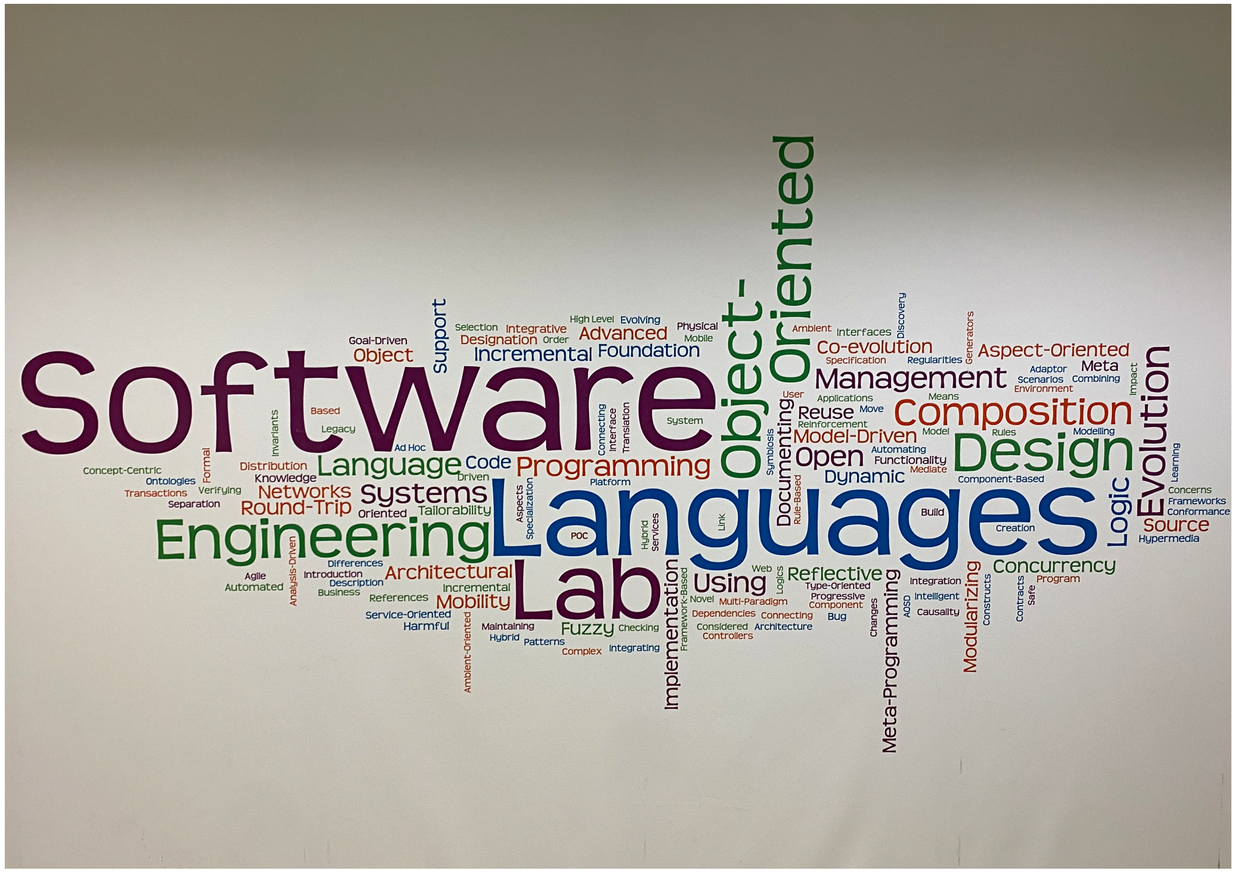
Software Languages Lab
Vrije Universiteit Brussel

