The Evolution of Vulnerability Management

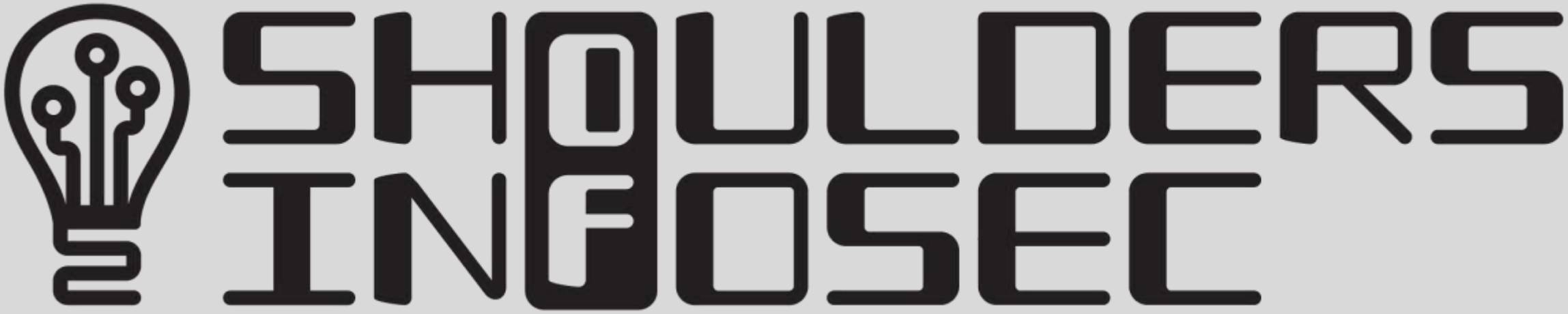
Jack Daniel

Security BSides | Tenable Network Security | jdaniel@tenable.com

But first

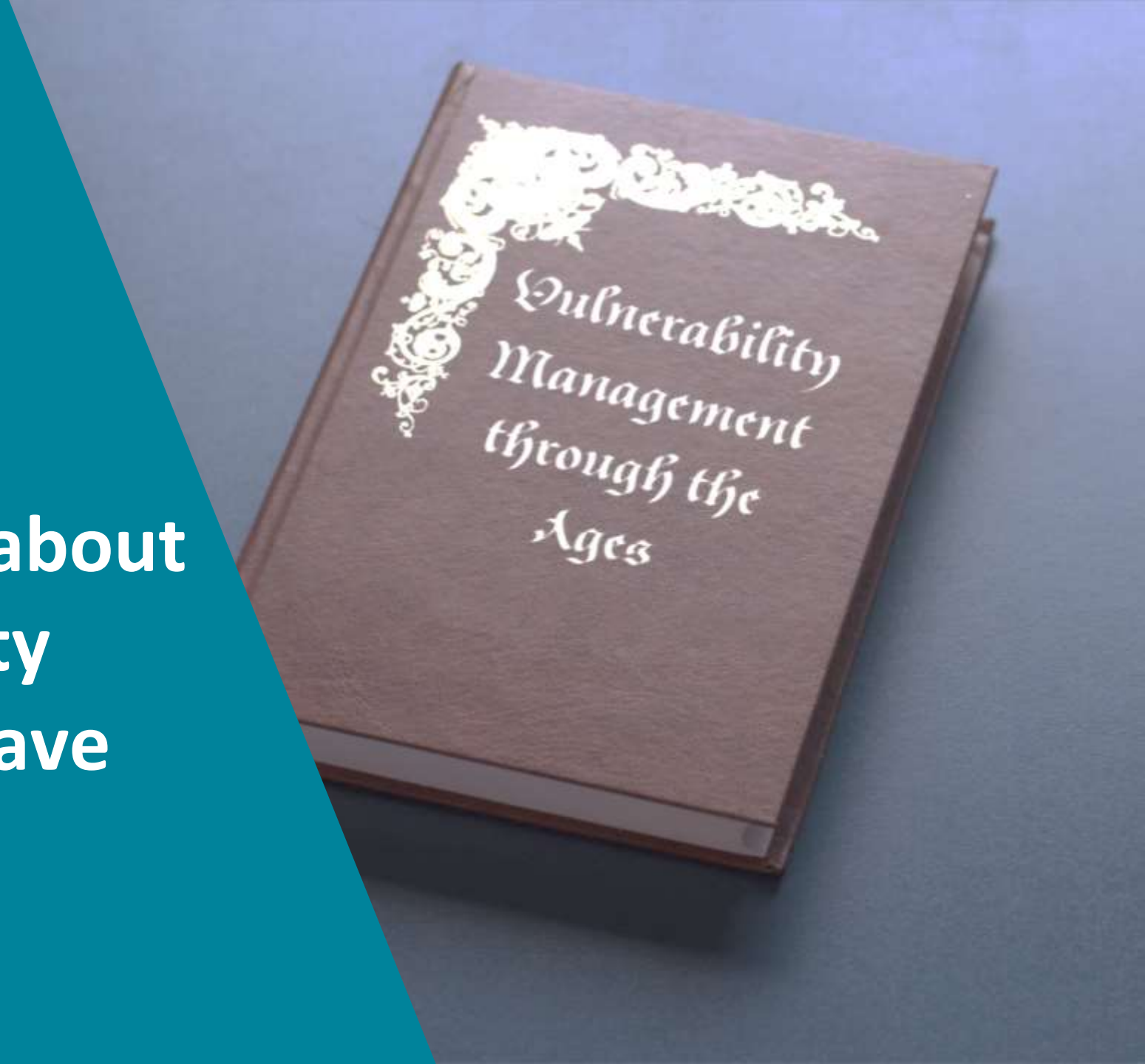
Goodbye Infomom

thanks for everything



shouldersofinfosec.org

Before we can talk about modern vulnerability management, we have to look at history



IT USED

TO BE EASY.


