FULLCYRCLE SECURITY

HUMAN BUFFER OVERFLOW

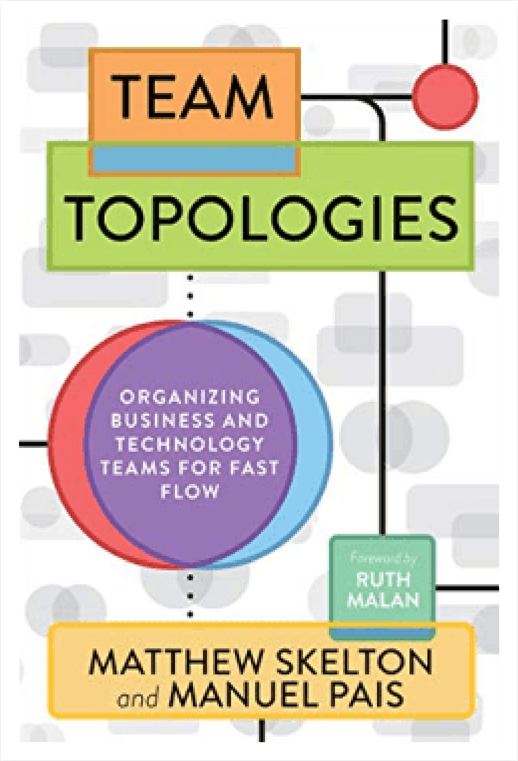
How to Deal with Cognitive Load in High-Performing Teams
Juliane Reimann

1958 AD

What we will cover today:

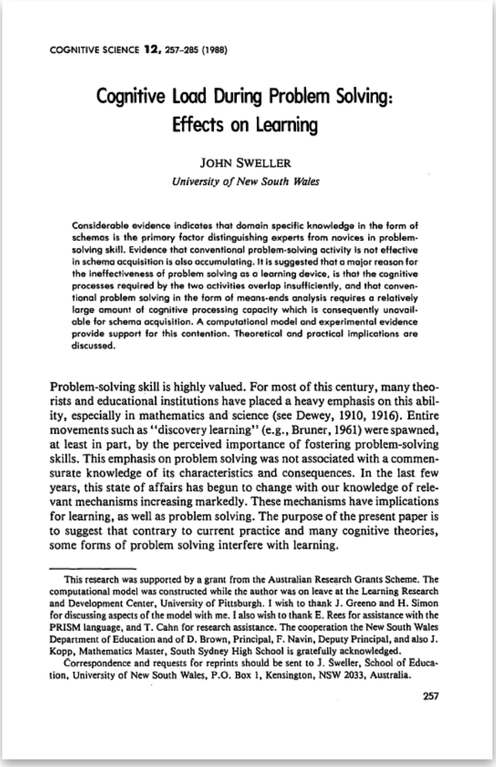
1. Cognitive Load Theory
2. How Security adds Cognitive Load
3. Real-life Examples for Addressing Cognitive Load

Cognitive Load Theory


TEAM
TOPOLOGIES
ORGANIZING BUSINESS AND TECHNOLOGY TEAMS FOR FAST FLOW
Foreword by
RUTH MALAN
MATTHEW SKELTON and MANUEL PAIS

Matthew Skelton, Manuel Pais (2019)

Team Topologies: Organizing Business and Technology for Fast Flow of Value



COGNITIVE SCIENCE **12,** 257–285 (1988)

Cognitive Load During Problem Solving: Effects on Learning

JOHN SWELLER
University of New South Wales

Considerable evidence indicates that domain specific knowledge in the form of schemas is the primary factor distinguishing experts from novices in problem-solving skill. Evidence that conventional problem-solving activity is not effective in schema acquisition is also accumulating. It is suggested that a major reason for the ineffectiveness of problem solving as a learning device, is that the cognitive processes required by the two activities overlap insufficiently, and that conventional problem solving in the form of means-ends analysis requires a relatively large amount of cognitive processing capacity which is consequently unavailable for schema acquisition. A computational model and experimental evidence provide support for this contention. Theoretical and practical implications are discussed.

