This publication is to be used as a supplement to NIST Special Publication 800-171. The publication contains recommendations for enhanced security requirements to provide additional protection for Controlled Unclassified Information in nonfederal systems and organizations when such information is part of a critical program or a high value asset. The enhanced security requirements are designed to respond to the advanced persistent threat (APT) and supplement the basic and derived security requirements in NIST Special Publication 800-171 that provide the foundational protection for CUI.

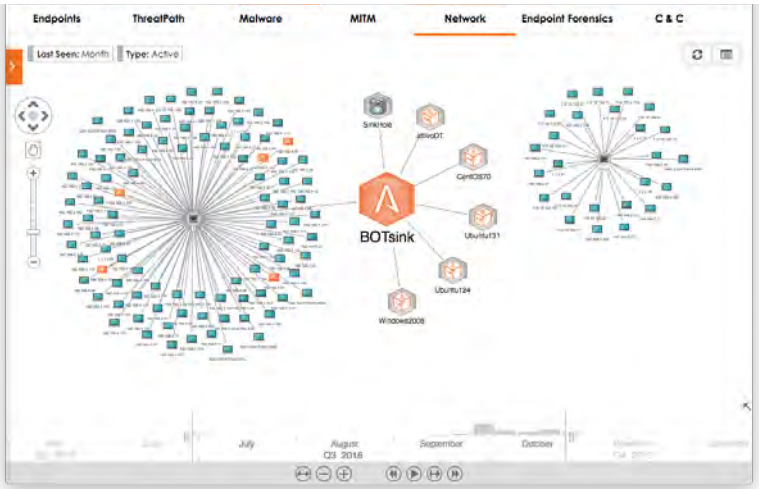
RON ROSS
VICTORIA PILLITTERI
GARY GUISSANIE
RYAN WAGNER
RICHARD GRAUBART
DEB BODEAU

3.13.3e **Employ technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation.**

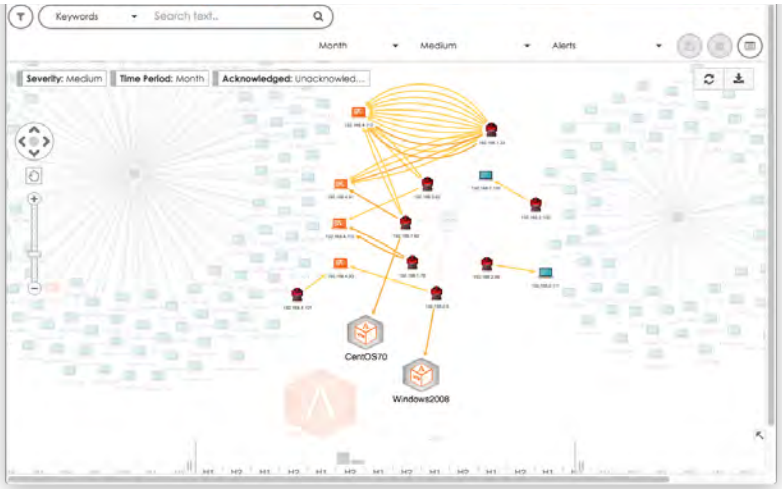
DISCUSSION

Deception is used to confuse and mislead adversaries regarding the information the adversaries use for decision making; the value and authenticity of the information the adversaries attempt to exfiltrate; or the environment in which the adversaries desire to operate. Such actions can impede the adversary's ability to conduct meaningful reconnaissance of the targeted organization; delay or degrade an adversary's ability to move laterally through a system or from one system to another system; divert the adversary away from systems or system components containing CUI; and increase observability of the adversary to the defender, revealing the presence of the adversary along with its TTPs. Misdirection can be achieved through deception environments (e.g., deception nets) which provide virtual sandboxes into which malicious code can be diverted and adversary TTP can be safely examined. Tainting involves embedding data or information in an organizational system or system component which the organization desires adversaries to exfiltrate. Tainting allows organizations to determine that information has been exfiltrated or improperly removed

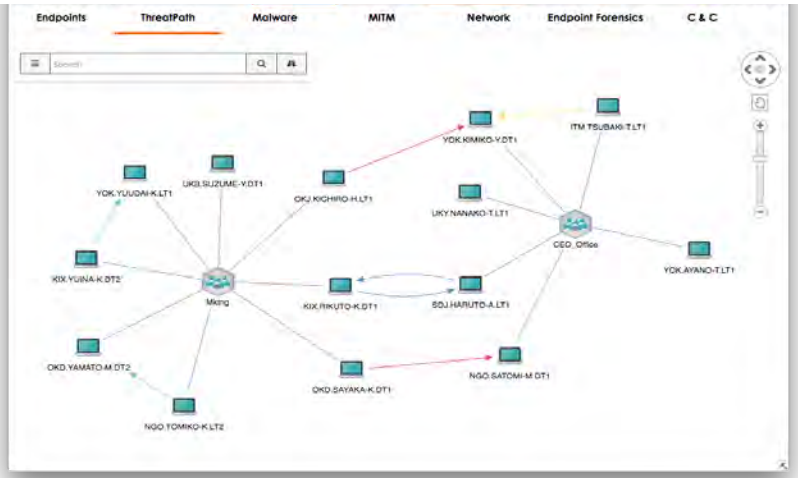
Visualization and Vulnerability Assessment Tools