BUG
HUNTERS

BUG!

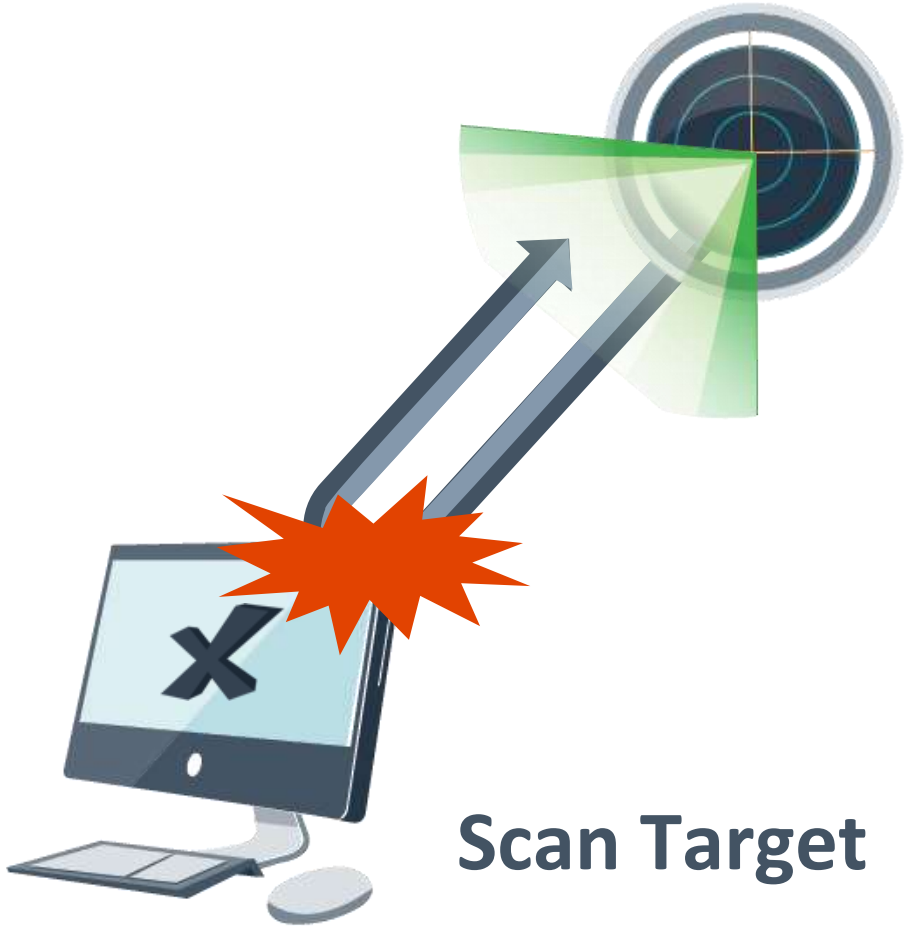
NEWS FLASH!

Break out the tools


Months or years
to address it.

SCAN!

MAYBE...



External scan, detections based on responses

Apply bandage, er patch.

No problem.
Like slow motion
Whack-A-Mole

No problem.
Like slow motion
Whack-A-Mole


EVERYONE IS HAPPY

Hit the Fast Forwar button

ONE

AT A TIME?

SPEAKING
OF TIME

PLAYING BY

THE RULES

WE DO (MOSTLY)

THEY DO NOT

We don’t even know who the bad guys are, there are so many to choose from. With different motives, objectives and resources.

We have people working, and attacking, from everywhere, with a myriad of different devices – many of which fit in our pockets.

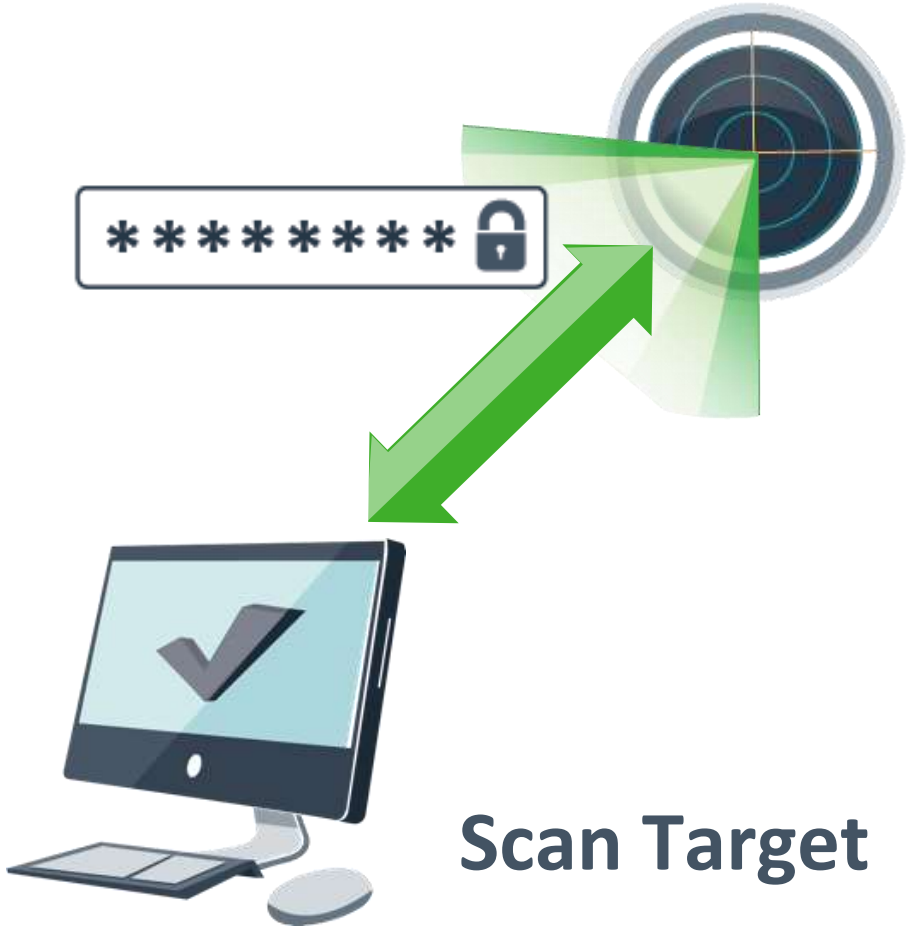
We have people working, and attacking, from everywhere, with a myriad of different devices – many of which fit in our pockets.

