LIGHTWEIGHT FOR REAL-TIME

Detection (AI-based)	RIDGEBACK Fact-based (FI*)
Is there malicious content?	What's actually happening?
Deep packet inspection	'Fact of' behavior (not content)
Data lakes to learn	Header data only

* Fact-based Intelligence

AUTOMATED FOR COUNTER-ENGAGEMENT

RIDGEBACK

Detection (AI-based)	Fact-based (FI*)
▪ Inferences	▪ No guessing
▪ After-the-fact	▪ Real time
▪ Central data lakes	▪ Local (and central)
▪ Humans in the loop	▪ Autonomous
▪ **Passive**	▪ **Fights back**

* Fact-based Intelligence

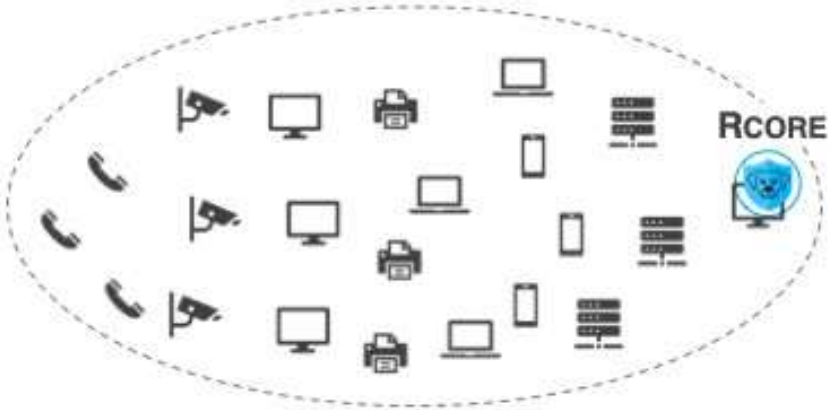
2

Flexible architecture

EASY, LIGHTWEIGHT, FLEXIBLE ARCHITECTURE

Rcore: A single <1MB file on one device per network segment

Enterprise / Edge / Ad hoc / OT Networks

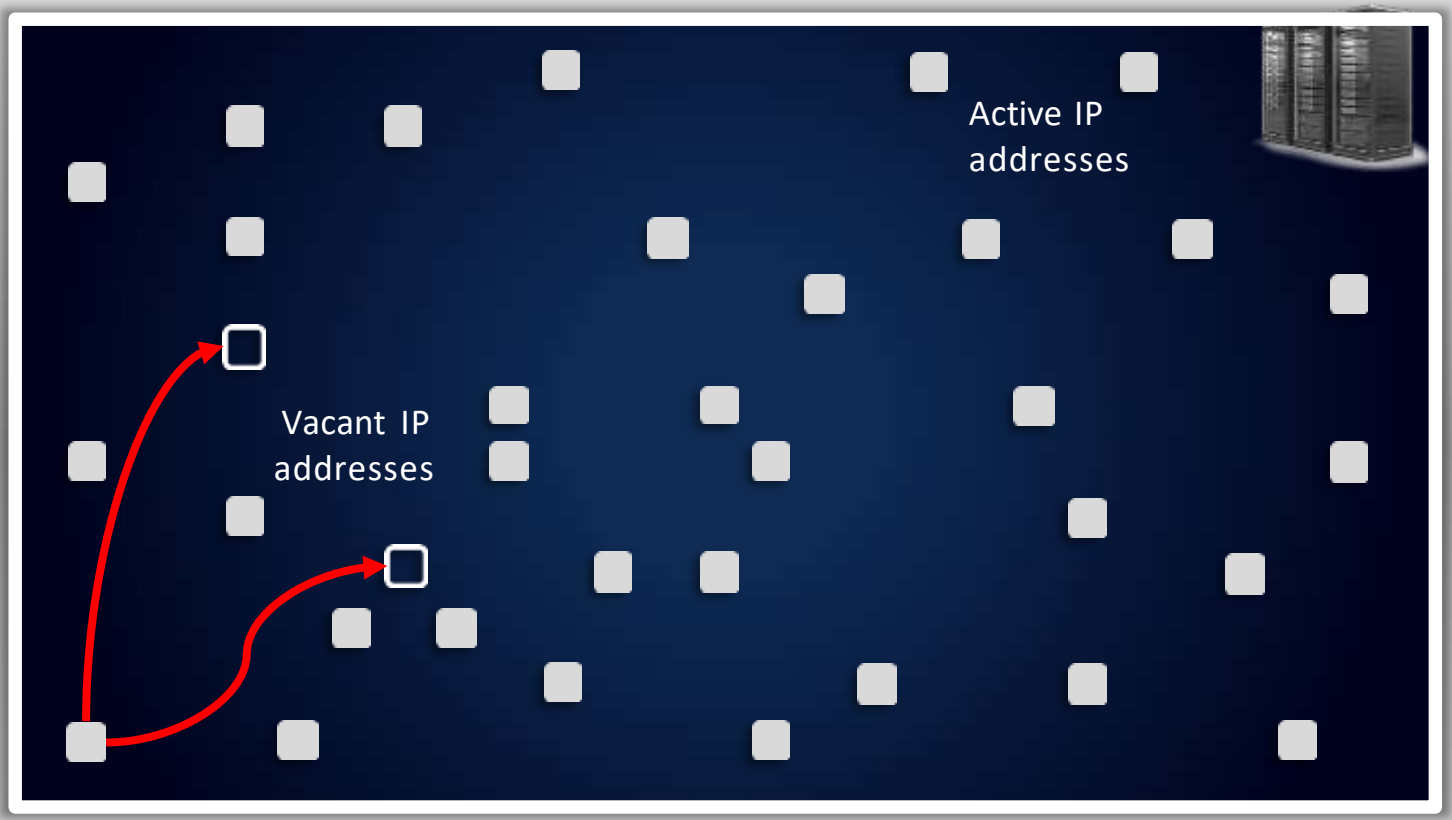


or
Standalone

3

Real-time operations

What do attempts to access the dark space mean?