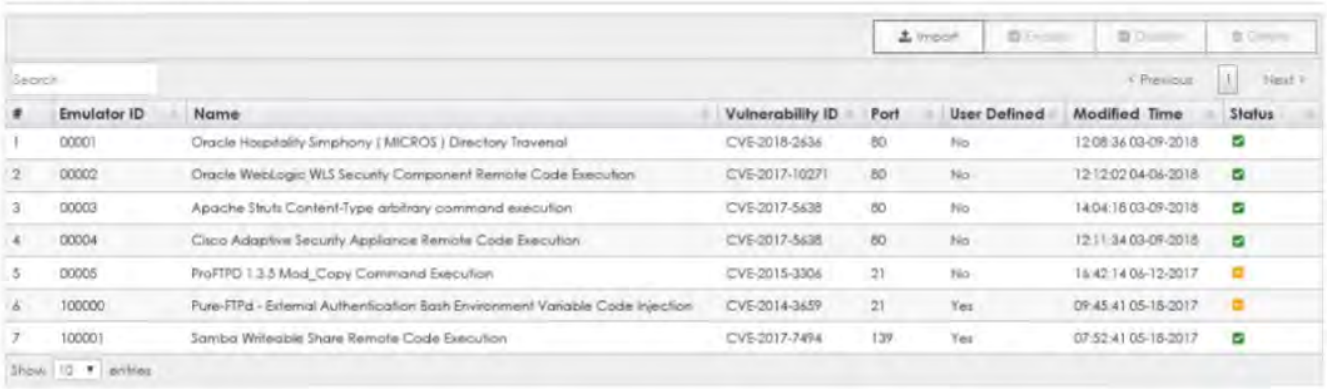
Network Visibility:
device changes over time



Attack Replay:
Time-lapsed attack insights



Attack Lateral Path Visibility:
Exposed credentials,
Misconfigurations



#	Emulator ID	Name	Vulnerability ID	Port	User Defined	Modified Time	Status
1	00001	Oracle Hospitality Simphony (MICROS) Directory Traversal	CVE-2018-2636	80	No	12:08:36 03-09-2018	
2	00002	Oracle WebLogic WLS Security Component Remote Code Execution	CVE-2017-10271	80	No	12:12:02 04-06-2018	
3	00003	Apache Struts Content-Type arbitrary command execution	CVE-2017-5638	80	No	14:04:16 03-09-2018	
4	00004	Cisco Adaptive Security Appliance Remote Code Execution	CVE-2017-5638	80	No	12:11:34 03-09-2018	
5	00005	ProFTPD 1.3.5 Mod_Copy Command Execution	CVE-2015-3306	21	No	16:42:14 06-12-2017	
6	100000	Pure-FTPd - External Authentication Bash Environment Variable Code Injection	CVE-2014-3659	21	Yes	09:45:41 05-18-2017	
7	100001	Samba Writeable Share Remote Code Execution	CVE-2017-7494	139	Yes	07:52:41 05-18-2017	

Vulnerability Simulator:
Detects specific attacks (CVE ID) that attackers try to exploit

LUXURY ITEM VS. LIFELINE

Testimonials

Organization Discovers Insider Threat

Concern

- The organization 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 organization and legal action are pending.

Value

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

“Attackers only have to be right once,

while security people have to be right all the time.

…DECEPTION flips that paradigm.…

now the criminals need to be right all of the time, too”

DJ Goldsworthy, Aflac

Director Security Operations
and Threat Management

Annual Penetration Testing for Compliance Validation

Concern

- Organization 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

- Organization 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 Organization successfully validated their security infrastructure resiliency for annual compliance requirements.

"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 organization'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

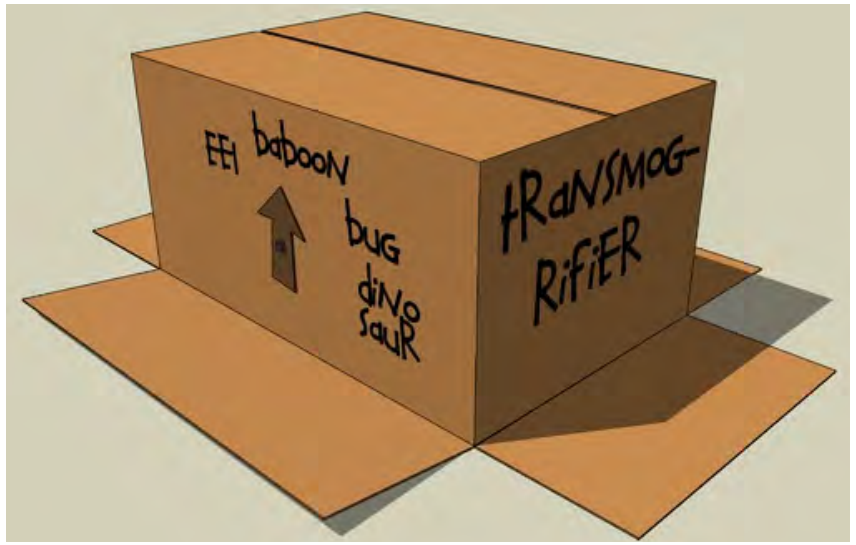
- Organization stealthily installed deception solution for network visibility and IR.
- Professional services engaged to help triage, respond, and remediate attacker presence across numerous environments.

