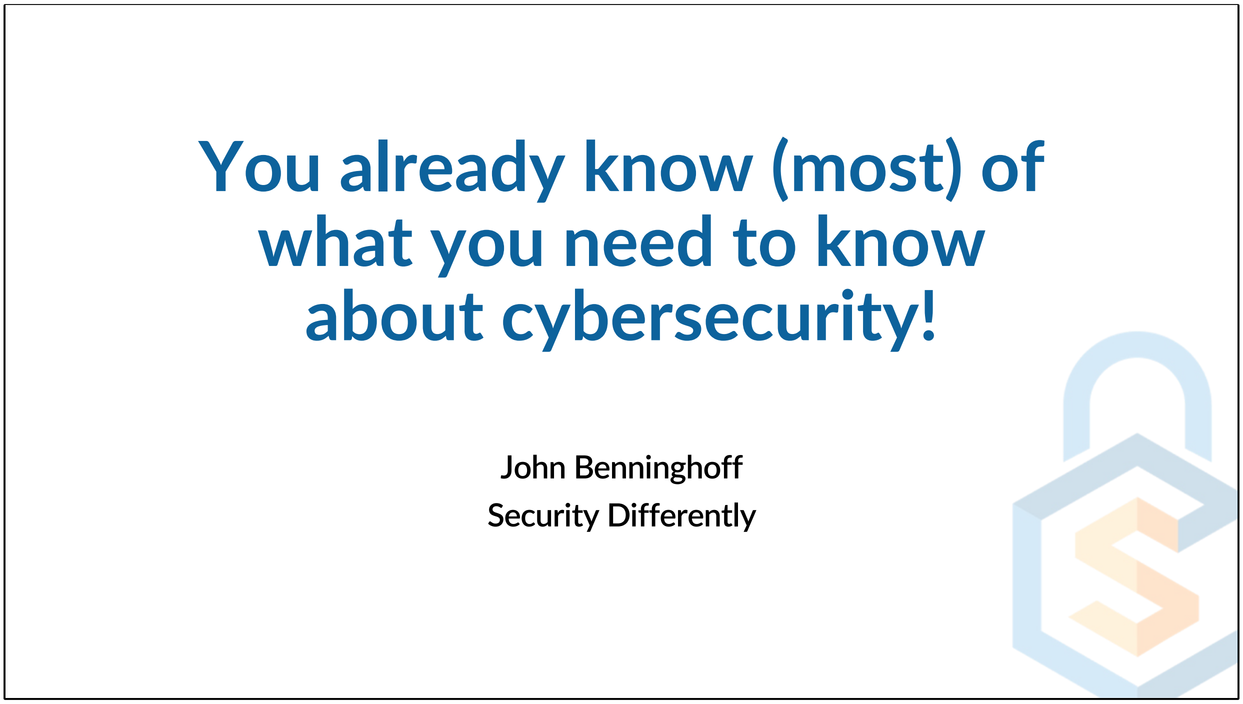


You already know (most) of what you need to know about cybersecurity!

John Benninghoff
Security Differently

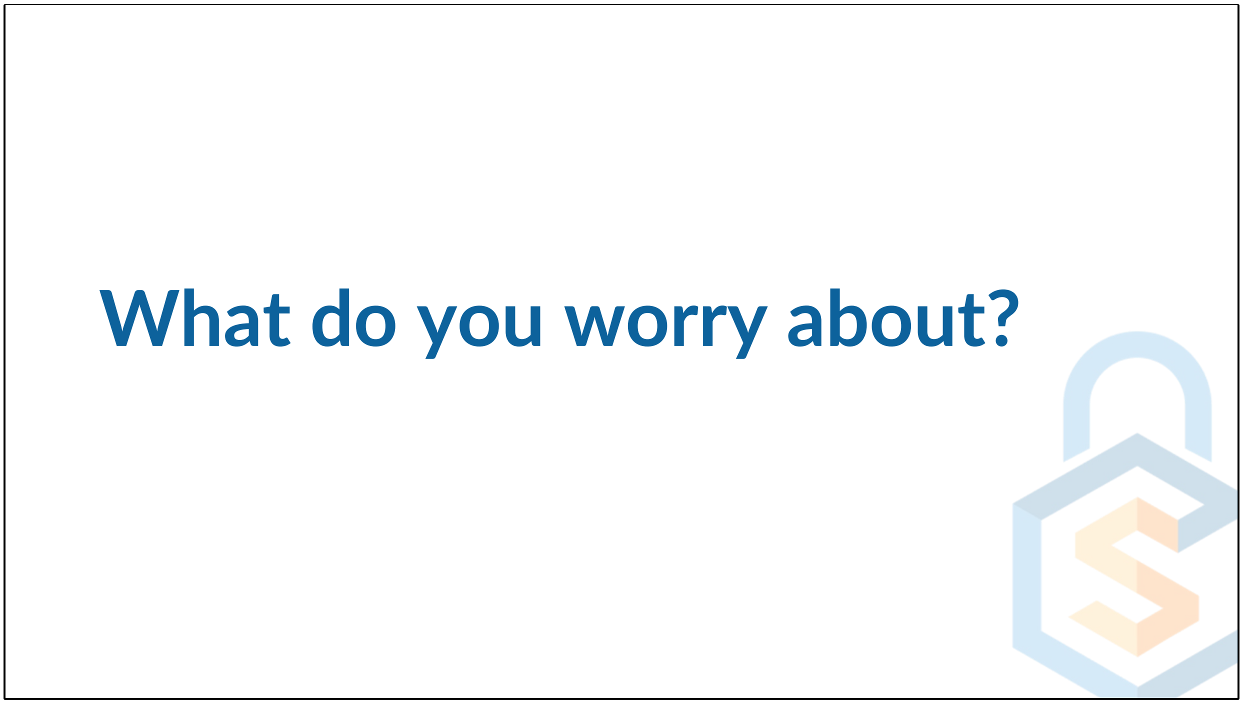
I'll have a QR code at the end for you to download the slides with notes and links to all the references.

I ♡ Interruptions!

I’m known to be guilty of interrupting. As this is a Minnebar talk, please feel free to jump in and ask questions!

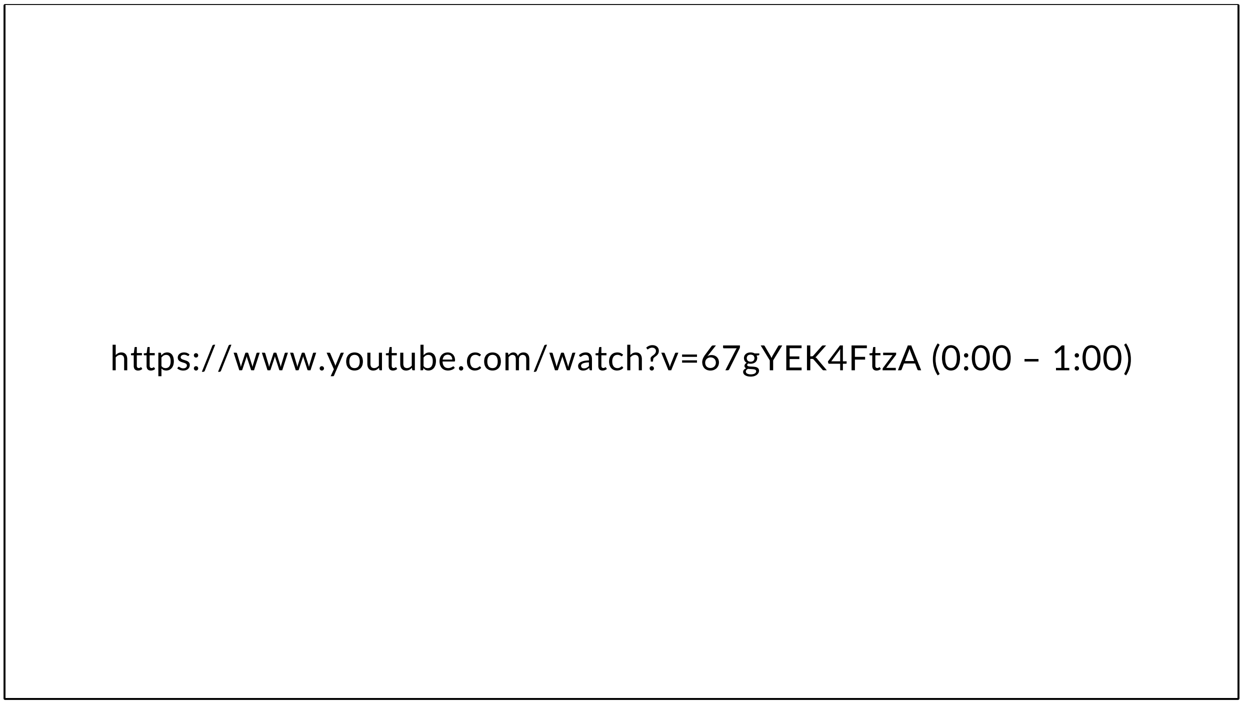
What’s my story? Me on upper left, wife Jolene and our dog Gertie. Started in security after attending SANS Network Security 1998. 20 years later, MSc in safety science (managing risk and systems change, 2018-2021). More recently, I worked in Site Reliability Engineering, starting in 2020, and spoke at SREcon earlier this year!

