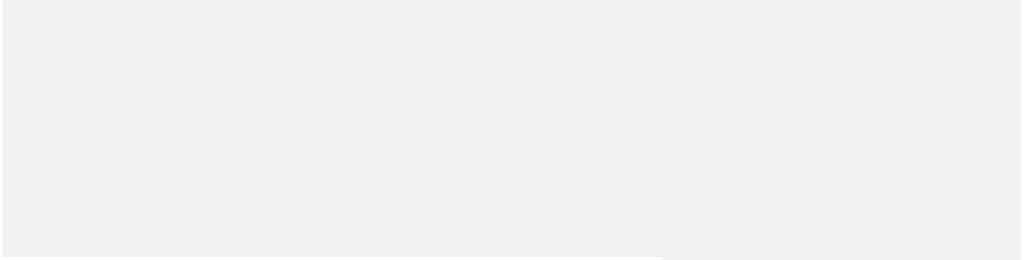


**YOU KEEP USING THAT WORD**

**I DO NOT THINK IT MEANS WHAT YOU  
THINK IT MEANS**



“Not considered viable for a  
DevSecOps platform.”

A photograph of a stage from a low angle, looking up. The stage is illuminated by numerous blue spotlights mounted on a truss system. The light rays fan out across the dark background, creating a dramatic and energetic atmosphere.

**where you are**



(Not considered viable for  
a DevSecOps platform)

## **LEVEL 1** **Patch Management**

Patching is manual and not enforceable as a requirement nor is the state of patches running machines discoverable



## **LEVEL 2**

### **Patch Management**

Security informs application owners of patches.

Application owners are responsible to be aware of those patches and implement them.

A large, three-dimensional white number '3' is positioned above a white number '4'. Both digits have a dark gray or black shadow effect, giving them a sense of depth and volume. They are set against a dark gray background.

## **LEVEL 3 & 4 Patch Management**

Application owners are automatically notified...

The platform automatically tests new patches...

A close-up photograph of a woman with dark hair and glasses, looking down at a computer screen. The screen displays a large amount of green text, likely code or terminal output. The background is blurred, showing what appears to be a city street at night.

**the model was not a  
roadmap**

A photograph of a modern urban landscape. In the foreground, a yellow and white traffic barrier gate is partially open on a curved asphalt road. Two surveillance cameras are mounted on poles, one on each side of the gate. The background features several large, modern office buildings with glass and steel facades. There are green trees and bushes lining the streets. A person is walking away from the camera on the sidewalk. The sky is clear and blue.

**the twist provided validity**

- Patch management
- Image Management
- Artifacts
- Platform Governance
- Change Management
- Application Dev, Testing, and Ops
- Availability and Performance Management
- Network Management
- Authority to Operate Process
- Backup and Data Lifecycles
- Financial Management





# codified in code

## High-Value Metrics

These metrics should be implemented first in a new platform. Not all platforms will have these metrics immediately available, but a fully mature environment typically will have all of these metrics.

| Metric  | Description  | Associated Domain(s)   |
|---|--|--|
| Deployment frequency                            | Number of deployments to production in a given time frame                                | Application Deployment; Authority to Operate Processes                         |
| Change lead time (for applications)             | Time between a code commit and production deployment of that code                        | Overarching; Authority to Operate Processes; Patch Management                  |
| Change volume (for applications)                | Number of user stories deployed in a given time frame                                    | Overarching  |
| Change failure rate                             | Percentage of production deployments that failed   | Application Deployment   |
| Mean time to recovery (MTTR) (for applications) | Time between a failed production deployment to full restoration of production operations | Application Deployment; Backup and Data Lifecycle Management; Patch Management |