Problem-solving skill is highly valued. For most of this century, many theorists and educational institutions have placed a heavy emphasis on this ability, especially in mathematics and science (see Dewey, 1910, 1916). Entire movements such as ''discovery learning'' (e.g., Bruner, 1961) were spawned, at least in part, by the perceived importance of fostering problem-solving skills. This emphasis on problem solving was not associated with a commensurate knowledge of its characteristics and consequences. In the last few years, this state of affairs has begun to change with our knowledge of relevant mechanisms increasing markedly. These mechanisms have implications for learning, as well as problem solving. The purpose of the present paper is to suggest that contrary to current practice and many cognitive theories, some forms of problem solving interfere with learning.

This research was supported by a grant from the Australian Research Grants Scheme. The computational model was constructed while the author was on leave at the Learning Research and Development Center, University of Pittsburgh. I wish to thank J. Greeno and H. Simon for discussing aspects of the model with me. I also wish to thank E. Rees for assistance with the PRISM language, and T. Cahn for research assistance. The cooperation the New South Wales Department of Education and of D. Brown, Principal, F. Navin, Deputy Principal, and also J. Kopp, Mathematics Master, South Sydney High School is gratefully acknowledged.

Correspondence and requests for reprints should be sent to J. Sweller, School of Education, University of New South Wales, P.O. Box 1, Kensington, NSW 2033, Australia.

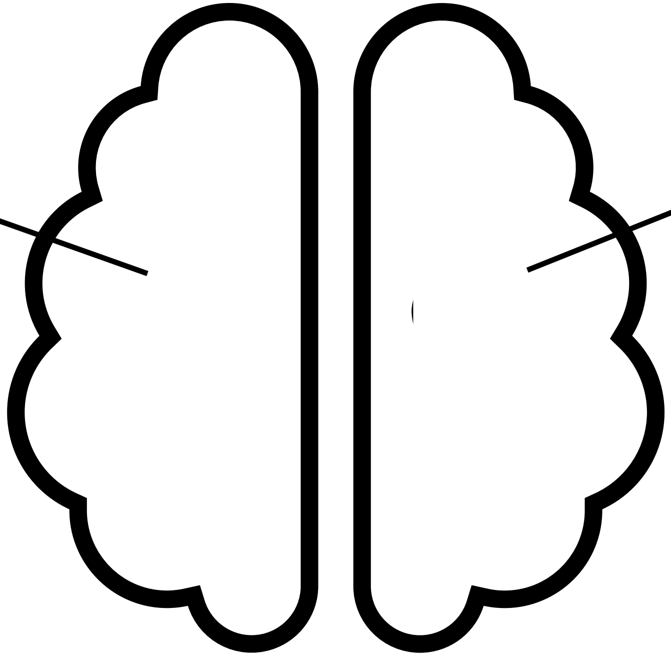
257

John Sweller (1988)