OH, AND

“CLOUD”

There’s no place like ::1

What has changed from the detection perspective?



Credentialed scan, detections based on direct interrogation

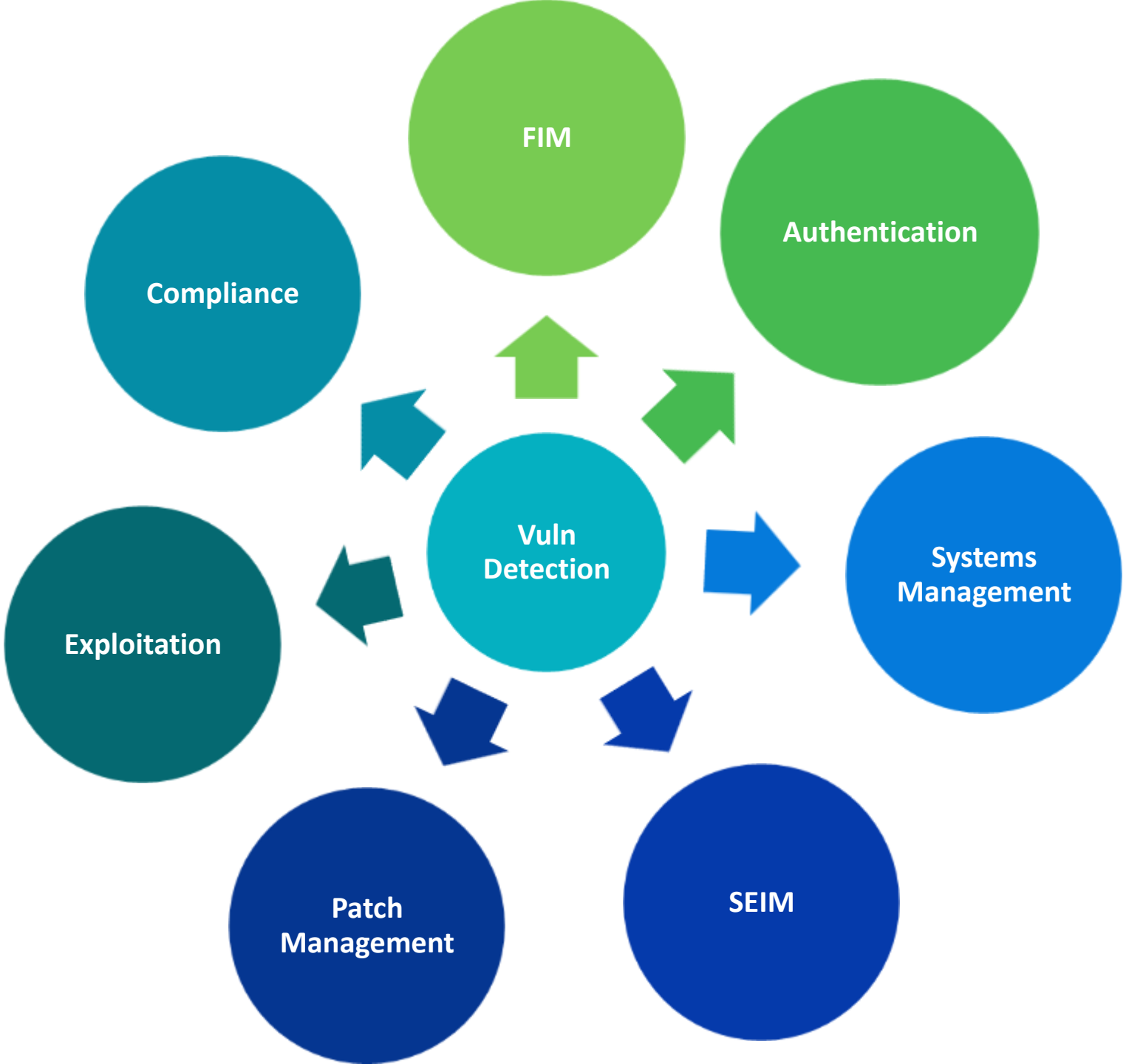
Agent-based scans, detections based on local inspection

AND WE SCAN MORE OFTEN.

