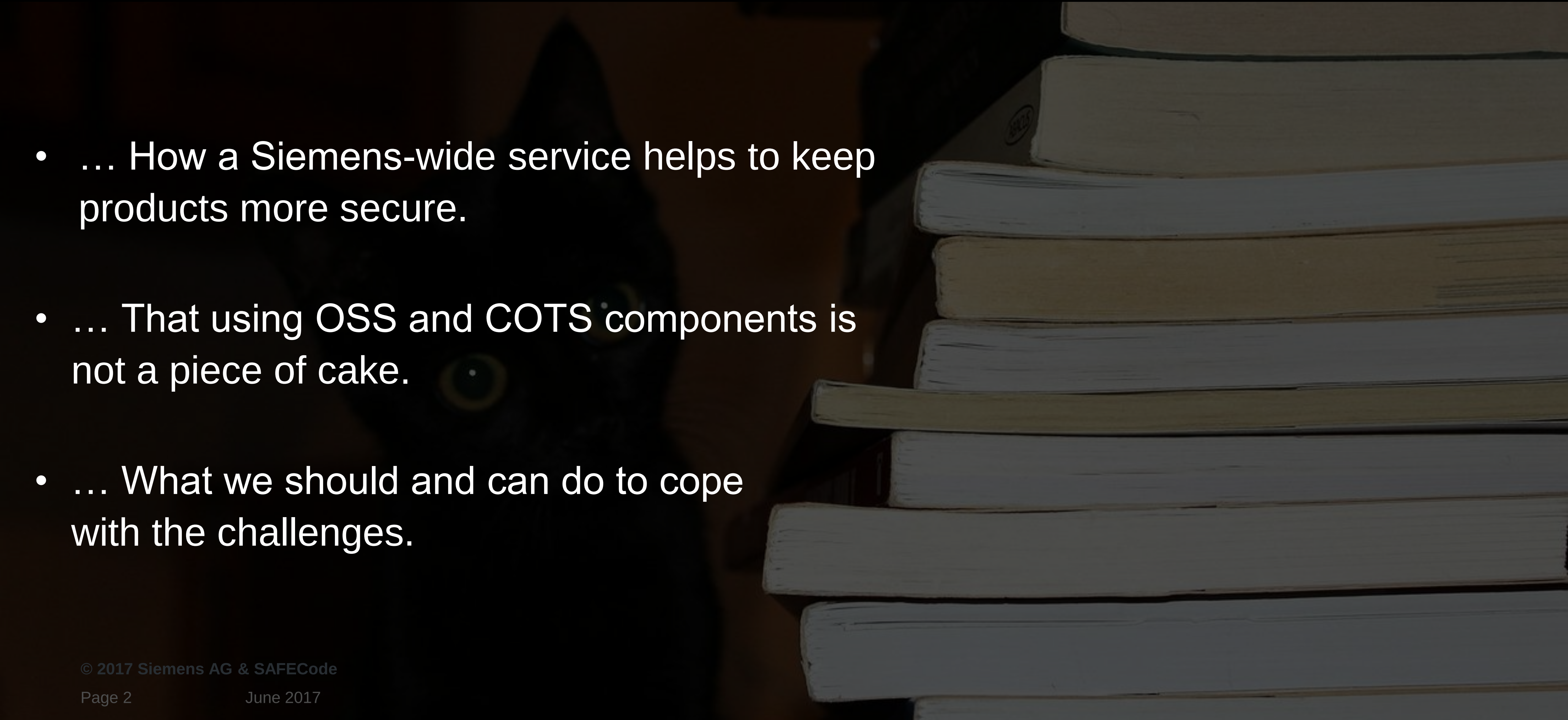
SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SIEMENS
Ingenuity for life

Experiences and Lessons Learned from a Siemens-Wide Security Patch Management Service for Products

29th Annual FIRST Conference, June 11 - 16, 2017
Manuel Ifland, CISSP

After This Presentation You Will Know …



- … How a Siemens-wide service helps to keep products more secure.
- … That using OSS and COTS components is not a piece of cake.
- … What we should and can do to cope with the challenges.

Why Are We Using OSS and COTS Components?