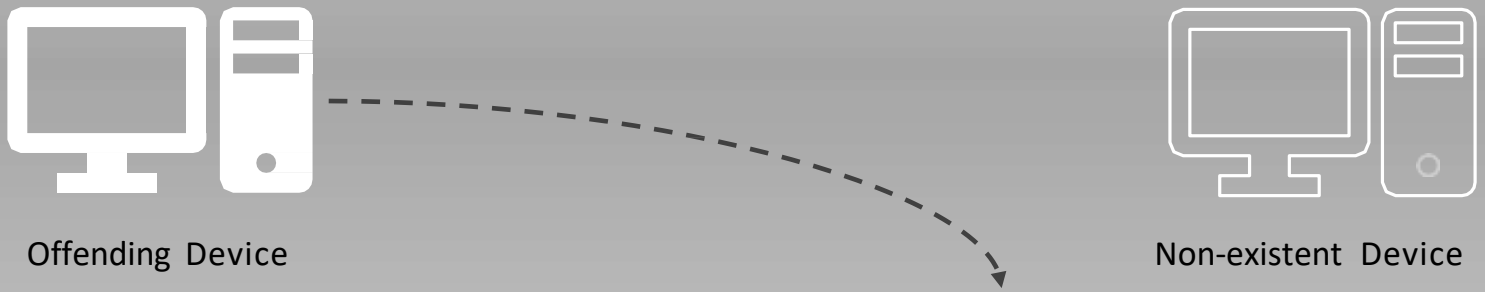
Attacks in Progress

- Discovery & Enumeration
- Malware Propagation

Productivity & Security Issues

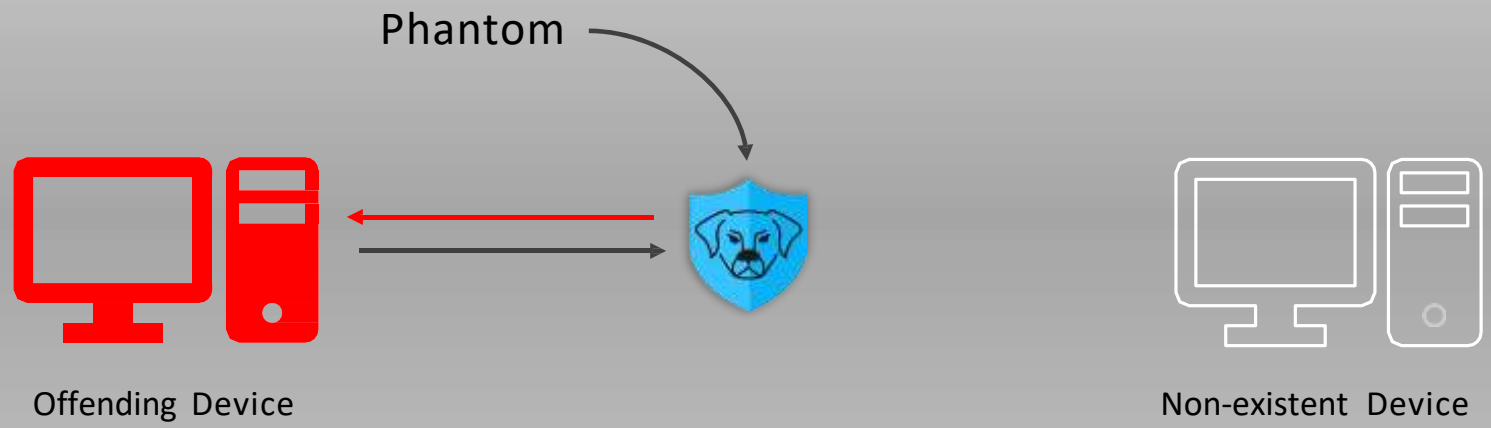
- Misconfigurations
- Signal Leaks

EXPLOITATION
DISCOVERY & ENUMERATION



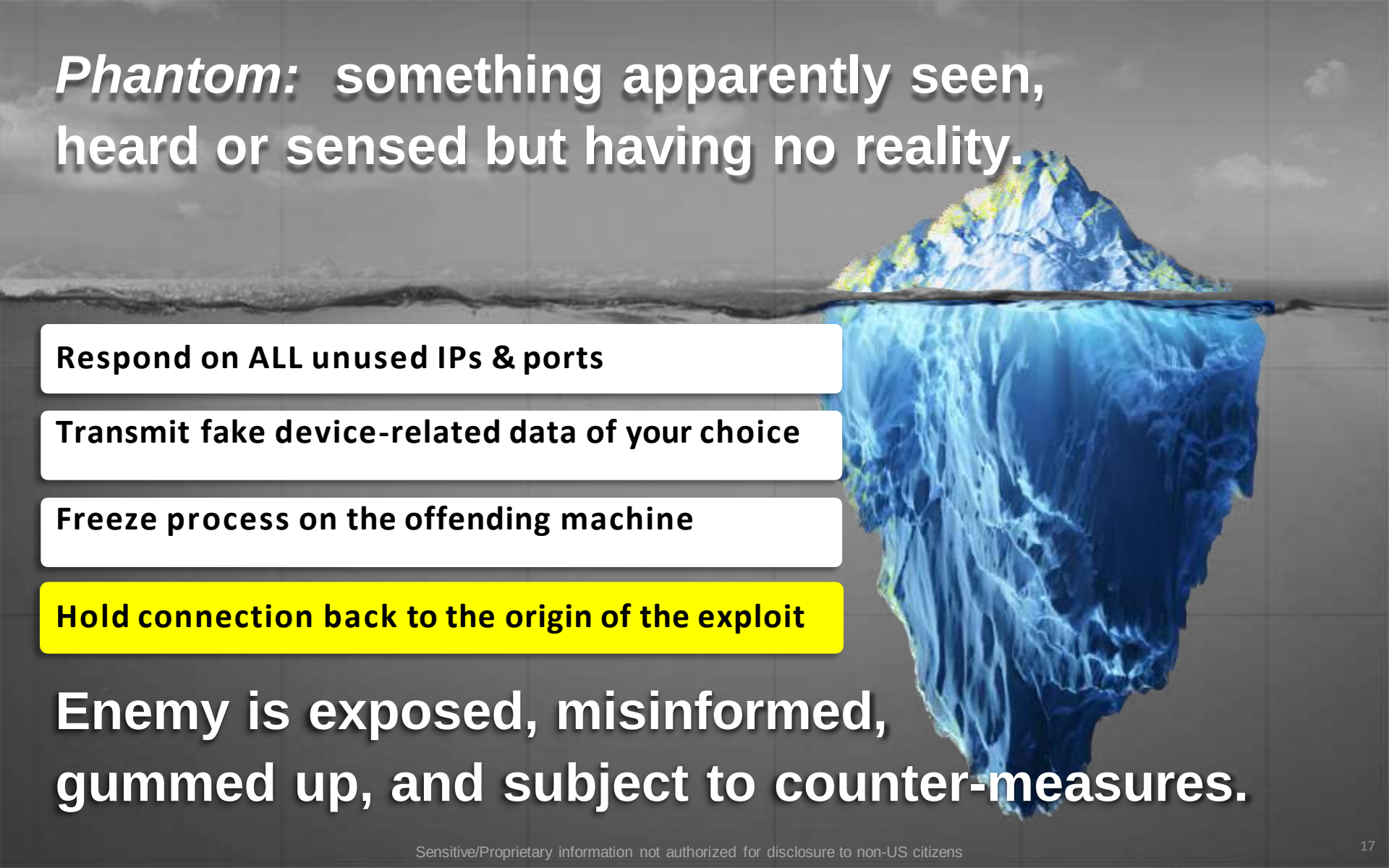