Cognitive Load During Problem Solving: Effects on Learning

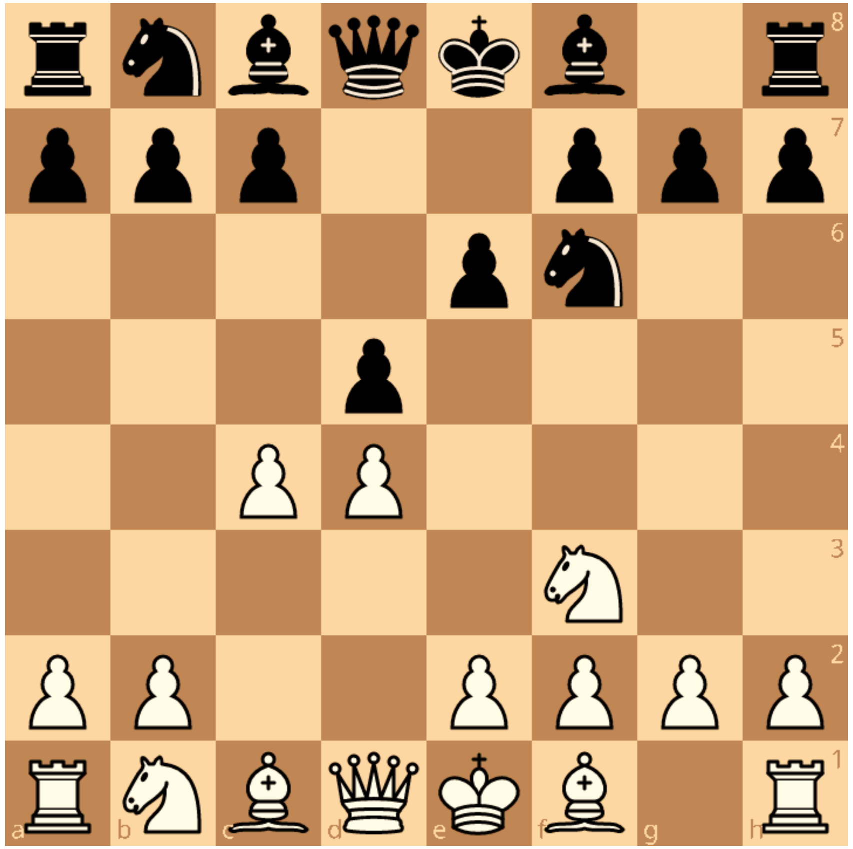
Long-Term Memory

- Store Knowledge
- Seemingly unlimited



Working Memory

- Process Information
- Up to 7 items at a time
- Call schemas as items



What is the next best move?

Schema: **categorization of elements of information**

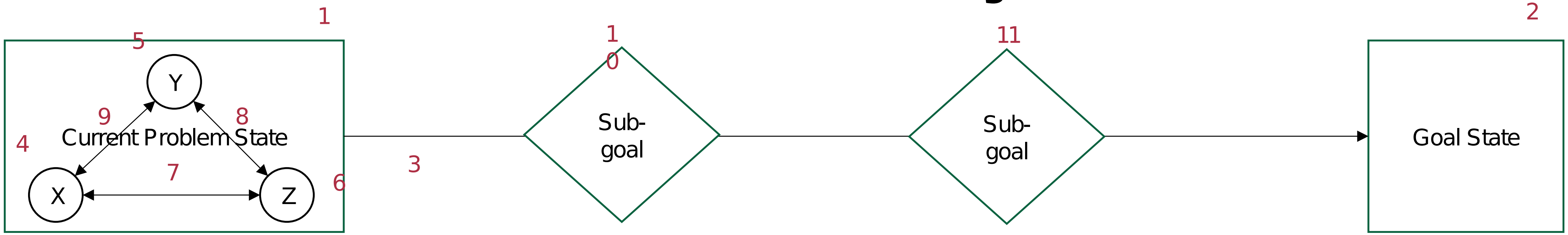
→ How we learn
→ Stored in long-term memory
→ accessed when needed
→ Reduce cognitive load

Problem Solving Strategies

Schema-driven problem solving

Access existing knowledge to recognize patterns

Means-End-Analysis



Types of Cognitive Load

	Intrinsic	Extraneous	Germane
Definition	• Mental effort related to the **inherent complexity** of a task • Depends on **number of interacting elements**	• Mental effort related to how information or tasks are **presented or handled** • **Controllable,** can be reduced	• connecting new information to what you already know, **forming new schemas** • "**good**" kind of load
Chess	Learning how the pieces move, understanding check / check mate	Learning from a poorly written book	Analyzing a specific board situation, thinking through possible moves, and recognizing a tactic you learned earlier
Software Development	Learning the Syntax of PHP or Java	Manual deployments / configuration	Figuring out how different components interact within a system