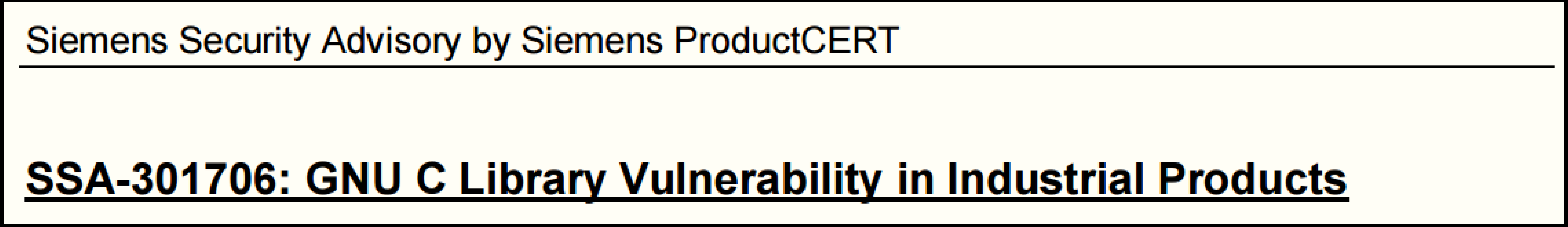
Pre-made building blocks

Faster time-to-market

Lower development costs

Where There is Light, There is Shadow.

- Products inherit security issues:



Siemens Security Advisory by Siemens ProductCERT

SSA-301706: GNU C Library Vulnerability in Industrial Products

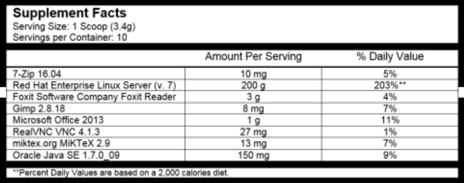
- Vulnerability information is spread all over the Internet
- Patching is not always an easy task

The Siemens-wide

Security Vulnerability Monitoring (SVM) Service.

Siemens Security Vulnerability Monitoring (SVM)

Product / Solution Owner

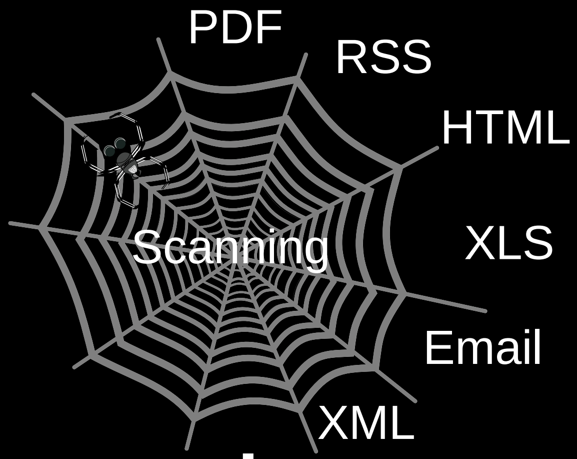


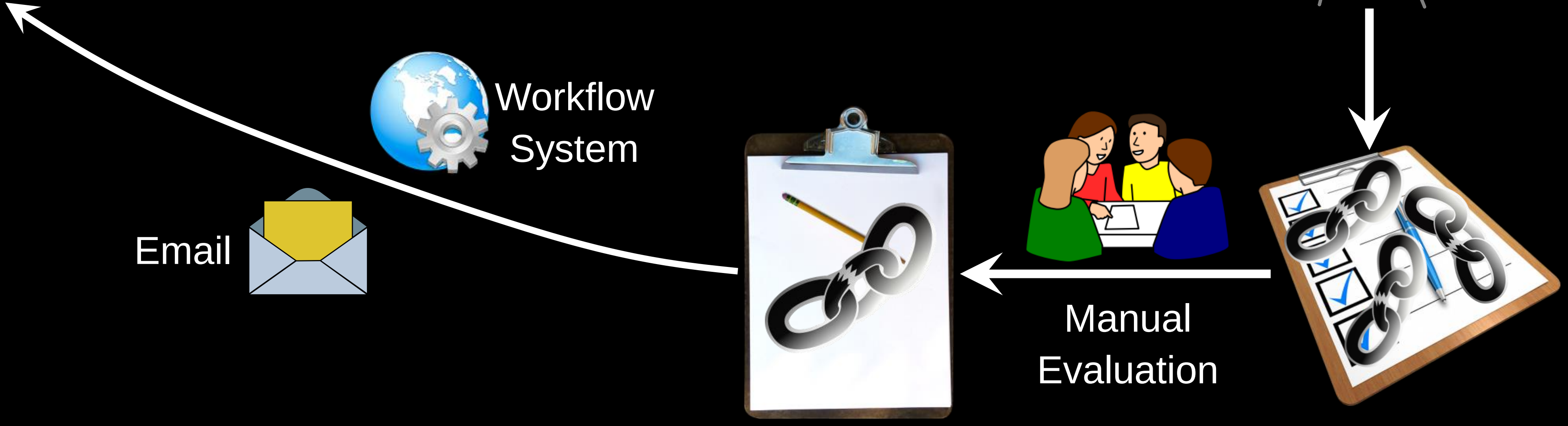
Supplement Facts
Serving Size: 1 Scoop (3.4g)
Servings per Container: 10