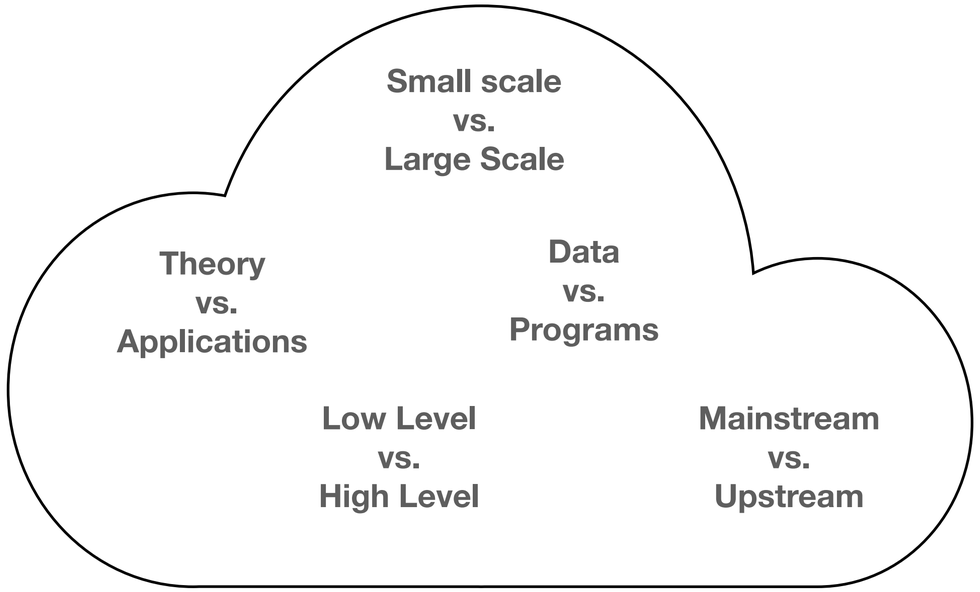
Coen De Roover - May 15th, 2025

SOFT in a nutshell



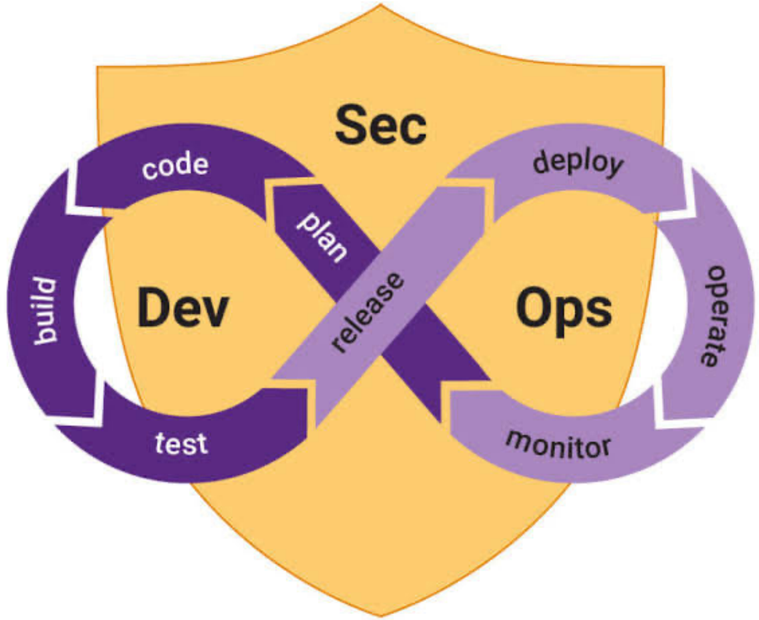
- 1 of 2 **large research groups** (other being AI) within the **Departement of Computer Science** (DINF) at **Vrije Universiteit Brussel** (VUB) in the capital of Belgium
- originating from the **2008 merger** of SSEL and PROG, both **founded in 1987** by Prof. emeriti V. Jonckers and T. D'Hondt
- currently counting about **20 pre-doctoral researchers, 8 post-docs, and 1 valorisation manager –led by 6 full-time faculty members**
- supported by portfolio covering entire **spectrum from fundamental over strategic basic to applied research**

Research scope



Research Diversity Dimensions at SOFT

“ SOFT researches **theories**, **technologies** and **methods** that are at the basis of, or help to improve, the **construction** **of** **software** at all layers of the **software stack** that **begins** where **computer engineering ends** and **goes up** to and includes **application construction**. ”



- empirical research into **secure practices**
- **reactive security** & incident management
- dynamic and static program **analyses**
- **tools** for SCA, SAST, DAST, IAST, RASP
- secure programming **abstractions**
- secure programming **languages**

