To Resiliency and Beyond!
How to engineer survivable systems
Today’s Map

- Status Quo Problem
- Security vs Quality
- DevSecOps Gaps
- Tactics
- Resiliency Playbook
About Me

[Image of a laptop, a padlock, and a ship with a formula] =

Matt Wiseman
Cybersecurity Engineer
at Fathom5
About the Maritime Domain
Has the status quo failed to protect critical systems?
Automation Support for Security Control Assessments

“predefined control sets have been applied to provide detailed technical requirements without documenting traceability of control items to more general requirements”

“many security programs have focused on the individual controls as a compliance checklist, with little consideration given to how the controls work together”
"The best projects today perform activities like threat modeling, security architecture, secure coding training, and security testing. However, it's generally unclear how these activities connect back to the business goals."

"Frequently these activities simply report vulnerabilities or risks that do not become part of any sort of coherent security strategy. In fact, most of these efforts create no lasting value, and are simply repeated from scratch after some period of time."

https://ruggedsoftware.org/
Is security a “functional” or “non-functional” requirement?
First, Some Definitions

Functional
▪ Unit of work
▪ What a thing does

Non-functional
▪ Measure of performance
▪ How well a thing works
Quality is Non-Functional

▪ Reliability
▪ Maintainability
▪ Usability

▪ Availability
▪ Portability
▪ “other –ilities…”

What about Security?
Security is Non-Functional

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-Repudiation
BUT WAIT

THERES MORE

This Photo by Unknown Author is licensed under CC BY-BA-NC
Security is Functional

- Cryptography
- Secrets Management
- Mutual Authentication
- Logging
- Auditing
- Intrusion Prevention
- ...
TO RESILIENCY AND BEYOND!

SECURITY ENGINEERING

CAPABILITY / FEATURE DEVELOPMENT

TEST / QA / RISK MGMT

https://www.flickr.com/photos/thisisrorydean/8000230363/
What does this say about our current approach to DevSecOps?
Today’s Best Practices

- SAST
- DAST
- SCA
- SBOMs
- Image Scanning
- Pen Testing

This is a non-functional approach to security! Security Engineering needs to go beyond the testing!
Recommendations for resiliency
“What functions do I need to engineer into my system to protect, detect, respond, and recover from cyber events?”

- Threat Modeling starts providing answers…

https://owasp.org/www-community/Threat_Modeling_Process
NISTIR 8011

“The four abstraction layers support integrated systems engineering by making the desired results of a security program clear and measurable at a concrete level. This, in turn, makes the results more understandable to non-security experts and thereby easier to link to desired business/mission results.”

1) Attack Step Layer
2) Functional Capability Layer
3) Sub-Capability Layer
4) Control Item Layer
Rugged Software

“rugged describes staying ahead of the threat over time. Rugged organizations create secure code as a byproduct of their culture. You are rugged because you run the gauntlet, instrument your organization and your code, constantly experiment to see if anything breaks, and survive the process of hardening yourself through real-world experience. Rugged organizations produce rugged code designed to withstand not just today’s threat, but future challenges as well.”
Nat’l Cyber Strat

“We will complement our efforts to out-innovate other countries with focused, coordinated action to optimize critical and emerging technologies for cybersecurity as they are developed and deployed. We will ensure that resilience is not a discretionary element of new technical capabilities but a commercially viable element of the innovation and deployment process.”

How do we operationalize this?
Our Cyber Resiliency Playbook

- Phase 1: Release the CVEs!
- Phase 2: Speed-Run MVS!
- Phase 3+: Malicious BDD ‘til Infinity!
We start by surfacing the known vulnerabilities and weaknesses, giving us the opportunity to kill risk at the source

✓ SAST
✓ DAST
✓ Image Scanning
✓ SBOM Generation + Scanning
✓ CVSS x EPSS x SSVC for a Risk-Based Approach to Vulnerability Triage

(1) Release the CVEs!
(2) Speed-Run Min Viable Security!

We prioritize the top 20% of functional specifications that buy down 80% of the attack surface, and deploy to prod

- Secure-by-Design/Default (per CISA)
- Pass Compliance Muster (can’t deploy an MVP otherwise)

https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

(3) Malicious BDD ‘til Infinity!

We put on our white hats to stress test system performance under malicious activity, and continuously engineer improvements

✓ System Modeling and Criticality Analysis
✓ Threat Modeling with Malicious Behavior Statements
✓ White Box Software Penetration Testing
✓ Engineer Protection, Detection, Response, and Recovery Capabilities
✓ Re-Test & Repeat

https://upload.wikimedia.org/wikipedia/en/e/e1/93tilinfinity.jpg
Summary

- Security needs to connect back to key mission outcomes to yield lasting value
- Security Engineering is both functional and non-functional
- DevSecOps culture is key to implementing it
- The more we break and fix, the higher our system resiliency can become with each new release
- We can demonstrate **clear measurable improvement in mission performance** from cybersecurity investments
Questions? Interested? Contact Me

Matt Wiseman
cyber@fathom5.co