	Amount Per Serving	% Daily Value
7-Zip 16.04	10 mg	5%
Red Hat Enterprise Linux Server (v. 7)	200 g	203%**
Foxit Software Company Foxit Reader	3 g	4%
Gimp 2.8.18	8 mg	7%
Microsoft Office 2013	1 g	11%
RealVNC VNC 4.1.3	27 mg	1%
miktex.org MiKTeX 2.9	13 mg	7%
Oracle Java SE 1.7.0_09	150 mg	9%

**Percent Daily Values are based on a 2,000 calories diet.

Components List

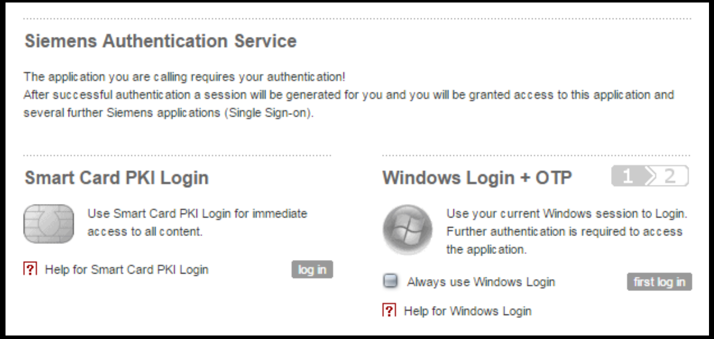




© 2017 Siemens AG & SAFECode

Key Advantages of SVM For Siemens

Confidential information stays in Siemens



Siemens Authentication Service

The application you are calling requires your authentication!
After successful authentication a session will be generated for you and you will be granted access to this application and several further Siemens applications (Single Sign-on).

Smart Card PKI Login

Use Smart Card PKI Login for immediate access to all content.

[?] Help for Smart Card PKI Login

Windows Login + OTP

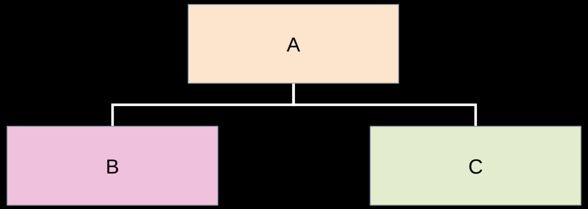
Use your current Windows session to Login. Further authentication is required to access the application.

□ Always use Windows Login

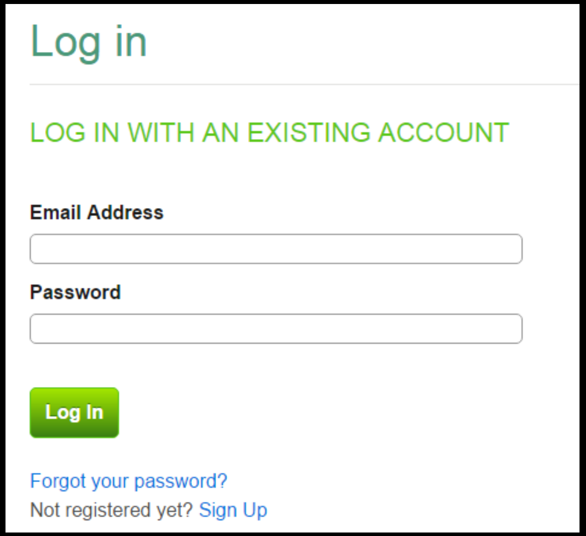
[?] Help for Windows Login

Neatly integrates into company’s infrastructure (e.g. SSO, email encryption)

Key Advantages of SVM For Siemens (Cont.)