The Role of Security

Cyber Security Knowledge	Development Workflow	Security Testing	Processes	Communication Barriers	Psychological Aspects
Understanding common vulnerabilities and risks	Late-stage security feedback (e.g., after implementation)	Understanding the purpose of different scanning tools	Unclear processes for handling findings	Knowing who to talk to for security questions	Fear of doing something wrong related to security
Understanding security terms (e.g., threat modeling, SAST)	Building up knowledge prior to resolving a security task	Understanding which tools are needed for your applications	Lack of guidance on prioritization	Receiving timely, helpful responses from the security team	Hesitation to ask security questions
Understanding security requirements	Switching between tools to complete security-related work	Interpreting scanner results (e.g., SAST, DAST)	Overlapping assessments from different security units (AppSec, SOX, CPP)	Receiving tickets or tasks with enough context	Feeling overwhelmed by security input
Knowing where to find reliable security guidance	Difficulty integrating security tasks into sprint/backlog planning	Configuring or tuning scans (e.g., exclusions, scope)	Missing templates or checklists for recurring security tasks	Navigating conflicting input from different security stakeholders	Feeling safe to experiment and learn about secure development
Secure implementation of features (e.g., auth, validation, encryption)		Dealing with false positives	Unfriendly assessment formats (e.g., Excel questionnaires)		
		Getting access to required security tools or platforms			

