FROM COMPLEXITY TO CLARITY

Understanding your Software Product Health

Jan-Niclas Strüwer

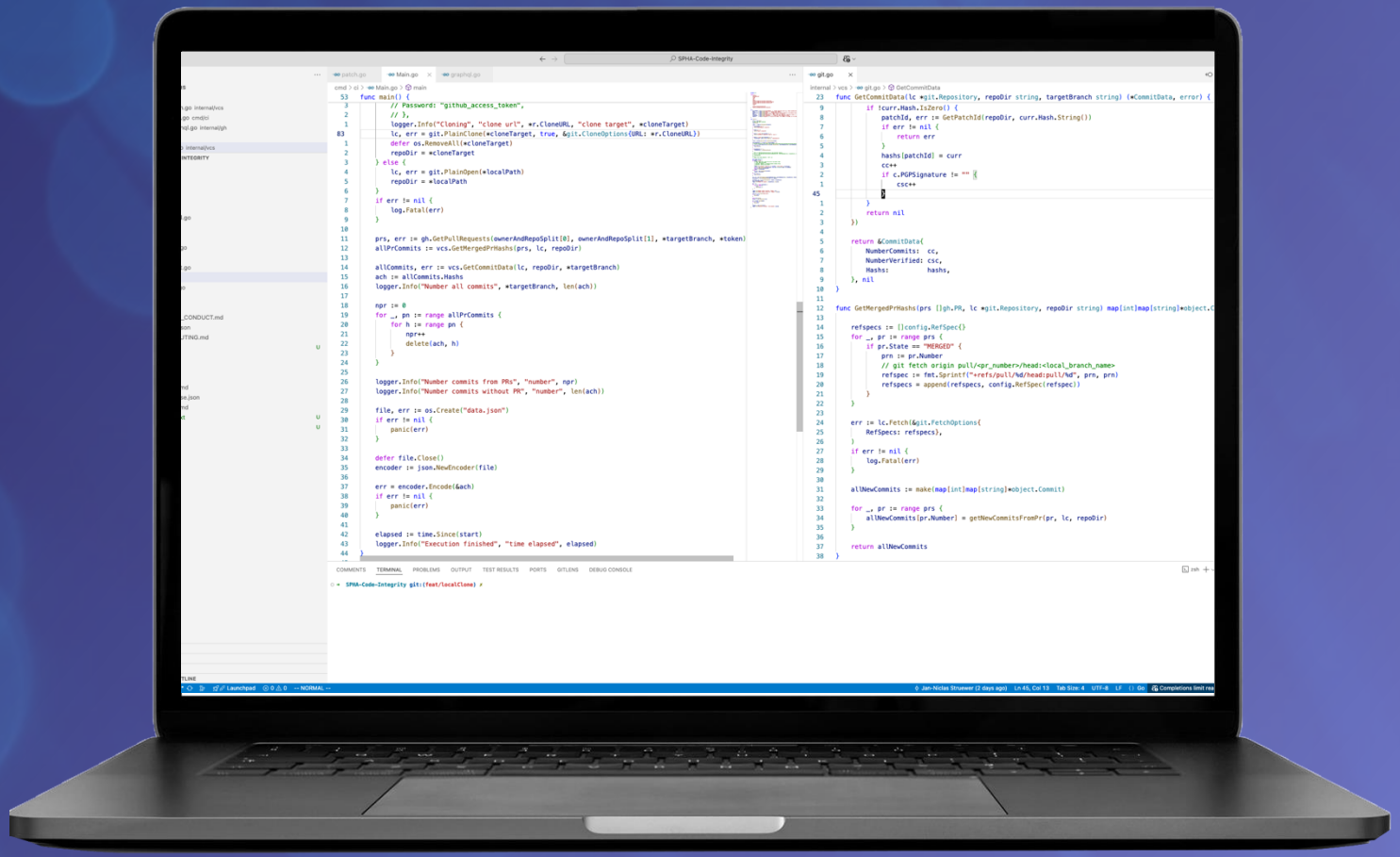
jan-niclas.struewer@iem.fraunhofer.de

struewer

Software **P**roduct **H**ealth **A**ssistant

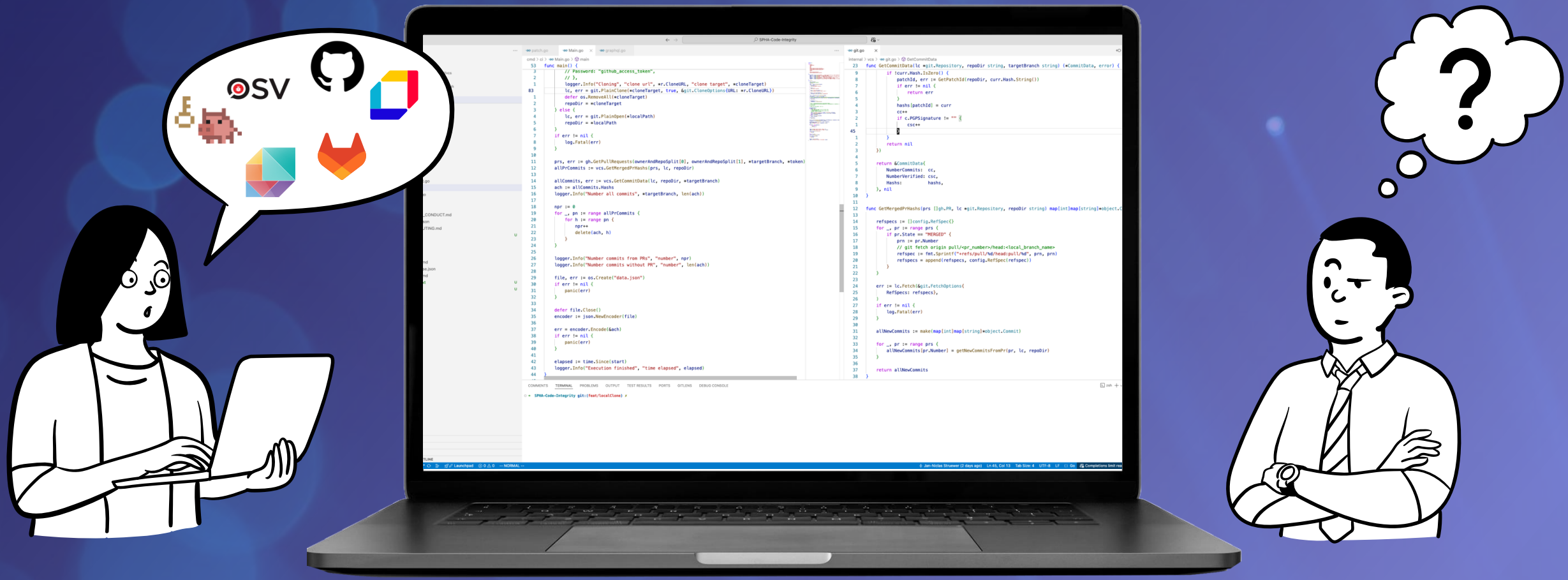
Software Development is Complex

