BUILDING SECURE PRODUCTS FOR STARTUPS

EMBRACING THE ODDS

#WHOAMI

- Hacking since 1998
- System administration & telco infrastructure background
- Security roles include penetration testing, operations, security engineering, security product management. Focused on Governance, Risk and Compliance since 2012. Independent consultant for Startups, UK Gov and Healthcare
- Strategy Advisor @ Practical DevSecOps and Head of Infosec @ CloudMargin
- Course creator “DevSecOps for Leaders” and trainer at OWASP AppSec days on “Compliance at the speed of DevOps“
- Speaker and Blogger (https://www.securitydifferently.com) on Security Strategy, Wardley Mapping, Cynefin framework, Safety & Resilience Engineering, Social Practice theory and other random nerdy stuff

THE PROBLEM - WHAT ARE THE ODDS ?

- Most organisations have a 1:100 ratio between Security staff and Engineers
- This **disproportionately** affects Startups
- Effective security requires a multitude of skills that few individuals will have (and the ones who do are likely expensive):
  - Deep technical understanding
  - Communication and persuasion
  - Balancing skills (with Engineers and Senior Management)

https://medium.com/itrevolution/1-in-100-how-to-design-teams-to-bridge-the-security-gap-985f17ebb5cc

"MY OBSERVATIONS ARE THAT IT CAN BE HARMFUL TO INTRODUCE DEDICATED SECURITY EMPLOYEES TOO EARLY AT A STARTUP. THIS INTRODUCTION OF A SPECIALIZED ROLE TO SOLVE A HORIZONTAL PROBLEM WILL OFTEN CAUSE EARLY FRAGMENTATION AND ORGANIZATIONAL DEBTS.
INSTEAD, STARTUPS DO BETTER OFF GETTING SHORT TERM GUIDANCE FROM EXTERNAL EXPERTISE AND TASKING EXISTING ENGINEERING TALENT WITH SECURITY PROJECTS."

Ryan McGeehan

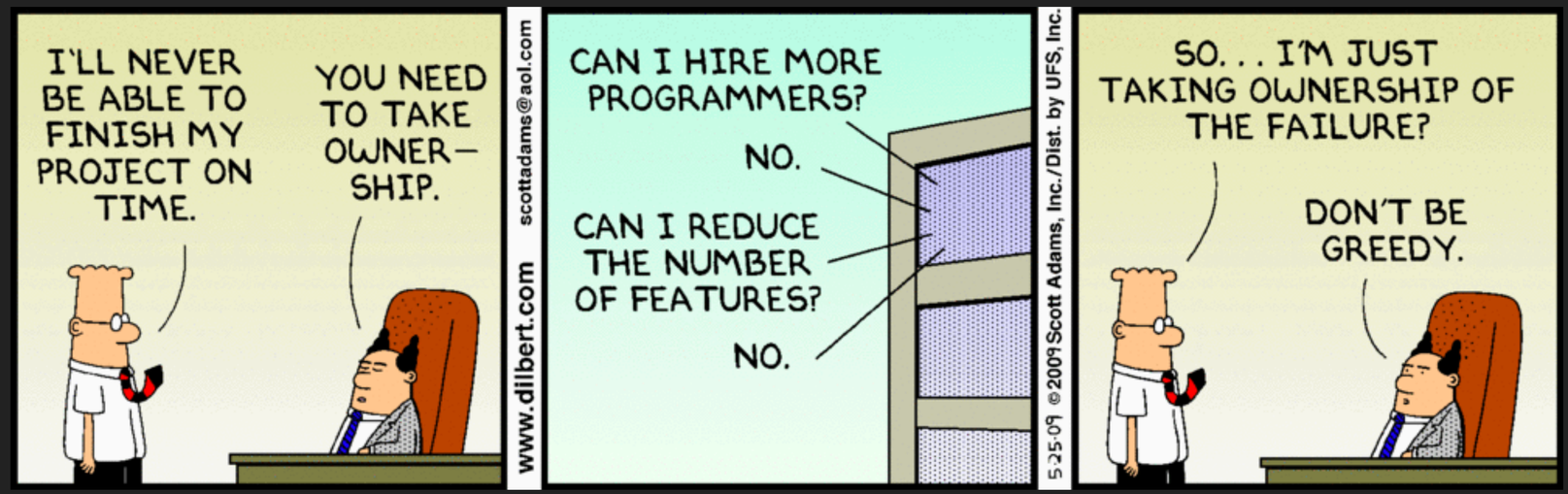
https://medium.com/starting-up-security/you-dont-need-a-chief-security-officer-3f8d1a76b924