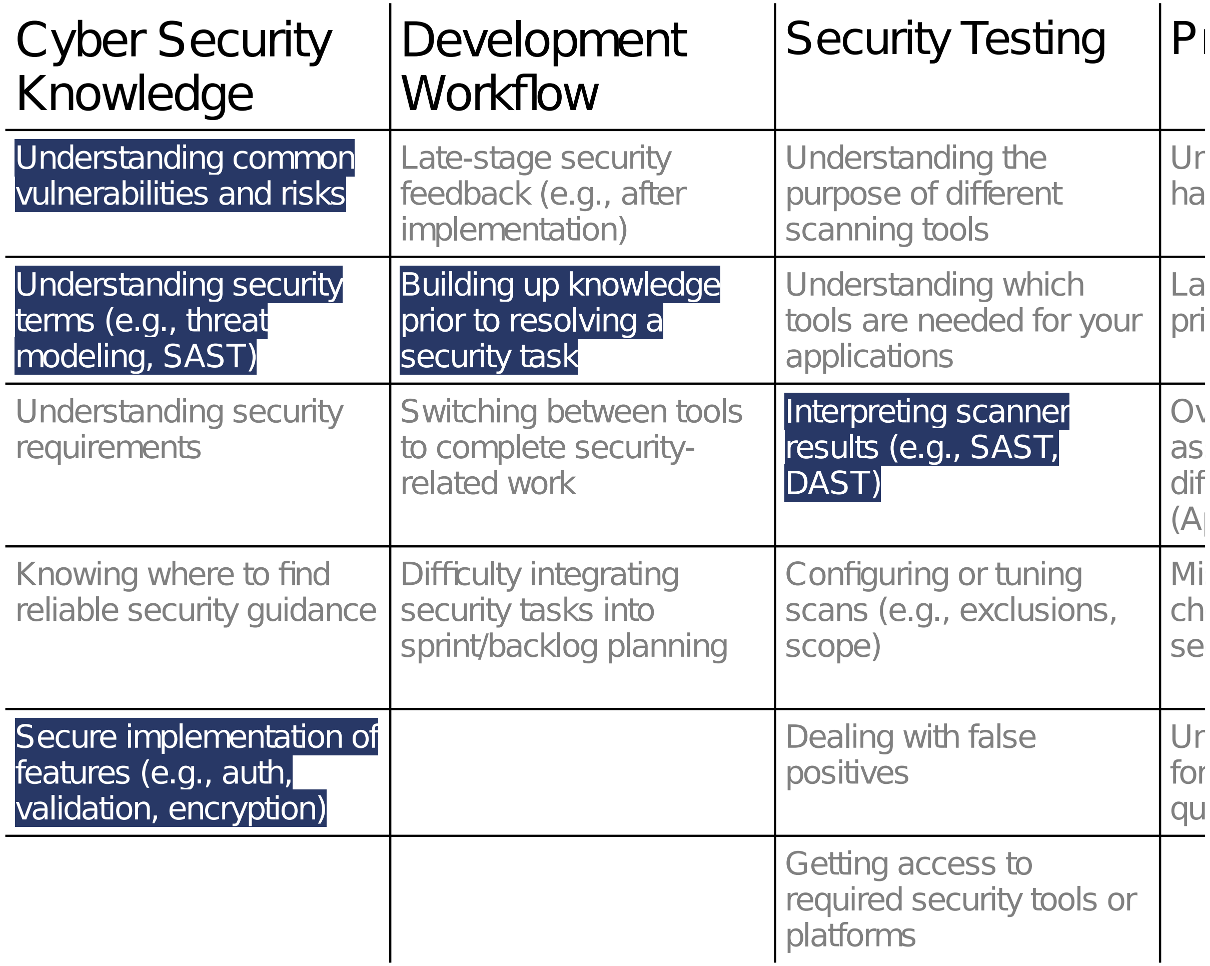
The Role of Security

🔵 INTRINSIC 🔴 EXTRANEOUS 🟡 GERMANE

Cyber Security Knowledge	Development Workflow	Security Testing	Processes	Communication Barriers	Psychological Aspects
🔵 Understanding common vulnerabilities and risks	🔴 Late-stage security feedback (e.g., after implementation)	🔴 Understanding the purpose of different scanning tools	🔴 Unclear processes for handling findings	🔴 Knowing who to talk to for security questions	🔴 Fear of doing something wrong related to security
🔵 Understanding security terms (e.g., threat modeling, SAST)	🔵 Building up knowledge prior to resolving a security task	🔴 Understanding which tools are needed for your applications	🔴 Lack of guidance on prioritization	🔴 Receiving timely, helpful responses from the security team	🔴 Hesitation to ask security questions
🔴 Understanding security requirements	🔴 Switching between tools to complete security-related work	🔵 Interpreting scanner results (e.g., SAST, DAST)	🔴 Overlapping assessments from different security units (AppSec, SOX, CPP)	🔴 Receiving tickets or tasks with enough context	🔴 Feeling overwhelmed by security input
🔴 Knowing where to find reliable security guidance	🔴 Difficulty integrating security tasks into sprint/backlog planning	🔴 Configuring or tuning scans (e.g., exclusions, scope)	🔴 Missing templates or checklists for recurring security tasks	🔴 Navigating conflicting input from different security stakeholders	🟡 Feeling safe to experiment and learn about secure development
🔵 Secure implementation of features (e.g., auth, validation, encryption)		🔴 Dealing with false positives	🔴 Unfriendly assessment formats (e.g., Excel questionnaires)		
		🔴 Getting access to required security tools or platforms			

The Role of Security

● INTRINSIC ● EXTRANEOUS ● GERMANE



Cyber Security Knowledge	Development Workflow	Security Testing	P
Understanding common vulnerabilities and risks	Late-stage security feedback (e.g., after implementation)	Understanding the purpose of different scanning tools	Ur ha
Understanding security terms (e.g., threat modeling, SAST)	Building up knowledge prior to resolving a security task	Understanding which tools are needed for your applications	La pri
Understanding security requirements	Switching between tools to complete security-related work	Interpreting scanner results (e.g., SAST, DAST)	Ov as dif (A
Knowing where to find reliable security guidance	Difficulty integrating security tasks into sprint/backlog planning	Configuring or tuning scans (e.g., exclusions, scope)	Mi ch se
Secure implementation of features (e.g., auth, validation, encryption)		Dealing with false positives	Ur for qu
		Getting access to required security tools or platforms	

Mitigation Strategies

- Secure Development **Training**
- **Pair-Programming**
- Clear and inclusive **communication** from the Security Team
- Living **Knowledge Base**
- **Expert Sessions**

