# SAFECode

## What's New This Month: June 2021



**Watch the SAFECode Members
Only Brown Bag Webinar:**

### Managing the challenges with Threat Modeling

Threat Modeling is a practice to understand security risk and identify the most proper mitigations. Lately, it is enjoying a significant increase in interest and adoption. But not all Threat Modeling practices are equally effective in providing the expected results. Therefore, it is of utmost importance to understand what works well and what does not.

[ Watch The Webinar Here ]

---

## Welcome New Member Siemens Energy

Siemens Energy is one of the world's leading energy technology companies. The company works with its customers and partners on energy systems for the future, thus supporting the transition to a more sustainable world. With its portfolio of products, solutions and services, Siemens Energy covers almost the entire energy value chain – from power generation and transmission to storage.

The portfolio includes conventional and renewable energy technology, such as gas and steam turbines, hybrid power plants operated with hydrogen, and power generators and transformers. More than 50 percent of the portfolio has already been decarbonized.

A majority stake in the listed company Siemens Gamesa Renewable Energy (SGRE) makes Siemens Energy a global market leader for renewable energies. An estimated one-sixth of the electricity generated worldwide is based on technologies from Siemens Energy. Siemens Energy employs more than 90,000 people worldwide in more than 90 countries and generated revenue of around €27.5 billion in fiscal year 2020. www.siemens-energy.com

---

## Help Us Change the Wold:

**DevSecOps:**

Please join the CSA Application Containers & Microservices and DevSecOps Working Group Annual Kickoff SAFECode members are invited to join the ACM and DevSecOps working groups coordinated by CSA. Join the call on 29 June to learn how you can participate in these important sessions.

[ Register Here ]

### Code Integrity: Best practices for protecting source code and build system

Recent attacks against SolarWinds or ASUS show that a secure development lifecycle along is not sufficient to prevent code from being exploited. Technology vendors also need to employ best practices to ensure that malicious code is not being inserted in the code they create for their customers. The goal of the working group is to discuss best practices to ensure code integrity during the code development or delivery process.

Currently seeking co-chairs to lead this effort.

[ Share your interest ]

**The Benefits of Being a SAFECode Volunteer**

- Participate in shaping the content of SAFECode publications
- Give back to the community by sharing your knowledge
- Improve the quality of blogs, papers, trainings, and more
- Change the World!

**What do I do next?** Let us know you'd like to get involved by **signing up here.** You can also forward this request to colleagues in your company that are experts in any of these areas.

---

## Projects in Flight

  

**DevSecOps**
SAFECode's partnership with CSA to create a comprehensive software development and secure management lifecycle that leverages principles and best practices of DevSecOps and Security Champions.

**Open Source Security Foundation**
SAFECode is a member of the OSSF under the Linux Foundation.

**OSSF Working Group**
This group will help to shape how SAFECode will continue to contribute to the OSSF's work.

 

**Code Integrity**
Recent attacks against SolarWinds or ASUS show that a secure development lifecycle alone is not sufficient to prevent code from being exploited.

**Post Quantum Crypto**
This working group is focused on the implications of post-quantum algorithms for developers and offers guidance on preparing for a smooth transition.

[ I want to participate ]

---

### In Case You Missed It: CIS Controls V8 and Companion Paper

This year, SAFECode worked closely with CIS to develop the Application Software Security control for Version 8 of the CIS Controls and a companion SAFECode paper. A recent addition to the CIS Controls, software security's inclusion reflects its evolution from a once highly specialized discipline largely limited to software engineers to a core focus for organizations that have come to recognize the need to manage the security risk of both in-house developed and acquired software. This evolution means many organizations must now have an understanding of software security practices as both buyers and creators of software.

Be sure to read what Steve Lipner has to say about the Center for Internet Security and how the partnership with SAFECode helped further what is now v6.

[ Read The Blog Here ]

[ Read The Paper Here ]

---