Dependencies



Log in

LOG IN WITH AN EXISTING ACCOUNT

Email Address

Password

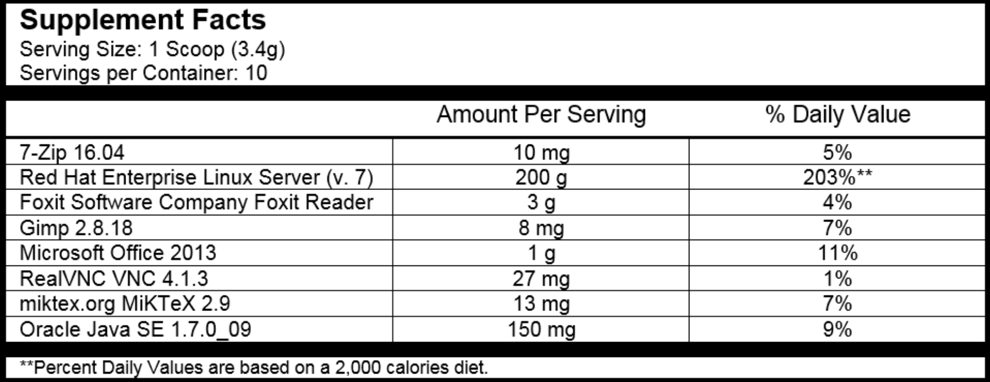
Forgot your password?

Not registered yet? Sign Up

Security information from sources where support contract is required

Challenges

Challenges

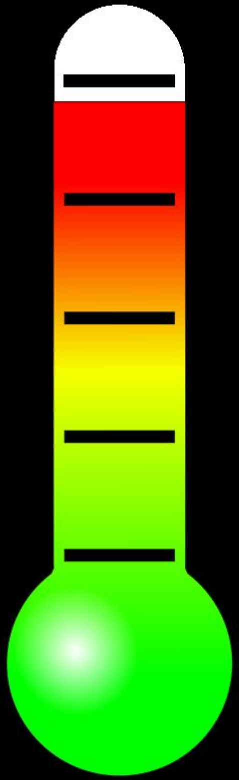


Supplement Facts
Serving Size: 1 Scoop (3.4g)
Servings per Container: 10

	Amount Per Serving	% Daily Value
7-Zip 16.04	10 mg	5%
Red Hat Enterprise Linux Server (v. 7)	200 g	203%**
Foxit Software Company Foxit Reader	3 g	4%
Gimp 2.8.18	8 mg	7%
Microsoft Office 2013	1 g	11%
RealVNC VNC 4.1.3	27 mg	1%
miktex.org MiKTeX 2.9	13 mg	7%
Oracle Java SE 1.7.0_09	150 mg	9%

**Percent Daily Values are based on a 2,000 calories diet.

Bill of Materials



Risk Estimation

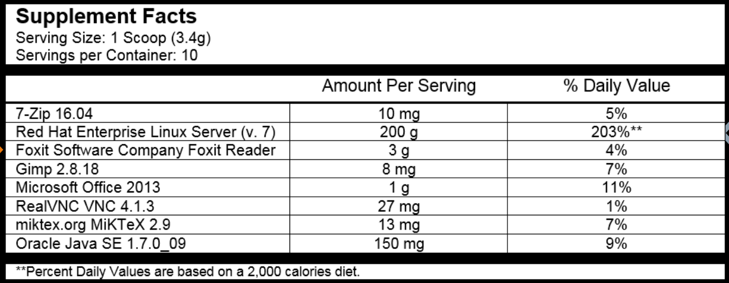
Names of Third-party Components

Best Practices from SAFECode Third-party Components Working Group

- Special Interest Group for Third-party Components (TPCs)
- Open Source (OSS) & Commercial off-the-shelf (COTS)
- Various member companies on board:
  - Adobe
  - Boeing
  - Intel
  - Microsoft
  - Siemens
  - Symantec

The Bill of Materials (BOM)