SANS: https://www.sans.org
TCD: https://psychology.tcd.ie/postgraduate/msc-riskandchange/, image: https://commons.wikimedia.org/wiki/File:Trinity_college_library.jpg
SREcon: https://www.usenix.org/srecon



What do you worry about?

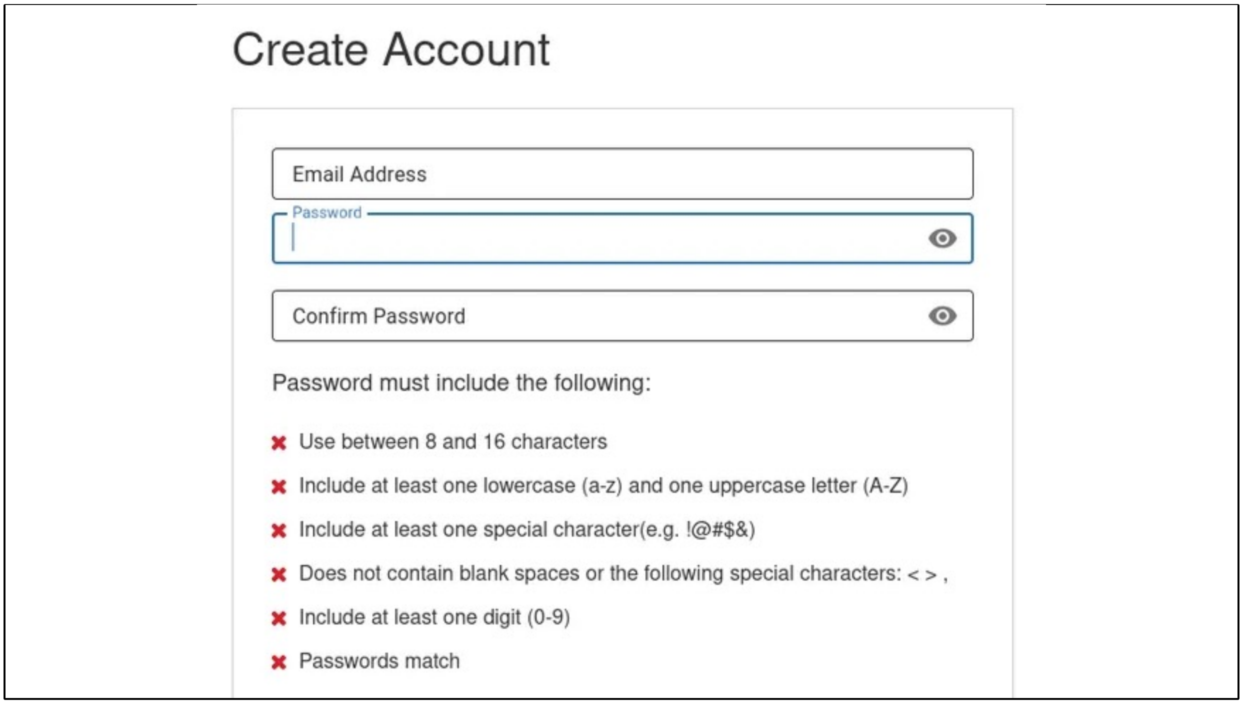
Question for the audience!



https://www.youtube.com/watch?v=67gYEK4FtzA (0:00 – 1:00)

Perception of security: Mr. Robot Hacking (Fear, Love)

https://www.youtube.com/watch?v=67gYEK4FtzA (0:00 – 1:00)



Create Account

Email Address

Password

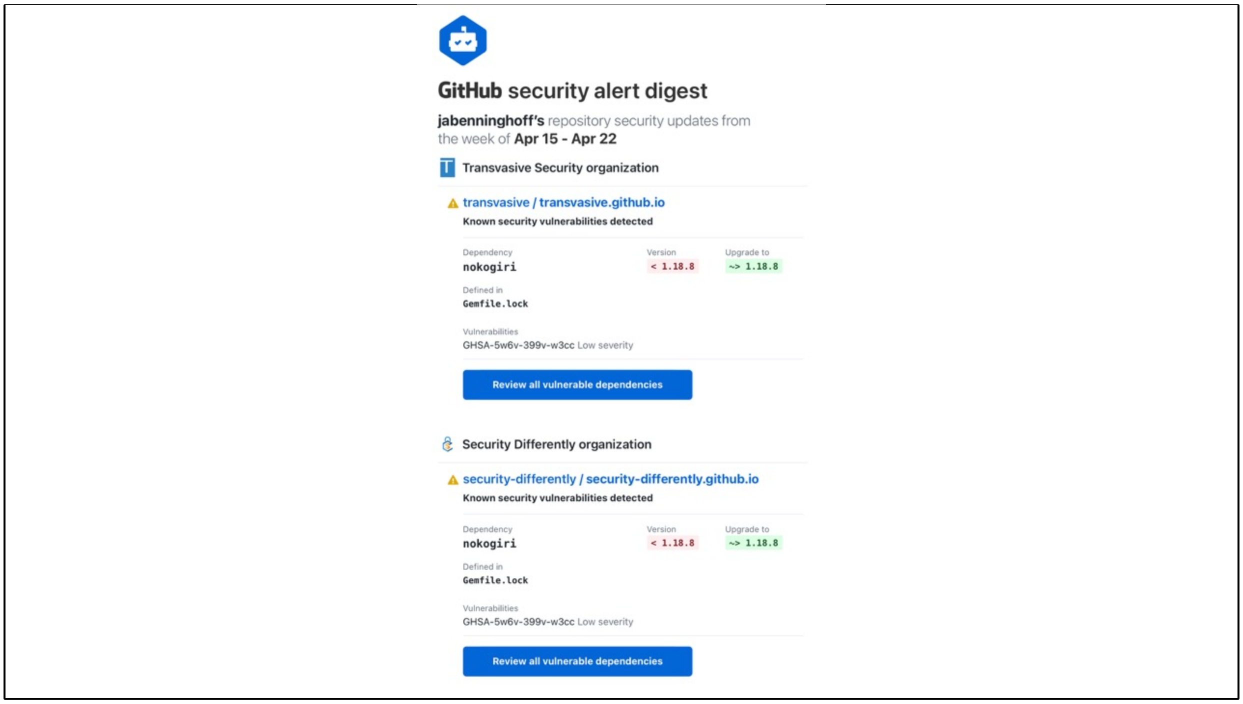
Confirm Password

Password must include the following:

- ✖ Use between 8 and 16 characters
- ✖ Include at least one lowercase (a-z) and one uppercase letter (A-Z)
- ✖ Include at least one special character(e.g. !@#$&)
- ✖ Does not contain blank spaces or the following special characters: < > ,
- ✖ Include at least one digit (0-9)
- ✖ Passwords match

Reality of security: dumb password rules (Hate)

https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules
https://dumbpasswordrules.com/sites/costco-com/
Thanks to https://www.schneier.com/blog/archives/2023/03/dumb-password-rules.html



GitHub security alert digest

jabenninghoff's repository security updates from the week of **Apr 15 - Apr 22**

Transvasive Security organization

⚠ transvasive / transvasive.github.io

Known security vulnerabilities detected

Dependency	Version	Upgrade to
`nokogiri`	`< 1.18.8`	`~> 1.18.8`

Defined in
`Gemfile.lock`

Vulnerabilities
GHSA-5w6v-399v-w3cc Low severity

Security Differently organization

⚠ security-differently / security-differently.github.io

Known security vulnerabilities detected

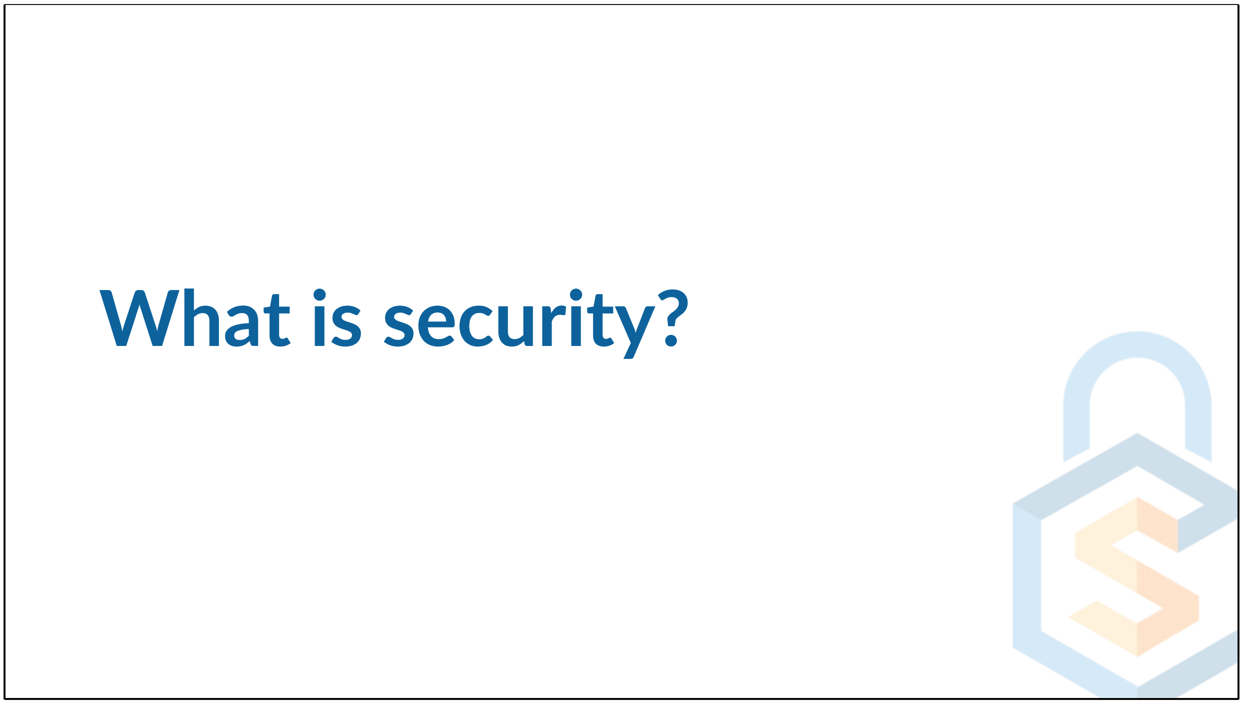
Dependency	Version	Upgrade to
`nokogiri`	`< 1.18.8`	`~> 1.18.8`