# GSA Tech Guides

[All guides](#) » DevSecOps guides

## DevSecOps Guide

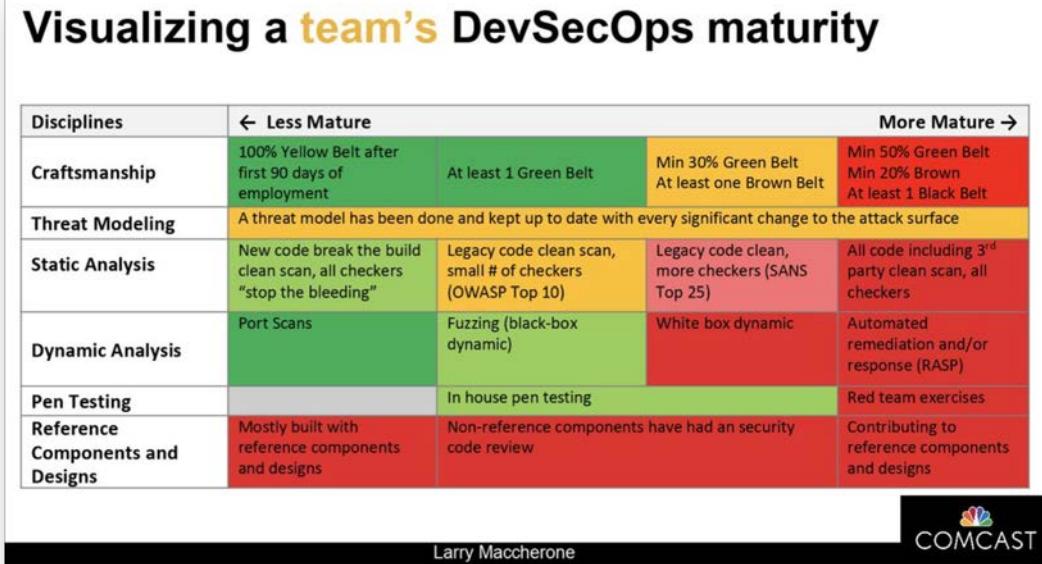
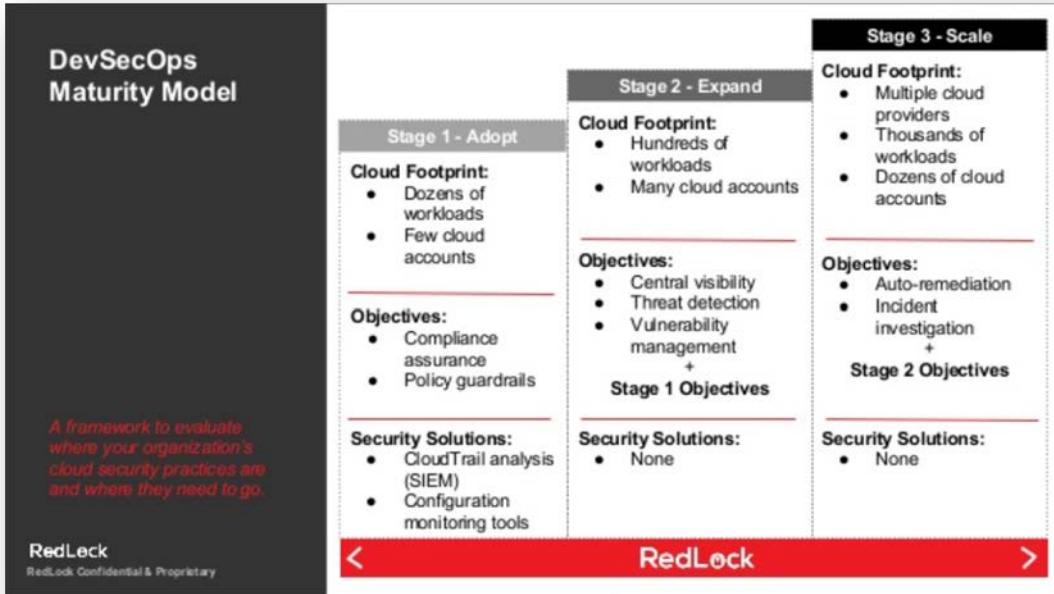
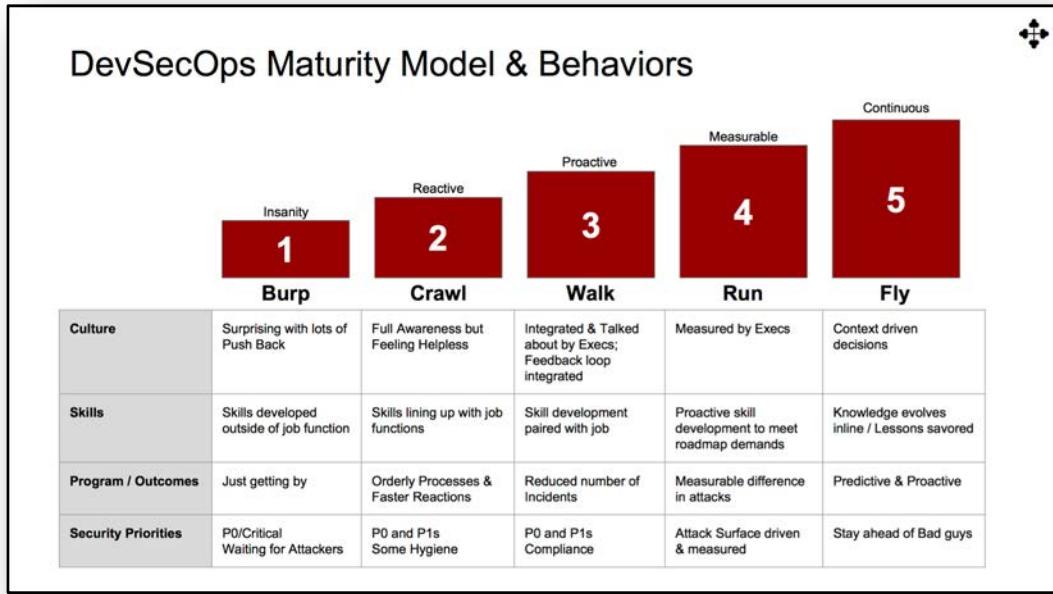
### Standard DevSecOps Platform Framework