Without Ridgeback, signals to dark IP addresses ‘fall on the floor’

Man-in-the-Middle
Scaled and Automated for Defense



With Ridgeback, signals to dark IP addresses trigger instant counter-engagement

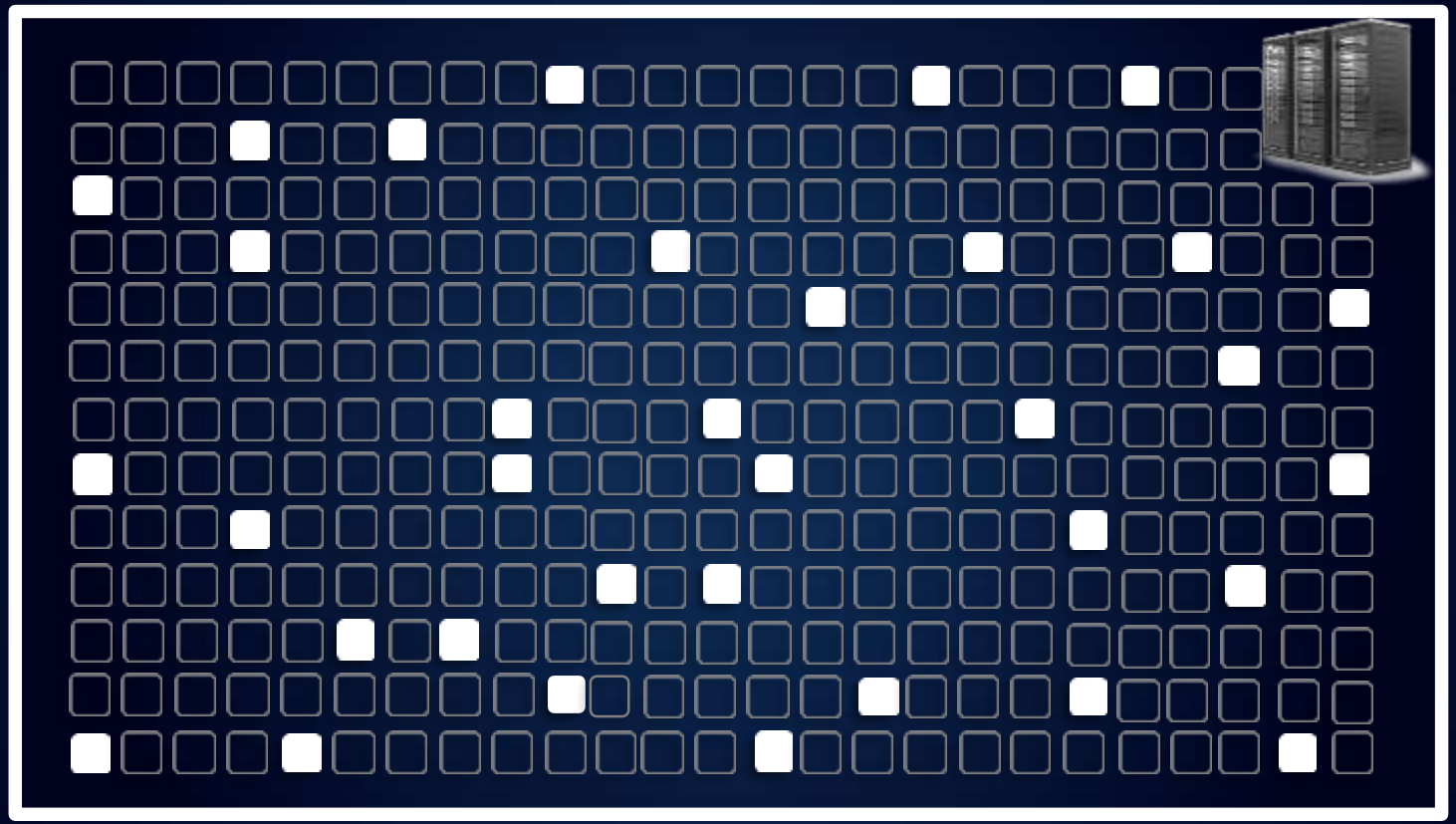
Phantom: something apparently seen, heard or sensed but having no reality.