Defined in
`Gemfile.lock`

Vulnerabilities
GHSA-5w6v-399v-w3cc Low severity

What's interesting about this?

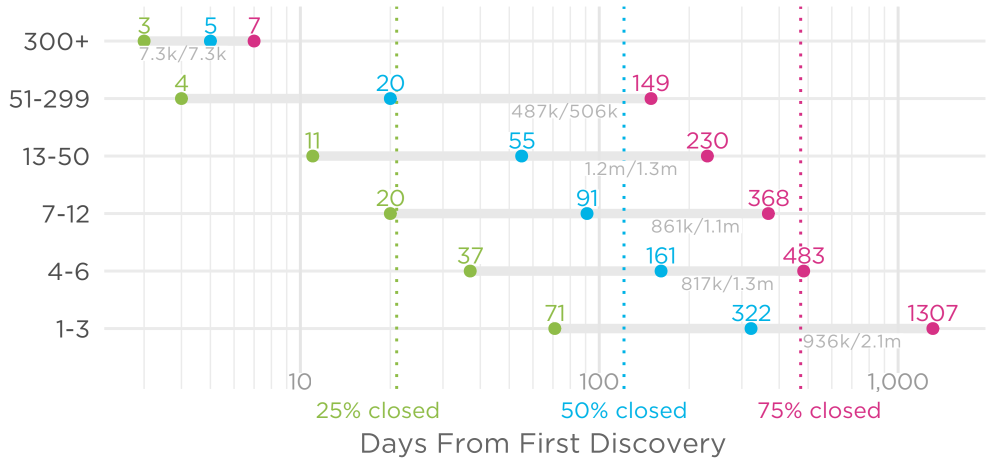
1. What's missing – information-safety.org , as I made a content update earlier in the day, and as a matter of course, updated all dependencies ("bundle update") [update frequency]
2. What's on the list? nokogiri, which is a PITA for security issues (it often shows up in my dependabot report)
3. Context? None of this really matters, since it's a component of my static site builder (Jekyll), where I control the input [attack surface]. My personal site, jbenninghoff.com will never trigger dependabot since the site has no code (built by Hugo).



What is security?

This is a question I’ve contemplated throughout my career.

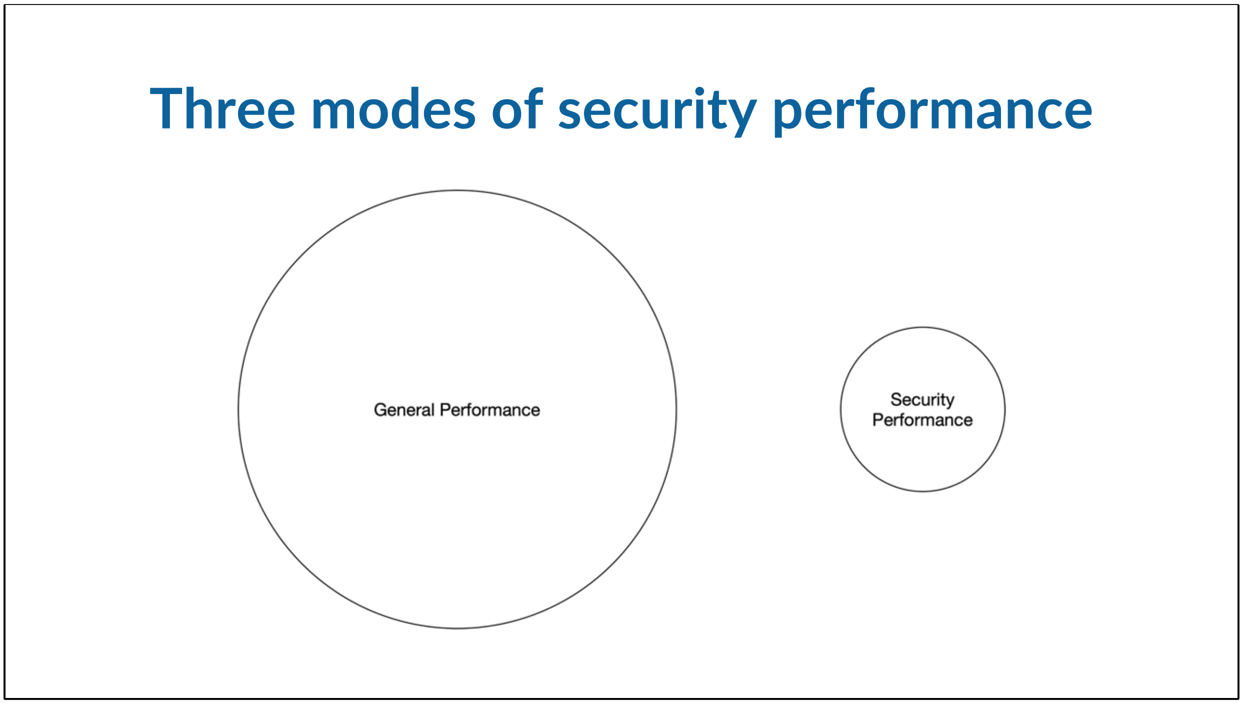
FIGURE 44: EFFECT OF SCAN FREQUENCY ON FLAW PERSISTENCE INTERVALS



Source: Veracode SOSS Volume 9

In 2019, Veracode and Cyentia published the State of Software Security Volume 9. This is the most significant finding from that report (the "wow" plot) – organizations that scan 300 or more times per year fix security bugs orders of magnitude faster.

Figure used with permission.
Veracode. (2019). State of Software Security Volume 9.
https://www.veracode.com/sites/default/files/pdf/resources/ipapers/state-of-software-security-volume-9/index.html



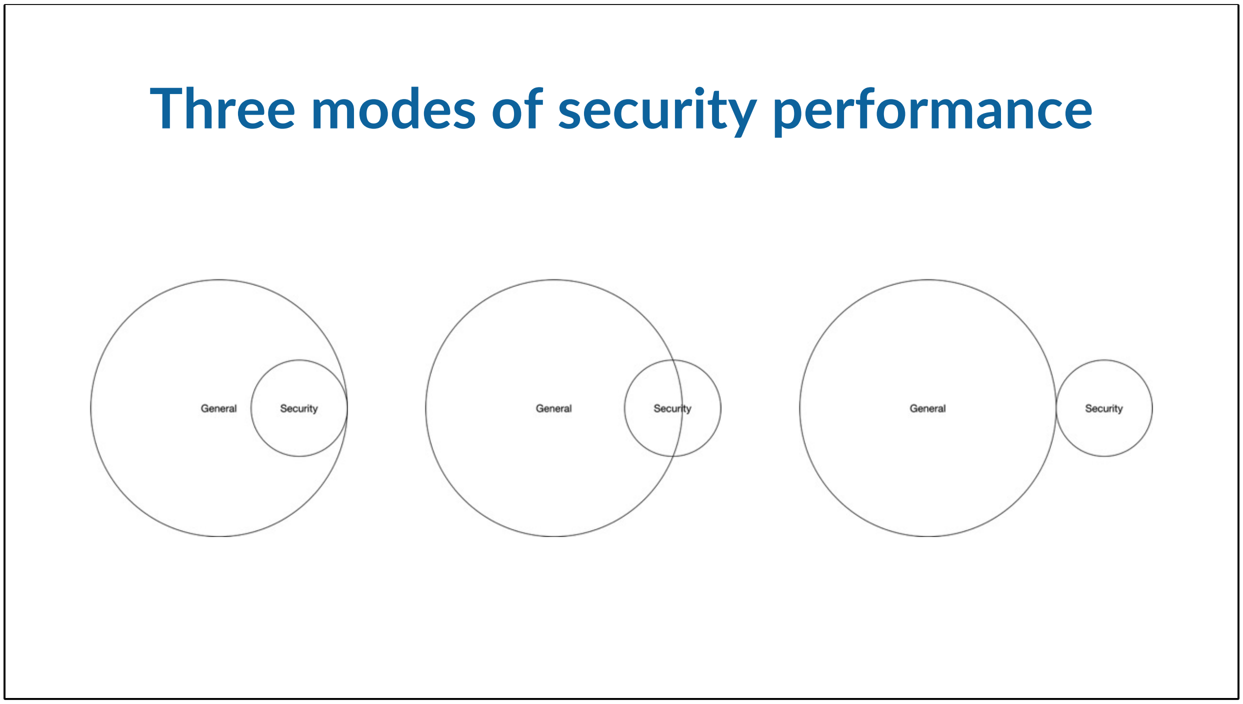
Three modes of security performance

General Performance

Security Performance

Safety taught me that security can’t be defined by the absence of breaches; it must be defined as working securely.