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

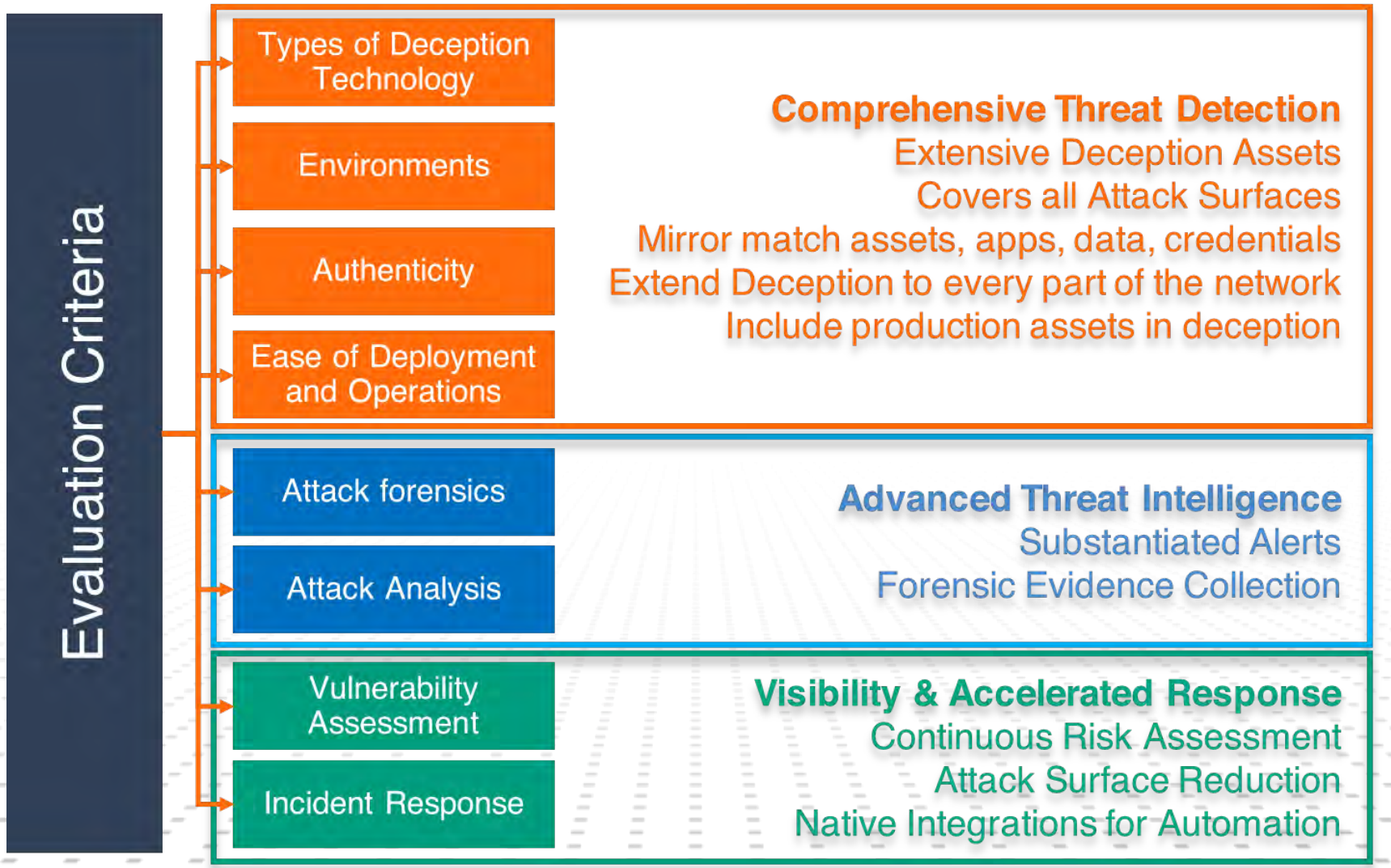
The organization used the deception solution for unparalleled network visibility to clean up the persistent presence without alerting the attacker.



All deception solutions are not created equal.

Mileage varies widely and you will want to do your homework.

Evaluating Deception Technology Offerings and Providers



QUESTIONS?

Let's Keep in Touch!

Joseph R. Salazar, CISSP, CEH, EnCE
jsalazar@attivonetworks.com