The Role of Security

● INTRINSIC ● EXTRANEOUS ● GERMANE

Cyber Security Knowledge	Development Workflow
Understanding common vulnerabilities and risks	Late-stage security feedback (e.g., after implementation)
Understanding security terms (e.g., threat modeling, SAST)	Building up knowledge prior to resolving a security task
Understanding security requirements	Switching between tools to complete security-related work
Knowing where to find reliable security guidance	Difficulty integrating security tasks into sprint/backlog planning
Secure implementation of features (e.g., auth, validation, encryption)	

platforms

Mitigation Strategies

- Defining a **clear point go-to person** for Security topics in the team
- **Centralized knowledge base**
- **Automation**
- Integrating security into **planning with visible backlog items**
- Improving the workflow: **IDE integrations**, **Jira-Integrations**
- Improving **communication** between different stakeholders
- **Relatable and easy to understand policies**
- Fostering the **shift-left mindset** and defining a **clear SSDLC**

The Role of Security

● INTRINSIC ● EXTRANEOUS ● GERMANE

Mitigation Strategies

- Positive **Security Culture**
- **Collaboration** between development teams and the security team
- **Knowledge Exchange** Formats
- **Secure Development Training**

required security tools or platforms

Communication Barriers	Psychological Aspects
Knowing who to talk to for security questions	Fear of doing something wrong related to security
Receiving timely, helpful responses from the security team	Hesitation to ask security questions
Receiving tickets or tasks with enough context	Feeling overwhelmed by security input
Navigating conflicting input from different security stakeholders	Feeling safe to experiment and learn about secure development