The model is an attempt to explain the relationship between general performance on technology activities, and provide insights to improving performance (and thus working securely)
The size of the circles are deliberate; security activities are small by comparison to everything else
How does security fit in with the larger picture? A small part of a larger team.



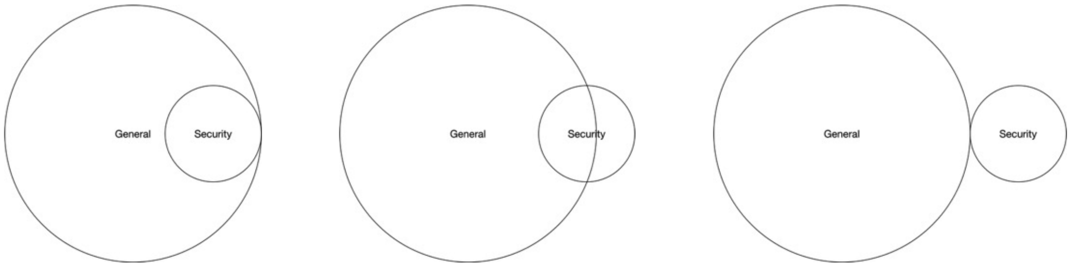
Three modes of security performance

Mode 1: Security is entirely contained within general performance <- our focus is here, I believe this helps the most

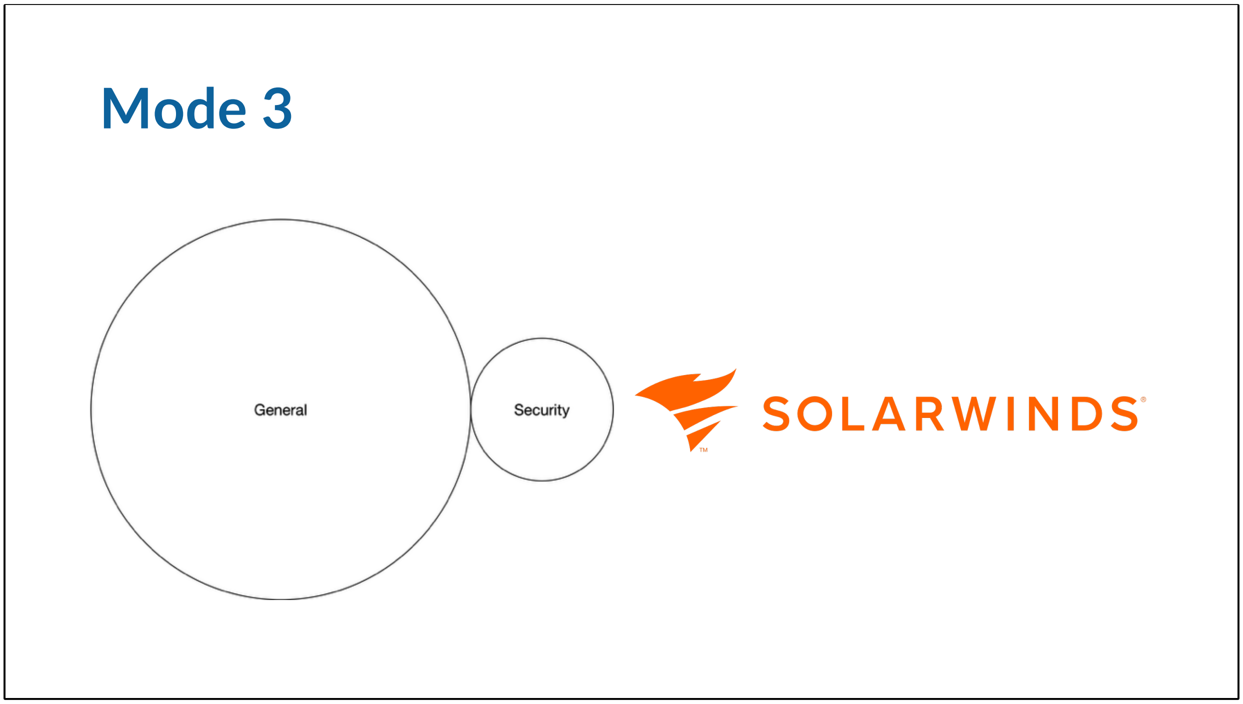
Mode 2: Security is partly outside of general performance

Mode 3: Security is entirely outside of general performance

Mode 1 ⇦ Mode 2 ⇦ Mode 3



Over time, performance transitions from mode 3 to mode 2 to mode 1 (really, general performance grows and absorbs security)

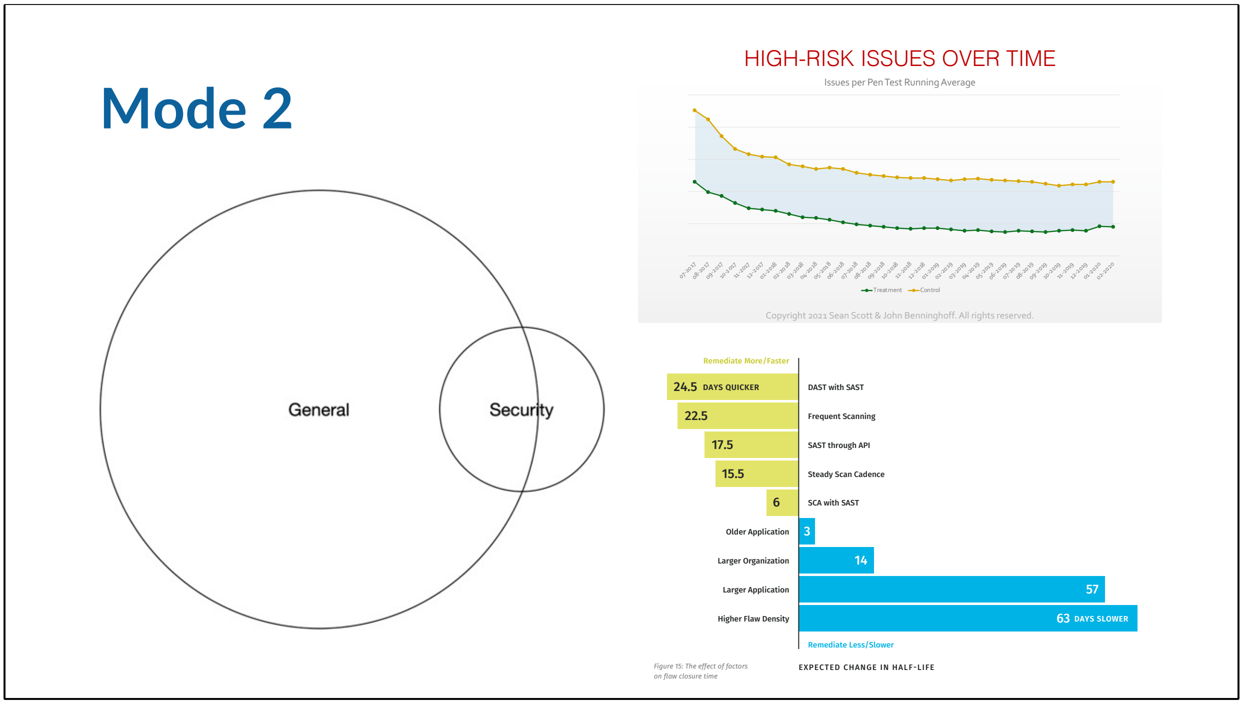


Mode 3

Rely on experts to build new defenses.

Example: supply chain attacks – a likely government-backed group hacked SolarWinds in 2020 and modified their software, which was downloaded and installed by US Government agencies as part of normal updates. This was a novel attack for which general technology performance offered no defense.

https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach
Image: https://commons.wikimedia.org/wiki/File:Official_SolarWinds_Logo.svg



Mode 2

Copyright 2021 Sean Scott & John Benninghoff. All rights reserved.