How can you measure and communicate this complexity?



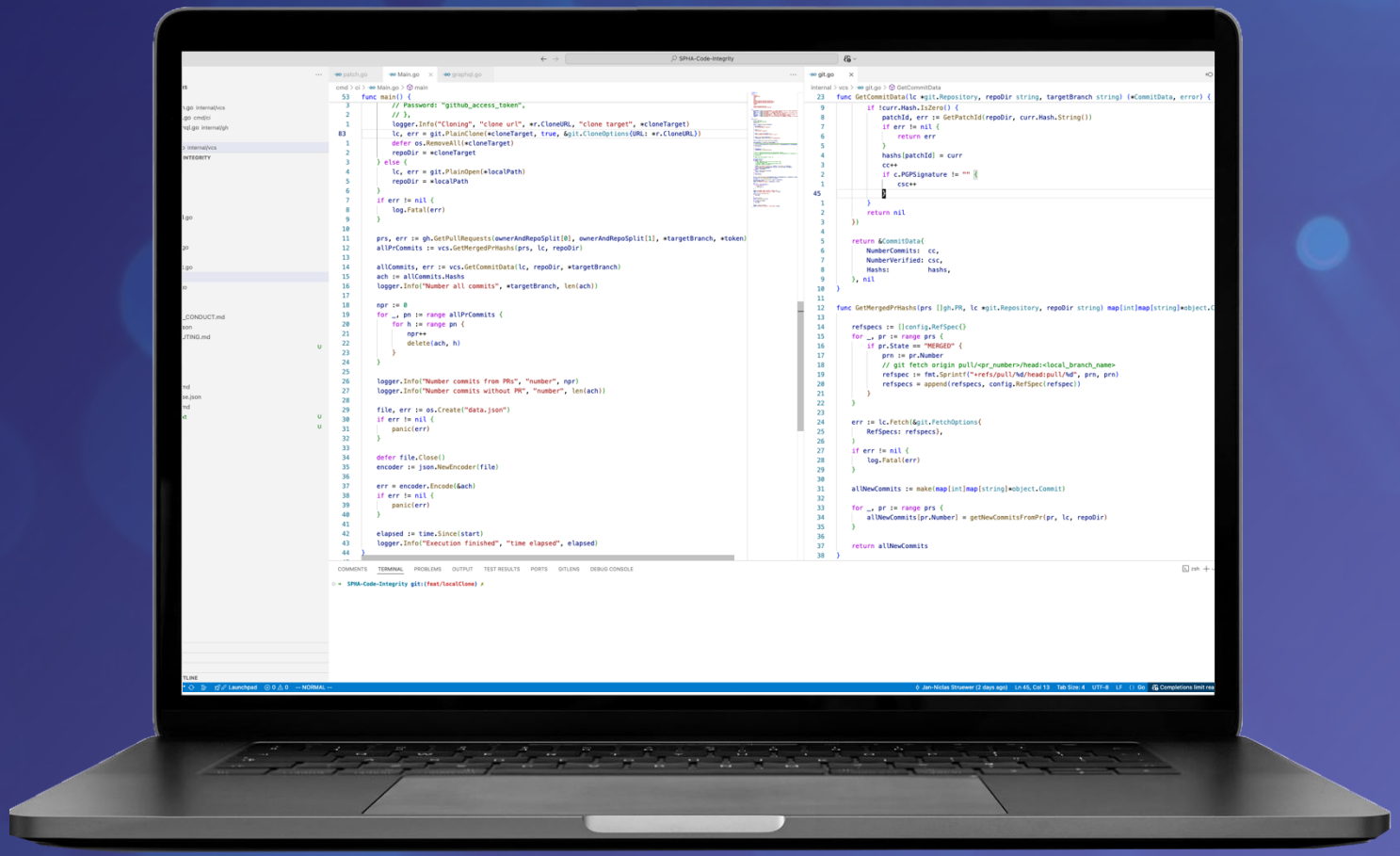
Software Development is Complex

How can you measure and communicate this complexity?



Software Development is Complex

How can you measure and communicate this complexity?