Full-time faculty members

Wolfgang De Meuter

2006

language design for reactive and event-based applications, low-code applications

Elisa Gonzalez Boix

2014

languages and tooling for concurrent and distributed systems

Coen De Roover

2015

program analysis design and applications in software quality

Bas Ketsman

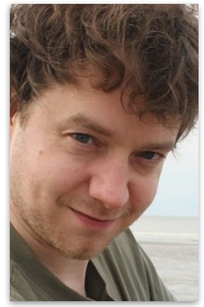
2019

scalable big data systems, query optimisation

Antonio Paolillo

2023

embedded software, operating systems

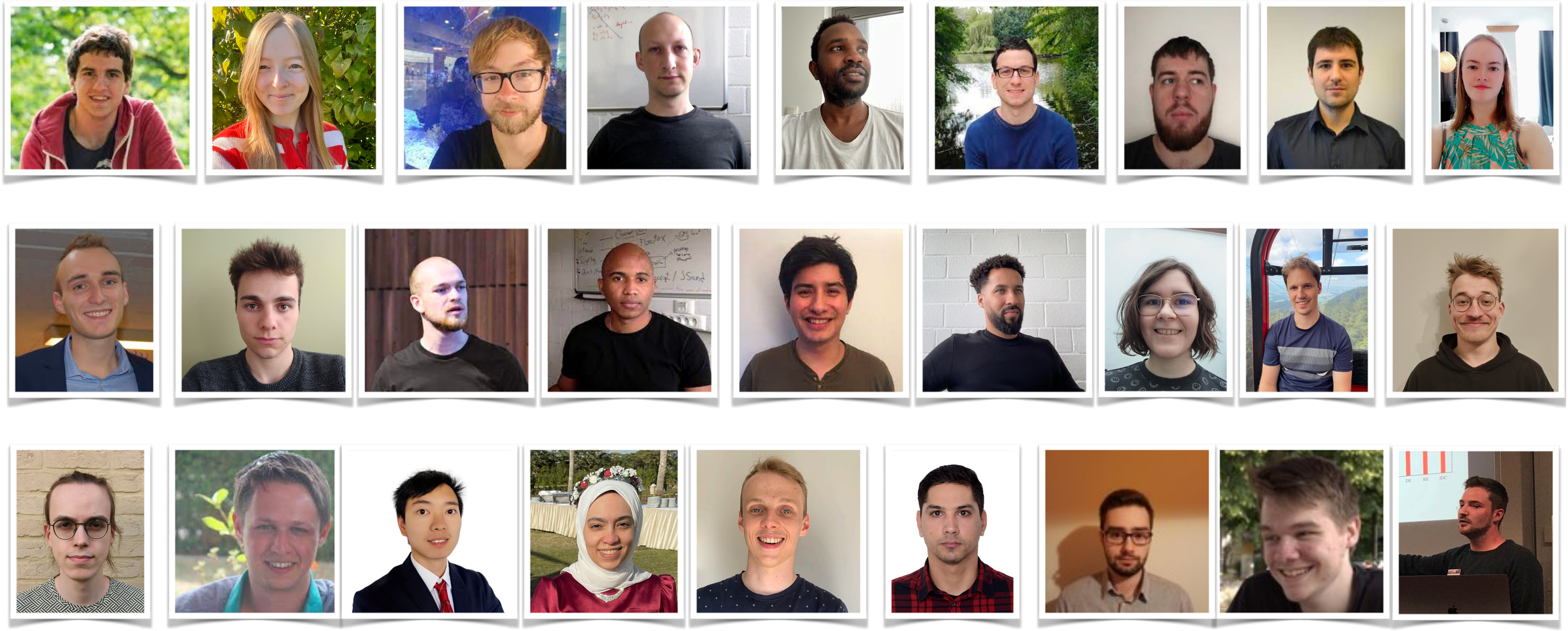


Jens Nicolay

2024

applied software research, reactive security

Researchers (with a picture)



SOFT Research highlights

Managing the software supply chain

Development dependencies

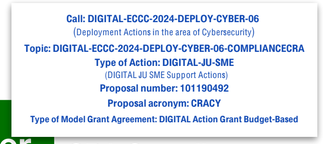
Vulnerable & outdated development dependencies

SBOMs and dependency management tooling

Deployment dependencies

Vulnerable & outdated deployment dependencies

SBOMs and container scanning tools



CRA Compliancy (Made Easy)

Configuration

Security weaknesses in configuration scripts

IaC scanners

Gasel tool

On the Impact of Security Vulnerabilities in the npm and RubyGems Dependency Networks
Ahmed Zerouali, Tom Mens, Alexandre Decan, Coen De Roover
In Empirical Software Engineering (EMSE), 2022

The Docker Hub Image Inheritance Network: Construction and Empirical Insights
Ruben Opdebeeck, Jonas Lesy, Ahmed Zerouali, Coen De Roover - SCAM 2023