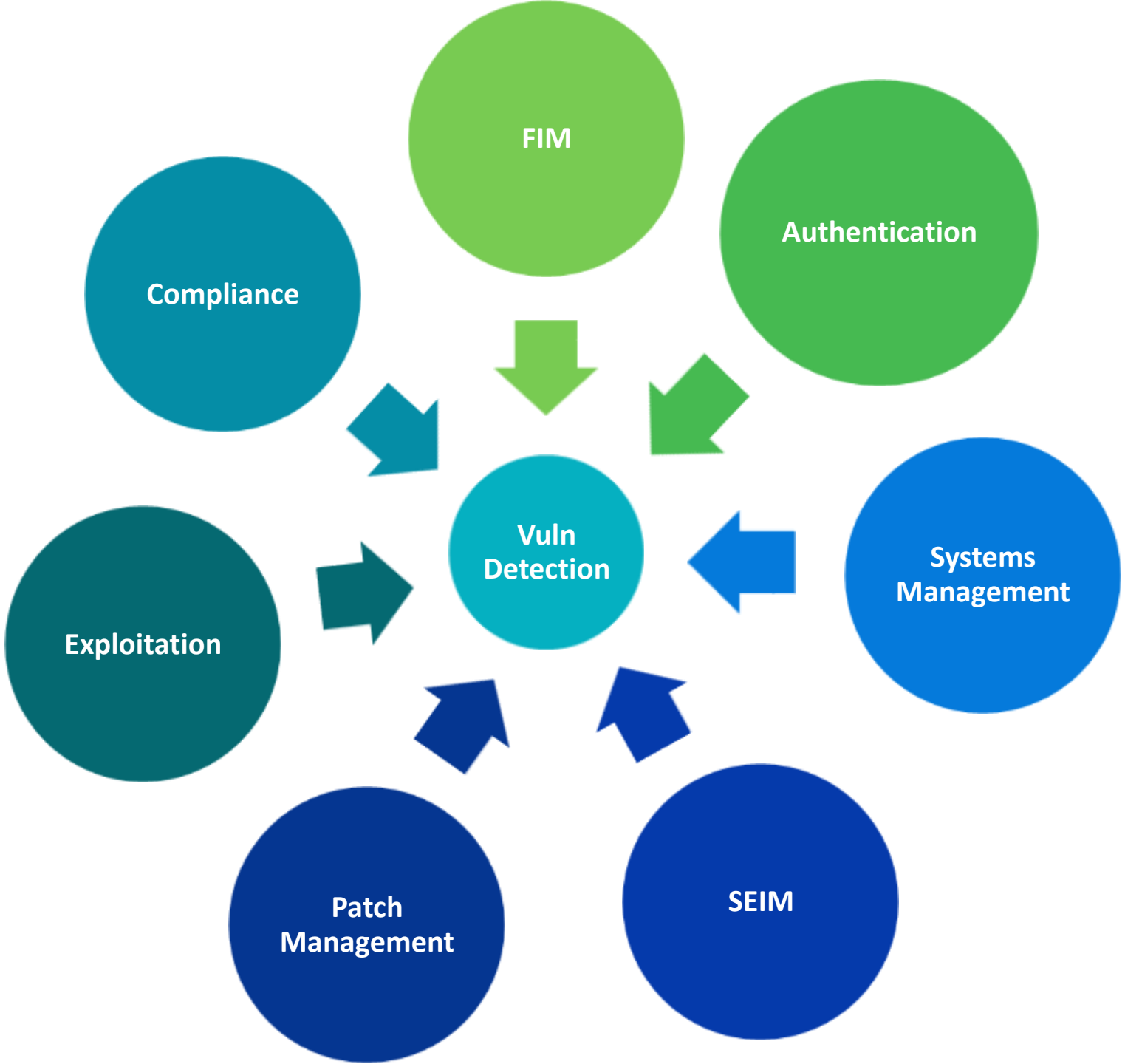
REGULARLY, EVEN.

MAYBE.

The Nature of Modern Vulnerability Management


FIM
Authentication
Compliance
Vuln Detection
Systems Management
Exploitation
Patch Management
SEIM

tenable™


FIM
Authentication
Compliance
Vuln Detection
Systems Management
Exploitation
Patch Management
SEIM

tenable™

The Nature of Modern Vulnerability Management

Vulnerability Management

is no longer just

Vulnerability Management

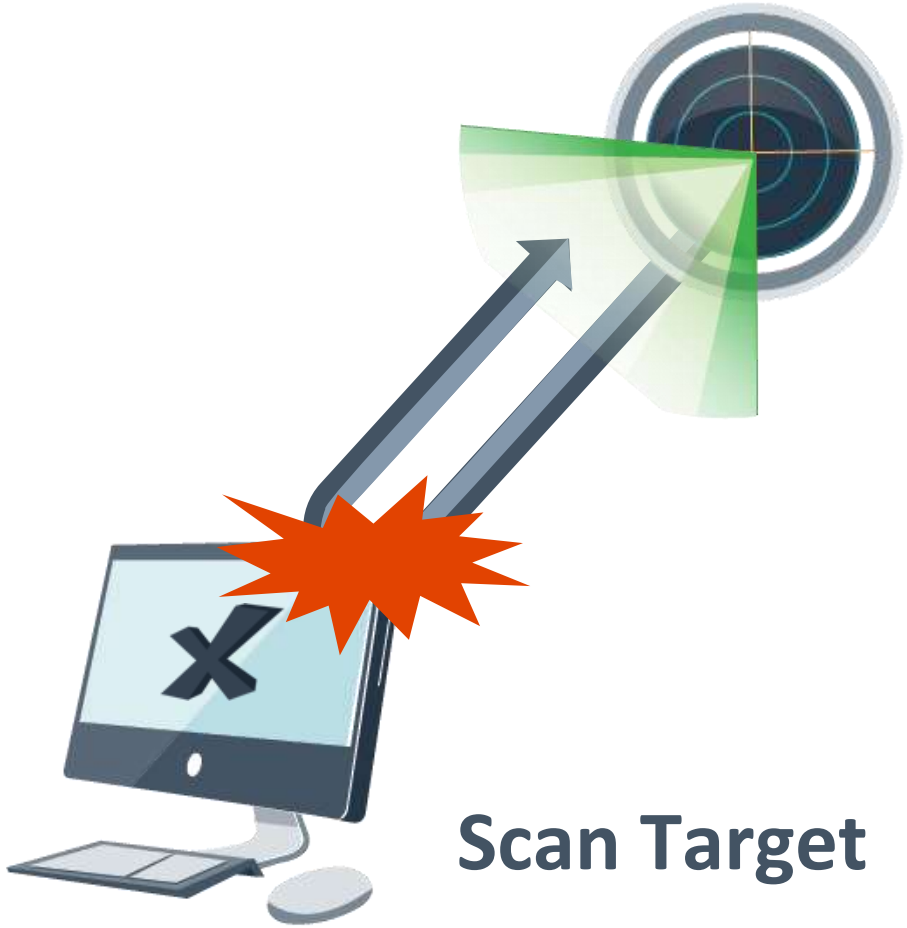
What about the future of vulnerability management?