SECURITY EXPERTS ARE USEFUL IN IDENTIFYING RISKS AND PRIORITIZING MITIGATIONS. THESE SKILLS ARE NOT NEEDED TO POINT OUT THE EARLIEST DEFENSES AT MOST COMPANIES. IF BROUGHT ON TOO EARLY, THIS EXPERTISE IS WASTED WHEN MOST EARLY DEFENSE WORK IS NOW VERY WELL KNOWN, EVEN AMONG NON-EXPERTS.

Ryan McGeehan

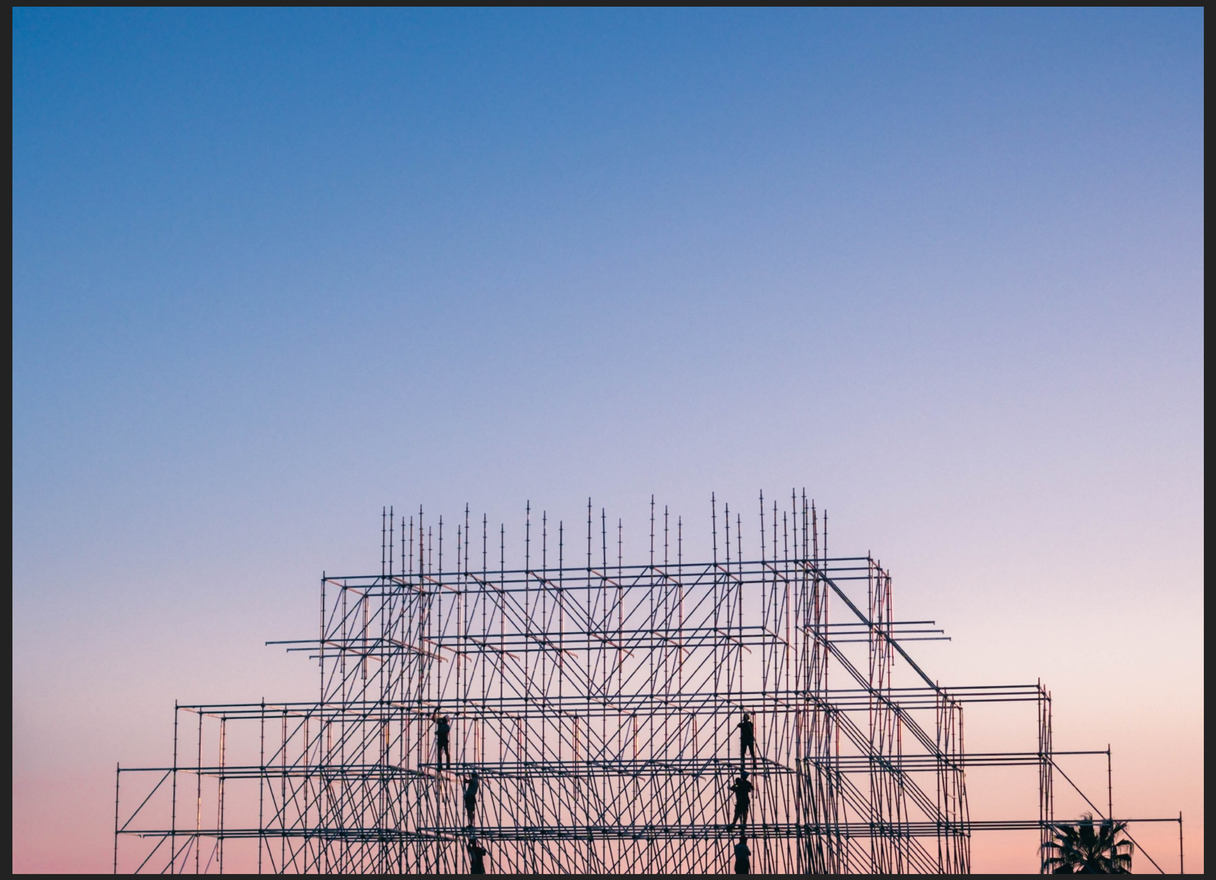
WHAT ARE THE CONSTRAINTS ?