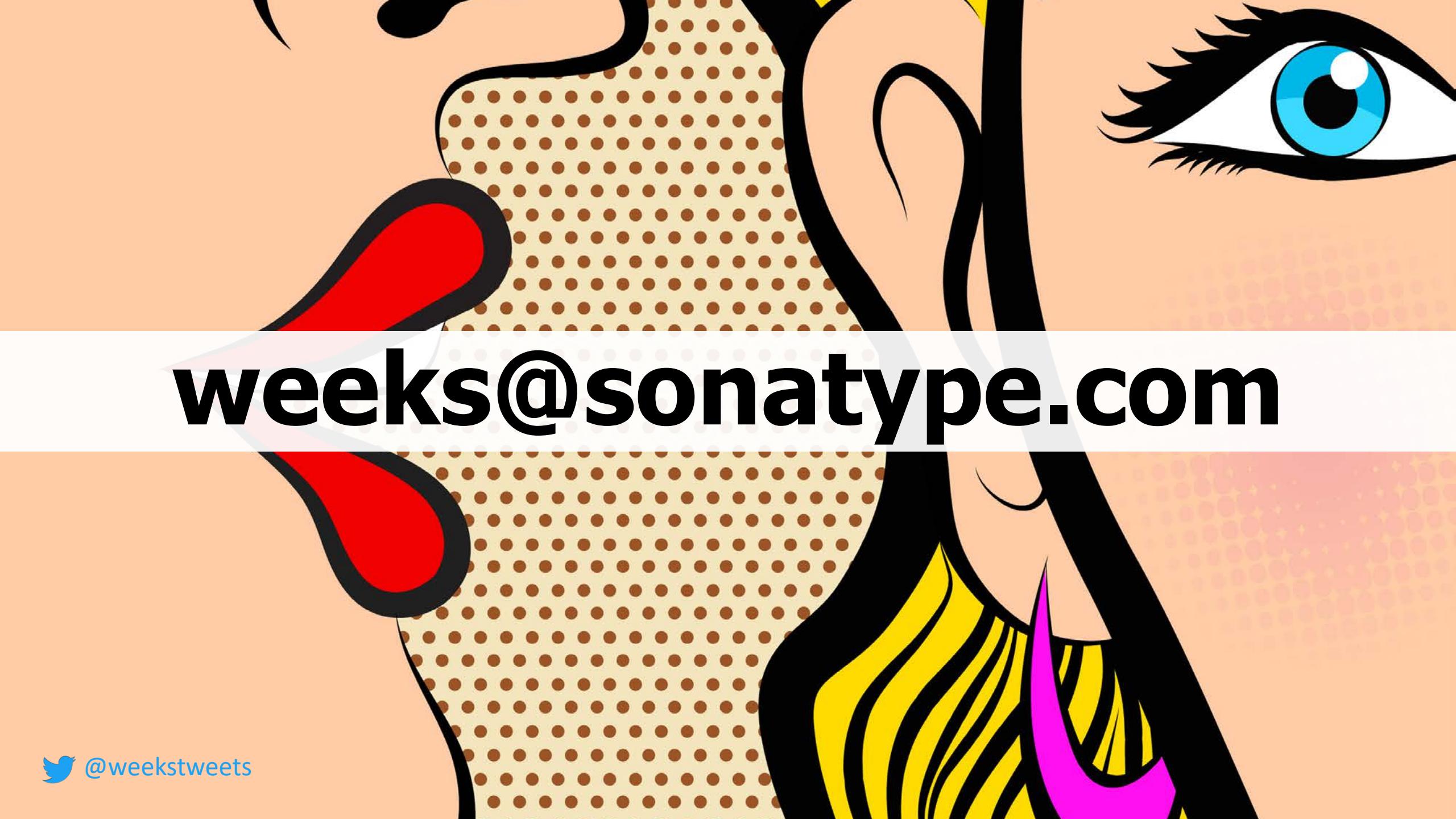
Goal: Safer Software Sooner

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

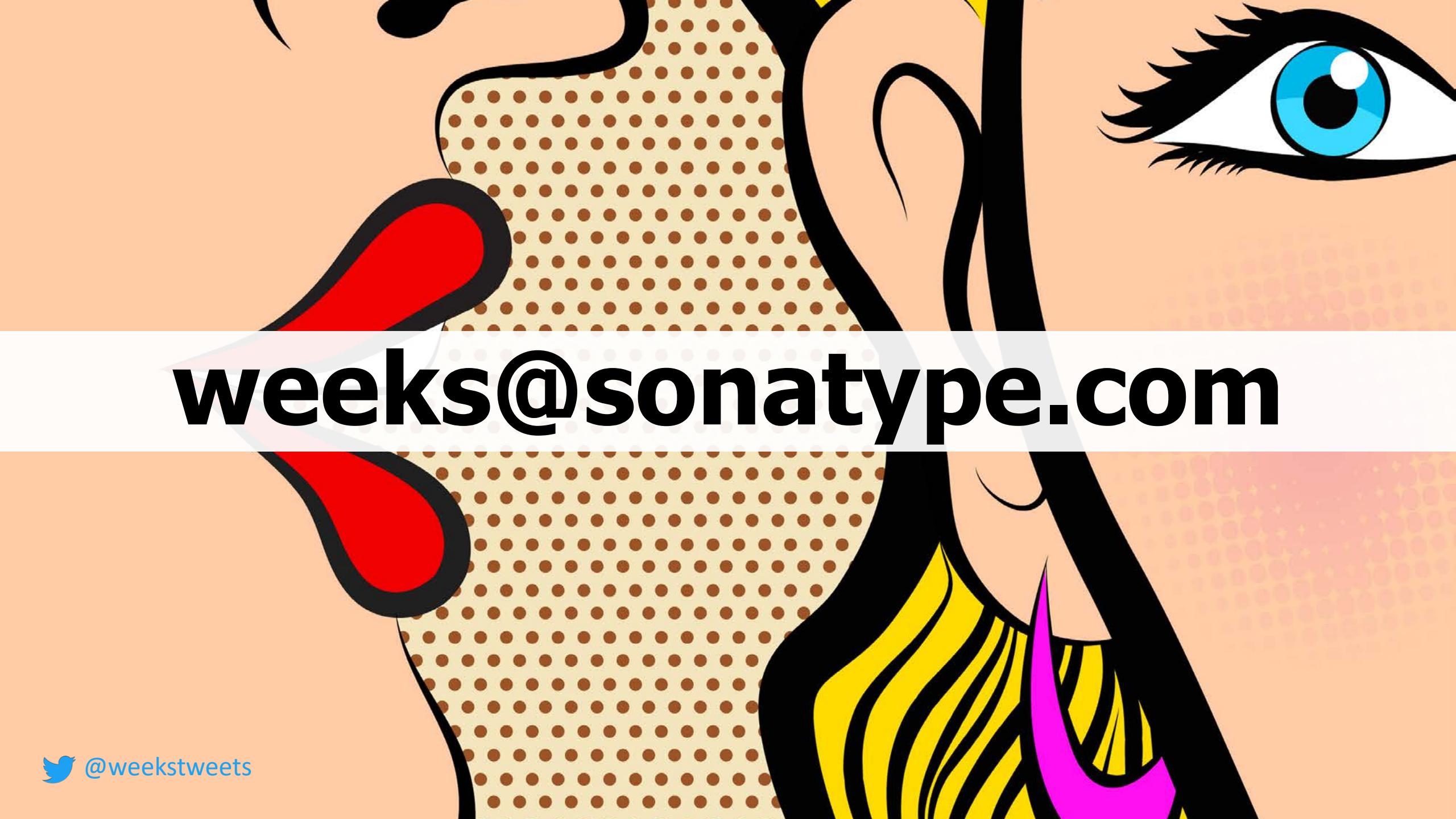
#### Baseline Definitions

**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





**weeks@sonatype.com**

A stylized, pop-art style illustration of a woman's face and upper body. The woman has large, expressive blue eyes with black eyelashes. Her hair is dark and wavy, with a yellow and pink striped pattern at the bottom. She is wearing a black top. The background features a halftone dot pattern in shades of brown and orange.

**weeks@sonatype.com**

“Not considered viable for our  
DevOps platform.”

[weeks@sonatype.com](mailto:weeks@sonatype.com)