REDSIEGE
INFORMATION SECURITY

Antisyphon Training: Close Security Gaps, Pass Audits, Stay Secure

WHO IS Kimber [bat] Amos

Principal Consultant

- 20 Years IT Experience
  - Detection & Response
  - Purple and Blue Teaming
  - IT, Sys Admin, & Security Expertise
- GIAC GCIH, GISP, ISC2 System Security Engineer
- Instructor, Mentor, and Speaker
- Tribe of Hackers x2
- Artist, Traveler, Mediocre Sailor, & Kid/Cat/Dog Mom
- Contact: mzbat on every platform

Overview

- What's security posture anyway?
- Assets
  - What counts?
- Analysis
  - Does this look right?
- Remediation Roadmaps
  - How important is the fix?
- Audit
  - Ready or not, here it comes!

What This Training Isn’t

- A complete guide for assessing security posture
- A complete guide for a successful audit
- A technical guide for scanning, penetration testing, and critical controls
- A replacement for a security posture review by an experienced security firm before tackling a formal compliance audit

Defining Security Posture

- Definition: Overall cybersecurity health, representing an organization’s ability to prevent, detect, respond to, and recover from threats and incidents.
- Key aspects of security posture include:
  - Holistic state of controls, policies, plans, user training
  - Ability to identify gaps
  - Effectiveness of existing security measures
- The purpose of (most) audits is to establish, measure, and improve security posture.
- Security posture can and should be evaluated before doing the heavy lift of a formal compliance audit.

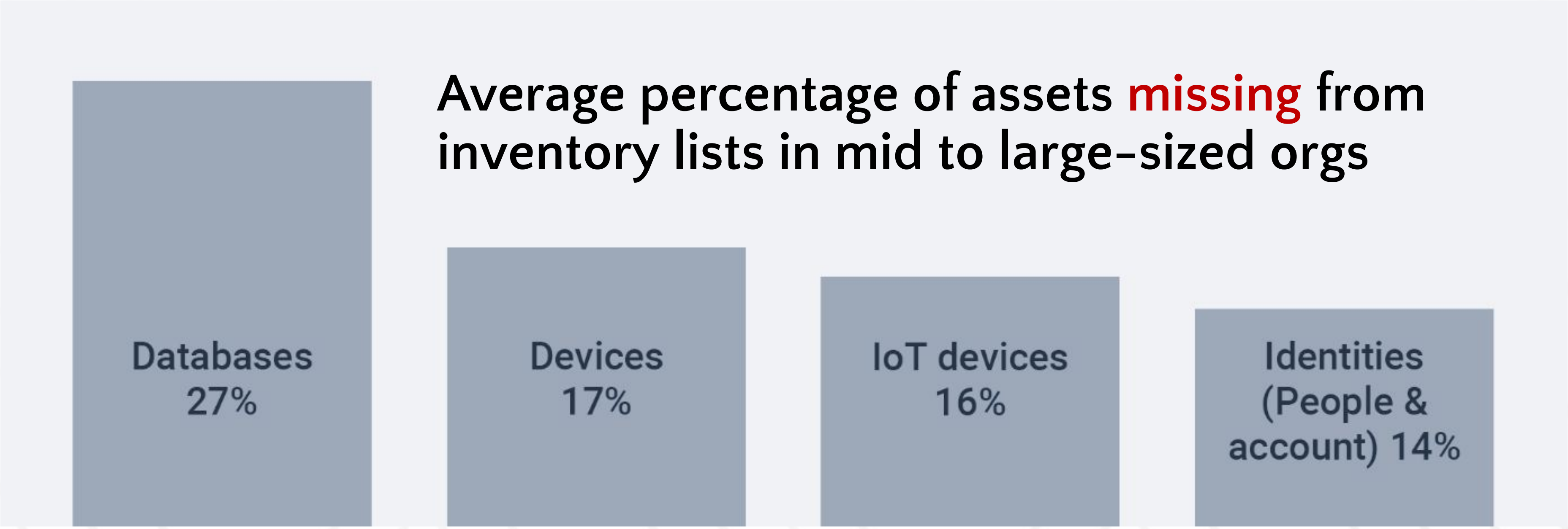
What Is An Asset?

- Assets aren’t just tagged computers anymore.
- In other words, an asset is any tangible or intangible resource that has value to an org and needs protection from threats, cyber or otherwise.

https://huguesjohnson.com/random/recycling/20161119_103219.jpg

What Are We Missing?

Even the best security teams struggle with visibility of assets, often missing or overlooking significant percentages in annual inventories.



Average percentage of assets missing from inventory lists in mid to large-sized orgs

https://panaseer.com/resources/reports/2022-security-leaders-peer-report

Rapid Asset Discovery

- Device/Agent discovery tools
- Network scanners and agents
- Active internal scanning (e.g. SNMP, WMI)
- Public data scraping for cloud-based and internet-facing assets
- Threat intel feeds/platforms
- Cloud provider APIs
- Domain scans
- Public code repo scans

Maintaining Asset Inventory

- **Centralize**
  - Consolidate all discovered asset information into a single platform for easier access and faster decision-making.
- **Automate**
  - Schedule regular, automated scans to ensure your asset inventory is continuously updated and detects new or unauthorized devices.
- **Integrate**
  - Connect your asset discovery solution with existing security tools (e.g. SIEM, vuln management) for a holistic view.
- **Prioritize**
  - Focus on identifying and monitoring high-value or critical assets to address their potential vulnerabilities first.
- **Validate**
  - Implement processes to regularly update and validate the accuracy of discovered asset information.

Time for Threat Analysis

https://www.techrepublic.com/article/why-your-data-analysis-may-be-doomed-from-the-start/

What Is Threat Analysis?