As William Gibson observed:

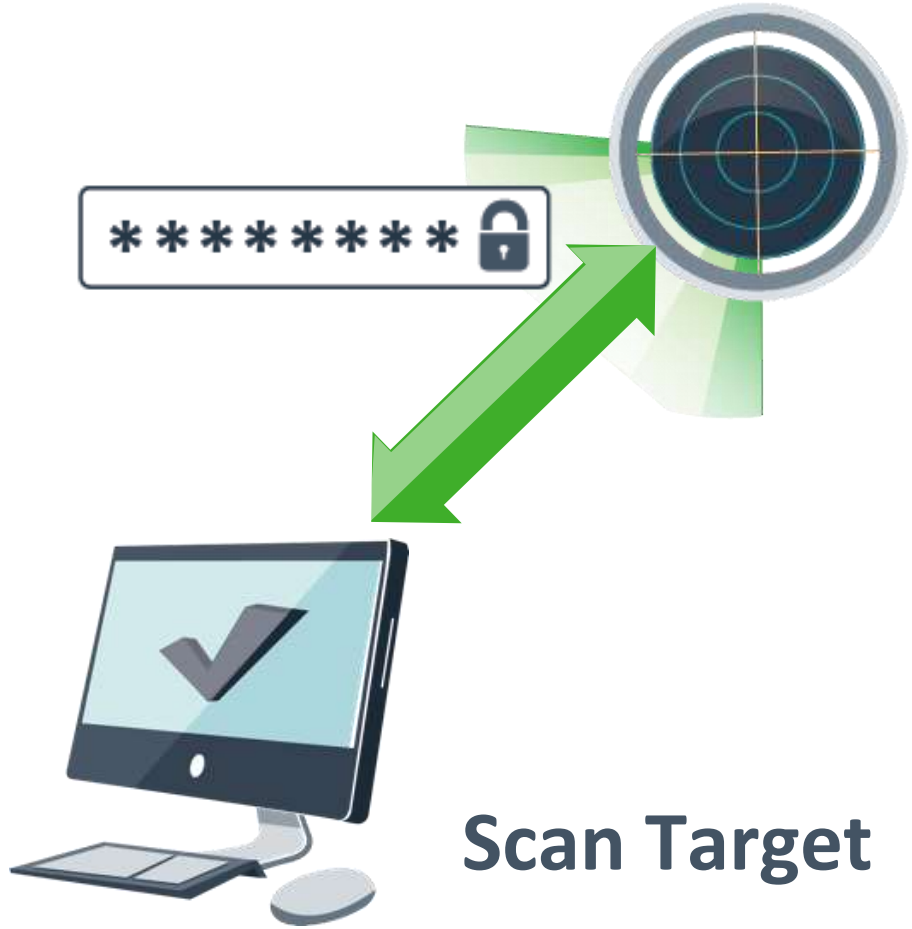
“The future is already here — it's just not very evenly distributed.”

tenable™

WHAT DOES THE FUTURE LOOK LIKE?

