The Art and Science of Deception
Empowering Response Actions and Threat Intelligence

Ray Kafity
Vice President
Attivo Networks
Why Today’s Security Defenses are Failing
Attackers Still Get In and Once Inside, Can Remain Undetected for Months

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

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

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

- 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.
Advanced Threat Detection Technology Choices

Analytics: Big Data Learning
- Network Anomaly
- SIEM Logs UBA

Deception Technology
- Deception Decoy
- Accurate Visibility

Investigate Everything: Millions of Logs and Alerts

Lures, Traps, and High Fidelity Alerts
Attack him where he is unprepared, appear where you are not expected.

Sun Tzu
Typical Attack Path Sequence
One Small Security Gap will Present Opportunity For Hackers
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

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?

- Forensics investigation: 47%
- Detection: 43%
- Incident scoping: 38%
- Malware analysis: 25%
- Containment: 22%
- Remediation: 22%
- Notification: 19%
Understanding Attacker Threat Paths

1. Discovers the paths attackers can traverse
2. Provides network map with possible lateral movement paths
3. Provides actionable insights to strengthen policies and prevent lateral movement
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
Proven Deception Use Cases

Visibility, Early and Accurate Detection, Accelerated Incident Response

1. Lateral Movement Detection
2. Insider & 3rd Party Threats
3. Stolen Credential
4. Man-in-the-Middle
5. Ransomware
6. Phishing
7. IoT Device and ICS- SCADA
8. Visibility and Streamline Incident Response
A Modern Day Deception and Response Platform Provides Accurate and Efficient Continuous Threat Management

- Prevention
- Real-time Detection
- Threat Path Assessment
- Incident Handling
- Scalable
- Complete
- Accurate
- Authentic
- Malware and Phishing Analysis
- Actionable Forensics
# Major Energy Company Protects Critical Infrastructure

<table>
<thead>
<tr>
<th>Problem</th>
<th>Overview</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Protection of critical infrastructure and business networks to prevent incidents from tampering or sabotage of field fuel sensor and refinery controls.</td>
<td>• The team had a mature security posture, but lacked visibility into attacker lateral movement within their industrial control networks.</td>
<td>• BOTsink engagement servers and SCADA decoys provide real-time visibility into lateral movement inside their network and high fidelity alerts on intrusions.</td>
</tr>
</tbody>
</table>

**Customer Value**
Pass penetration tests that they have failed with their other security devices.
Penetration Test with Deception Financial Institution

Problem

- Team failed multiple penetration tests because of their inability 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 stolen credentials the red team used during the penetration test.

Customer Value

Real-time detection and accurate alerting to industrial control network intrusions.
Penetration Test with Deception Financial Institution

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.
“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

Attivo Networks exemplifies a modern-day approach to deception.

Mike Suby – Frost and Sullivan

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

Technavio – IT Market Research

"Block & Detect shifts to Detect & Respond"

"Deception should be a 2016 initiative."

Eric Ouellet – Gartner

Paradigm shifts in information security

RSAC Analyst 2016 Views
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.

Ray Kafity
Vice President
Attivo Networks
Ray@attivonetworks.com