- Definition: Formal process of identifying, assessing, and evaluating potential security risks and threats to an organization’s IT systems, assets, and networks.
- In other words, threat analysis can be approached a lot like asset discovery, but instead of identifying assets, teams identify and analyze the risks and threats to those assets.

https://www.pokemon.com/us

Analyze Threats to Assets

- **Identify** weaknesses before attackers do
  - Vulnerability scanning
  - Penetration tests
  - Assumed breach red team exercises
  - Ransomware readiness red team exercises
- **Leverage** threat intelligence
  - Threat intel feeds
  - Industry reports
  - Breaking security news
- **Classify and Prioritize** vulnerabilities and risks
  - Assess business impact of security risks and incidents
  - Prioritize business critical systems*

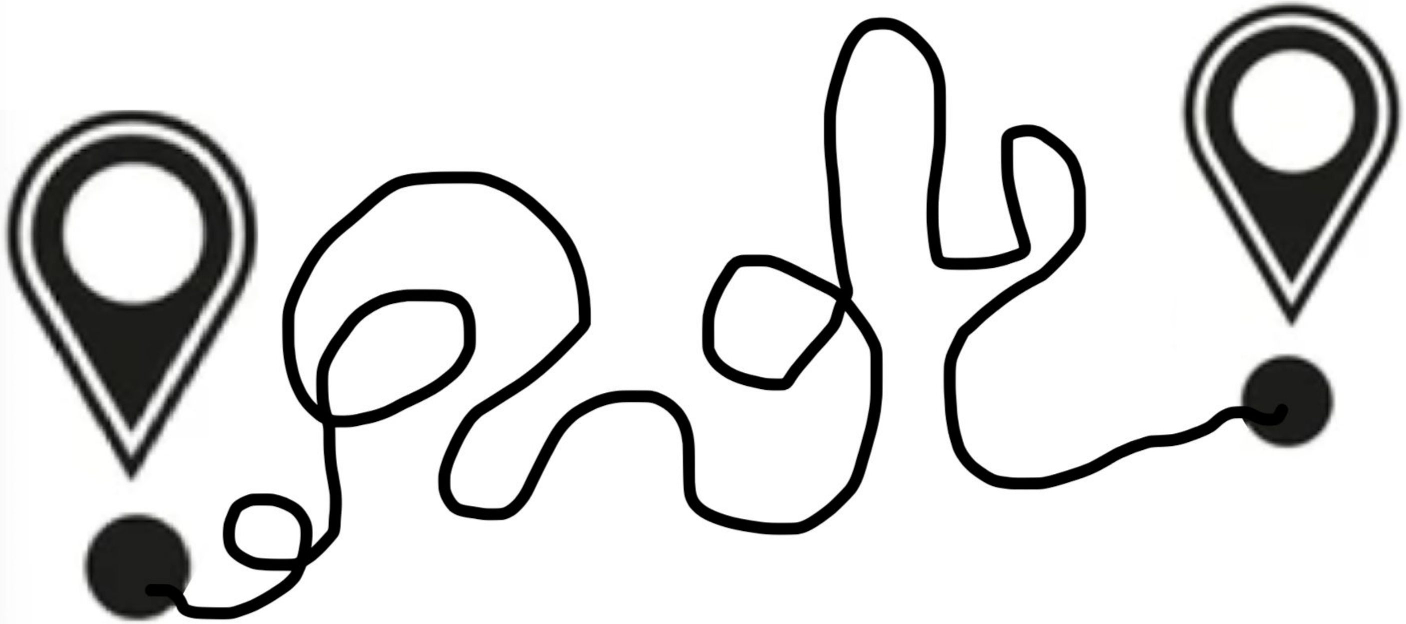
    **This might require a cost-benefit analysis*

Protect Assets

- Update asset inventory
  - Yes, this is **at least** the third time I've mentioned this
  - Critical to understanding and analyzing attack surface
  - Difficult to protect what's not on the radar
- Practice good cyber hygiene
  - Strong passwords and policies
  - Automated patching
  - Data encryption
  - Strong access control
- Maintain solid documentation (everyone's favorite)
  - Security policies: access controls, network, data security, etc.
  - Plans: Incident Response, Business Continuity, Disaster Recovery
  - Assigned roles and responsibilities – the clearer, the better.

Remediation Roadmap Planning

Don’t panic.



Iterative Security Roadmap

- **Prioritize** risk and threats
  - Existing compromise
  - Risk scores
  - Emerging threats
- **Integrate** threat analysis into roadmap planning
- **Outline** standard remediation process that includes mitigation and target time/date
- **Refine** remediation processes to improve benchmarks
- **Prepare** to advocate for out of band patching, bug squashes, and roadmap detours
- When all else fails, **send PM baked goods**

What Got You Here

Won’t Get You There

https://www.kanakkupillai.com/learn/audits-for-private-limited-companies-a-comprehensive-guide-to-compliance/

Audit Preparation

It’s all about (the) **control**(s).

CIS Controls : 18 with 150+ safeguards
ISO-27001 : 93 in 4 themes

SOC2 : 60-100+ based on choice of 5 Trust Services Criteria (TSCs)

NIST 800-171 rev2 : 110 in 14 families

PCI DSS : 240+ in 6 objectives

CMMC 2.0

- Level 1: 17
- Level 2: 110 (NIST 800-171 rev2)
- Level 3: All Level 2 controls plus 24 from 800-172

NIST 800-53 rev5: 1000+ (yes, over ONE THOUSAND)

Ready for an Audit?

Trust but verify.

OUR DEVICES ARE NOW 100% SECURE.
HOW DID YOU DO THAT?
I TURNED THEM ALL OFF.
© D.Fletcher for CloudTweaks.com

https://cloudtweaks.com/author/david/

Questions?