Figure 15: The effect of factors on flaw closure time

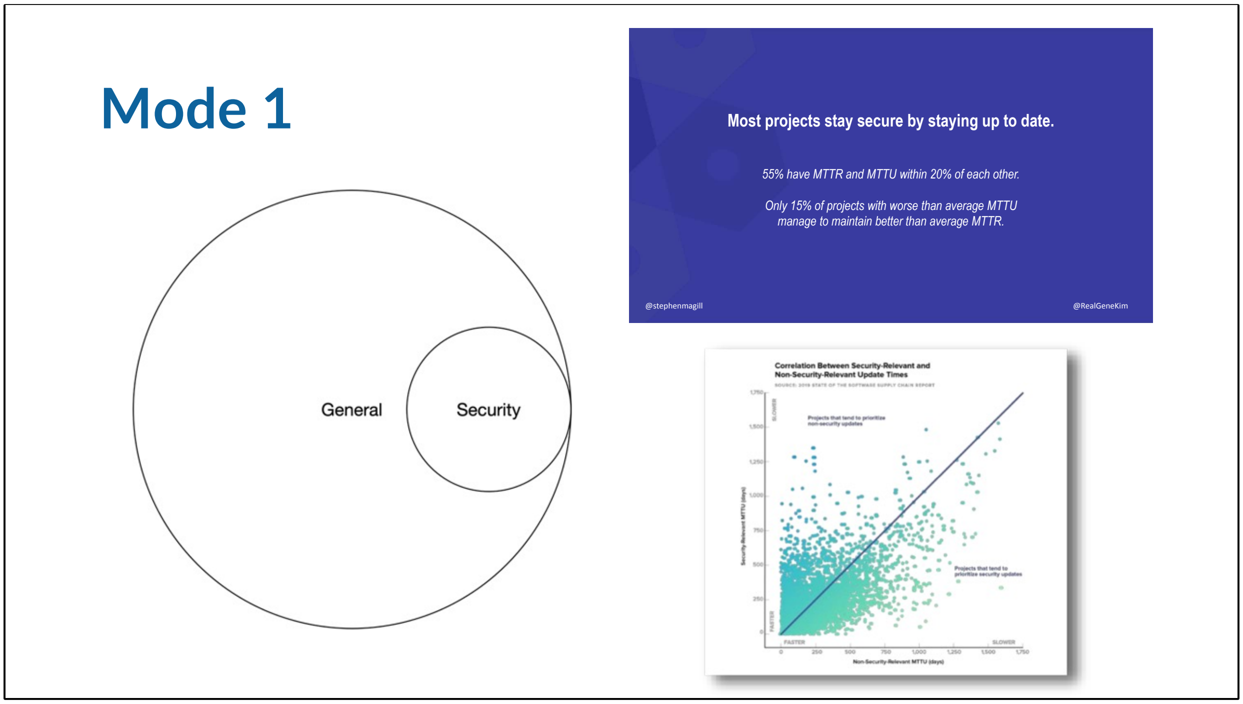
Add security enhancements to general performance.

AppSec is an example where security performance overlaps but is not contained within general performance (writing software vs writing secure software) – development teams our AppSec team worked with had a 50% reduction in new high pen-test findings.
A later Veracode/Cyentia study found that regular automated testing reduced the time to fix vulnerabilities.

References:

Scott, S. (2021). Secure Coding in Large Enterprises: Does Application Security Coaching, Training, and Consulting Increase a Development Team's Ability to Deliver Secure Code. University of Missouri-St Louis. Talk: https://www.information-safety.org/2024/05/22/measuring-security-effectiveness/
Veracode. (2020). State of Software Security Volume 11. https://info.veracode.com/report-state-of-software-security-volume-11.html

Images: Scott (2021) (top), Veracode (2020) (bottom)



Mode 1

Most projects stay secure by staying up to date.

55% have MTTR and MTTU within 20% of each other.

Only 15% of projects with worse than average MTTU manage to maintain better than average MTTR.

@stephenmagill

@RealGeneKim

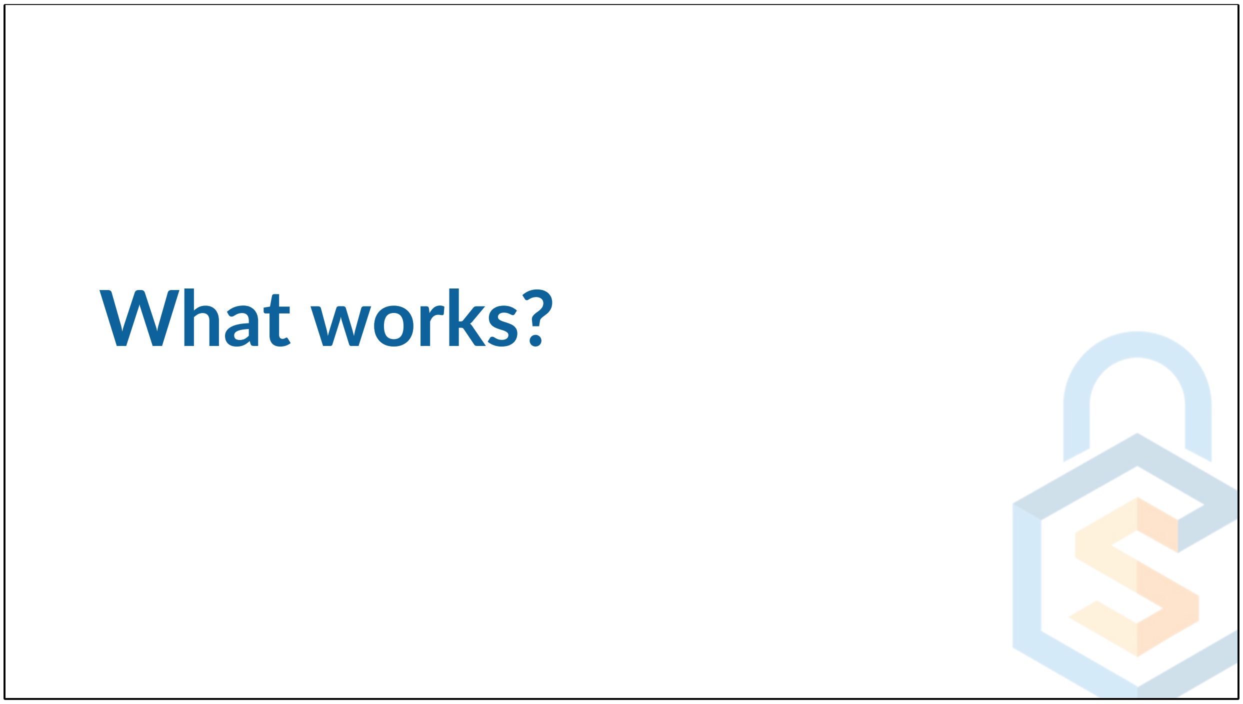
Correlation Between Security-Relevant and Non-Security-Relevant Update Times

SOURCE: 2019 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT

Improve general performance.

Gene Kim work with Stephen Magill: Java dependencies in Maven ecosystem, security is achieved through staying up to date – not a separate or security specific activity!
2021 Security Outcomes (Cyentia/Cisco): the biggest factor in reported security program success: proactive refresh of technology.
Earlier work on the correlation between SSL/TLS vulnerabilities (which reflected **maintenance**) and likelihood of breach.

References:
The 2021 Security Outcomes Study. (2020). Cisco, YouGov, Cyentia. https://www.cisco.com/c/en/us/products/security/security-outcomes-study.html
Magill, S., & Kim, G. (2019). A data-driven look at practices behind exemplar open source projects. https://www.youtube.com/watch?v=YoWkuFzEYFs
sonatype, galois, & IT Revolution. (2019). 2019 State of the Software Supply Chain. https://www.sonatype.com/en-us/2019ssc
Images: Magill, S., & Kim, G. (2019)



What works?

What works in security? For a long time, we were only guessing, but we've started to get enough data (publicly reported breaches and insurance claims) to answer that question.

- Reduce attack surface
- Patch and update faster
- Use multi-factor authentication

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2024.2335461

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Evidence-based cybersecurity policy? A meta-review of security control effectiveness

Daniel W. Woods[a,b] and Sezaneh Seymour[b]

[a]School of Informatics, University of Edinburgh, Edinburgh, United Kingdom; [b]Coalition Inc., San Francisco, United States of America