One Software Product Health ***Score*** for a clear communication

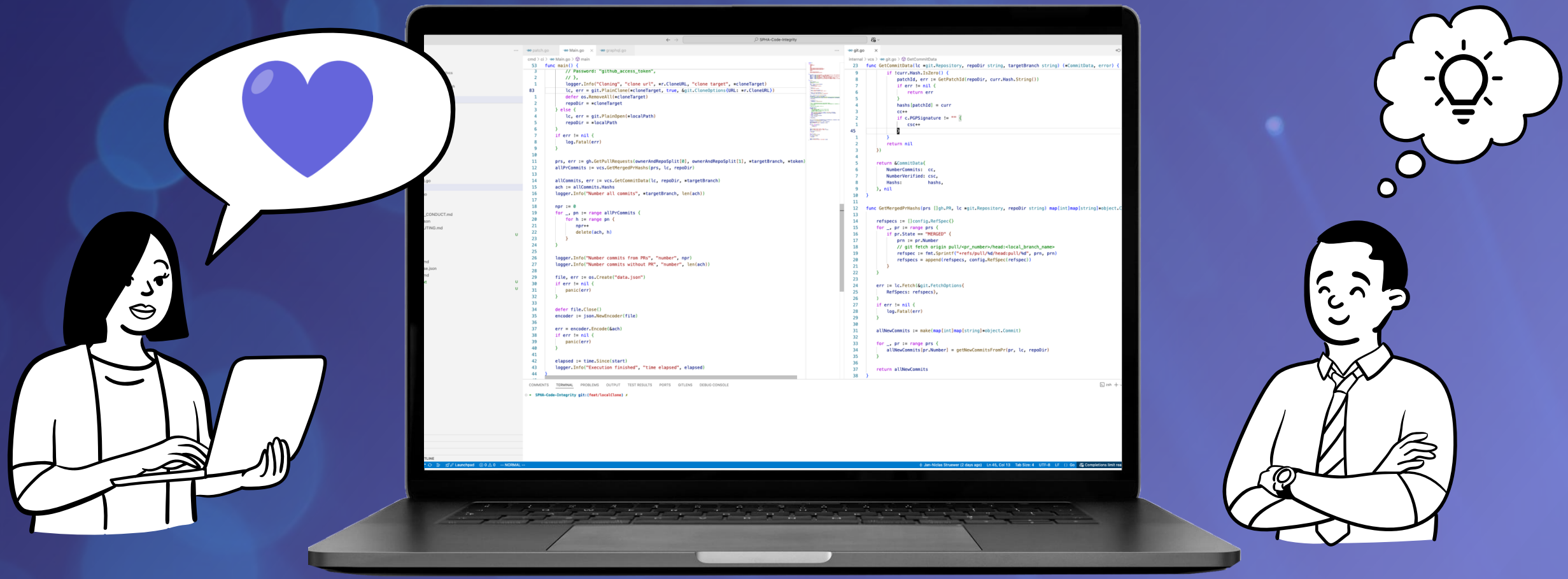
Software Product Health Assistant

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Software Development is Complex

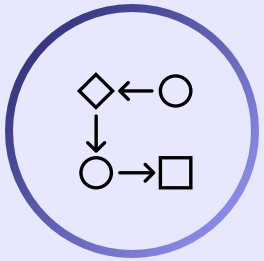
How can you measure and communicate this complexity?



Keeping track of your software product health is cumbersome

Communicating it to all relevant stakeholders is just as difficult

Companies face various challenges when assessing and communicating software product health



Often cumbersome and manual process
The current state of your software product depends on a multitude of *product specific* factors and is often assessed manually

Communication of software product health
Creating a bigger picture from the results of expert tools and communicating it to (non-technical) stakeholders is difficult