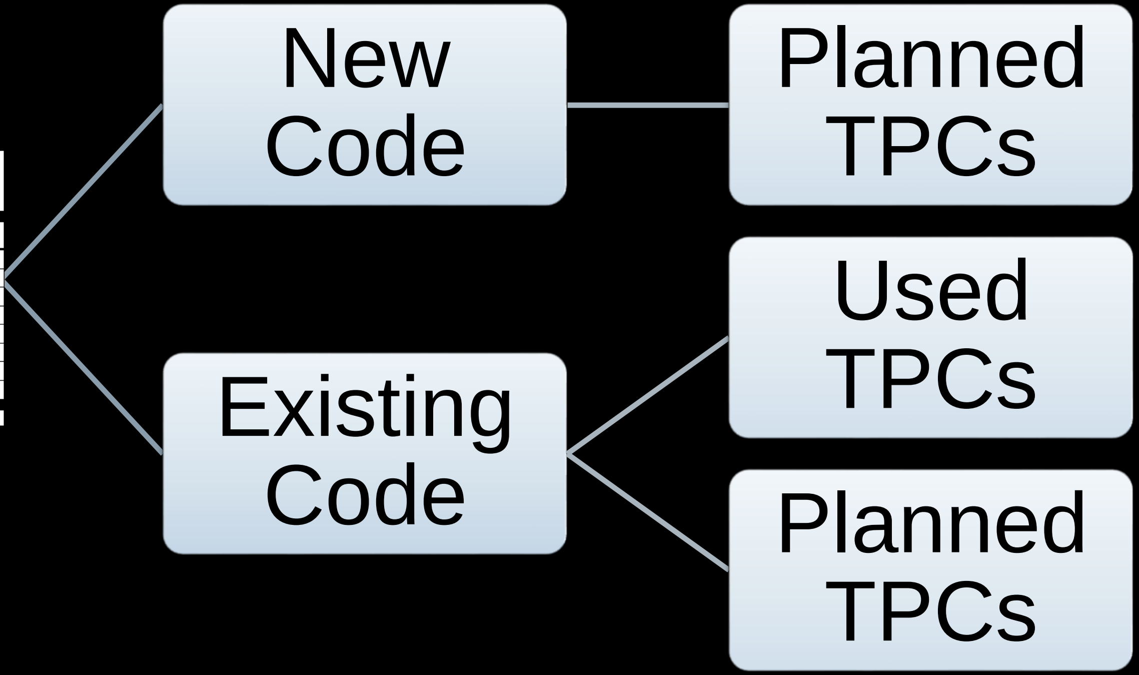
- First and foremost step!
- It depends on where you are in the food chain:



Supplement Facts
Serving Size: 1 Scoop (3.4g)
Servings per Container: 10

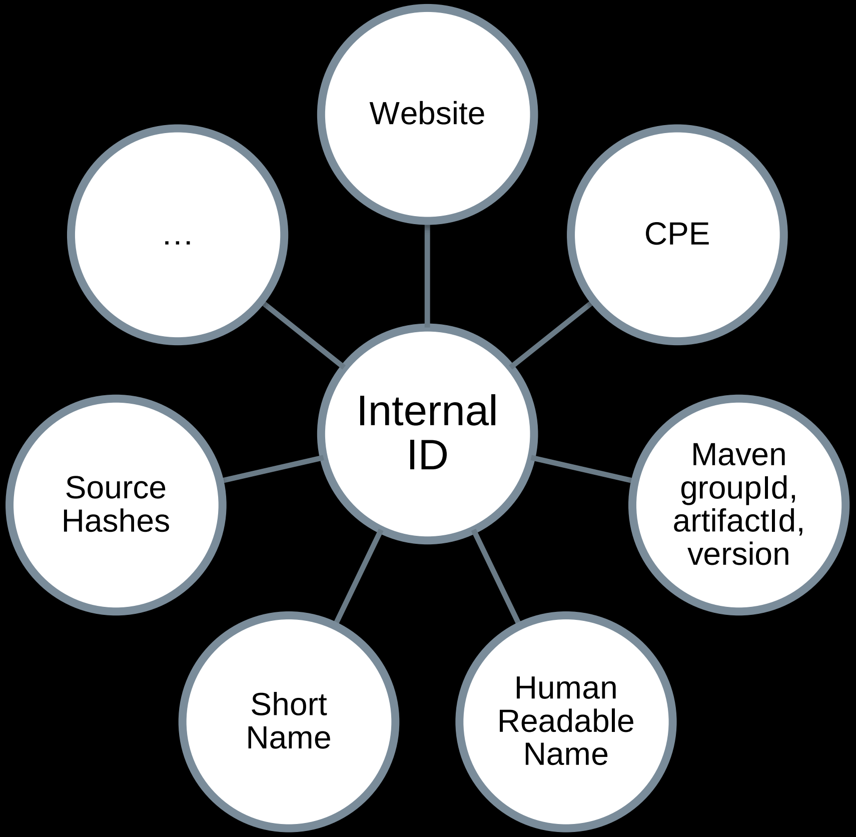
	Amount Per Serving	% Daily Value
7-Zip 16.04	10 mg	5%
Red Hat Enterprise Linux Server (v. 7)	200 g	203%**
Foxit Software Company Foxit Reader	3 g	4%
Gimp 2.8.18	8 mg	7%
Microsoft Office 2013	1 g	11%
RealVNC VNC 4.1.3	27 mg	1%
miktex.org MiKTeX 2.9	13 mg	7%
Oracle Java SE 1.7.0_09	150 mg	9%