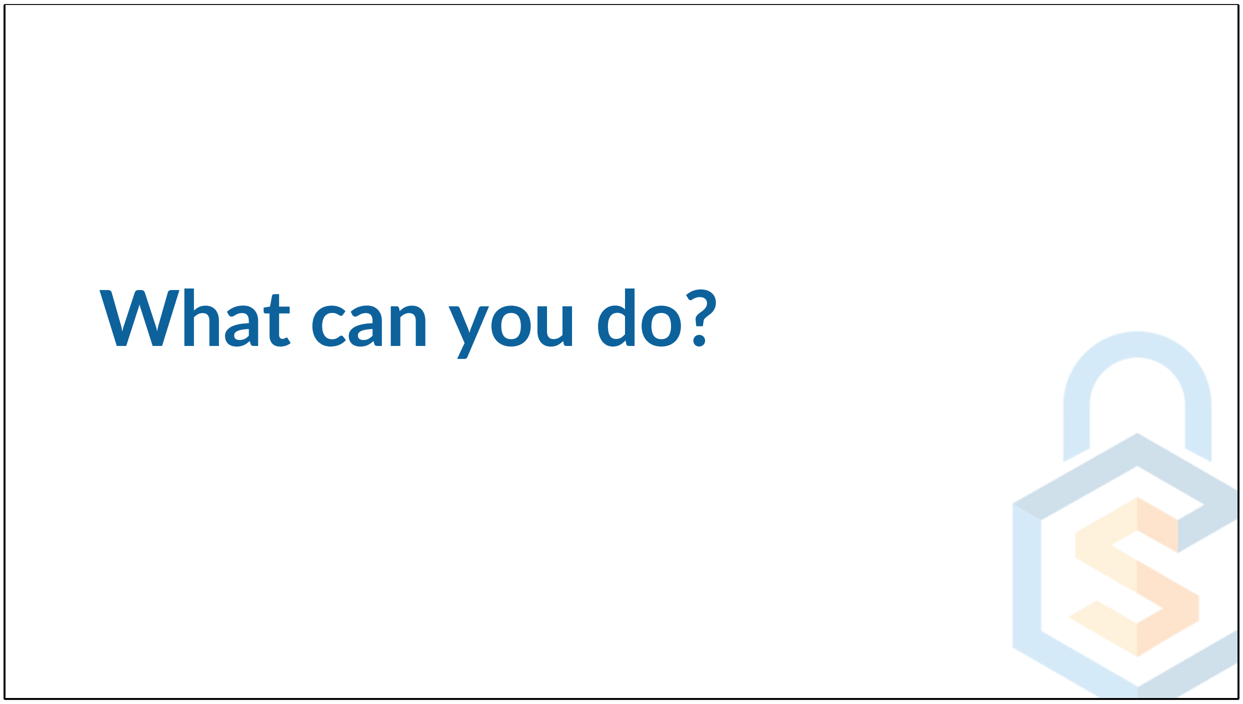
ABSTRACT
Cybersecurity policy should guide firms towards implementing the most effective security controls and procedures. However, there is no authority that collects evidence and ranks cybersecurity controls by efficacy. The evidence needed by policymakers is distributed across academic studies and industry white papers. To address this gap, we conduct a meta-review of studies that empirically evaluate the efficacy of cybersecurity interventions. Attack surface management and patch cadence were consistently the first and second most effective interventions. Reduced cyber

ARTICLE HISTORY
Received 4 August 2023
Revised 30 November 2023
Accepted 19 January 2024

KEYWORDS
Cybersecurity policy; science of cybersecurity; security controls; meta-review; evidence-based policy

A paper published in 2024 suggests an answer – the three most effective ways of improving security are: 1. reducing attack surface, 2. patching faster, and 3. *fully* implementing MFA. These are all (mostly) Mode 1 activities –measures of organizational effectiveness, driven primarily by operations, infrastructure and development, not security.

Paper: https://doi.org/10.1080/23738871.2024.2335461



What can you do?

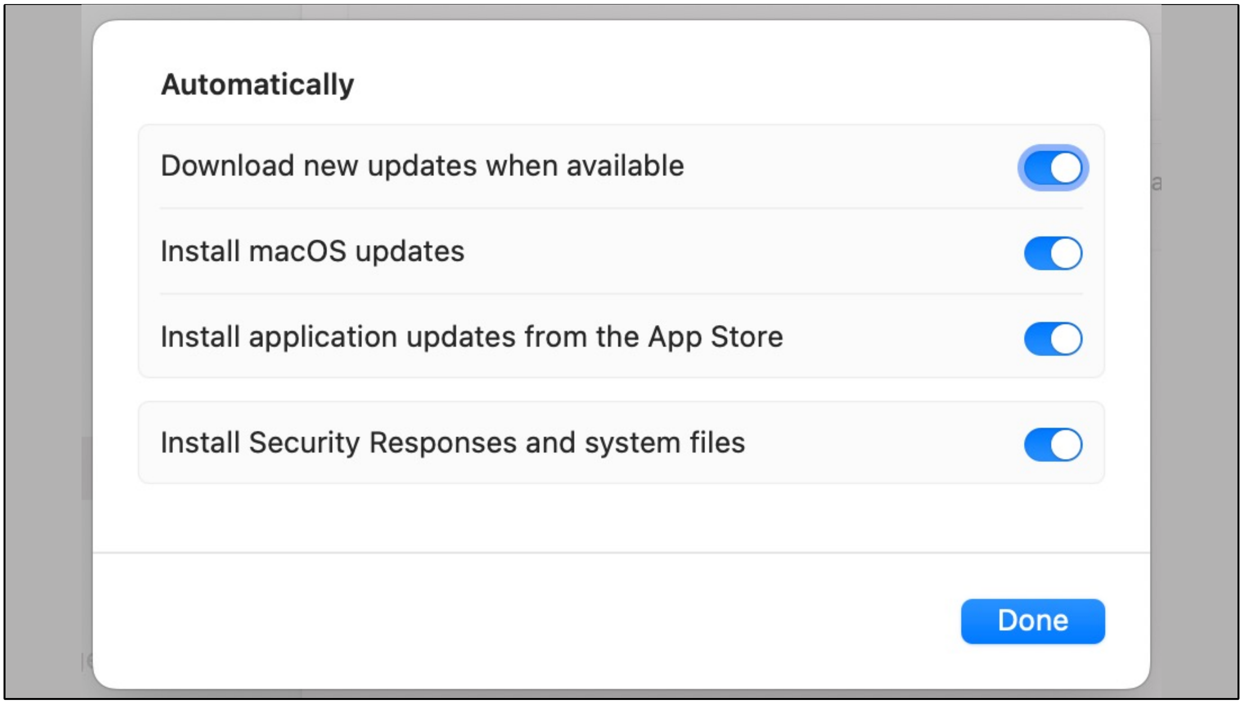
If you’re not a cybersecurity expert, what can you do?

Stop using Windows.

Reduce attack surface by choosing devices with stronger built-in security: iPhone/iPad > Android/Chromebook > macOS > Linux > Windows (my grounded opinion). Always use curated lists to install software: App Stores, package managers (Homebrew, apt-get, Chocolatey, npm, pypi, maven, rubygems).

Choose higher quality services (SaaS and otherwise). Don’t install what you don’t need/use.

Photo: https://commons.wikimedia.org/wiki/File:IPad_with_Magic_Keyboard_(51013601847).jpg



Automatically

Download new updates when available: on

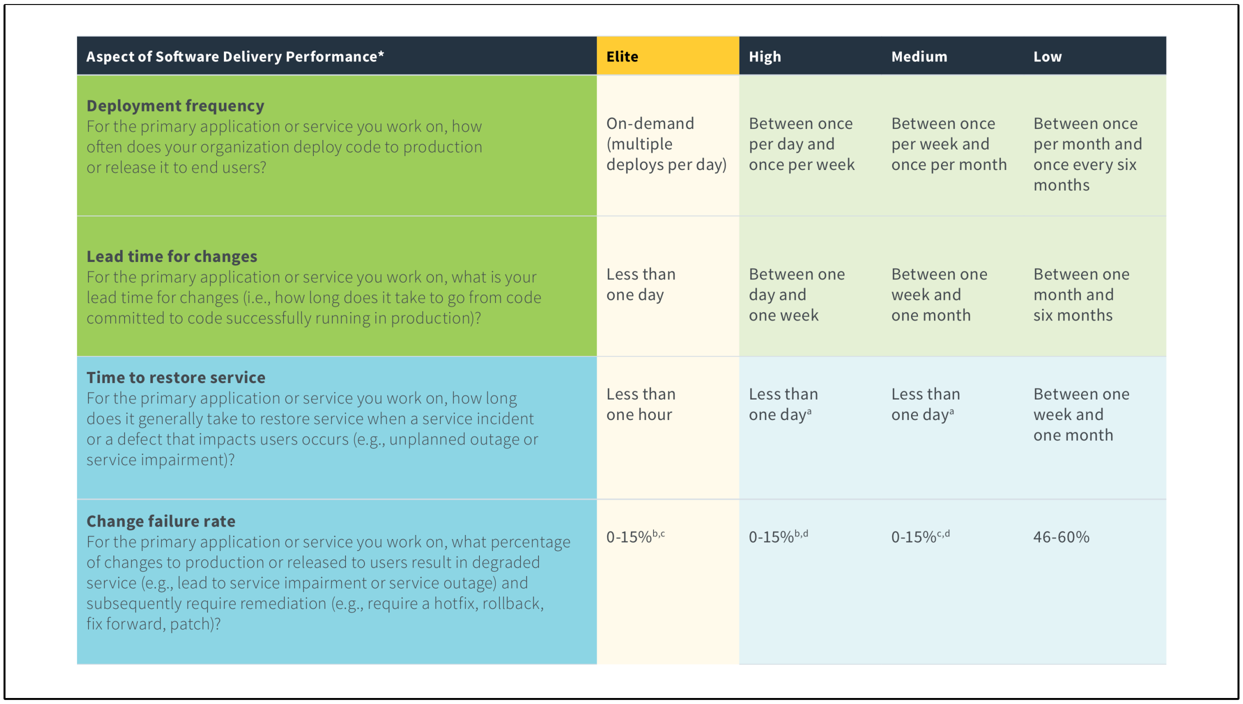
Install macOS updates: on

Install application updates from the App Store: on

Install Security Responses and system files: on

Auto-update everything.

