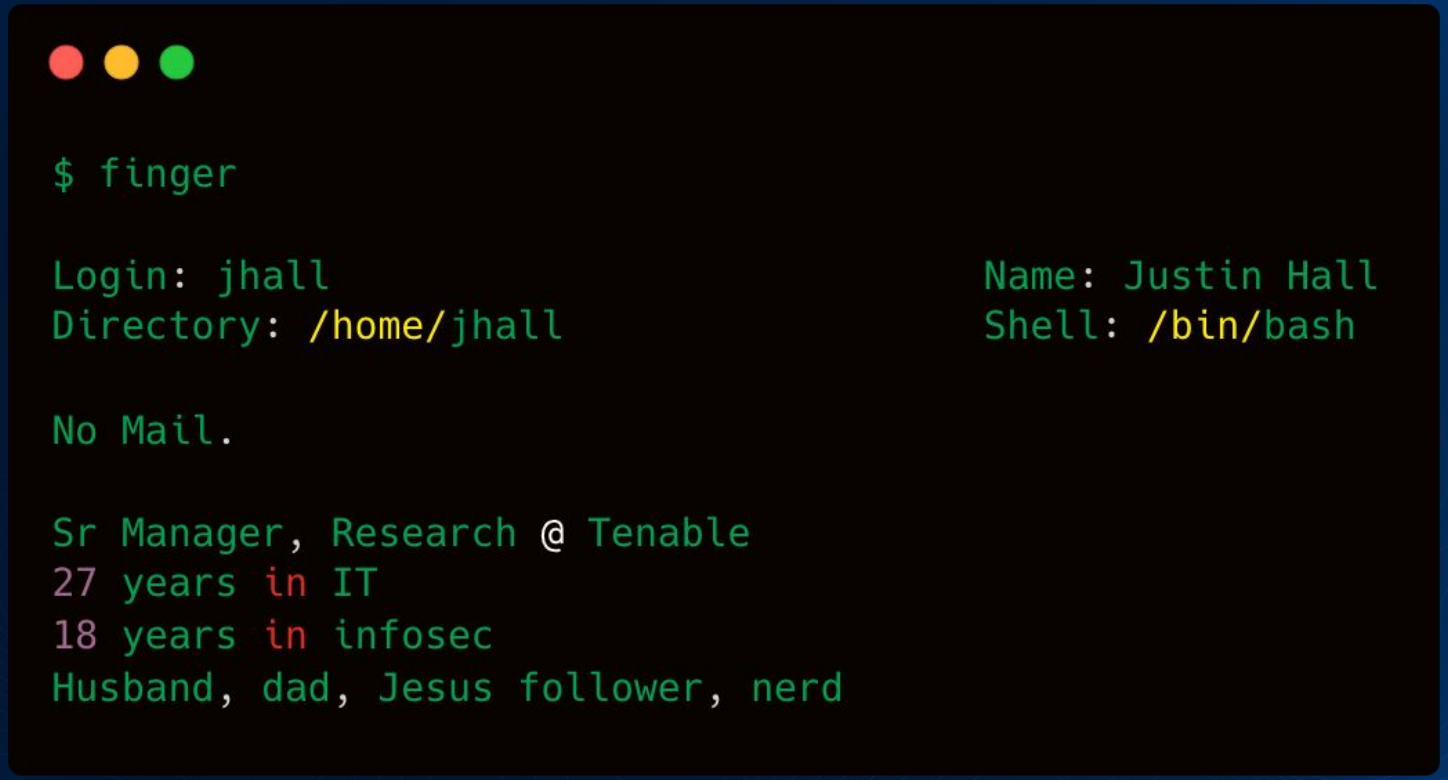
Asset Inventory

#1 on the charts, #1 in our ❤️s

Justin Hall

Sr Manager, Research

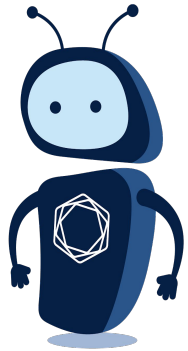

$ finger
Login: jhall
Name: Justin Hall
Directory: /home/jhall
Shell: /bin/bash
No Mail.
Sr Manager, Research @ Tenable
27 years in IT
18 years in infosec
Husband, dad, Jesus follower, nerd

Let's go back to

2005

tenable

When good guys run a bad asset inventory, it is a good thing for bad guys.