Helm Charts for Kubernetes Applications: Evolution, Outdatedness and Security Risks
Ahmed Zerouali, Ruben Opdebeeck and Coen De Roover - MSR 2023

Control and Data Flow in Security Smell Detection for Infrastructure as Code: Is It Worth the Effort?
Ruben Opdebeeck, Ahmed Zerouali and Coen De Roover - MSR 2023

SOFT Research highlights

Dynamic application security testing

CS ICON Project APAX : Automated Posture Analysis that Scales

De Roover, Coen (Administrative Promotor), Loeckx, Johan (Co-Promotor)

Software Languages Lab, Informatics and Applied Informatics, Federated labs AI and Robotics

Flanders Innovation and Entrepreneurship, Toreon, Awingu, Ceeyu, L-Sec

VLAIO

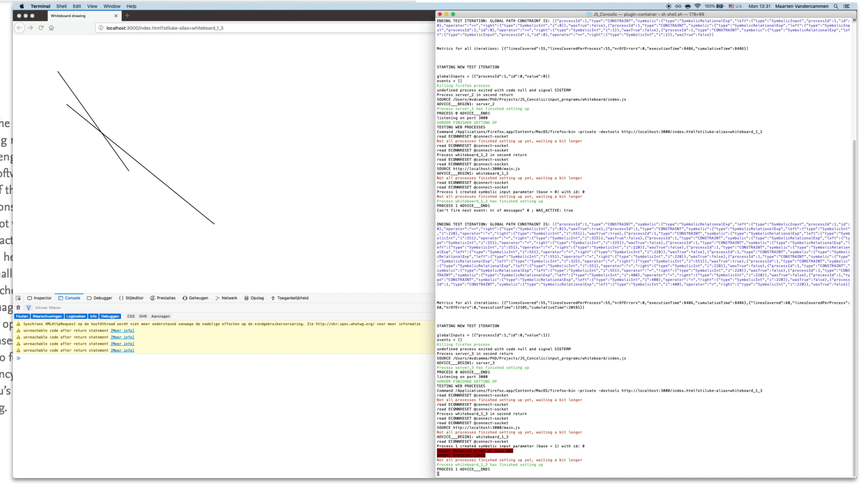
Overview | Fingerprint | Research output (1)

Project Details

Description

In the Automated Posture Analysis that Scales (APAX) project, the
Toreon and Awingu have the ambition to apply existing ongoing
future works to help automate the analysis of threats and challeng
unique expertise and works from research partners from the Soft
Intelligence Labs from VUB, together with LSEC. The impact of th
continuous evolving cloud, internet technologies and application
CyberSecurity challenges appear while many older ones have not
the goal is to avoid malicious activities to happen and to avoid act
applications from becoming inaccessible, infringed, unreliable, h
means to trade illicit content. In order to keep up with these chall
will need to further evolve from manual labor-intensive approach
detection, mitigation, reaction, incident handling, process manag
recovery. But this has to happen in close collaboration with the o
business, people and processes. Maximizing automation increas
reduces the repetitive work of security experts, allowing them to f
Automated Posture from the APAX-project increases the efficienc
Toreon, further enhances the Posture product offering of Ceeyu's
improves the cybersecurity of the Awingu remote office offering.

Acronym	VLAAI4
Status	Finished
Effective start/end date	1/03/22 → 31/07/24



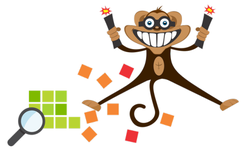
concolic testing for event-driven systems

fwo

Basecamp Zero

Zero-touch Testing of Cloud-native Applications

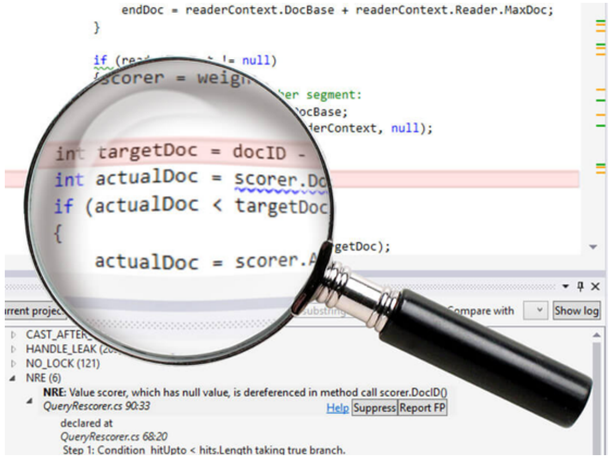
resilience testing through fault injection