Informed management decisions lead to better prioritization of development tasks

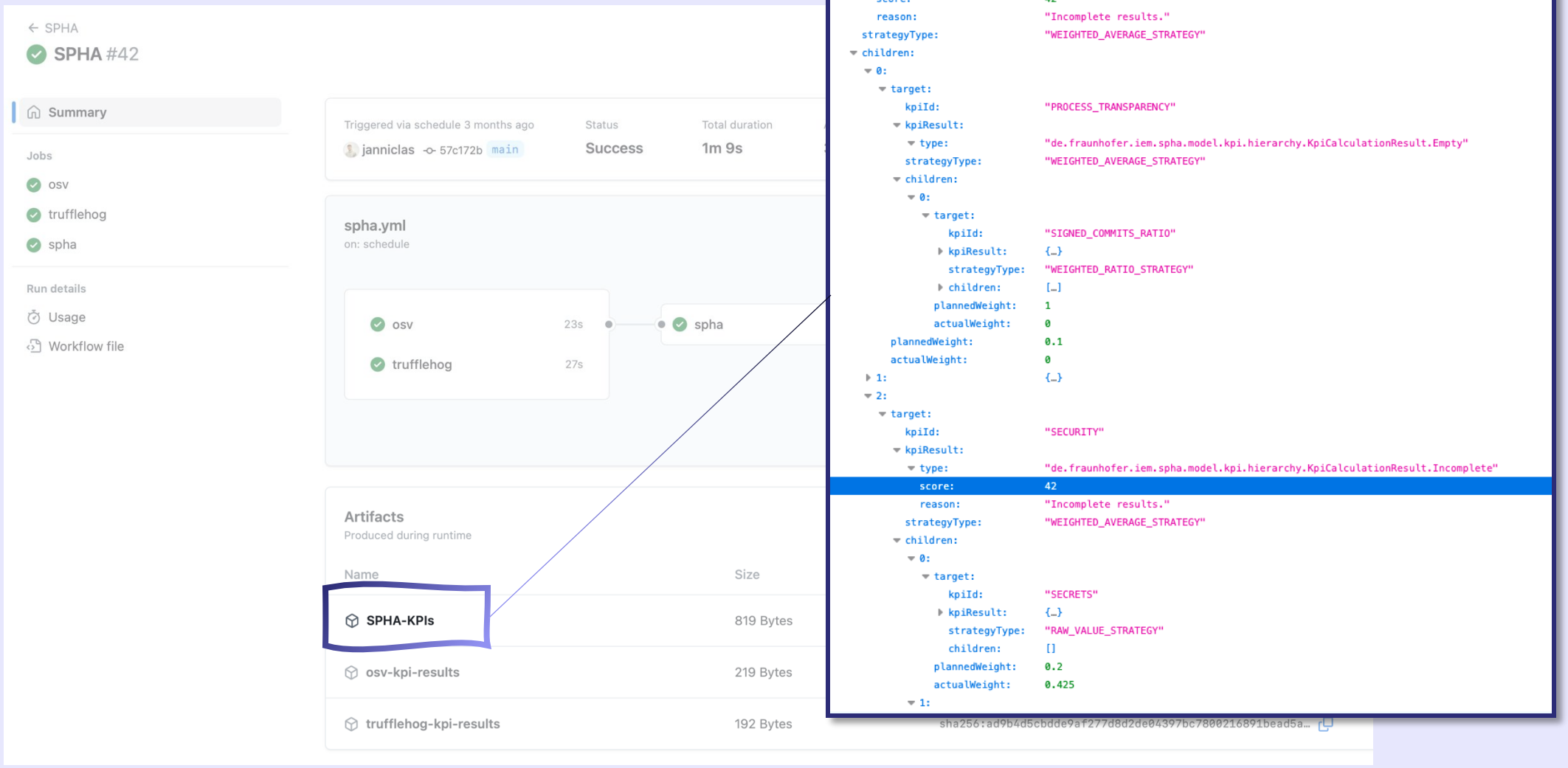
Software Product Health Assistant

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

SPHA-core Demo

github.com/fraunhofer-iem/spha-demo



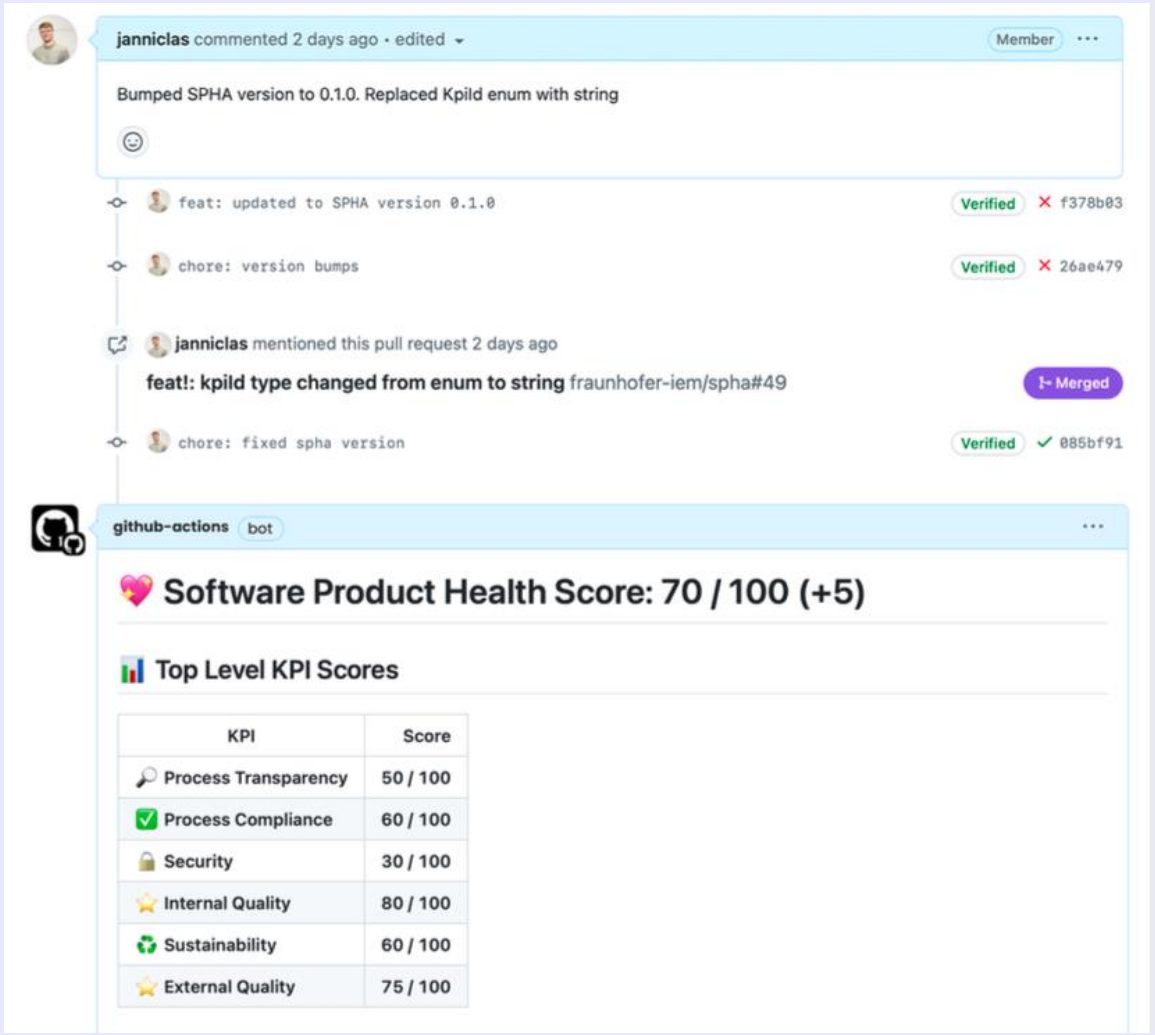
Software Product Health Assistant

HEINZ NIXDORF INSTITUT UNIVERSITÄT PADERBORN

Fraunhofer IEM

SPHA-core Demo

github.com/fraunhofer-iem/spha-demo



Software Product Health Assistant

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Assessment & Communication of Software Product Security