- Expertise & Governance
  - Technical
  - Practices
  - Policies
  - Patterns & References
- Resources & Structure
  - Money
  - Attention



SCAFFOLDING

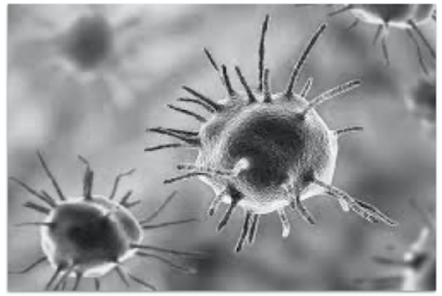
- Security is another element of **Quality Assurance**
- Managing Security is part of managing **Business Risk**
- If you fix or improve those first, you get better ROI



APPROACHING STRATEGY

Strategy analogies from Nature

Parasites	Scavengers	Apex Predator
Symbiotic/Parasite	**Hyena**	**Yosemite Wolves**



APPROACHING STRATEGY

Strategy analogies from Nature

Parasites	Scavengers	Apex Predator
Symbiotic/Parasite	**Hyena**	**Yosemite Wolves**

Energy gradient

Integrating into other's transformations

Recovering from incidents & situations

Setting own plans, compete for resources

TECHNICAL CONTROL HEURISTICS – THE 4 SECURITY THINGS

- Check your dependencies
- Protect your secrets
- Scan your code
- Harden your config

ORGANISATIONAL PRACTICES

- Risk Identification
  - Open Information Security Risk Universe (OISRU)
    - Who/What can cause a risk to materialise ? (Sources of Risk)
    - What events can occur that would cause consequences ? (Risk Events)
    - What possible harms can come from those events ? (Risk Consequences)

https://oisru.org/

Breakout Room 2

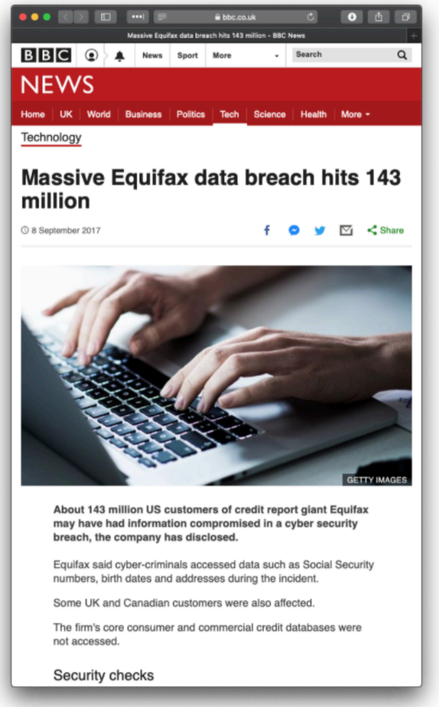
Equifax / Data breach

RISK SCENARIO:

<We hold personal information for our consumers, this may become available through the website if we have do not adequately protect our code or third party components. This may result in regulatory action/fines and reputational damage.>

The story… bbc.co.uk

- Equifax are a credit reference agency, holding large quantities of personal data
- An attacker exploited an unpatched vulnerability in Apache Struts to gain access
- Over 76 days they collated and exfiltrated information on 143 million U.S. citizens