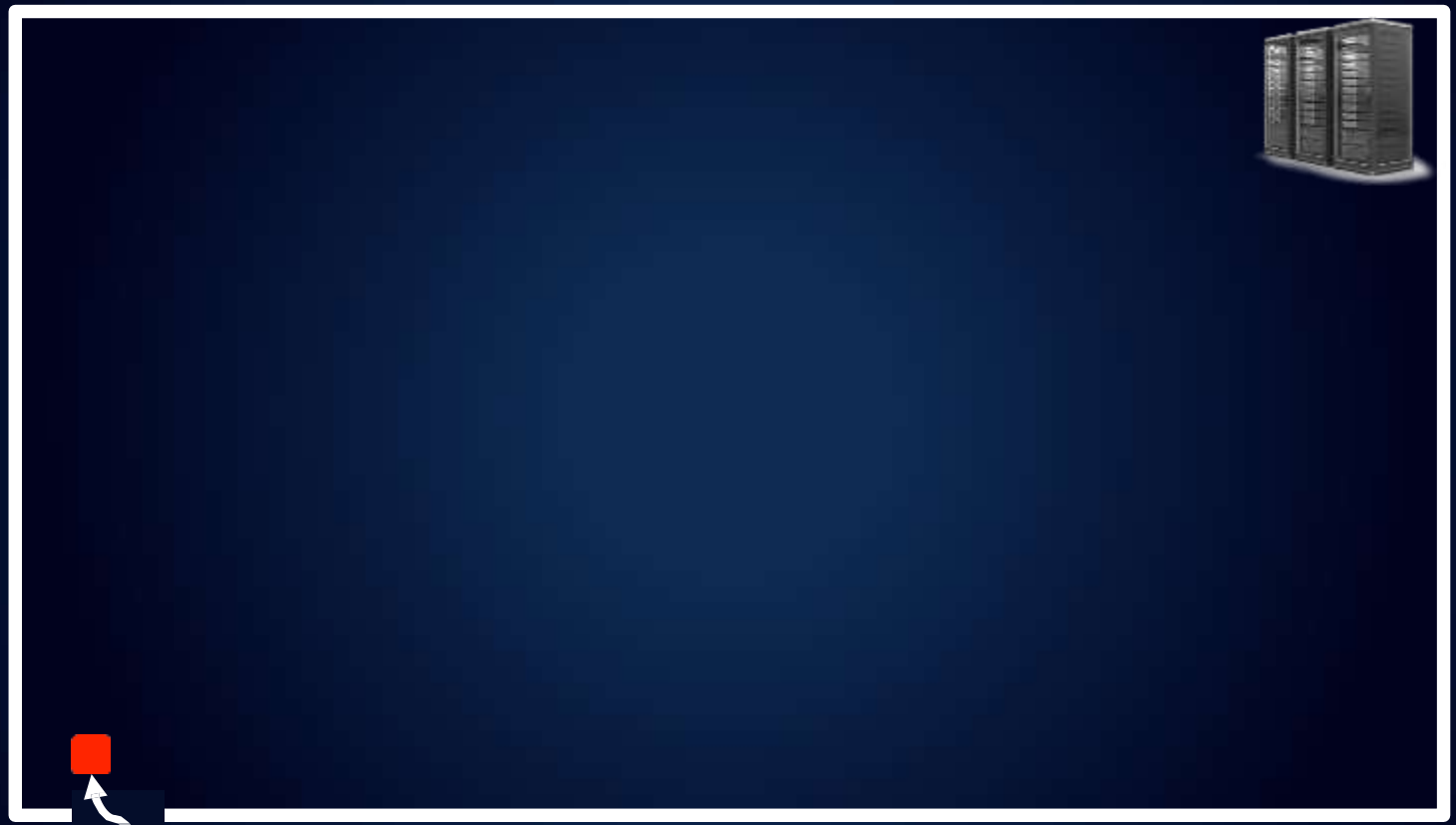
- Respond on ALL unused IPs & ports
- Transmit fake device-related data of your choice
- Freeze process on the offending machine
- Hold connection back to the origin of the exploit

Enemy is exposed, misinformed, gummed up, and subject to counter-measures.