Utilizing data from existing & established tools

Calculate Software Product Health for the given KPI hierarchy

Transform data into SPHA's KPI format

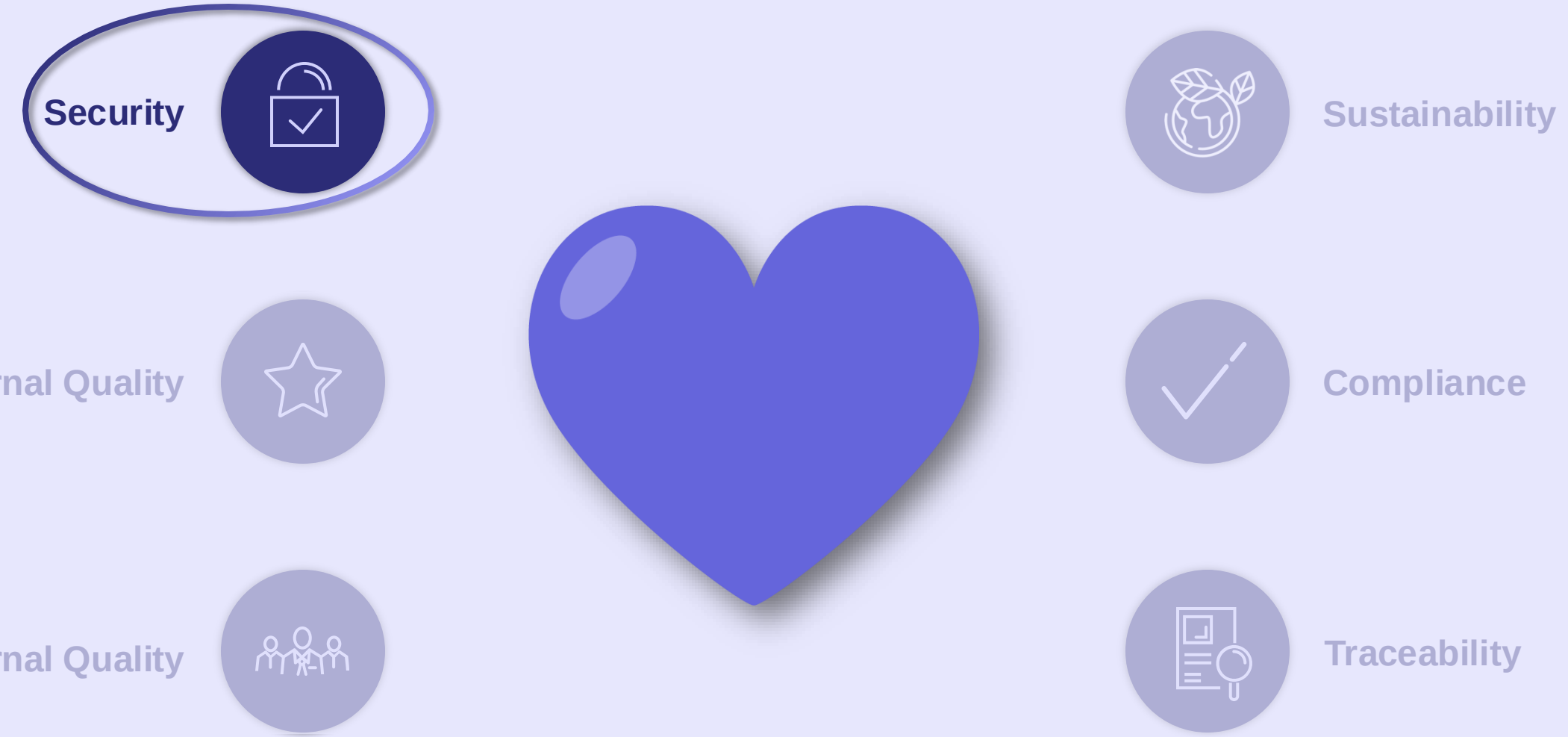
Collect data from dev process with focus on existing tools