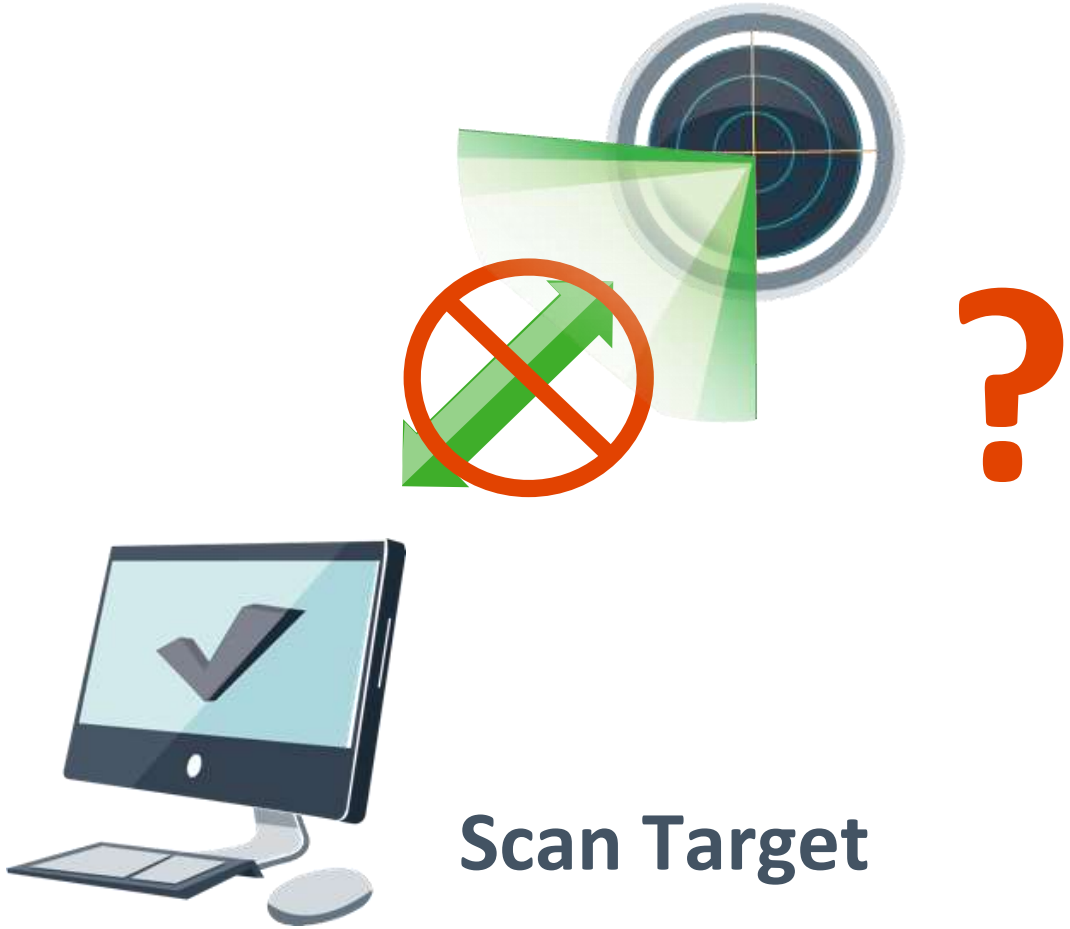


External scan, detections based on responses



Credentialed scan, detections based on direct interrogation

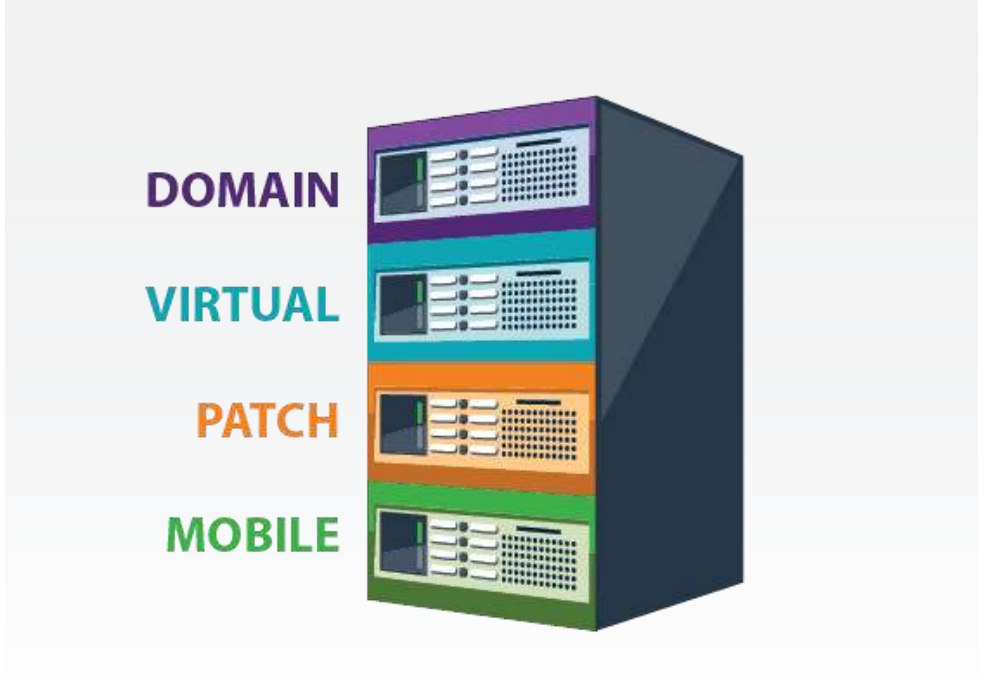
Agent-based scans, detections based on local inspection