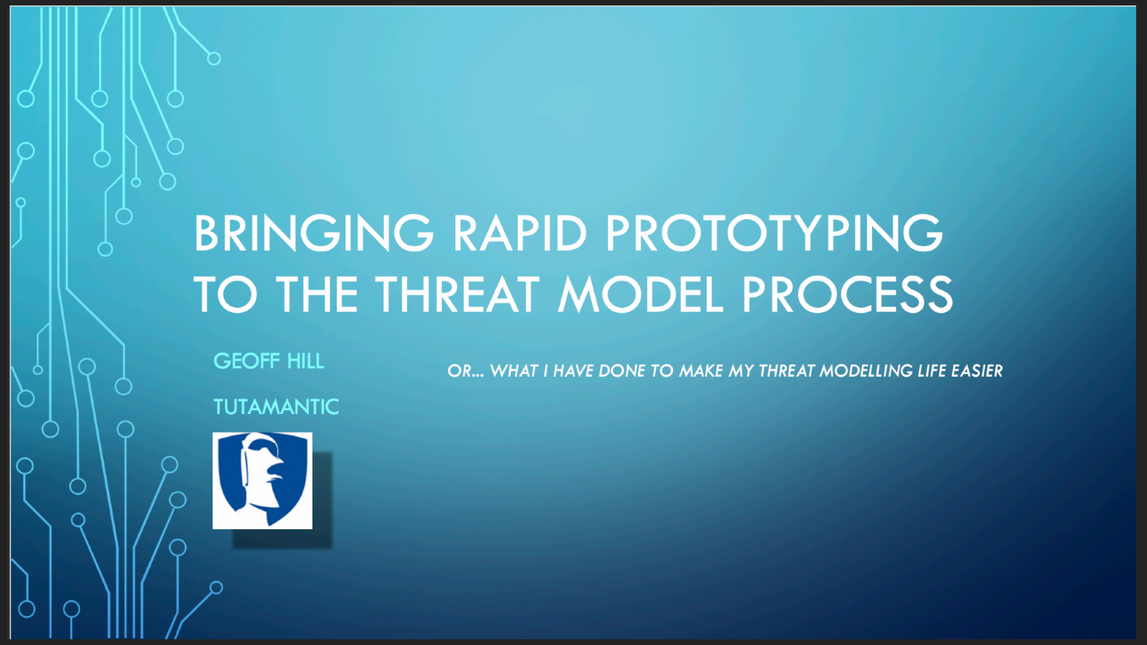
RISK STATEMENT:

SOURCE	EVENT	CONSEQUENCE
1. External Malicious (criminal) 2. Internal Non-Malicious (ineffective/accidental)	<Information Breach - Unauthorised access to the system resulting in unauthorised access to data (confidentiality and integrity)>	<Regulatory Fines, Unexpected Costs and reputational damage>

https://github.com/oracuk/oisru/blob/master/oss2020/OSS2020_-_Open_Information_Security_Risk_Universe_(OISRU).pdf

ORGANISATIONAL PRACTICES

- Threat Modelling
  - What are we building ?
  - What can go wrong ?
  - What are we going to do about it ?
  - How good a job have we done ?
    - Breadth
    - **Continuous validation**