Software Product Health Assistant

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

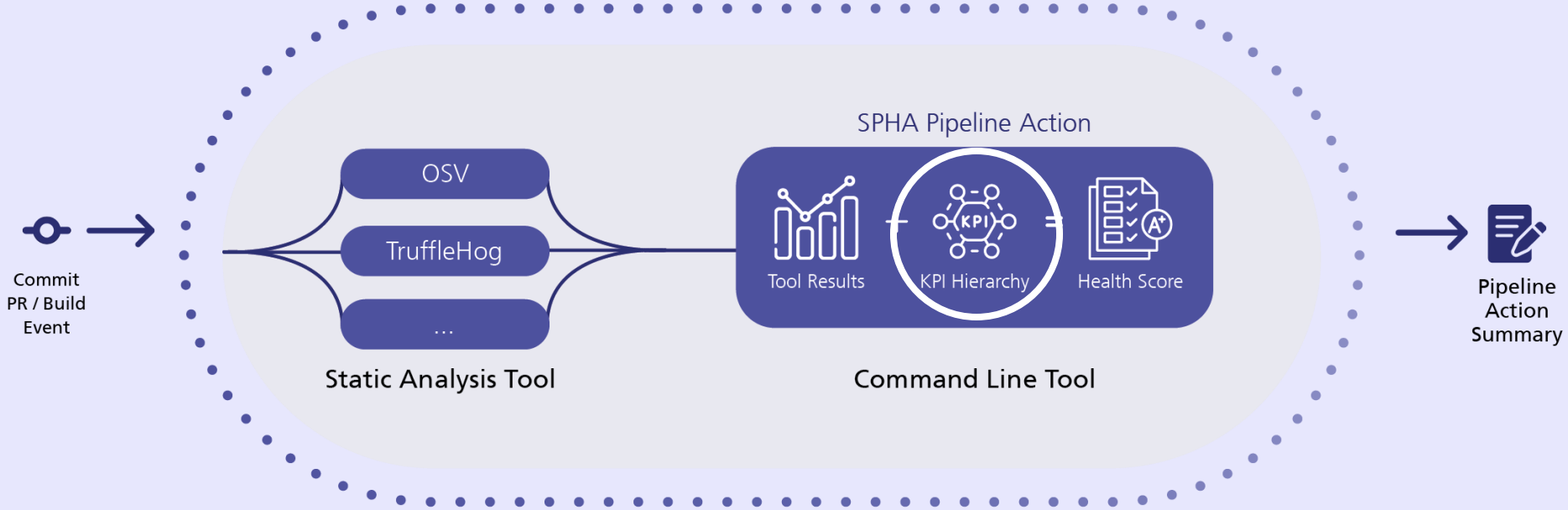
Fraunhofer IEM

Six Aspects of Software Product Health



SPHA is a Framework

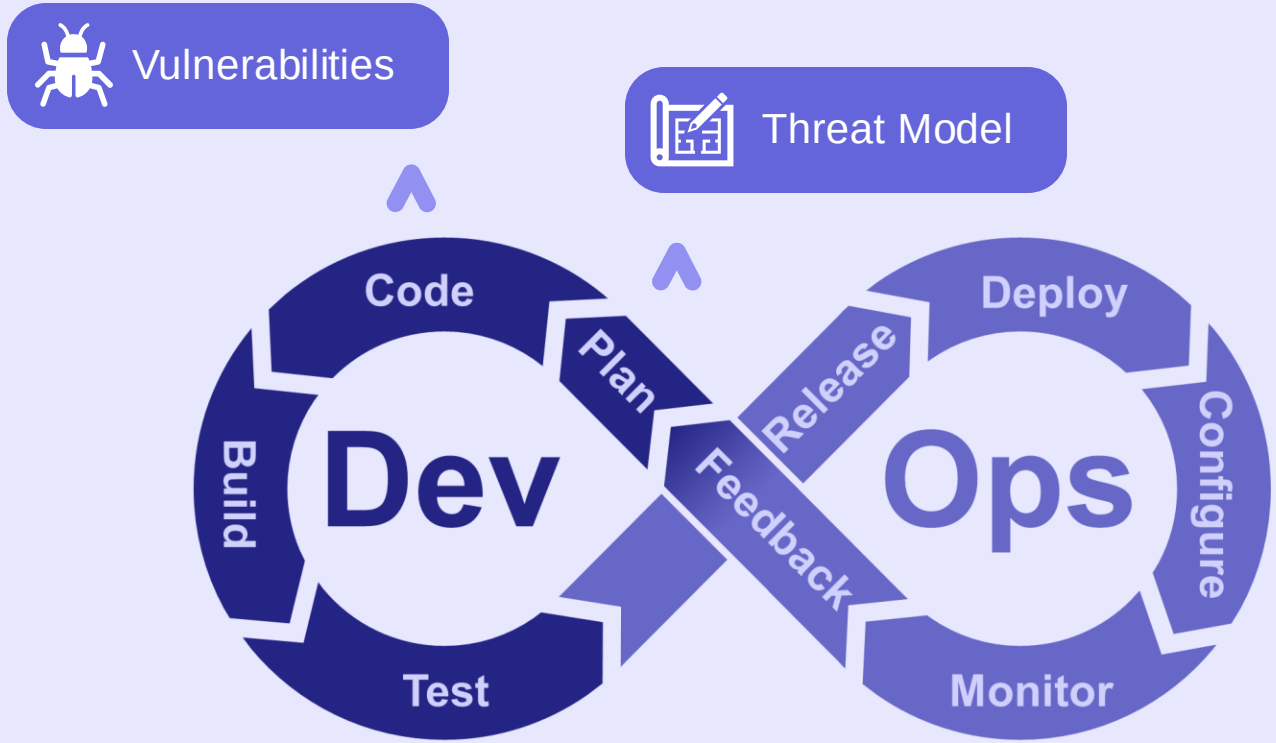
Customization is Key



SPHA is a *framework* can be used for everything and nothing it all depends on the configured *hierarchy*, *edge weights*, and the connected *data sources*

Architectural, threat informed data flow information give context for vulnerabilities

Include data from all phases of the development process



SPHA's strength is to combine data from different tools in all phases of the development process