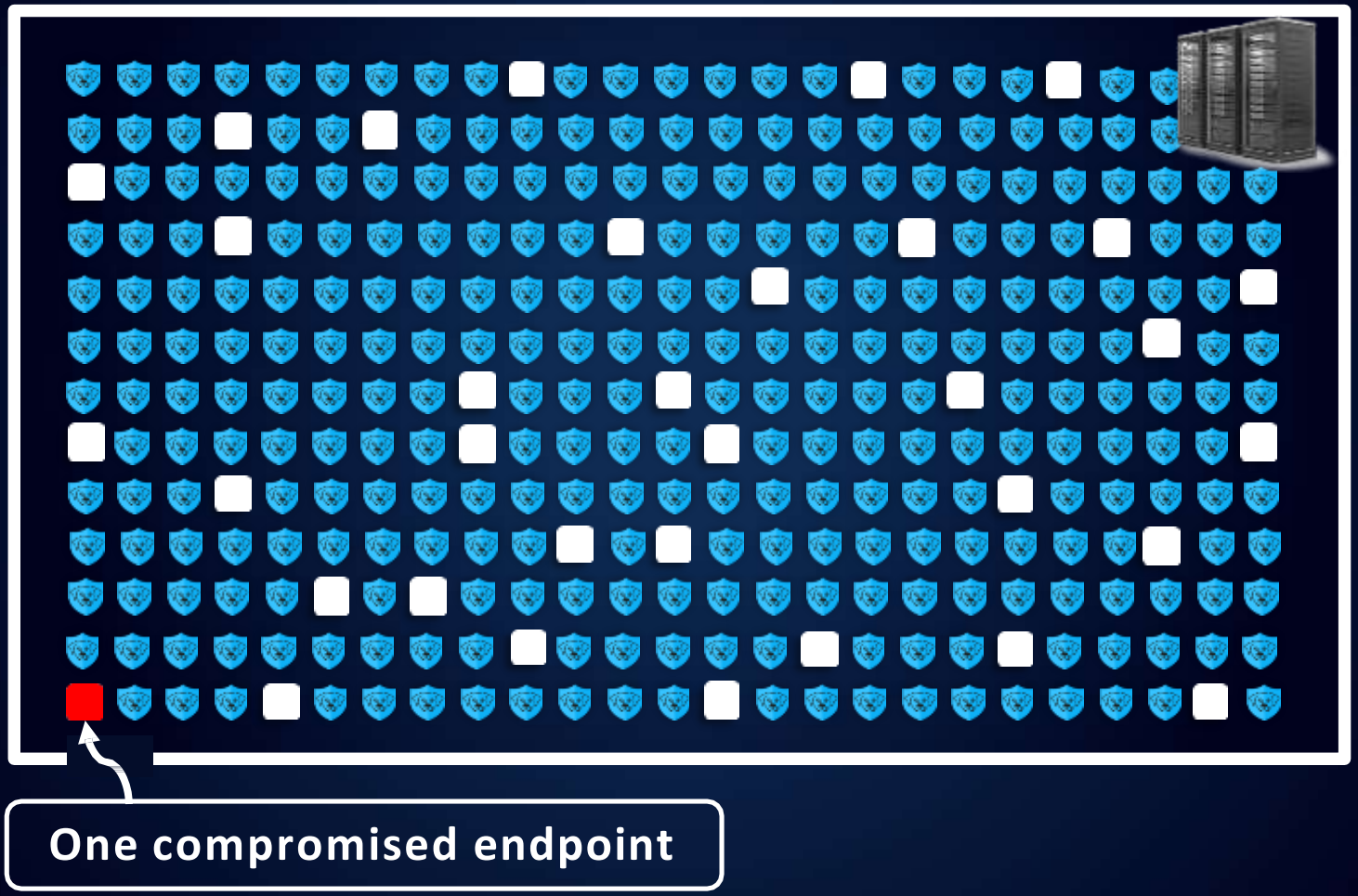
Know which IP addresses are live, and all IP addresses that aren't



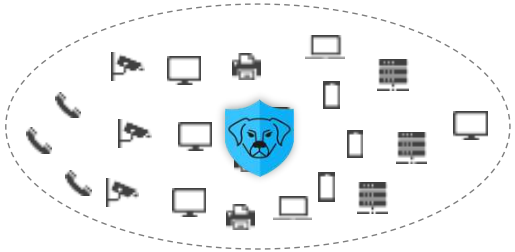
Unassigned IP Addresses



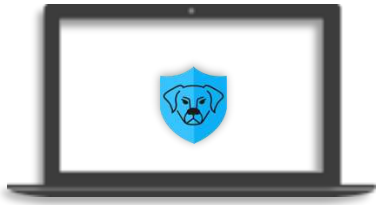
Unassigned IP addresses act as a virtual minefield stopping the adversary real-time, rather than trying to detect and chase them through systems post-facto.



