



The AppSec Journey @ Equinor

How we protect our software

Ipsita Mishra and Lars Kåre Skjørestad
23.05.2023

This event will not be recorded

Agenda

1. Why did we start an AppSec team?
2. Current AppSec Themes (focus areas)
 - Threat Modelling
 - Software Composition Analysis++
 - Security Champion Network
 - Other Activities
3. Reach Out To Us
4. Q&A (post in chat or save to the end)

Why did we start an AppSec Team?

- Software and code is a key asset for Equinor to reach it's goals
- We are moving into the cloud at an unprecedented speed
- We are increasing our code base, more software are created, more coders and more no-coders
- Everything becomes code, code moves to the plant floor
- We come from a culture where «someone else is protecting us» to «security is shifting left» – much more responsibility is moved down to our teams
- This scenario of opportunities has a large set of cybersecurity risks attached to it.
- The purpose of the AppSec team is to reduce cybersecurity risk in Equinor's SDLC - Software Development Life Cycle (DevOps teams).

Who is AppSec @ Equinor

- A dedicated team established February 1st, 2022
- We are organized as part of Equinor Information Security efforts
- Our team are localized in Bergen, Stavanger and Trondheim
- We serve the Equinor Software Development Community – We are an “enabler team”
- We make as much as possible of our work (guidelines, workshop material ++) open to the world!

(And there you have a small culture clash with traditional security)



Andrea Brambilla
Leading Advi IT SE Cyber Sec



Ipsita Mishra
Sr Analyst IT



Benjamin Løking
Sr Engineer IT Info Sec



Kristian Reed
Sr Analyst IT Info Sec



Lars Kåre Skjørestad
Sr. Advisor IT Info Sec



Stein-Arne Sivertsen
Prin Analyst IT SE Cyber Sec



Marius Myrestrand
Manager IT Info Sec

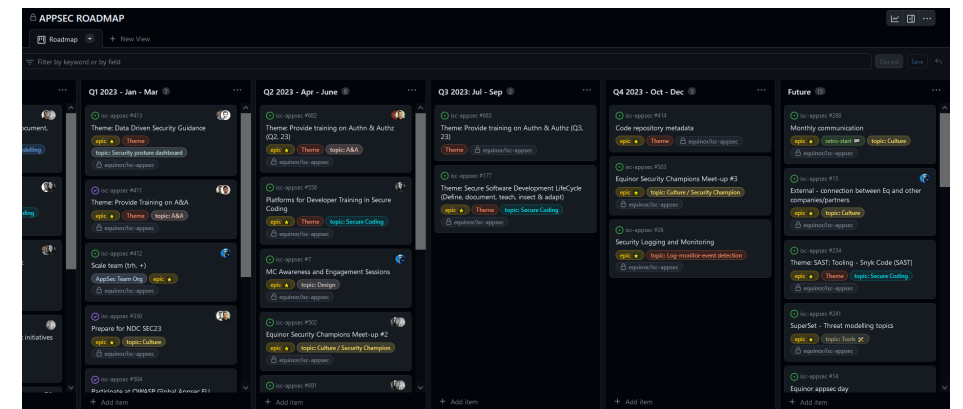
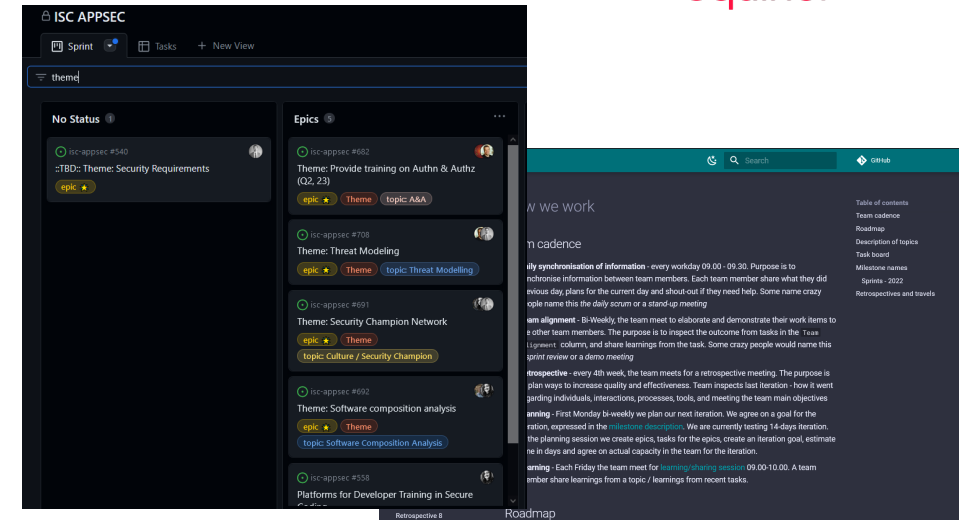
Our mission: Reduce cyber security risk in Equinor's SDLC – Software Development Life Cycle

How do we work ?