**Percent Daily Values are based on a 2,000 calories diet.



Naming of Third-party Components

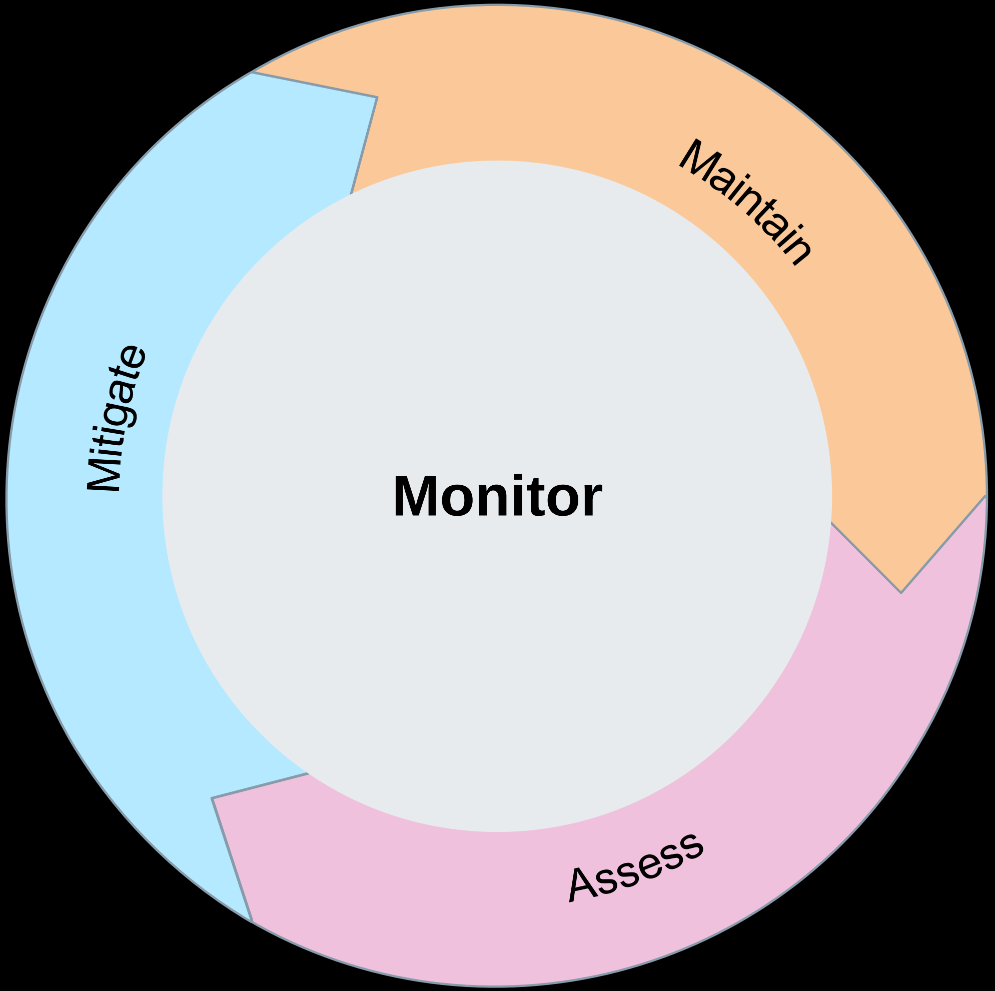
- BOM TPCs need to be clearly and uniquely identifiable
- Compatibility with external databases is the key!



