



How to be your Security Team's Best Friend



Why listen to me talk about Ops and Security?

PAST

- UNIX SysAdmin/Operations background
- Transitioned to Security Incident Response/Security Research

CURRENT

- Senior Security Engineer at **AGARI**
- Mentor for SANS' Women's CyberTalent Immersion Academy

CONTACT

- Twitter: @unixgeekem



Talk Agenda

1. Introduction
2. CIS Critical Security Controls
3. More Security Thoughts

Standard Disclaimer: The opinions expressed in this talk are my own and do not represent the views of my employer.

Non-Standard Disclaimer: I hope you like cat photos.



SwiftOnSecurity

@SwiftOnSecurity

Following



Broke: I wish I worked in Computer Security it's so cool compared to Ops
Woke: Your Ops ass already works in Computer Security

4:51 PM - 11 May 2018

36 Retweets 204 Likes



7



36



204





**Not
Rocket
Science**

The CIS Critical Security Controls

- Industry consensus guidelines
- Your security/compliance officer likes these
- 3 types: Basic, Foundational, and Organizational¹

1. #TeamOxfordComma



#1: Hardware / Asset Inventory

CSC 1: Inventory and Control of Hardware Assets

Questions you need to answer about your hardware/instances/containers:

- Network Access Control - how do you know what's on your network?
- Automation - how do you keep your assets in a known state?
- Asset Management - how do you keep track of assets?
 - No, saying “a spreadsheet” or “a database” doesn't count



#2: Software Inventory



CSC 2: Inventory and Control of Software Assets

Questions you need to answer about your software:

- What software is running/installed in your infrastructure?
- Who installed the software?
- What does the software do?

Track Expiration Dates Too

- Software Licenses
- Domains
- SSL Certificates

Don't be this site →





#3: Continuous Vulnerability Management

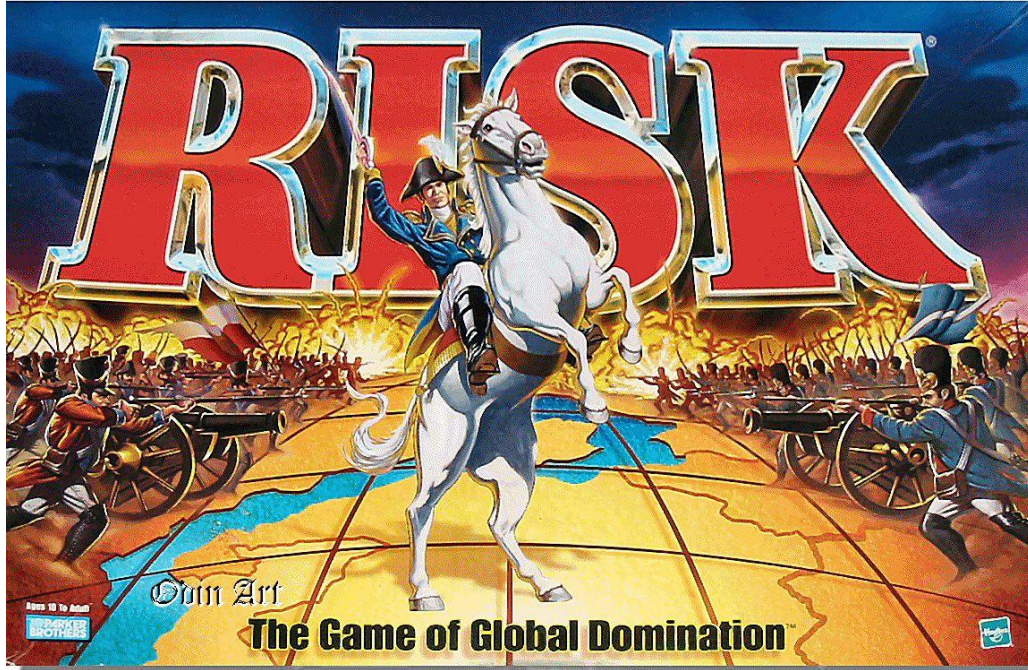
CSC 3: Continuous Vulnerability Management: Scanning

- Logos create buzz!
- Scan early, scan often
 - Authenticated and non-authenticated
- Scan from inside and outside your perimeter²



2. If you have a perimeter

A digression: Threat + Vulnerability = Risk





CSC 3: Continuous Vulnerability Management: Patching

- Understand your risks, and remediate the serious vulnerabilities.
 - Highest risk first is the best practice
- Use your automation to ensure updates are applied everywhere.
 - Though maybe you test first before you upgrade Python/Ruby in your Production environment...