Regularly update all installed software – OS, applications, and packages installed with package managers.

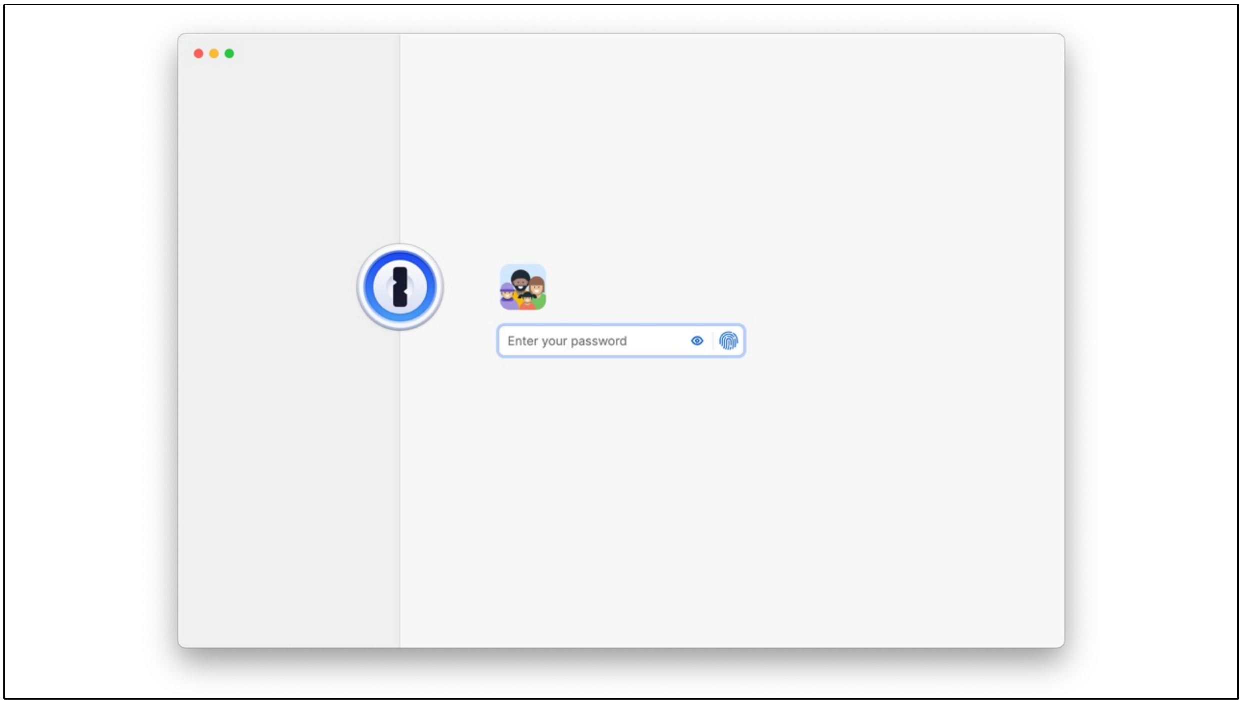


Aspect of Software Delivery Performance*	Elite	High	Medium	Low
Deployment frequency For the primary application or service you work on, how often does your organization deploy code to production or release it to end users?	On-demand (multiple deploys per day)	Between once per day and once per week	Between once per week and once per month	Between once per month and once every six months
Lead time for changes For the primary application or service you work on, what is your lead time for changes (i.e., how long does it take to go from code committed to code successfully running in production)?	Less than one day	Between one day and one week	Between one week and one month	Between one month and six months
Time to restore service For the primary application or service you work on, how long does it generally take to restore service when a service incident or a defect that impacts users occurs (e.g., unplanned outage or service impairment)?	Less than one hour	Less than one day[a]	Less than one day[a]	Between one week and one month
Change failure rate For the primary application or service you work on, what percentage of changes to production or released to users result in degraded service (e.g., lead to service impairment or service outage) and subsequently require remediation (e.g., require a hotfix, rollback, fix forward, patch)?	0-15%[b,c]	0-15%[b,d]	0-15%[c,d]	46-60%

DevOps.

This also applies to software development – practice "maintenance first" and update dependencies before starting software development. Adopt DevOps capabilities to improve your performance, which will improve security.

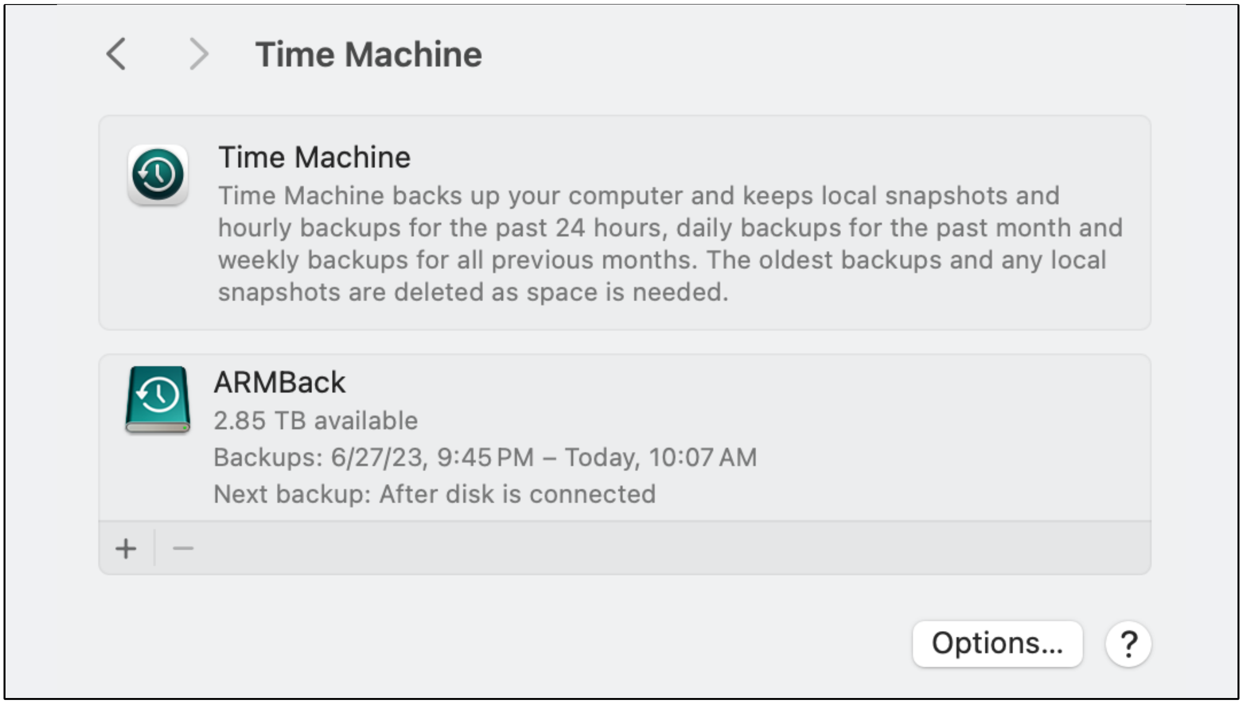
Forsgren, N., Smith, D., Humble, J., & Frazelle, J. (2019). 2019 Accelerate State of DevOps Report. DORA & Google Cloud. https://research.google/pubs/pub48455/
https://dora.dev



Use a dedicated password manager, like 1Password.

Safest ways to authenticate? Passkeys > MFA (app-based) > MFA (SMS-based) > Passwords. Password managers help significantly by generating unique random passwords per-site, inform you when MFA or Passkeys are available, and when your password should be changed due to compromise. A bridge until we can sort out the Passkey platform lock-in problem…

https://fidoalliance.org/passkeys/
https://www.consumerreports.org/electronics-computers/password-managers/best-password-managers-review-digital-security-privacy-ease-of-use-a7337649384/



Time Machine

Time Machine backs up your computer and keeps local snapshots and hourly backups for the past 24 hours, daily backups for the past month and weekly backups for all previous months. The oldest backups and any local snapshots are deleted as space is needed.