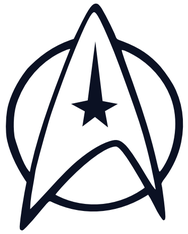


fault reproduction through fuzzing

SOFT Research highlights

Static application security testing

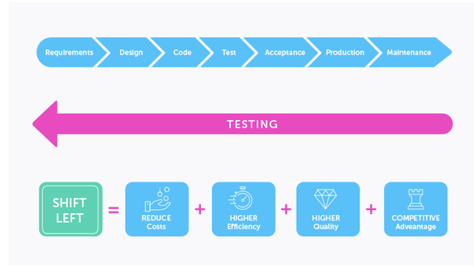




“to boldy go where no SAST tool has gone before”

binaries

deployment automation



analysis designs for “shift left”

- **Static Stack-Preserving Intra-Procedural Slicing of WebAssembly Binaries**
  Quentin Stiévenart, Dave Binkley and Coen De Roover – ICSE 2022
- **Compositional Information Flow Analysis for WebAssembly Programs**
  Quentin Stiévenart and Coen De Roover – SCAM 2020
- **Control and Data Flow in Security Smell Detection for Infrastructure as Code: Is It Worth the Effort?**
  Ruben Opdebeeck, Ahmed Zerouali and Coen De Roover - MSR 2023

- **Result Invalidation for Incremental Modular Analyses**
  Jens Van der Plas, Quentin Stiévenart and Coen De Roover – VMCAI 2023
- **Change Pattern Detection for Optimising Incremental Static Analysis**
  Cindy Wauters, Jens Van der Plas, Quentin Stiévenart and Coen De Roover – SCAM 2023
- **A Parallel Worklist Algorithm and Its Exploration Heuristics for Static Modular Analyses**
  Quentin Stiévenart, Noah Van Es, Jens Van der Plas, and Coen De Roover - In JSS 2021

Secure Deployment Automation

Deployment automation

```yaml
- name: Ensure default user account is deleted
  user:
    name: "{{ default_user_name }}"
    state: absent
  when: default_user_name is defined
  become: true

- name: Ensure default user group is deleted
  group:
    name: "{{ default_user_group }}"
    state: absent
  when: default_user_group is defined

- name: Ensure root password is changed
  user:
    name: root
    password: >-
      {{
        root_password
        | password_hash(
          'sha512',
          65534 | random(seed=inventory_hostname) | string)
      }}
    update_password: always
    state: present
  become: true

- name: Ensure sshd configuration is correct
  template:
    src: sshd_config.j2
    dest: /etc/ssh/sshd_config
    owner: root
    group: root
    mode: 0600
  become: true
  notify: restart sshd

- include_role:
    name: Oefenweb.ufw
    apply:
      become: true
  vars:
    ufw_logging: "on"
    ufw_rules:
      - rule: allow
        direction: in
        to_port: "{{ ansible_port }}"
        protocol: tcp
        interface: "{{ ansible_default_ipv4.interface }}"
        comment: Allow incoming SSH traffic

- include_role:
    name: fail2ban
```