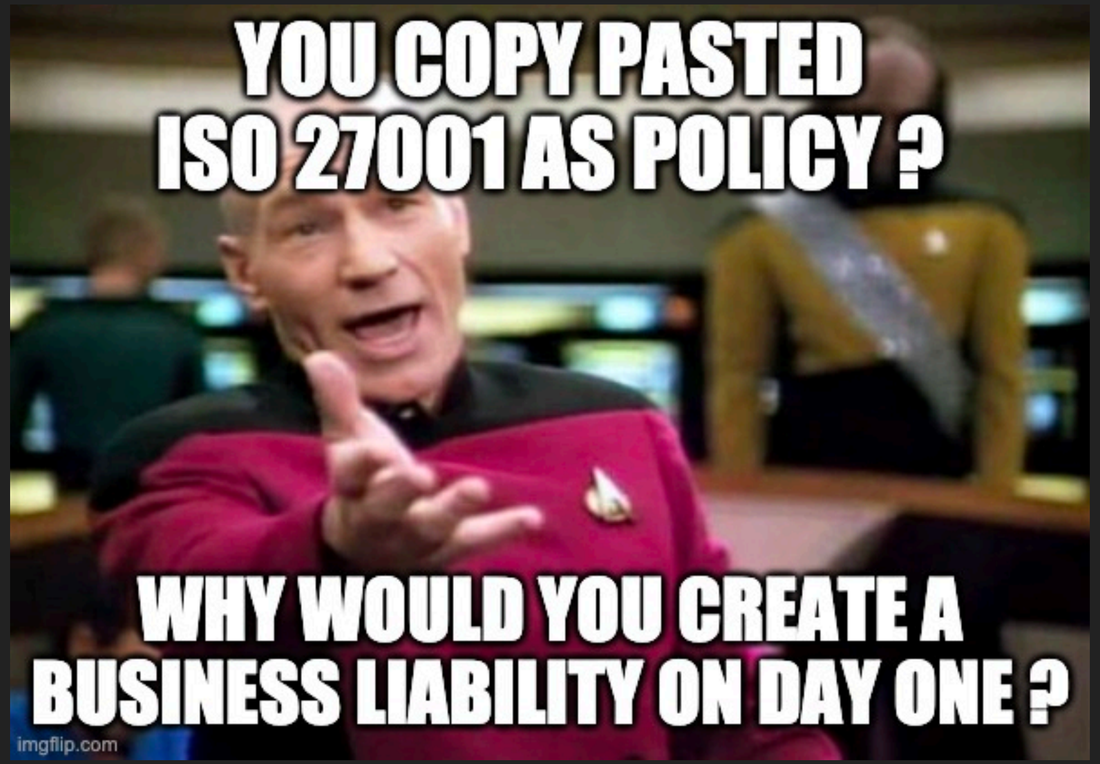


https://github.com/geoffrey-hill-tutamantic/rapid-threat-model-prototyping-docs

BEING SENSIBLE ABOUT POLICIES

- Blindness to the gap between policy and practice leads to unfunded or inappropriate commitments

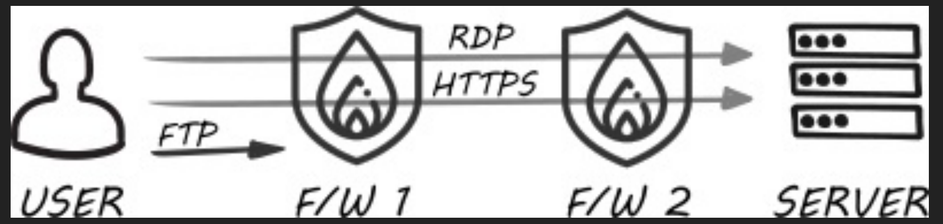
- What's the alternative ?
  - Understand front line work
  - Query your IT environment before setting policy
  - Base policy and control objectives on outcomes of risk identification and threat modelling

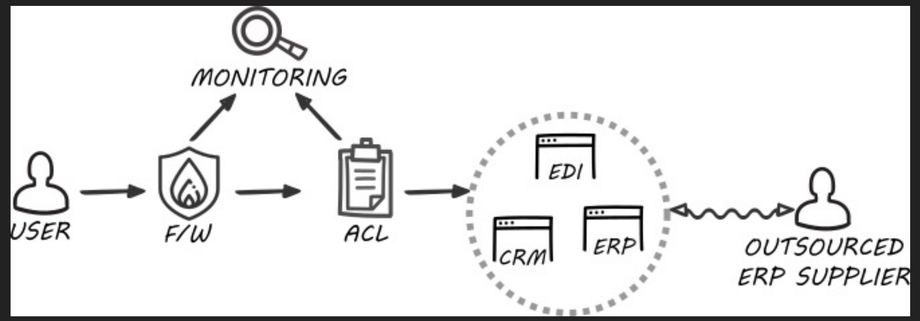


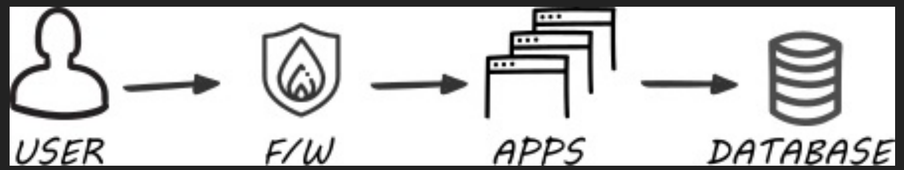
https://www.securitydifferently.com/why-your-security-policies-are-a-business-liability-and-what-to-do-about-it-f43609ba3417/