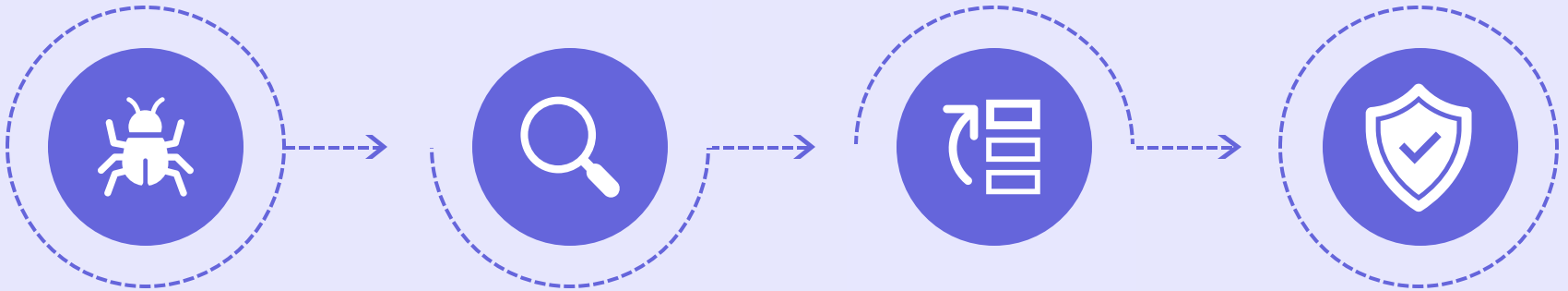
Software Product Health Assistant

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Vulnerability Management

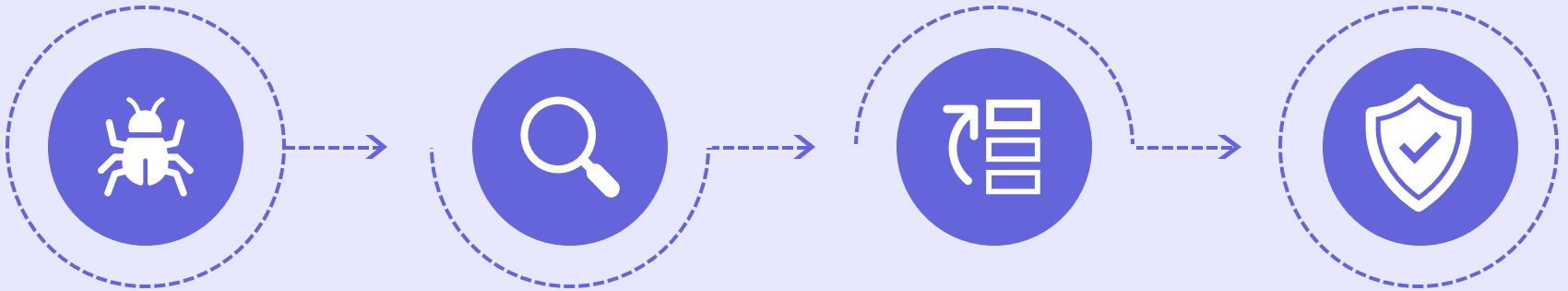
A practical example



	Detect	Assess	Prioritize	Fix
Tasks	Vulnerability scanners find vulnerabilities in code, configurations, and deployments	Assess the relevance, impact and risk associated to each vulnerability	Assign priorities and plan when to fix them	Remediate the vulnerability or accept the risk and move on

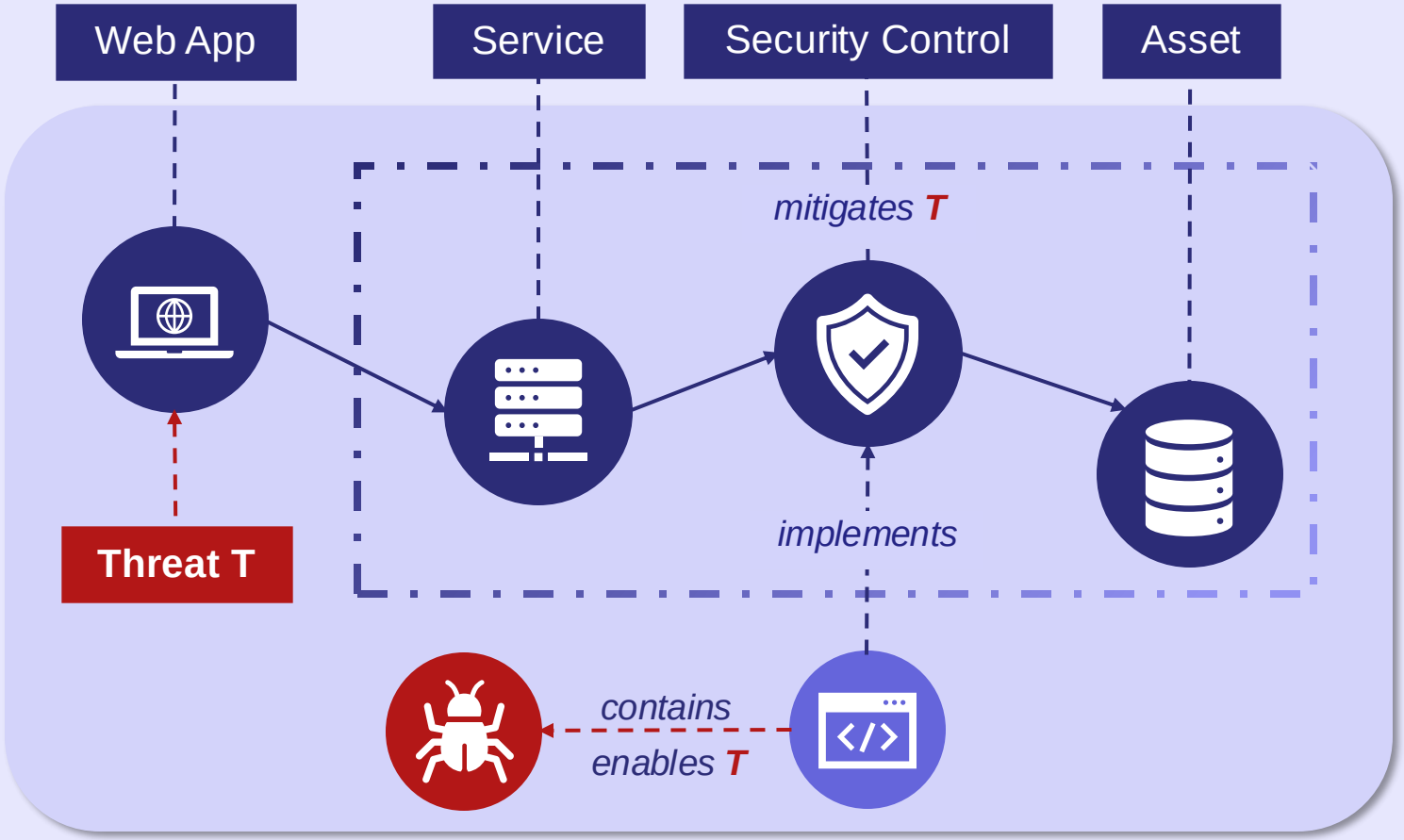
Vulnerability Management

A practical example



	Detect	Assess	Prioritize	Fix
Challenges	Number of vulnerabilities found and the lack of ***context***	Relies on additional data and expert knowledge	Requires information about the bigger picture and communication with (non-technical) stakeholders	Depends on the vulnerability and can be arbitrarily complex