Deployment Alternatives Create Versatile Use-cases



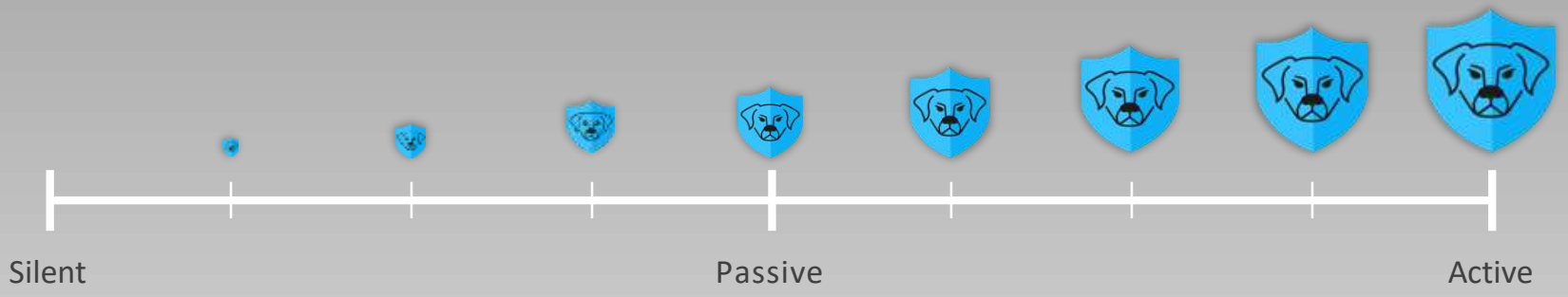
Network



Portable

Micro

Mobile



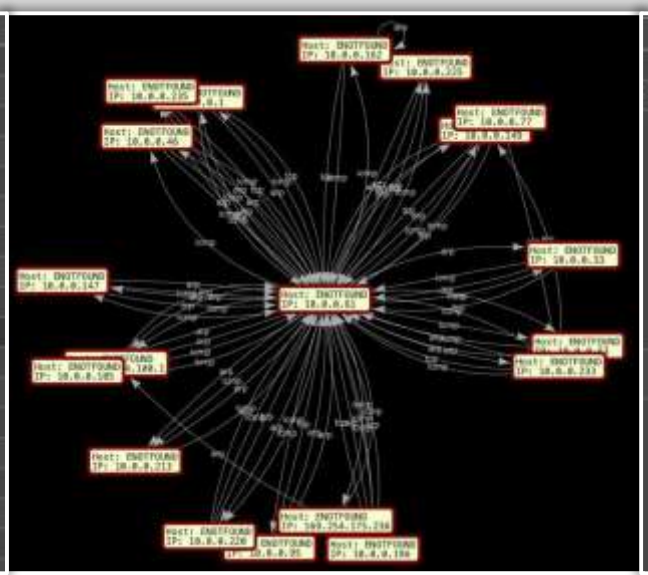
Rcore is configurable along a spectrum from purely observational to aggressively active.

4

A range of valuable use-cases

Real-time Situational Awareness

IP address	Mac address	OUI Org	Pressure
1.0.0.10	ac:4c:a5:41:36:7d	Vantiva USA LLC	1
1.100.254.169	ac:4c:a5:41:36:7d	Vantiva USA LLC	1
10.0.0.1	ac:4c:a5:41:36:7d	Vantiva USA LLC	6
10.0.0.33	80:b9:7a:e5:2c:d2	eero inc.	4
10.0.0.46	80:b9:7a:98:76:d2	eero inc.	4
10.0.0.53	34:36:3b:75:b4:e0	Apple, Inc.	2
10.0.0.61	f8:ff:c2:3a:cb:b3	Apple, Inc.	52
10.0.0.77	fa:39:8e:36:9a:2a		6
10.0.0.95	ac:41:6a:4f:2e:f8	Amazon Technolog...	4
10.0.0.105	04:c2:9b:b6:ef:2e	Aura Home, Inc.	3
10.0.0.147	80:b9:7a:f7:43:6b	eero inc.	4
10.0.0.149	a2:ae:9e:c0:4a:75		7
10.0.0.162	e2:4e:10:e9:83:fe		6
10.0.0.196	80:b9:7a:82:5e:72	eero inc.	4
10.0.0.213	bc:d7:d4:59:86:b5	Roku, Inc	7
10.0.0.220	70:77:81:73:a7:58	Hon Hai Precision I...	6
10.0.0.225	e0:6d:17:e3:ae:24	Apple, Inc.	8



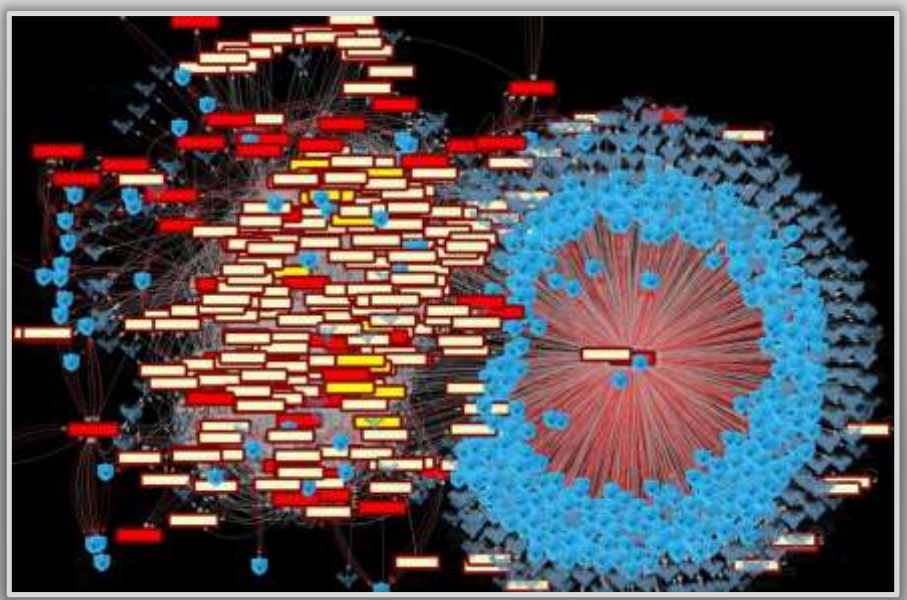
IP address	Attack surface
10.0.0.213	Ignored State: closed (100)
169.254.175.236	Ignored State: filtered (100)
169.254.100.1	22/filtered/tcp//ssh/// 23/filtered/tcp//telnet/// 80/open/tcp//http/// 111/filtered/tcp//rpcbind/// 389/filtered/tcp//ldap/// 427/filtered/tcp//svrloc/// 443/open/tcp//https/// 1029/filtered/tcp//ms-lsa/// 2000/filtered/tcp//cisco-sccp/// 5800/filtered/tcp//vnc-http/// 8080/filtered/tcp//http-proxy/// Ignored Sta closed (89)
10.0.0.233	49153/open/tcp//unknown/// Ignored State: cl (99)
10.0.0.1	22/filtered/tcp//ssh/// 23/filtered/tcp//telnet/// 53/open/tcp//domain/// 80/open/tcp//http/// 111/filtered/tcp//rpcbind/// 389/filtered/tcp//ldap/// 427/filtered/tcp//svrloc/// 443/open/tcp//https/// 1029/filtered/tcp//ms-lsa///