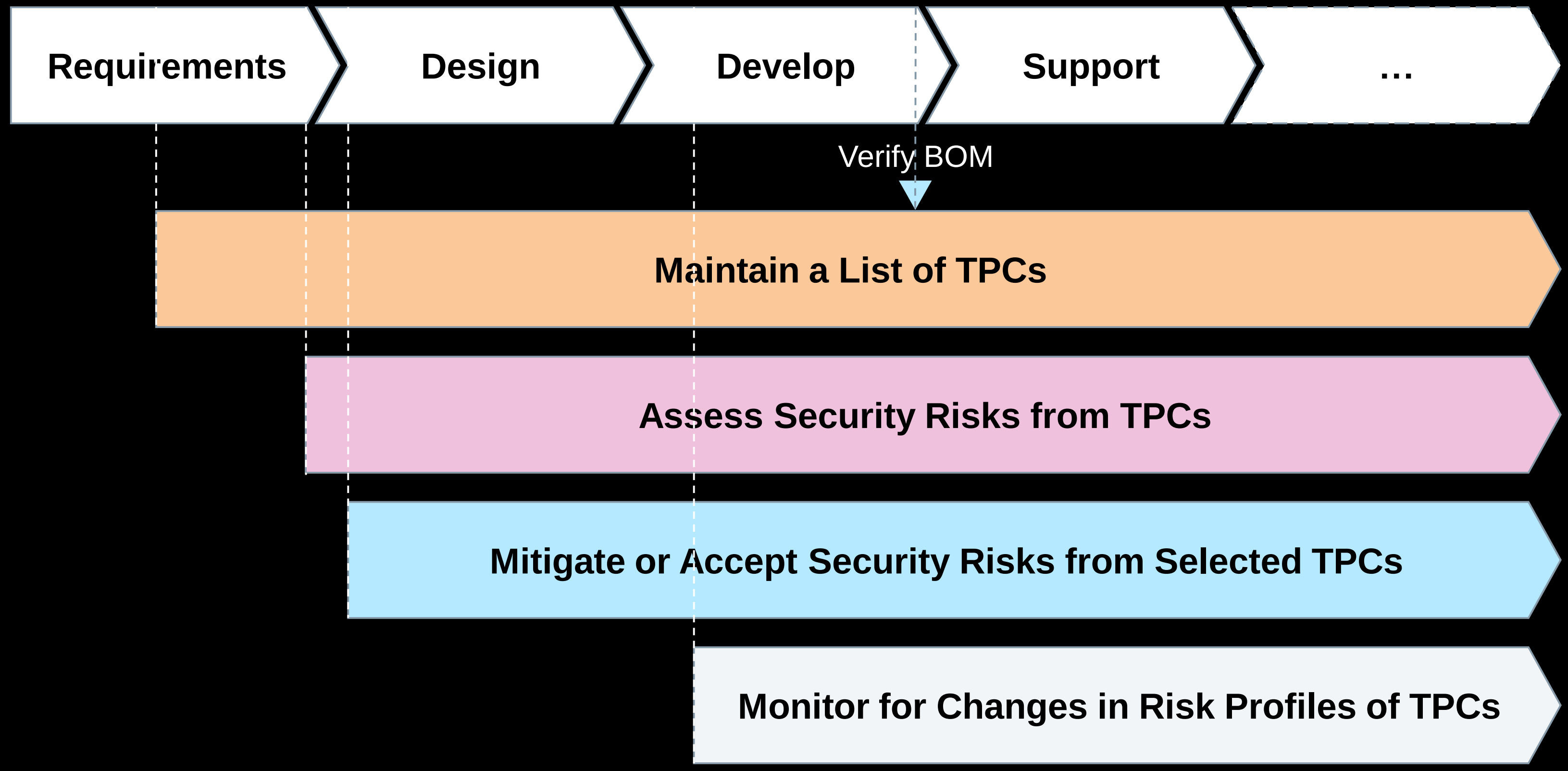
Which TPCs Should We Use?

- TPCs are often chosen purely based on functionality
- The following should be considered however:
  - Component Maintenance
  - Development Practices
  - Security Vulnerabilities
  - End of Life

TPC Management Life Cycle – High Level Steps

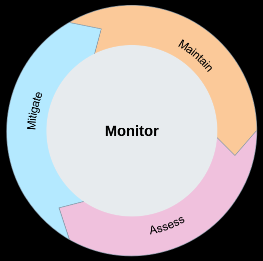


SDLC and TPC Management Life Cycle Go Hand in Hand

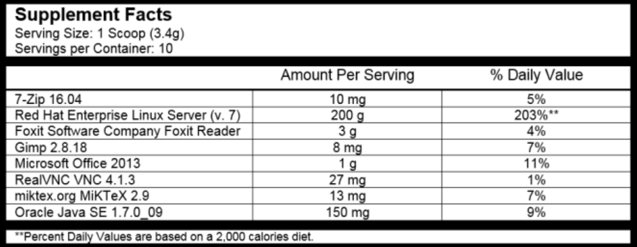

Requirements
Design
Develop
Support
…
Verify BOM
Maintain a List of TPCs
Assess Security Risks from TPCs
Mitigate or Accept Security Risks from Selected TPCs
Monitor for Changes in Risk Profiles of TPCs

Key Takeaways:
Towards Supply Chain Security

OSS and COTS components can increase security risks



Establish a process and perform constant monitoring



Supplement Facts
Serving Size: 1 Scoop (3.4g)
Servings per Container: 10

	Amount Per Serving	% Daily Value
7-Zip 16.04	10 mg	5%
Red Hat Enterprise Linux Server (v. 7)	200 g	203%**
Foxit Software Company Foxit Reader	3 g	4%
Gimp 2.8.18	8 mg	7%
Microsoft Office 2013	1 g	11%
RealVNC VNC 4.1.3	27 mg	1%
miktex.org MiKTeX 2.9	13 mg	7%
Oracle Java SE 1.7.0_09	150 mg	9%