- Our cadence
 - Road map sessions each quarter
 - 2-4 week iterations – with iteration goals and planning meeting
 - 3 weekly timeboxed sync meetings (30m)
 - 1 weekly alignment meeting (30m)
 - Monthly retrospectives
 - 1 bi-weekly internal demo/sharing session
- Work categories
 - Epics (a few iterations)
 - Themes (year(s))
 - Explore tasks
- How we spend our time:
 - 50% on themes, 30% on explore tasks, 20% learning and educating our selves.

Fast feedbackloops rocks

Sufficient slack makes a huge difference!>



Some current key themes and initiatives in AppSec @ Equinor

isc-appsec #691

Theme: Security Champion Network

epic ★ Theme

topic: Culture / Security Champion

equinor/isc-appsec

isc-appsec #413

Theme: Data Driven Security Guidance

epic ★ Theme

topic: Security posture dashboard

equinor/isc-appsec

isc-appsec #708

Theme: Threat Modeling

epic ★ Theme topic: Threat Modelling

equinor/isc-appsec

isc-appsec #692

Theme: Software composition analysis

epic ★ Theme

topic: Software Composition Analysis

equinor/isc-appsec

isc-appsec #411

Theme: Provide Training on A&A

epic ★ Theme topic: A&A

equinor/isc-appsec

https://appsec.equinor.com


Equinor AppSec

Home Resources Security ch


Example explore tasks:

- Secret Scanning
- Building Secure Docker images
- OWASP ZAP Headless Security Scanning
- Security Keys
- OWASP ASVS
- Participate and speak at events
(NDC Security, OWASP Dublin, BlackHat & Defcon, ...)

appsec ▾ Everything Security in Application D...



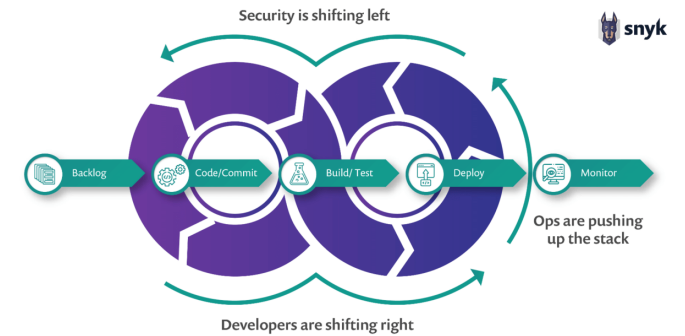
Theme: Threat Modeling

- “**We understand and manage risk**” – A key Equinor Mindset
- Threat modeling* is a required, continuous effort, in all Equinor IT activities
- “Threat modeling is analyzing representations of a system to highlight concerns about **security** and **privacy** characteristics”
- Our developer community have limited experience with **continuous** threat modeling
- We aim help teams build and operate more secure systems by incorporating threat modelling into their daily work
- The AppSec Team provide
 - Guidelines, Training (A full day workshop), A Community
 - Capability to assist teams in their threat modeling effort
- We threat model both the way we work (the SDLC) and the products/systems we develop and operate
- We have been teaching threat modeling to 170+ participants this far
- Current statistics and empiric data show that most teams find hard to include threat modeling in their daily work!

* “Cyber security risk related to the deliveries ... shall be identified and managed ..”

Theme: Software Composition Analysis++

- Part of a complex ecosystem with **150+ technologies** in our SCM system, dealing with an **evolving threat landscape** while delicately **balancing functionality and security** in different types of applications.
- Hundreds of autonomous teams developing thousands of applications.
- With our focus on open source, we **create, contribute and consume a lot of open source software**.
- It is important to secure what we write and what we add to our apps along with protecting the supply chain.
- Undertake a **data driven approach** to application security and try to shift-left in the SDLC using scalable measures which complement dev workflows.
- We use  for scanning and monitoring. We make teams aware on the signals and also help act on them.



Snyk Code (SAST)

Secure your code as it's written



Snyk Open Source (SCA)

Avoid vulnerable dependencies



Snyk Container

Keep your base images secure



Snyk Infrastructure as Code

Develop secure cloud infrastructure

Theme: Security Champions Network


- A network of team's "**security ambassadors**" started in 2022
- A security champion does not have to be a security expert
- Be curious and interested in security
- Current network consist of **110+ teams** and **180+ members**
- Driven by a **core group** from the community



AppSec provide:

- Network facilitation and energy
- Merch's
- Weekly morning coffee community sessions
- Monthly virtual seminars – **open for all**
- 2 yearly physical meetups

7th June 2023

When	What
08.00 - 08:30	Morning Coffee
08.30 - 08:45	Safety Moment
08.45 - 09:00	Introduction and Agenda
09:00 - 11:00	CTF time!

Other Activities



Authn/z workshop



Secure Coding Platforms



Security processes



#Appsec
Community



OWASP TOP 10 Workshop



Juiceshop CTF



Data Dashboard

Reach Out To Us

We welcome you to reach out to us to discuss further on the topic, learn from us or share your experiences!

- We can be reached over traditional email: appsec@equinor.com
- We are sometimes represented in the Security Champions Norway community and slack channel organized by NAV.
More info: <https://securitychampions.no/>
- Our website: <https://appsec.equinor.com>



Questions and Answers