I am going to show you today how to get more secure applications delivered faster.
But first I am going to tell you how we got less secure applications delivered more slowly....
Storytime...
Key dynamics:

- Everyone had **many responsibilities**. No matter what the official priorities, compliance paperwork came last.
- Dev had already **damaged trust**.
- Security was **severely underresourced**.
- **Compliance** sucked the oxygen from security.
- At any point, the director could have made this happen... but didn’t.
Truly, everyone did the best job he or she could, given what was known at the time, his or her skills and abilities, the resources available, and the situation at hand.
We could have been here.
But we spent our time here instead
Why bring security into the development process? [Crowdsourced]

- In any org with formal compliance, ignoring security may mean delivering late or not at all.
- Can select what controls are important to YOU
  - Can also be platform specific
- Improves security - devs should understand what they might do to cause a breach. Educate them early.
- Cost of fixing vulnerability is exponential
- Reduces schedule drift - improved flow
- Understand which tools can/can’t be used.
- Task may not be allowed at all
- May need to do major refactoring to incorporate, e.g. encryption
- Platform-level security practices.
- Brand reputation ***
DevSecOps 101
DevOps is...

A combination of philosophies, practices and tools that increases an organization’s ability to deliver applications and services at high velocity

- AWS [What is DevOps?](https://aws.amazon.com/devops/) *(Dev Perspective)*
DevOps is...

[A way to] reduce waste and make releases boring

- Jez Humble, Author & 18F Alumni (Ops perspective)

DevSecOps @ElizAyer
DevOps is...

An approach that resolves the apparent conflict between speed and reliability.
Why isn’t security within the Ops in DevOps?

We call out security separately because:

1) Security is truly a specialist discipline
2) Security got left out of the first wave of DevOps
3) Security is used to encompass compliance, and that’s definitely not part of DevOps
Everyone seemed to like this representation of DevOps and Security from my talk at #devopsdays Austin

https://slack.engineering/moving-fast-and-securing-things-540e6c5ae58a
Why isn’t security within the Ops in DevOps?

We call out security separately because:

1) Security is truly a **specialist discipline**
2) Security got **left out** of the first wave of DevOps
3) Security is used to **encompass compliance**, and that’s **definitely** not part of DevOps
DevSecOps Guide

Standard DevSecOps Platform Framework

Goal: Safer Software Sooner

The following document describes, at a high-level, the expectations, scope of responsibilities, maturity model, and metrics associated of any DevSecOps platform at GSA.
DevSecOps is...

Development + Security + Operations = Safer Software Sooner
Digression: Why DevSecOps, not DevOpsSec?
The DevOps Value Pyramid

1. PEOPLE
2. PROCESS
3. TOOLS
The DevOps Value Pyramid
1. **People: the DevOps culture**

**One team** handles a software system through inception, delivery, maintenance, end-of-life of a system.
1. People: the DevOps culture

- **Shared responsibility** for how software behaves in production
- **Continuous feedback** results in tighter processes that get better and better
- **Optimization of the full system**, not just one piece, department, or interest.
- Open communications and **knowledge sharing** enhance trust within the team
The DevOps Value Pyramid

1. PEOPLE
2. PROCESS
3. TOOLS
2. Process: Empowered Teams & Shift Left

An empowered team contains the skills and authority it needs to develop & operate its systems.

For DevSecOps, the team needs basic security skills and access to expertise.
2. Process: Empowered Teams & Shift Left

“Shift Left” means that operability concerns should be considered as early in the dev cycle as possible.
2. Process: Empowered Teams & Shift Left

Evil User Story (aka Abuser Story) 1:

As a hacker, I want to have somebody’s benefits paid to me instead.
2. Process: Empowered Teams & Shift Left

Evil User Story (aka Abuser Story) 2:

As the Russian government, I want to steal data and release it so that I undermine confidence of the American people in democracy.
The DevOps Value Pyramid

1. PEOPLE
2. PROCESS
3. TOOLS
3. **Tools: CI/CD**

- Source Code Management
- CI/CD Systems
- Unit test framework
- Infrastructure-as-code
- etc.
3. Tools: Development Pipeline

https://dzone.com/articles/learn-how-to-setup-a-cicd-pipeline-from-scratch
3. Tools: Development Pipeline

Evil User Stories

https://dzone.com/articles/learn-how-to-setup-a-cicd-pipeline-from-scratch
3. Tools: Development Pipeline

Static Code Analysis

https://dzone.com/articles/learn-how-to-setup-a-cicd-pipeline-from-scratch
3. Enhancing the Pipeline for Security

Static Application Security Testing (SAST) tools scan for code patterns likely to cause vulnerabilities.

Examples: SonarQube (Open Source), Fortify, Coverity, Veracode

https://www.owasp.org/index.php/Source_Code_Analysis_Tools
3. Tools: Development Pipeline

Dynamic Analysis

https://dzone.com/articles/learn-how-to-setup-a-cicd-pipeline-from-scratch
3. Enhancing the Pipeline for Security

Dynamic Application Security Testing (DAST) tools scan a running application for vulnerabilities or assist in manual penetration testing.

OSS Examples: Arachni, Metasploit, sqlmap*
Why would you *not* point hacker tools at your application? They will!
Back to the story...
Would any of this have helped our Eligibility System deliver?