puppet

ANSIBLE

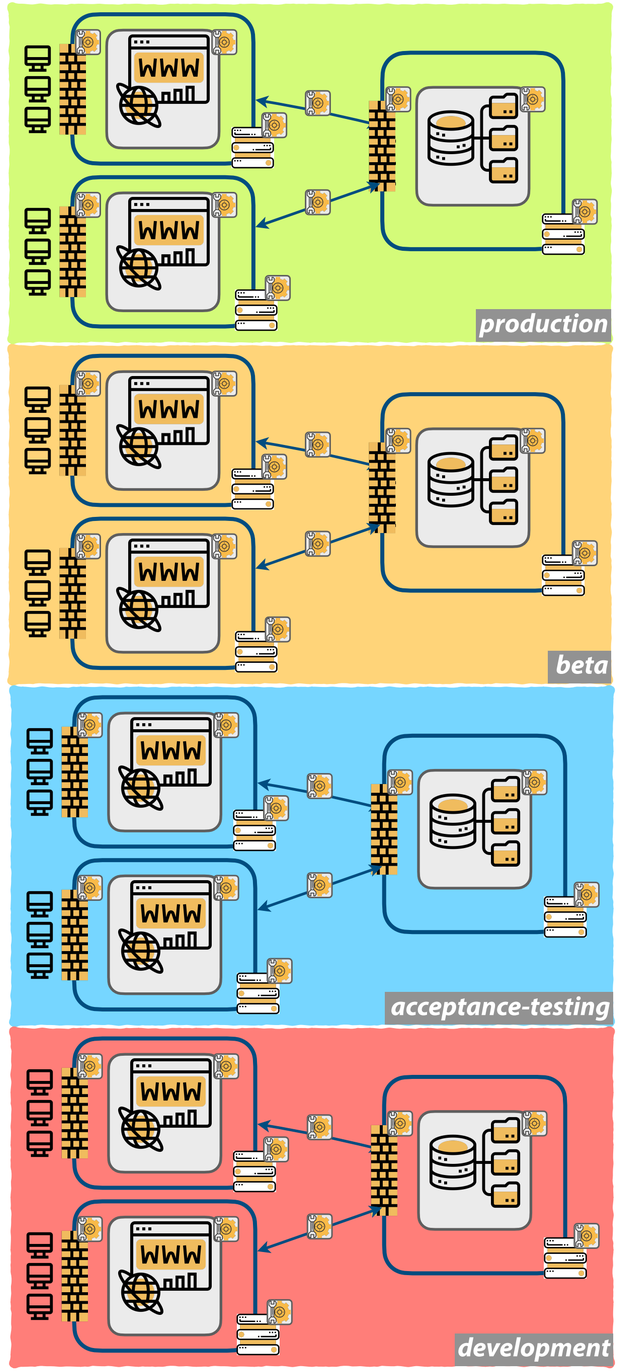
HashiCorp Terraform

pulumi

Provision

Configure

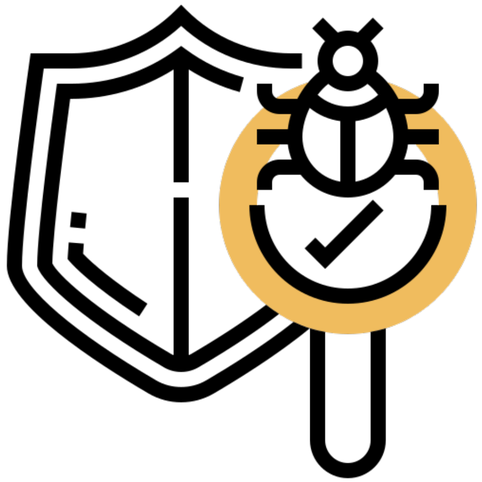
Manage



Our Solutions

GASEL

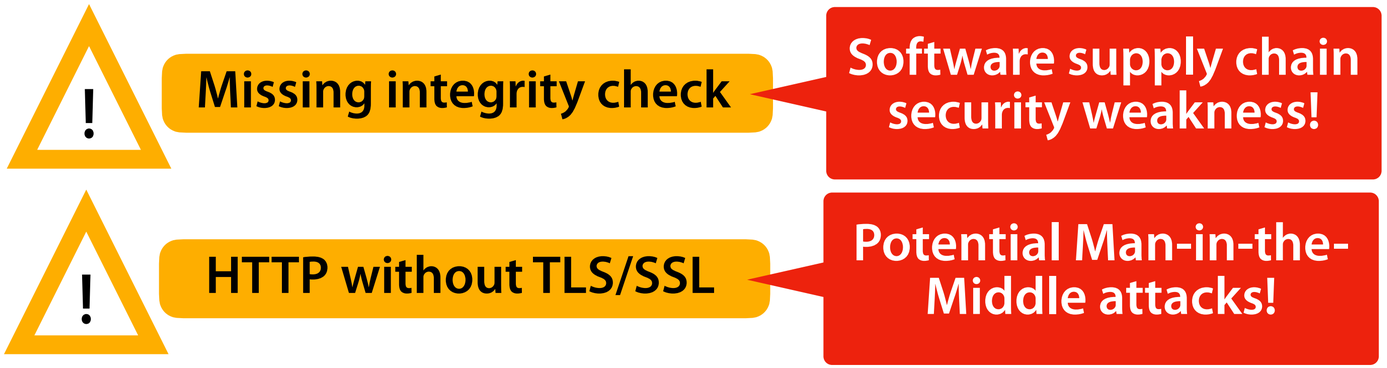
***G**raph-based **A**nsible **Se**curity **L**inter*