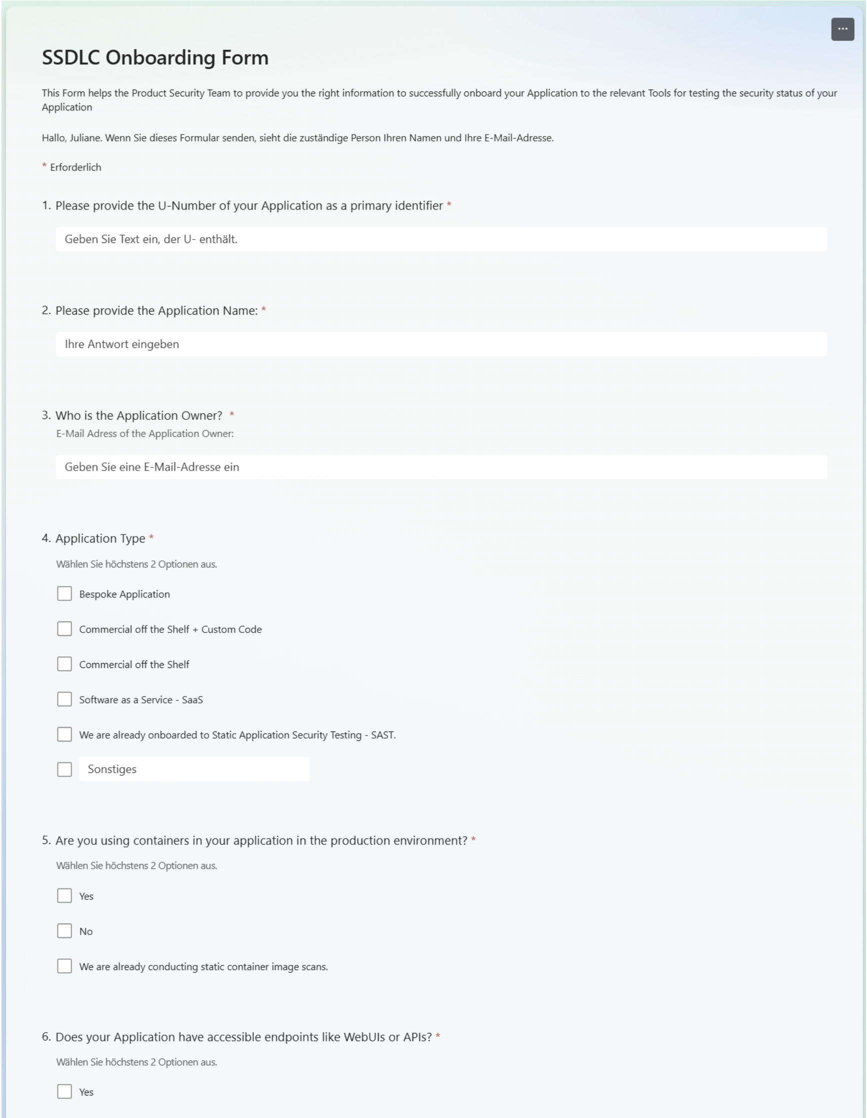
Real-life Examples

#1 Pipeline Abstraction Layer (PAL)

- **Standardized way** to integrate security scanning with **pre-configured** container images
- Centralized documentation of integration
- Centralized maintenance of the images by Security
- No tool-specific UIs or configurations for the Dev Teams
- Tools can be switched under the hood

#2 Adaptive Questionnaire for SSDLC Onboarding

- **Relevant questions** based on application type
- **Automation**
  - **Background-checks** for existing accounts
  - creation of **tool accounts** via API
  - **e-mail** with relevant setup instructions
  - **ticket creation** progress tracking
- **Enable Dev Teams** to **independently** start the process
- Only **relevant information** are passed to the Dev Teams



SSDLC Onboarding Form

This Form helps the Product Security Team to provide you the right information to successfully onboard your Application to the relevant Tools for testing the security status of your Application

Hallo, Juliane. Wenn Sie dieses Formular senden, sieht die zuständige Person Ihren Namen und Ihre E-Mail-Adresse.

* Erforderlich

1. Please provide the U-Number of your Application as a primary identifier *

   Geben Sie Text ein, der U- enthält.

2. Please provide the Application Name: *

   Ihre Antwort eingeben

3. Who is the Application Owner? *

   E-Mail Adress of the Application Owner:

   Geben Sie eine E-Mail-Adresse ein

4. Application Type *

   Wählen Sie höchstens 2 Optionen aus.

   □ Bespoke Application
   □ Commercial off the Shelf + Custom Code
   □ Commercial off the Shelf
   □ Software as a Service - SaaS
   □ We are already onboarded to Static Application Security Testing - SAST.
   □ Sonstiges

5. Are you using containers in your application in the production environment? *

   Wählen Sie höchstens 2 Optionen aus.

   □ Yes
   □ No
   □ We are already conducting static container image scans.

6. Does your Application have accessible endpoints like WebUIs or APIs? *

   Wählen Sie höchstens 2 Optionen aus.

   □ Yes

FULLCYRCLE SECURITY

#3 Building a Security Champions Program

- Regular **knowledge exchange** sessions
- **Shared communication channel** between Security Team and Dev Teams
- Publish **internal articles** on relevant security topics
- Launched a **role-based training program** on threat modeling
- Security Community as a **safe space** for learning and growth

Thank you

for your attention!

Connect with me on LinkedIn

Resources

Carpenter, Perry; Roer, Kai (2022): The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer. Wiley.

Driskell, J. E., & Salas, E. (1992). Collective behavior and team performance. Human Factors, 34(3), 277–288.

Skelton, Matthew; Pais, Manuel (2019): Team Topologies. Organizing Business and Technology Teams for fast Flow. IT Revolution, Portland, Oregon.

Sweller, John (1988) „Cognitive Load During Problem Solving: Effects on Learning.“ Cognitive Science 12. N. 2 (1988): 257-285.

Sweller, John; Merrienboer, Jeroen J. G. Van; Paas, Freed (1998): Cognitive Architecture and Instructional Design. Educational Psychology Review 10(3) (1998): 251-296.

Sweller, John; Merrienboer, Jeroen J. G. Van; Paas, Freed (2019): Cognitive Architecture and Instructional Design: 20 Years Later. Educational Psychology Review 31 (2019): 261-292.

Wager, Michael (2025): Standardisierte Security Scans für CI/CD Pipelines. (https://www.secure-io.de/standardisierte-security-scans-fuer-ci-cd-pipelines/)