ARMBack

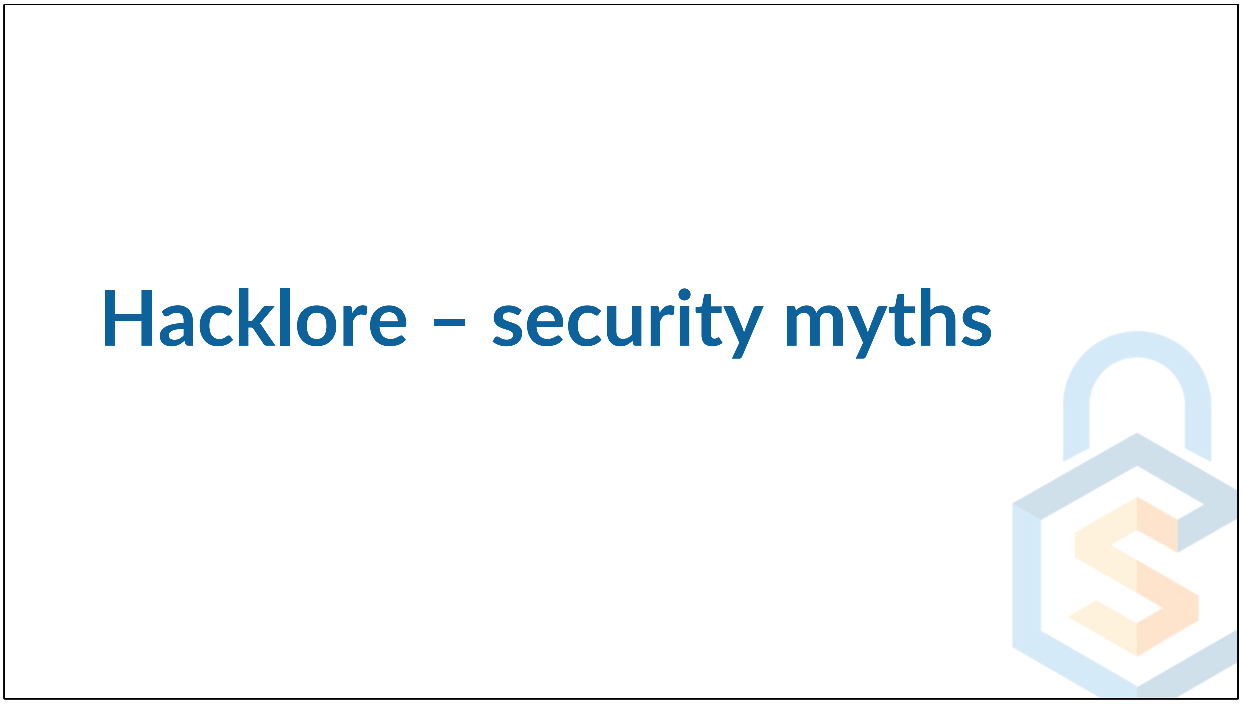
2.85 TB available

Backups: 6/27/23, 9:45 PM – Today, 10:07 AM

Next backup: After disk is connected

Backups.

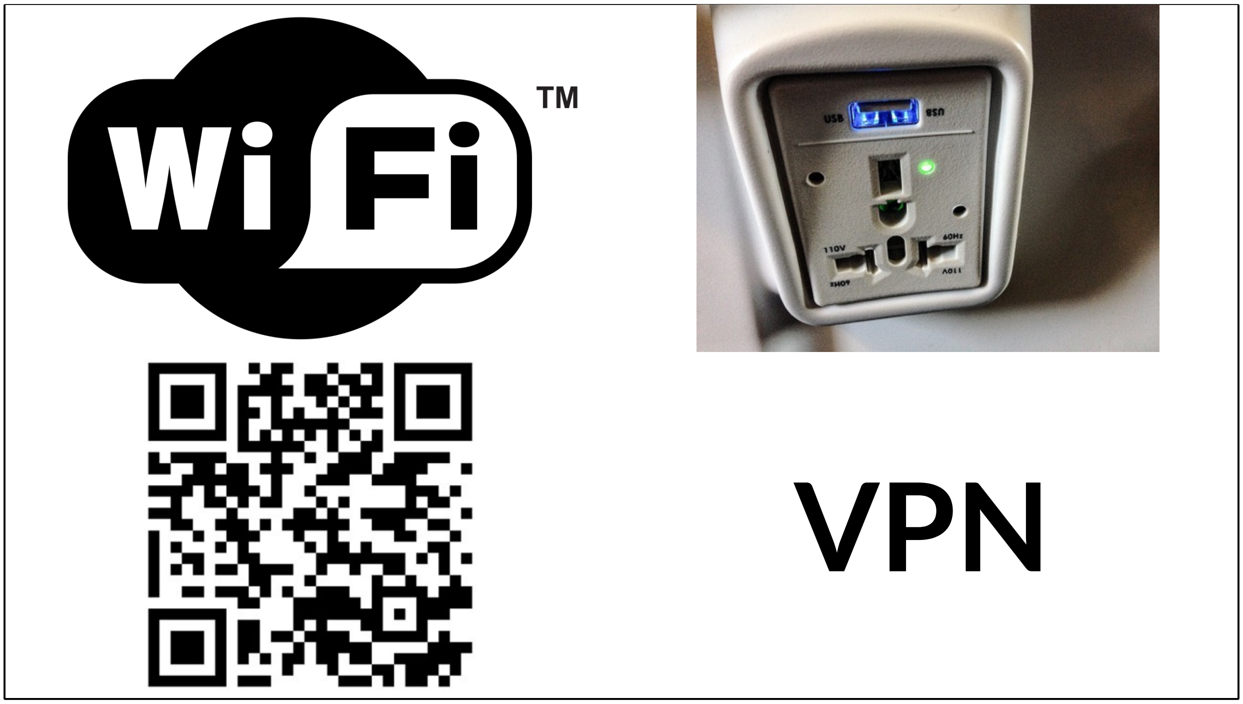
Regularly backing up your data and systems, and periodically testing a restoration provides resilience: the ability to recover from both known and unknown adverse events. Use backup software; cloud sync (Google Drive) doesn't count. Needs to run automatically, test restoration.



Hacklore – security myths

Bob Lord coined the term ”Hacklore” to describe persistent (and harmful) security myths – harmful because they distract from what’s really important.

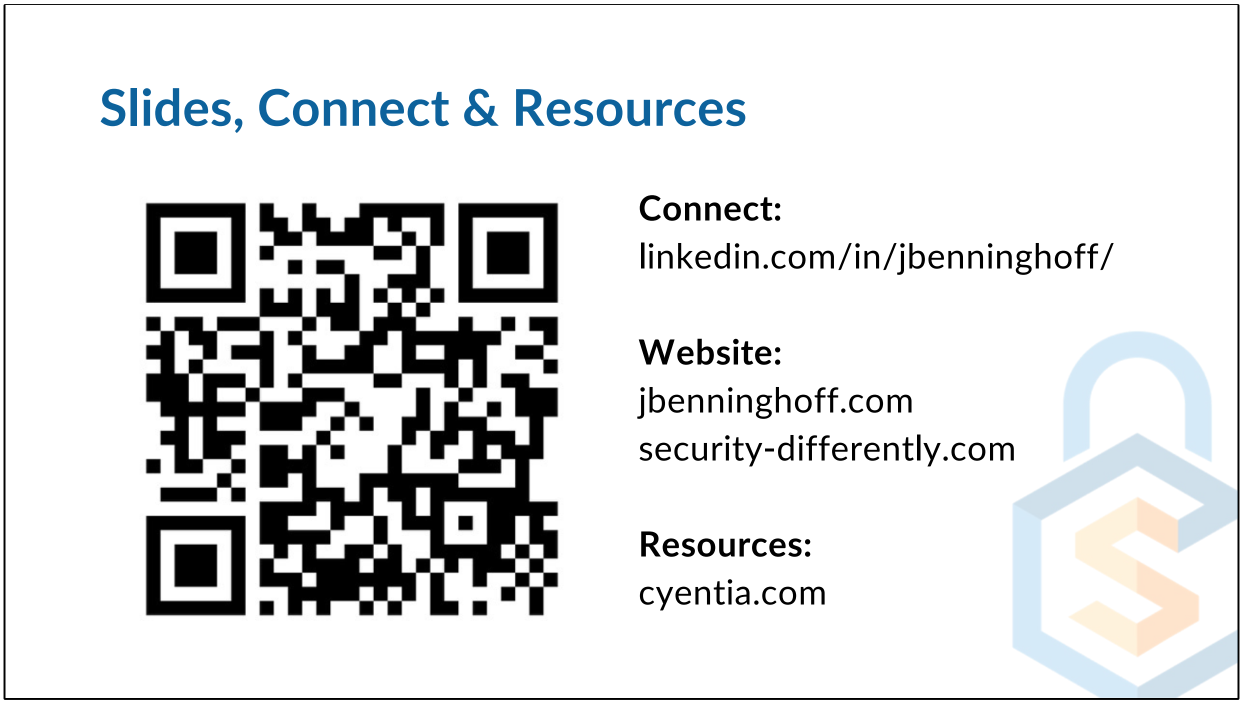
Articles:
https://www.linkedin.com/posts/lordbob_i-frequently-speak-out-against-what-i-call-activity-7165122311371653120-S4Mh/
https://medium.com/@boblord/cybersecurity-hacklore-8a5be4e8fa3e
https://medium.com/@boblord/attack-of-the-evil-baristas-b204436f0853
https://chrisbt.me/posts/hacklore-wifi/



VPN

“Don’t use public wifi”, “Don’t use public USB chargers”, “Don’t scan QR codes”, “Use a VPN”

Photos:
https://commons.wikimedia.org/wiki/File:WiFi_Logo.svg
https://commons.wikimedia.org/wiki/File:Alaska_Airlines_International_Power_Outlets.jpg



Slides, Connect & Resources

Connect:
linkedin.com/in/jbenninghoff/

Website:
jbenninghoff.com
security-differently.com

Resources:
cyentia.com

Scan the QR code for slides and more! Questions?