Deep static application security testing (SAST)

GASEL: Security Smell Detection

```
- name: Deploy application software
  unarchive:
    src: http://my.apps.com/my/app.zip
    dest: /app/
    remote_src: true
```



GASEL detects 7 types of security “smells” in Infrastructure as Code

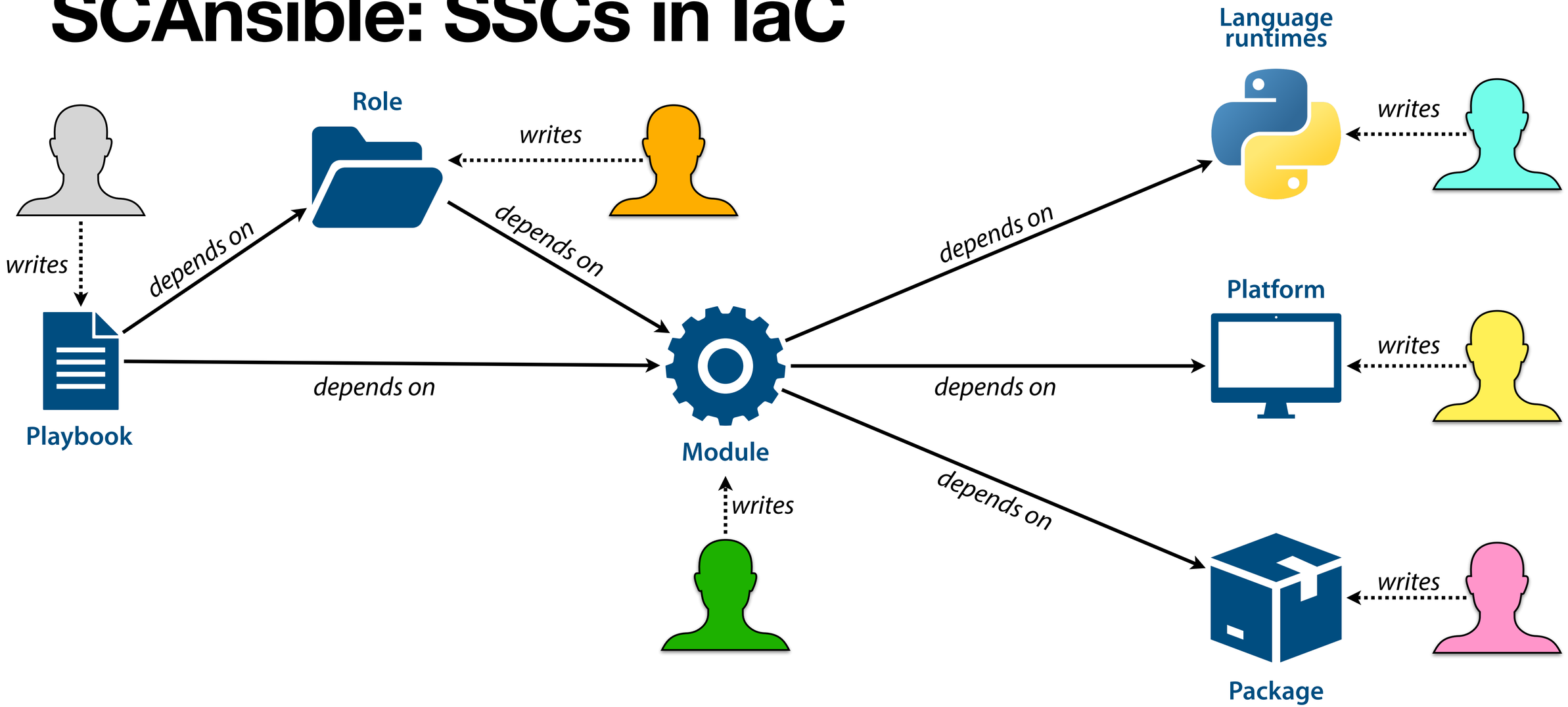
Our Solutions

SCAnsible

***S**oftware **C**omposition **An**alysis for **An**sible*

Deep software composition analysis (SCA)