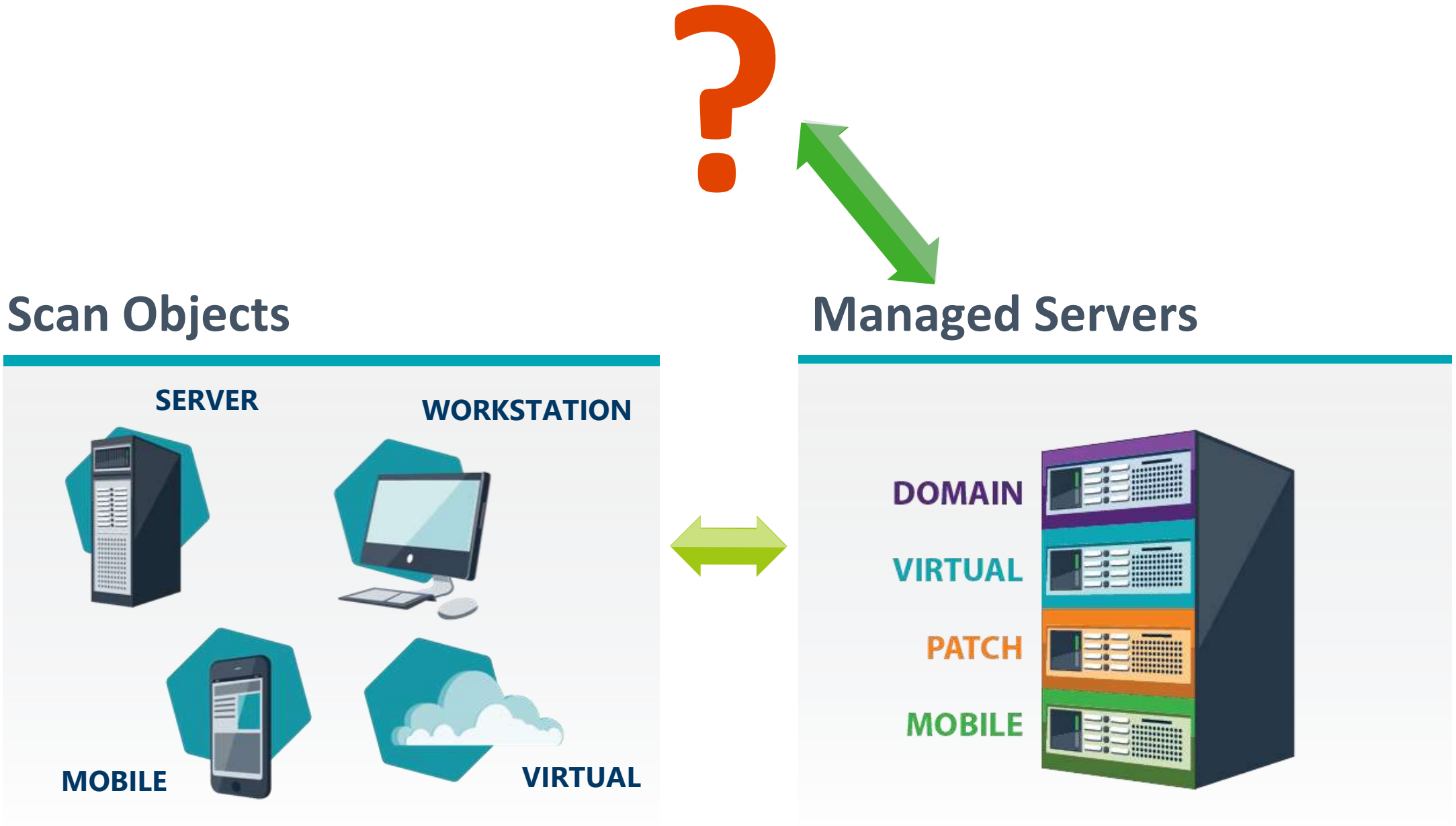


What if you can’t connect to the system, or need more information than an external scan can provide?

Managed Systems

Managed Servers




Scan Objects
SERVER
WORKSTATION
MOBILE
VIRTUAL
Managed Servers
DOMAIN
VIRTUAL
PATCH
MOBILE