#4: Control Admin Privileges





CSC 4: Controlled Use of Admin Privileges

- Separate out admin accounts from user accounts if you can.
- Use groups or roles.
- Consider functional names for your groups.
 - “sec-logging-read-only” is more informative than “logging”



Least Privilege, Passwords, and Passphrases

Any resemblance to actual companies, existing or defunct, or actual events, is purely coincidental.

What if there was a company that didn't set a root password for their databases...

What if there was a company that didn't change default credentials to the admin interface of their website...

What if there was a company that let everyone ssh in as root...



#5: Secure Default Configs



CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

- Base your secure configs on a security standard.
- Don't install software you don't need to run your systems!
- Use Automation/Configuration Management tools to enforce security.
- Regularly evaluate the security of your Gold Images.
- Transition from policies to automation as your company grows.



#6: Log All the Things, and Review the Logs



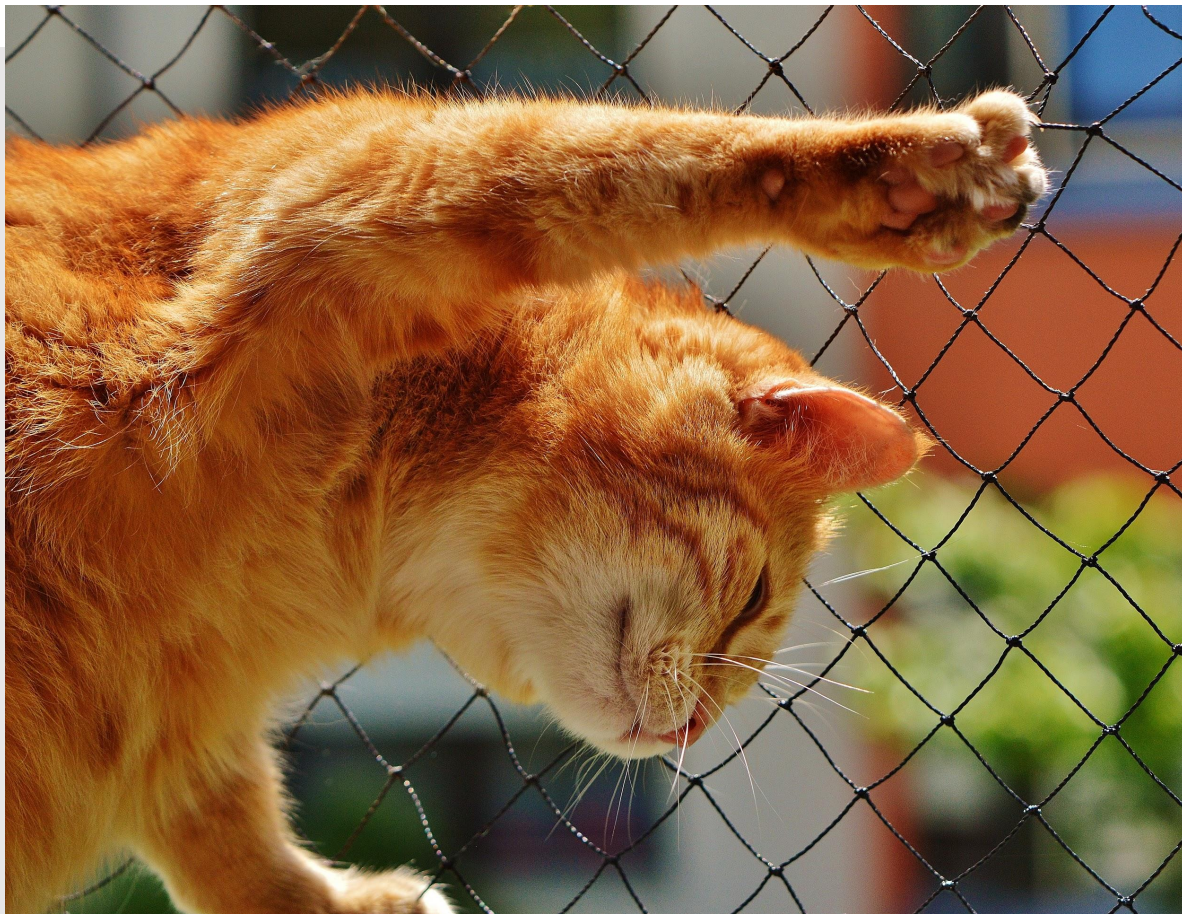
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