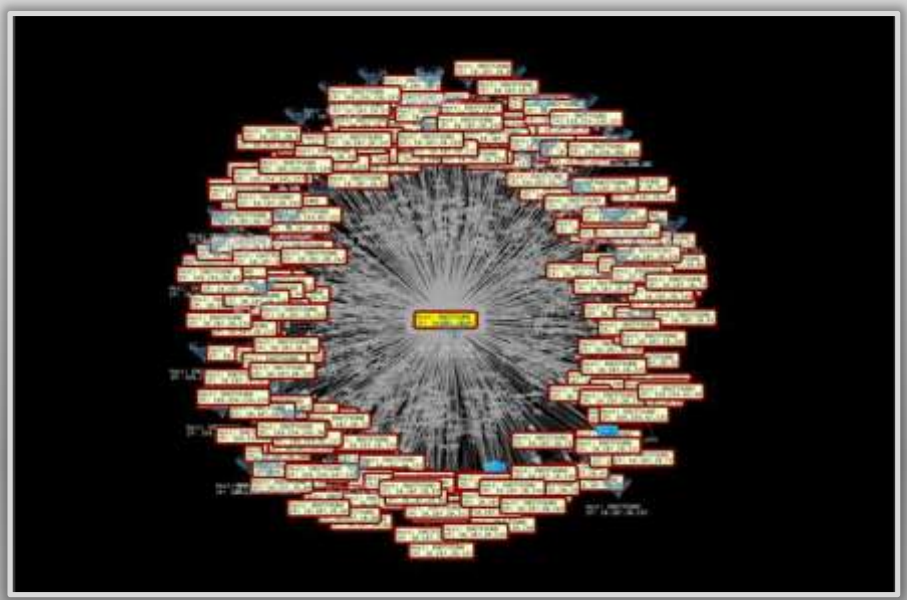
- See all devices on the network, know when they join or leave.
- Visualize internal network signals in motion, real-time.
- See the attack surface – all ports and services in use.

For example, see:

- Unauthorized devices
- Unapproved services
- Errors in firewall settings
- Errors in segmentation
- Insecure protocols
- Improper signals into & out of IoT and OT
- Faults in IT / security implementations
- DNS errors