Rob Joyce
@NSA_CSDirector

Attackers will work to know your network better than you do. They will find shadow IT, misconfigurations, weak authentication and unpatched devices containing n-days. Discover and fix it before them.
#KnowledgeIsPower #KnowledgeIsSecurity

7:05 AM · Oct 18, 2023 · **25.1K** Views

Your Asset Inventory is Critical.

CIS Controls

Control #1

Inventory & Control of Enterprise Assets

NIST Cybersecurity Framework

Function #1: Identify

Category #1: ID.AM - Asset Management

International Organization for Standardization ISO 27001

CCM™ Cloud Controls Matrix

Australian Government Australian Signals Directorate

ACSC Australian Cyber Security Centre

NIST 800-171

NIST 800-53

tenable

Your Asset Inventory is Critical.

CIS Controls

Control #1

Inventory & Control of Enterprise Assets

NIST

Cybersecurity Framework

Function #1: Identify

Category #1: ID.AM Asset Management

WHY?

ISO 27001

CCM™ Cloud Controls Matrix

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

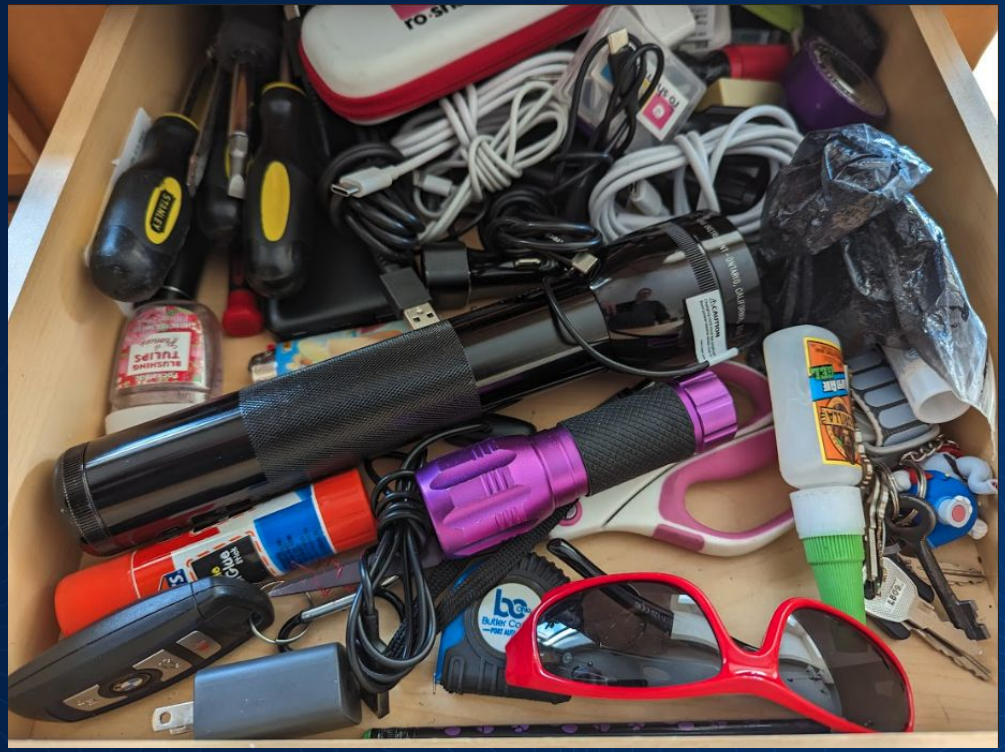
NIST 800-171 800-53

tenable

You can't protect what you can't manage, and you can't manage what you can't see.

tenable

Bad Asset Inventories are like junk drawers.