- Log all the things.
 - Systems, security devices, applications, access points
- Collect all your logs somewhere and review them.
 - Review: not all done by hand!
- **Outbound traffic is always interesting.**

Plus 14 More

- Email and Web Browser Protections
- Malware Defenses
- Limitation and Control of Network Ports, Protocols, and Services
- Data Recovery Capabilities
- Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
- Boundary Defense
- Data Protection
- Controlled Access Based on the Need to Know
- Wireless Access Control
- Account Monitoring and Control
- Implement a Security Awareness and Training Program
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises

Data Protection: it's been in the news a lot lately



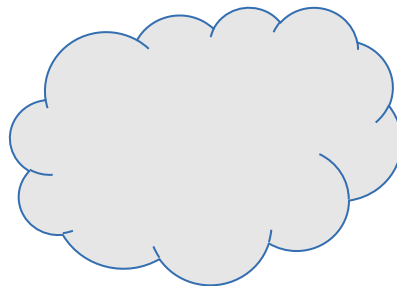
Emily Gladstone Cole

@unixgeekem

Think before you check into GitHub

So many **interesting** things can be found in publicly-available GitHub repositories:

- Hardcoded passwords
- AWS Keys
- SSH Keys
- PGP Private Keys
- Internal hostnames



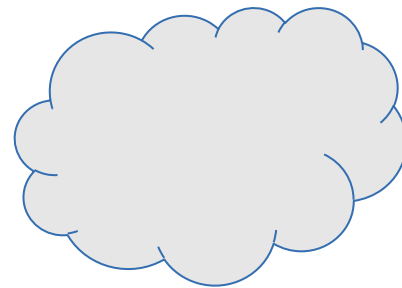
Think AFTER you check into GitHub

So you've checked in some sensitive information?

- If you commit over it, it's still in your commit history.
- **Remove** that commit.
- Rotate those credentials.
- Use TruffleHog to search for any remaining sensitive data in your old commits.



Remember those S3 Buckets



- AWS now sets S3 Buckets to be private by default.
- Amazon Macie monitors S3 to find insecure buckets.
- AWS Trusted Advisor will tell you about insecure buckets.
- **Pro Tip:** the “Authenticated Users” group means anyone who has logged in to **any** AWS account, not just yours!

**But Wait,
There's
More**





Security Mindset

What would a malicious user do?

How can someone manipulate this URL?

Can someone submit a modified form?

What do my error messages tell an attacker about my infrastructure?