Real-time Situational Awareness



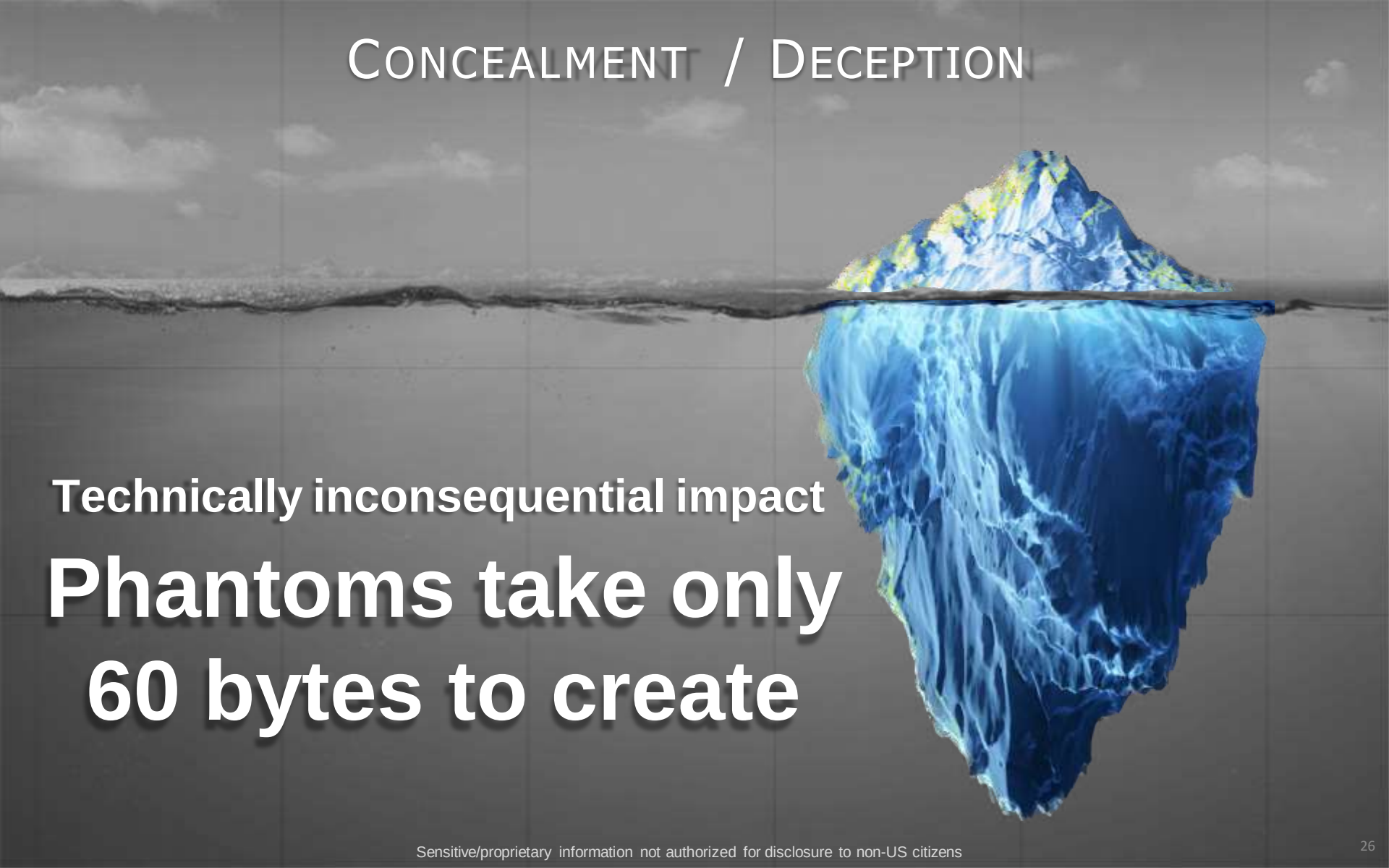


- See all devices on the network, know when they join or leave.
- Visualize internal network signals in motion, real-time.
- See the attack surface – all ports and services in use.

For example, see:

- Unauthorized devices
- Unapproved services
- Errors in firewall settings
- Errors in segmentation
- Insecure protocols
- Improper signals into & out of IoT and OT
- Faults in IT / security implementations
- DNS errors

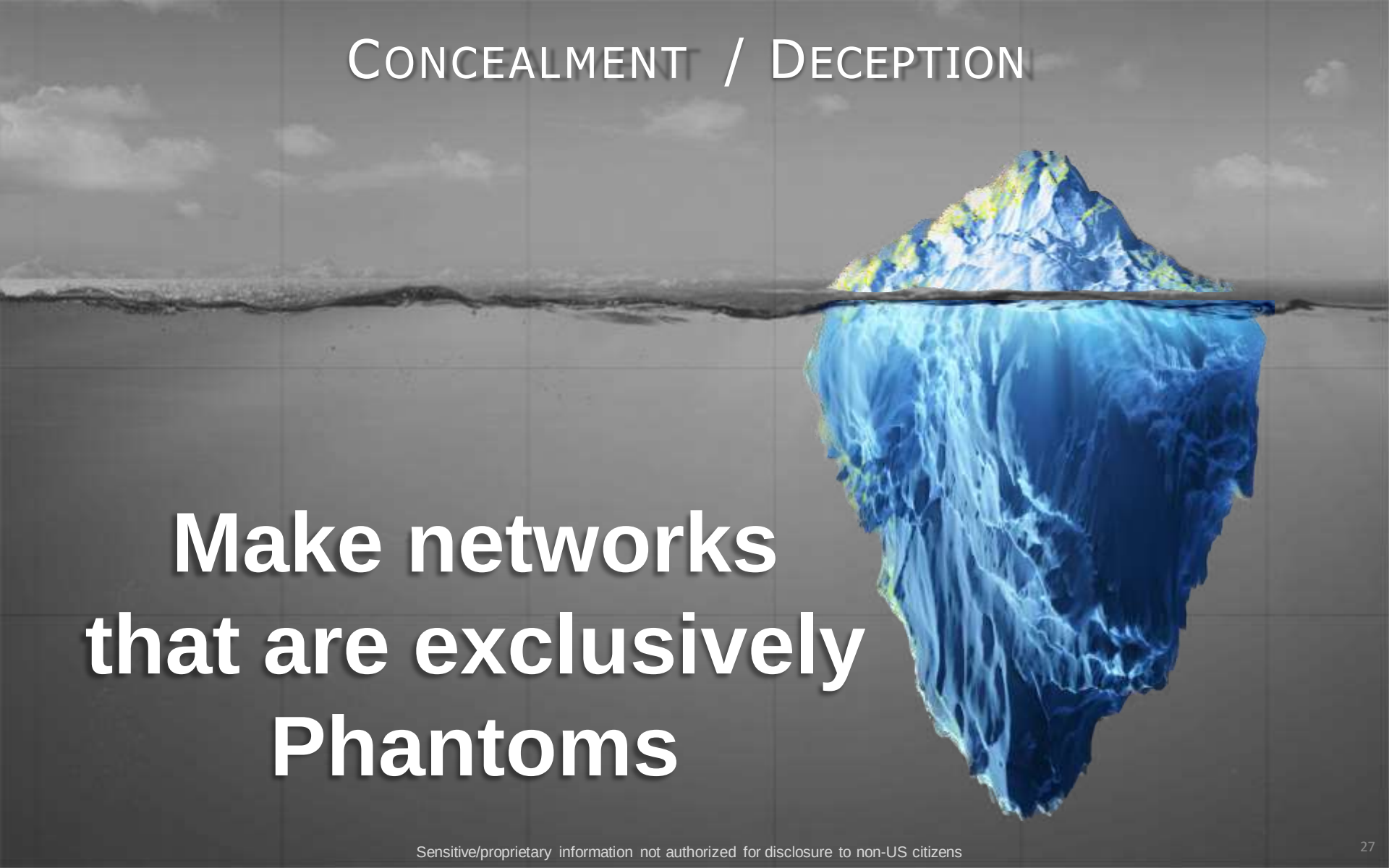
Concealment / Deception



Technically inconsequential impact

Phantoms take only 60 bytes to create

Concealment / Deception



Make networks that are exclusively Phantoms

What does it take to get started?

One Operator, one laptop, one hour.

Immediately expedite day-to-day work, large project implementations and deliver previously unachievable impacts.