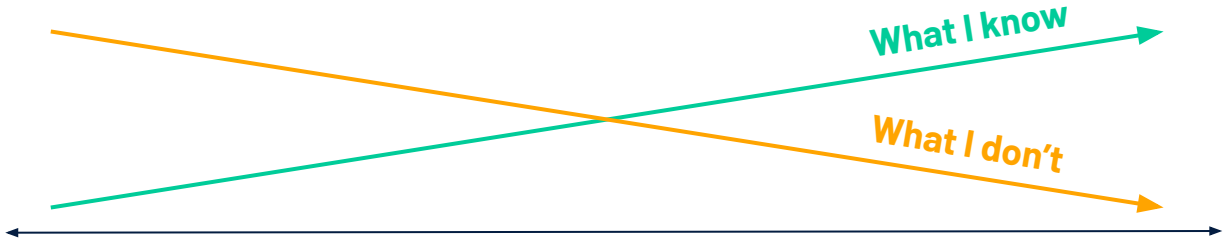
So how do we get there?

Don’t just buy a product and assume it’ll organize everything for you.

tenable

2

Start small.
Aim for progress.



tenable

Get the devices, and then get the details.

tenable

Get the devices, and then get the details.

What details?

What do you need to know in an investigation?

tenable

Interesting asset data

Hardware

Make

Model

Serial

Device class

Network

IP

Subnet

Static/Dynamic?

Interface

Hostname/FQDN

Open ports

Software

Software inventory

CPEs

Services/daemons

Data

Is there sensitive data?

Data categories

Classification level

Regulatory relevance

Operating System

Release version

Patchlevel

Last reboot

Identity

Asset owner

Contact info

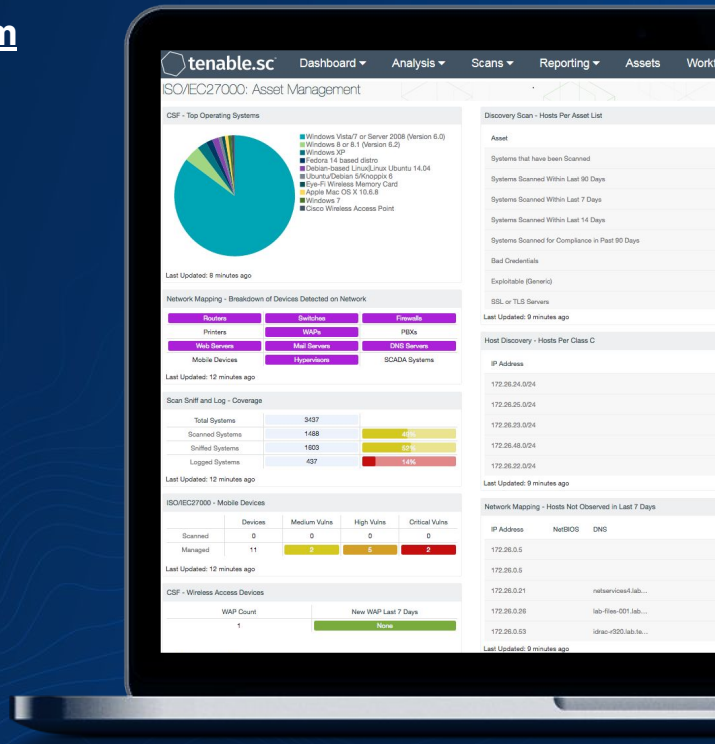
Username

Domain

Auth source

MFA info

Geolocation



Make sure your data sources are trustworthy.

Be careful who gets access to your inventory.

6 Aim for automation. Don't make this someone's job.

More Resources

NIST SP 1800-5, IT Asset Management

Tenable One Cyber Asset Management

tenable

Thanks for attending!

Q&A

tenable