Threat Modeling

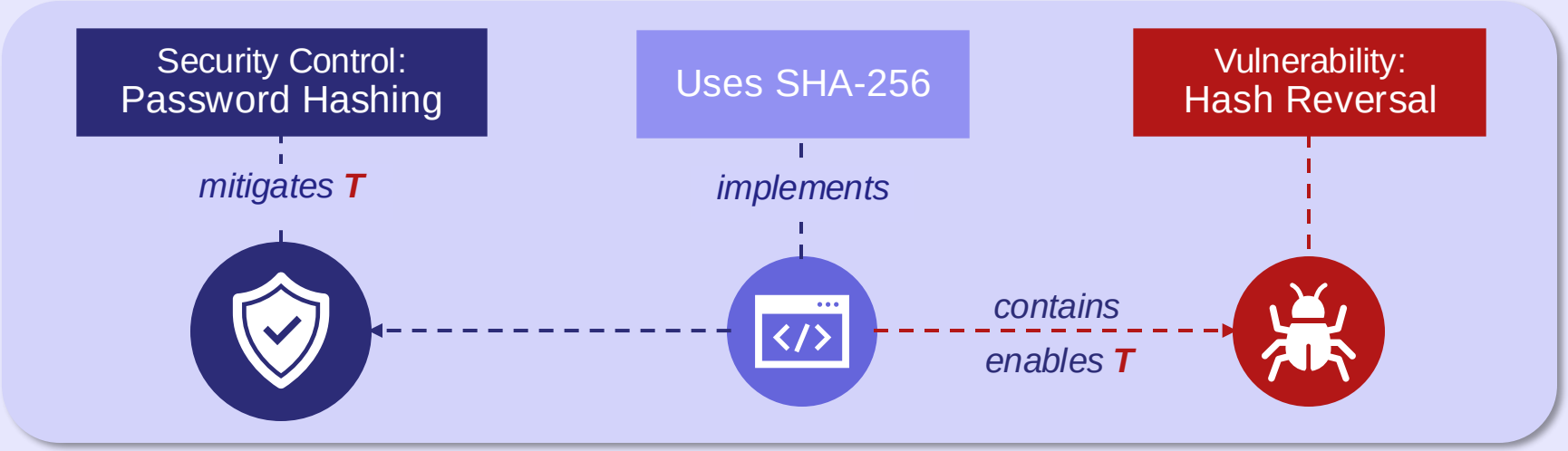


> *Any sensible threat modeling must "**assume breach**": We must finally rid ourselves of good-weather threat modeling […].*
> ***Software is vulnerable**, and so are its defenses.*
> *Hence, assuming the **security failure** of at least individual **subsystems** is the only realistic assumption.*
>
> *Bodden et al., 2024, Evaluating Security Through Isolation and Defense in Depth*

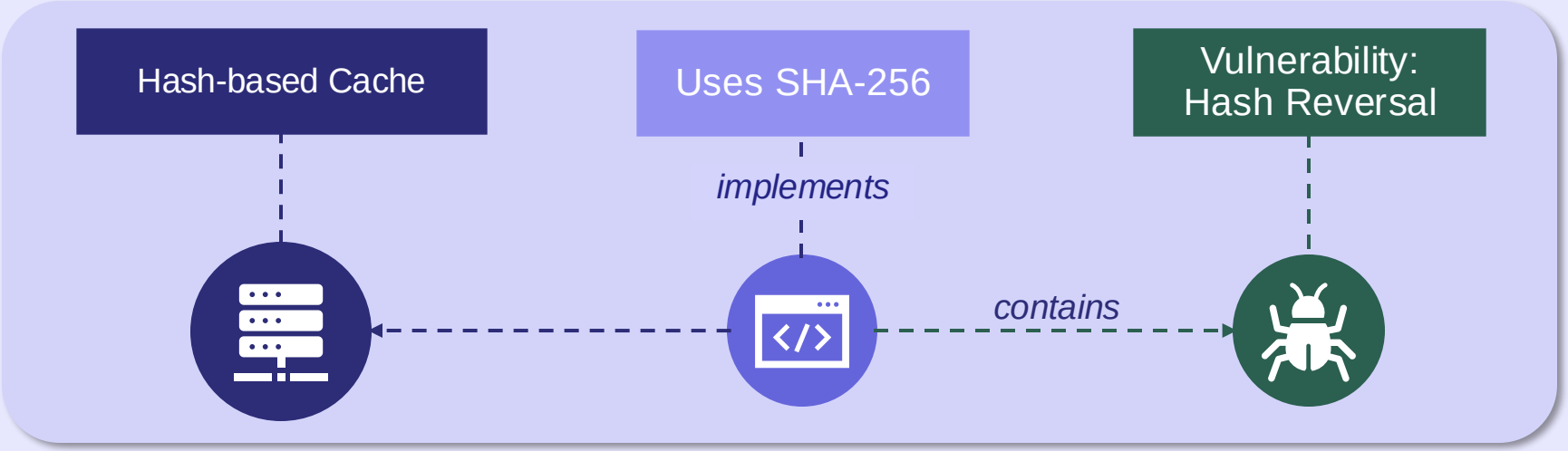
Providing Context to Vulnerabilities

Hash Reversal

Threat T:
Password Theft



Vulnerability
most likely not
applicable



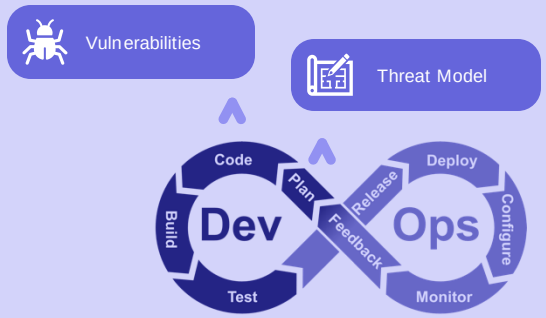
Software Product
Health Assistant

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

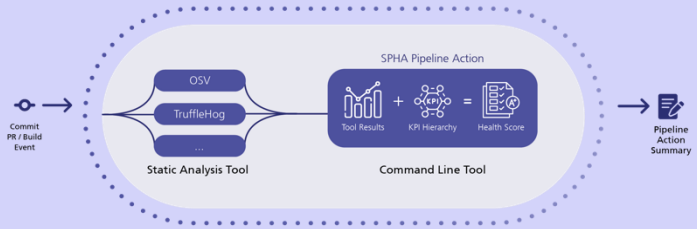
Fraunhofer
IEM

Communicate

Customize



Automate



From Complexity to Clarity

Software Product Health Assistant

Jan-Niclas Strüwer

jan-niclas.struewer@iem.fraunhofer.de

struewer

/fraunhofer-iem/spha