Nope.
That project was held up by compliance.
In order to be compliant, you generally need controls or a **POAM** - a Plan of Action and Milestones.
In order to agree what to POAM, you need a threat model.
How to get towards DevSecOps
Threat modeling: the key to initiating DevSecOps
Help translate fears into a threat model.
Help translate fears into a threat model.
Help translate fears into a threat model.
What is a threat model? (OWASP)

“Most of the time, a threat model includes:

● A description / design / model of what you’re worried about
● A list of assumptions that can be checked or challenged in the future as the threat landscape changes
● A list of potential threats to the system
● A list of actions to be taken for each threat
● A way of validating the model and threats, and verification of success of actions taken

Our motto is: Threat modelling: the sooner the better, but never too late.”

https://www.owasp.org/index.php/Application_Threat_Modeling
Threat Modelling Exercise:

Your trip home from Agile 2019 (from here to when you walk in your front door).

1. What could go wrong?
What could go wrong Agile 2019-> Home
[Crowdsourced]

- Flight delay, cancelled,
- TSA
- Lost luggage, passport/id
- Forget keys (house, car)
- Random act of violence
- Shut down freeways/metro, beltway traffic
- Car accident
- Personal sickness
- Lose your phone -
- GPS malfunction

- Wrong airport
- Alien abduction
- Uber goes out of business
- Water taxi piracy
- Car stolen/hacked
- Call from work for actual problem, miss transport
- Oversleep
Threat Modelling Exercise:

Your trip home from Agile 2019 (from here to when you walk in your front door).

2. What could you do to prevent or mitigate the threats?
For me....

I would have threat modelled car accidents, traffic, missed or delayed flights....
For me what did happen

I failed to get permissions until literally the last possible second.

All sane flights were gone by the time I could book them.

I did my best and ended up with two separate bookings.

SeaTac immigration was a madhouse, and I missed the second.

They booked me into a hotel room without a bed or shower.

I’ve revised my threat model
Why do threat modeling? (OWASP)

- Build a secure design
- Efficient investment of resources; appropriately prioritize security, development, and other tasks
- Bring Security and Development together to collaborate on a shared understanding, informing development of the system
- Identify threats and compliance requirements, and evaluate their risk
- Define and build required controls.
- Balance risks, controls, and usability
- Identify where building a control is unnecessary, based on acceptable risk
- Identification of security test cases / security test scenarios to test the security requirements

https://www.owasp.org/index.php/Application_Threat_Modeling (abridged)
Identify & prioritize security improvements

Standard DevSecOps Platform Framework

Goal: Safer Software Sooner

The following document describes, at a high-level, the expectations, scope of responsibilities, maturity model, and metrics associated of any DevSecOps platform at GSA.

Baseline Definitions

**DevSecOps**: A cultural and engineering practice that breaks down barriers and opens collaboration between development, security, and operations organizations using automation to focus on rapid, frequent delivery of secure infrastructure and software to production. It encompasses intake to release of software and manages those flows predictably, transparently, and with minimal human intervention/effort.

Common Expectations

Successful DevSecOps teams have processes characterized by repeatability, low redundancy, high collaboration with dispersion of collective efforts; in order to achieve this most efficiently, automation and auditable is prized above subjective decision-making. The decisions that would drive successful release should be codified in code. If it is not feasible to capture in code, checklists with clear yes/no decision points are preferred to heavily documented standard operating procedures (SOPs). SOPs can be subjectively interpreted more so than these first options.

[https://tech.gsa.gov.guides/dev_sec_ops_guide/](https://tech.gsa.gov.guides/dev_sec_ops_guide/)
Identify & prioritize security improvements

2. Security checklist

- **Project uses a written threat model.** (More information from [OWASP](https://owasp.org/).)
  - Threat model created as a collaboration between security team, developers, sysadmins/ops, business side, and subject-matter experts.
  - Threat model is communicated to the development team and used to guide technical decisions.

- **Project uses a prioritized list of security improvements.**
  - Prioritized list of improvements created as a collaboration between security team, developers, and sysadmins/ops.
  - Security issues are triaged appropriately.
    - Urgent, exploitable vulnerabilities are addressed immediately.
    - Development time and effort is regularly and consistently invested in completing security improvement work from the backlog.

- **Security team is consulted early and often.**
  - Developers consult security before embarking on a risky or critical new feature, not afterwards.
  - Security team is invited to meetings at a regular cadence.
  - Security team helps review security-related pull requests and consults on security questions frequently.

- **HTTPS enforced on every public endpoint with properly managed certificates.** (More from [Before You Ship Guide, 18F](https://18f.gov/before-you-ship-guide) and [Eric Mills, 18F](https://ericmills.com).)
  - Websites do not display any certification-related warnings when visited using Chrome, Firefox, Safari, or Internet Explorer.
Identify & prioritize security improvements

Case study:

DevOps and Security on a Small Team by Aidan Feldman, 18F
In Summary...

To fully realize the joint benefits of speed and reliability, Security/Compliance must be brought into DevOps...
In Summary...

Incorporating Security is primarily a people activity. Threat modelling helps develop a shared language and set of concerns...
In Summary...

But Security is typically severely underresourced compared to Development, so we can’t use the same team structures. We need:

1) Basic dev team security education
2) Dev team access to expertise
3) Enough security capacity to engage

... which generally requires Senior Management Support!
In Summary...

Automation helps scale security.

You’ll get the most out of your tools investment by prioritizing according to your threat model, involving Security and Product.
DevSecOps is...

Development + Security + Operations = Safer Software Sooner
Resources!

DevSecOps: The Missing Link in Delivering on the Promise of Business Velocity (Webinar feat. @realgenekim @wickett)
https://xebialabs.com/community/webinars/devsecops-missing-link-of-business-velocity/

The Open Web Application Security Project
https://www.owasp.org/

GSA DevSecOps Guide https://tech.gsa.gov/guides/dev_sec_ops_guide/

Agile Application Security (Book)
Discussion