NCSC ANTI-PATTERNS

- #1 - ‘Browse-up’ for administration
- #2 - Management bypass
- #3 - Back-to-back firewalls
- #4 - Building ‘on-prem’ solution in cloud
- #5 - Uncontrolled and unobserved third party access
- #6 - The un-patchable system



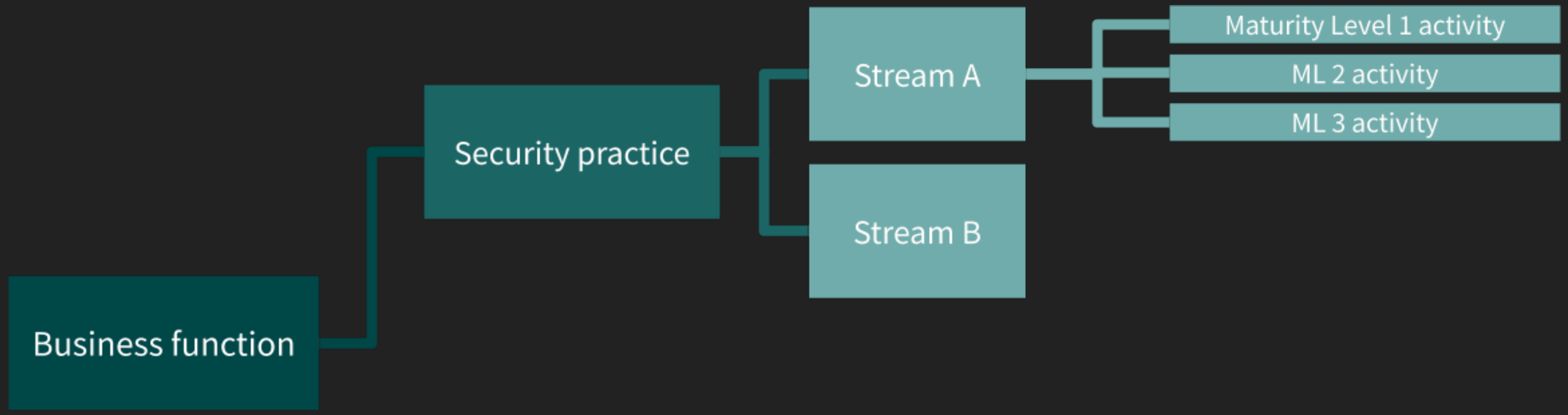




https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns

OWASP SAMM

- Software Assurance Maturity Model
  - 12 security practices
  - 5 business functions



OWASP PROACTIVE CONTROLS

- Most important control categories that all projects should meet

- C1: Define Security Requirements
- C2: Leverage Security Frameworks and Libraries
- C3: Secure Database Access
- C4: Encode and Escape Data
- C5: Validate All Inputs
- C6: Implement Digital Identity
- C7: Enforce Access Controls
- C8: Protect Data Everywhere
- C9: Implement Security Logging and Monitoring
- C10: Handle All Errors and Exceptions

OWASP ASVS

- Application Security Verification Standard
  - 14 domains
  - 3 Assurance levels
    - 1 for a defensible baseline / low assurance
    - 2 for apps containing sensitive data
    - 3 for critical apps - high value transactions, sensitive medical data, high trust

Use Case:

- As metric
- As guidance
- For procurement
- As guide for automated tests
- For training

OWASP CHEATSHEETS

- Cheatsheets
  - Dozens of them
  - Explanations & Rules
  - Code examples in multiple languages
  - Mappings to ASVS and Proactive Controls