**Percent Daily Values are based on a 2,000 calories diet.

Identify components and maintain a BOM

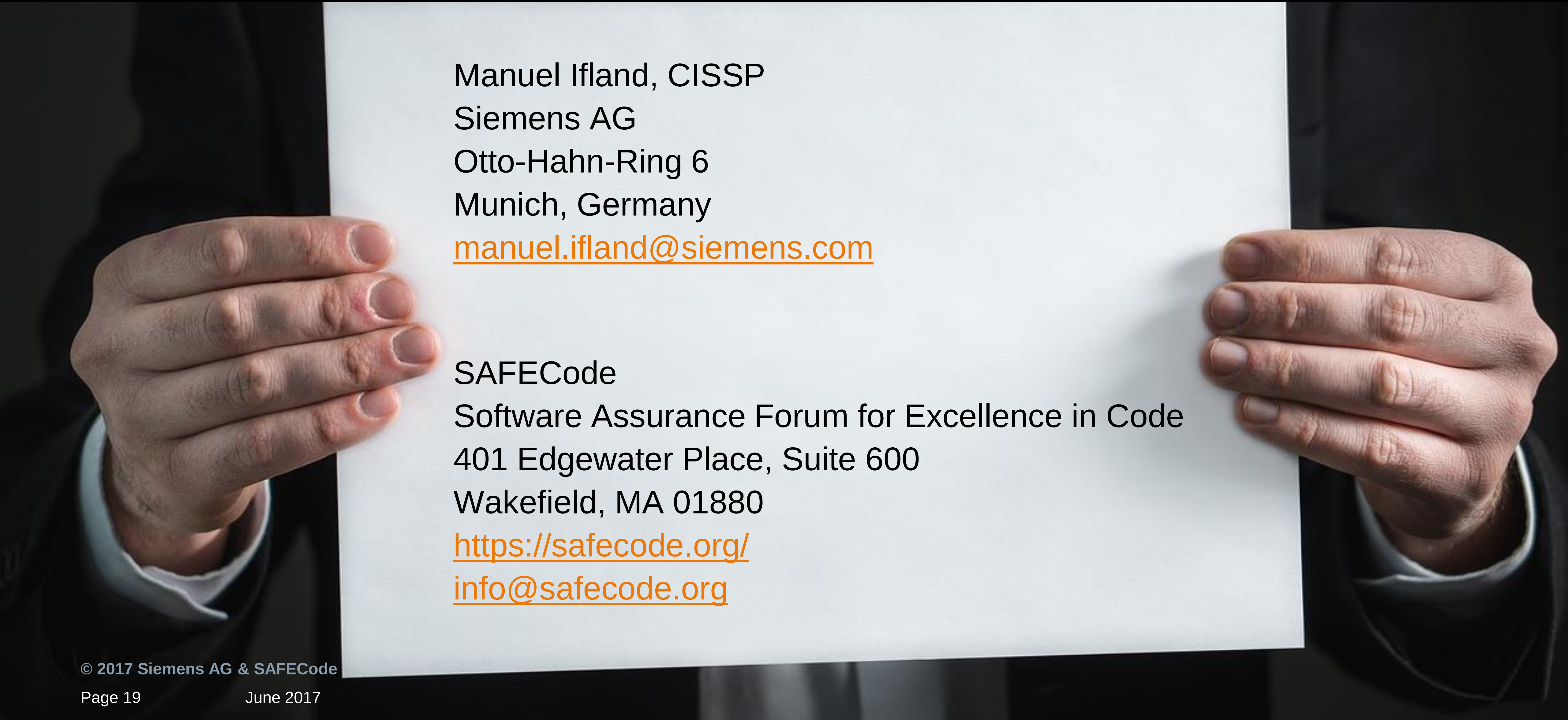
Want to Know More?

Interested in Managing Security for Third Party Components?
Read SAFECode's new white paper!
SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

http://safecode.org/

http://bit.ly/2qNSdej

Contact



Manuel Ifland, CISSP
Siemens AG
Otto-Hahn-Ring 6
Munich, Germany
manuel.ifland@siemens.com

SAFECode
Software Assurance Forum for Excellence in Code
401 Edgewater Place, Suite 600
Wakefield, MA 01880
https://safecode.org/
info@safecode.org