MUST PLAY

WELL WITH OTHERS

Continuous Monitoring

Use all available data sources

Prioritize for your environment

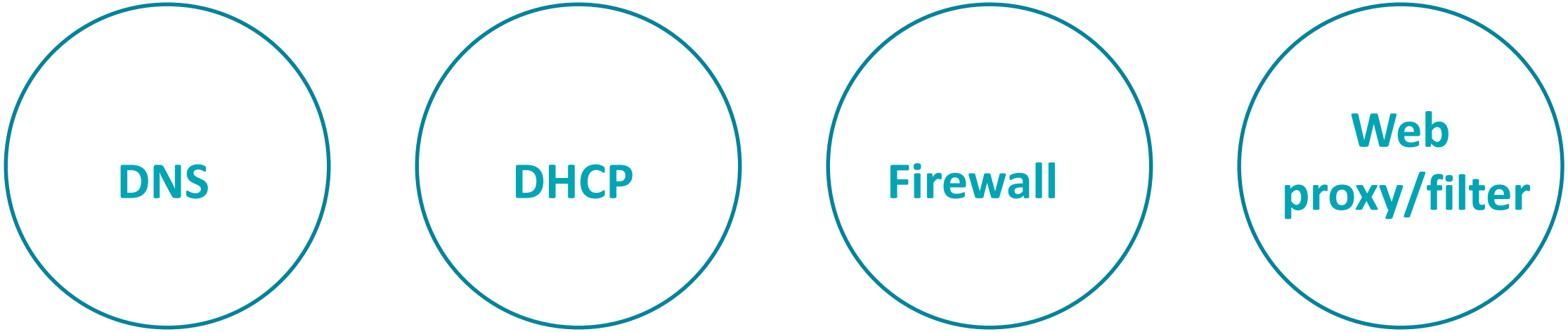
Find everything

Manage many small actions, not a few large ones

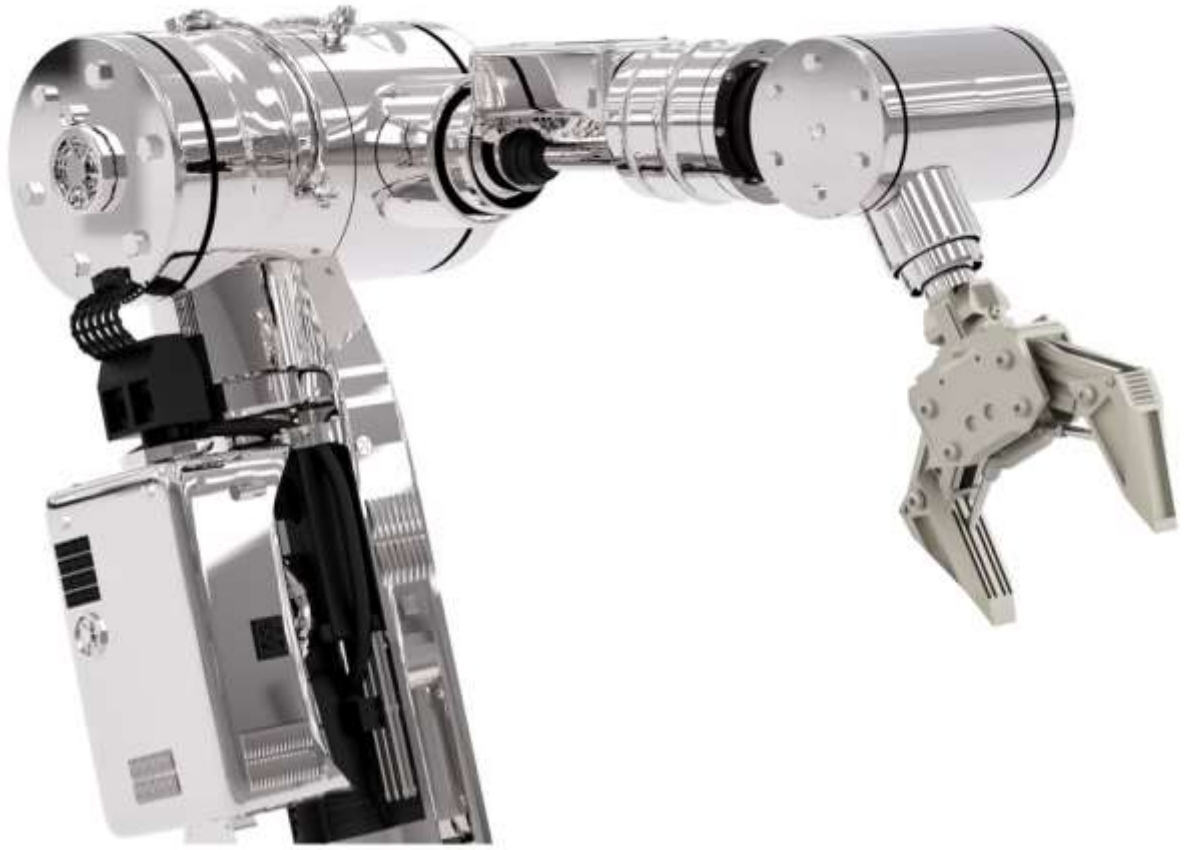
tenable™

Old School
“Big Data”

Four Logs of the Awareness



tenable™



AUTOMATION

We have to get rid of all three to move forward. We have to listen, watch and report. Continuously.

CONTEXT IS CRITICAL

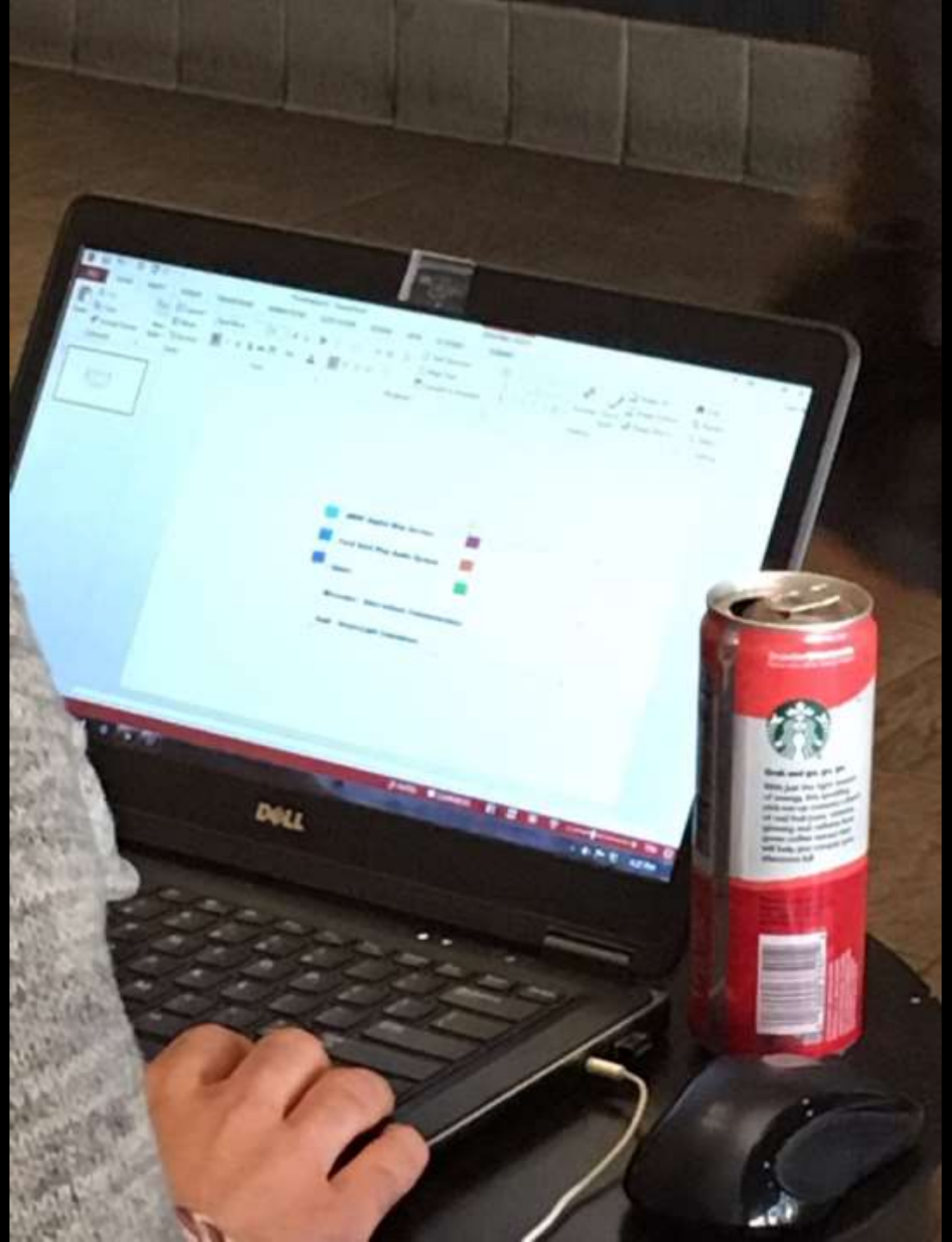
tenable™


F-250
SUPER DUTY
SECEDE
JAN Massachusetts 15
The Spirit of America

THREAT MODELING


15

EFFECTIVE DEFENSES?


DELL

~~The End~~

The Beginning