MONEY CONSTRAINT ? LEVERAGE OPEN-SOURCE & CLOUD NATIVE

Security Thing	Application	Infrastructure
Check your dependencies	OWASP Dependency-check npm audit Safety (Python)	CoreOS/Clair Anchore Aqua Trivy
Protect your secrets	Environment variables Configuration management Secrets Management systems	
Scan your code	SonarQube (Security) Bandit (Python) Go AST Scanner (GAS) Brakeman (Ruby)	Chekov TFLint Kube-bench
Harden your config	Ansible playbooks (dev-sec.io) Open Policy Agent / conftest Chef Inspec Hashicorp Sentinel	

DEV-SEC.IO

Identify security issues and misconfiguration

INSPEC

Remediate with your automation tooling

ANSIBLE

CHEF
CHEF.IO

puppet labs

Overview

DevSec Hardening Framework Baselines

✓ Applications	MySQL	PostgreSQL
	Apache	Nginx
✗ Operations	Logging / Monitoring	User Management
✓ Components	SSH, SSL	Docker, K8S
✓ OS	Linux	Windows
✗ Network	Intrusion Detection	Firewall

✓ included ✗ not in scope

VISIBILITY AND TRACEABILITY

- **Visibility**
  - Using metadata in tickets to provide product-level view of security work identified (outputs of tooling, threat modelling, audit points, customer requirements)
- **Traceability**
  - To (relevant) security standards
  - Policy requirements
  - Compliance and/or contractual requirements
  - Identified risks

TIME-BOUND SECURITY

- **Define clear criteria for security work, then stick to it:**
  - We do risk analysis in these conditions when start a new business initiative
  - We perform threat modelling for 1h whenever we start building a new feature
- Ensure you retain evidence you've performed these

RECOVERING FROM INCIDENTS

- Incidents are investments you already made. Ensure you get ROI
- Don’t just do the bare minimum. At least identify what CONTRIBUTED to the failure, and add to a backlog what you should be doing to improve that
- GOLDEN RULE: “Human error is a symptom of a system in need of re-design” Nancy Leveson
- Don’t “blame people” for contributing to incidents. More than likely, it’s the pressure you’re putting on them that is making them cut corners

BE CLEAR ABOUT WHAT YOU WANT FROM A CONSULTANT

- You don’t need a “regurgitation” of best practices. You can do that by yourself
- Few people have both Governance and Technical skills. Identify and service YOUR needs
- Identify specific things you require and ensure that consultants don’t just “do things” but teach your teams to be self-sufficient. Focus on facilitation and avoid ‘rabbit holes’

FOR STARTUPS, YOUR INITIAL MILEAGE IS YOURS TO WALK

- Bringing security expertise too early is detrimental for long-term role identities of your Engineering teams
- The basics are well documented. You don’t need consultants or staff to tell you what those are. Leverage Open Source resources
- When you do ‘get stuck’, then at least you know exactly what you’re struggling with and know what to get from a consultant
- If you don’t have any security items on your backlog, you’re just “talking about it”

WRAPPING UP


KEEP
CALM
AND ADD SECURITY
THINGS TO
THE MANAGED BACKLOG
imgflip.com

CERTIFIED DEVSECOPS LEADER - PRACTICAL-DEVSECOPS.COM

Certified DevSecOps Leader CDL

The DevSecOps Leader course helps leaders and managers in influencing DevSecOps transformation practices in the enterprise.

In this course, you will be able to:

1. Understand the basics of DevSecOps from the business perspective
2. Assess the DevSecOps Maturity of the organization(PDSOMM)
3. Design the DevSecOps Strategy for an organization(Wardley mapping and Cynefin)
4. Influence organizational's culture for shift left approach
5. Gain confidence in steering the organization in the right direction
6. Increase the productivity of your team by prioritizing the GRC efforts

This DevSecOps Certification Course is practical in nature with 15+ case studies, hands-on exercises, and demos in our state of the art online labs.

https://www.practical-devsecops.com/certified-devsecops-leader/

Q & A

Mario Platt – @madplatt