Security and Technical Debt

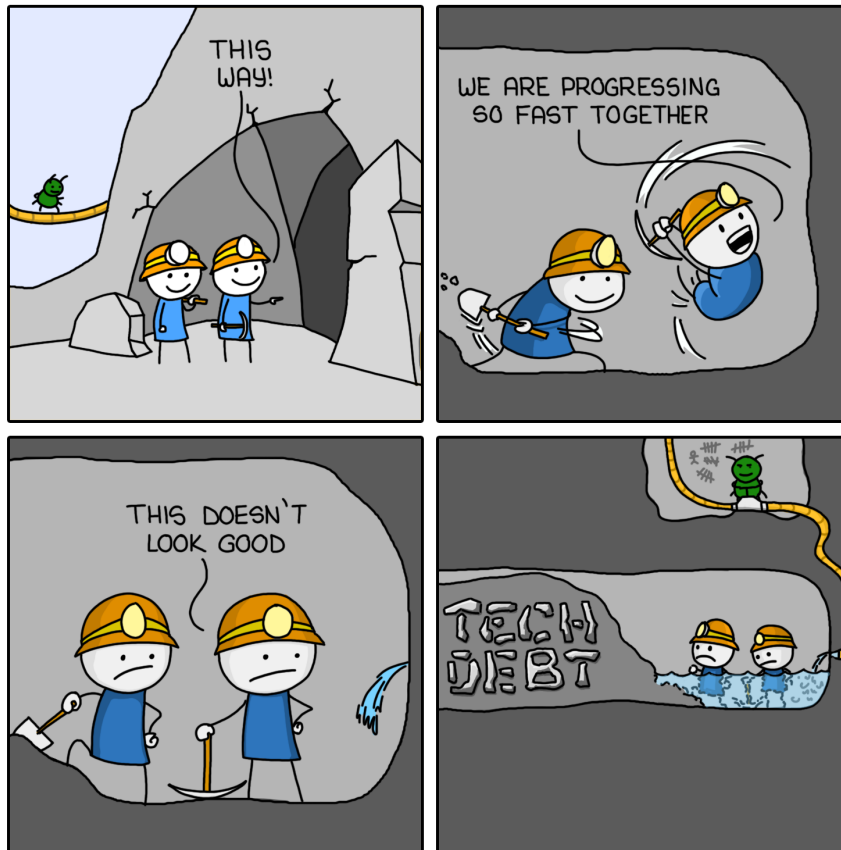
Like logging, security is harder to do well when you're adding it on after the fact.

“I’ll set up security later” - will management let you fix that later if they don’t agree it’s important to work on security now?

**Please address
your technical
debt.**


Your security team
can help prioritize it if
you like.

TECH DEBT



MONKEYUSER.COM

@unixgeekem



Security technical debt is not friendly credit card debt. Security technical debt is the kind where the debt collector mails you a piece of someone precious to you as a reminder when a payment is overdue. --unixorn on Hangops



Some other good Security Practices

- Use secure coding principles (OWASP can help define these).
 - Remember to sanitize those inputs (aka Data Validation)
- Build security tests into your CI/CD pipeline.
- External reviewers can find things you miss.
- Diverse teammates bring different perspectives and make your products and company stronger. Listen to them.

Summing Up

- Keeping an inventory helps for security, operations, and lifecycle management.
- Perfect security can be hard. The basics aren't.
- Don't blame users for security issues. Write/buy better tools for them instead.



TL;DR - Ops probably already is your security team's best friend.

You're already doing most of the things I discussed, right? If not, please consider doing them. Your security team will thank you.



Thank you



Emily Gladstone Cole

@unixgeekem

References

- CIS Critical Security Controls: <https://www.cisecurity.org/controls/>
- NIST 800-53 Framework: <https://nvd.nist.gov/800-53>
- <https://blog.rapid7.com/2017/04/19/the-cis-critical-security-controls-series/>
- Rob Joyce at Enigma 2016: <https://www.youtube.com/watch?v=bDJb8WOJYdA>
- Dylan Ayrey at BSides SF 2018: <https://www.youtube.com/watch?v=TV2hHeKj4-4>
- truffleHog finds secrets in GitHub repos: <https://github.com/dxa4481/truffleHog>
- Security Training: <https://www.sans.org/>
- OWASP Developer Guide: https://www.owasp.org/index.php/OWASP_Guide_Project
- Tech Debt from @ismonkeyuser: <https://www.monkeyuser.com/2018/tech-debt/>
- Cat images from pexels.com

Got Questions?

- @unixgeekem on Twitter
- @unixgeekem on Hangops