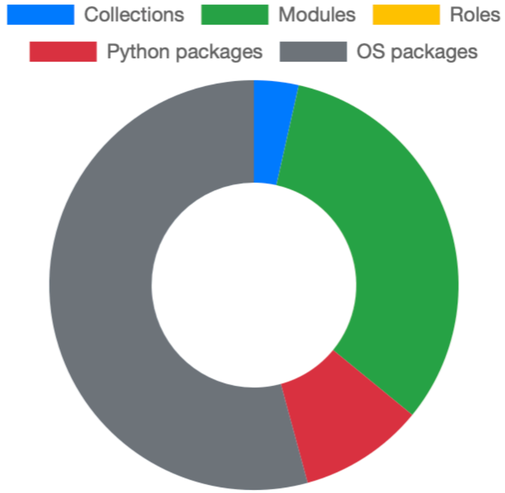
SCAnsible: SSCs in IaC



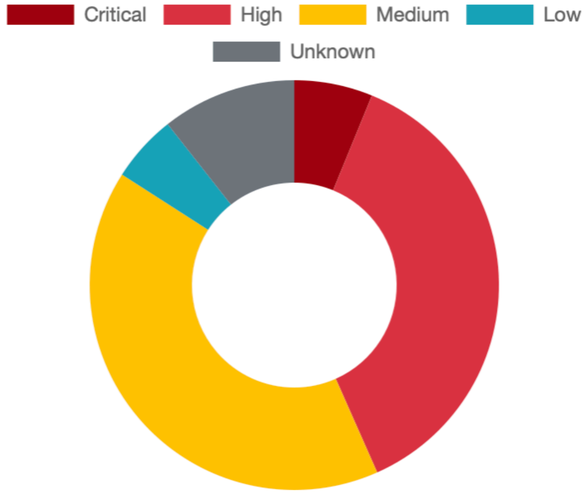
First exploration of Software Supply Chains in Infrastructure as Code

Demo

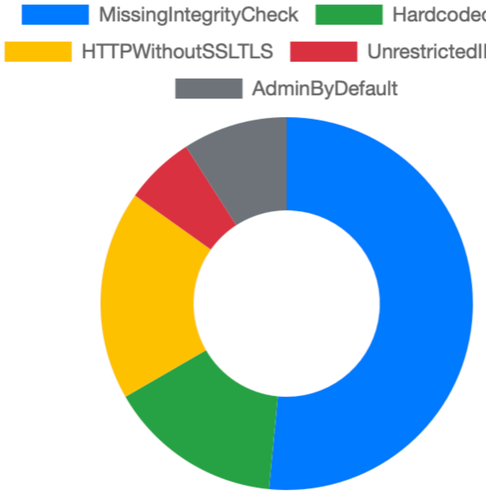
Dependency types



Vulnerabilities



Weaknesses



Top collections

Collection	#usages	#modules
ansible.builtin	487	30
community.general	19	10
community.mysql	10	3
community.postgresql	3	2
ansible.posix	2	1

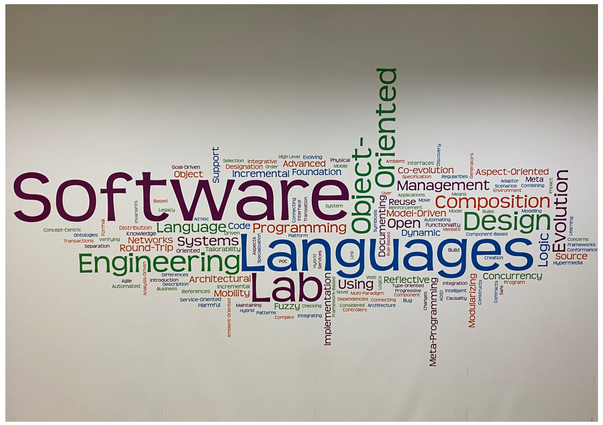
Top modules

Module	#usages
ansible.builtin.file	78
ansible.builtin.command	62
ansible.builtin.template	58
ansible.builtin.apt	50
ansible.builtin.service	47

Top dependencies

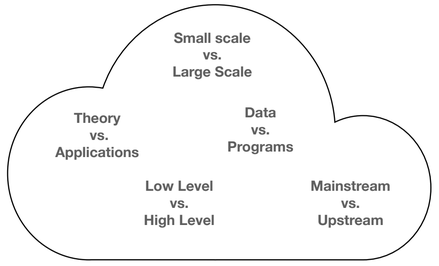
Dependency	#usages
lsattr OS	10
chattr OS	9
md5 Python	5
sha Python	5
rpm Python	3

SOFT in a nutshell



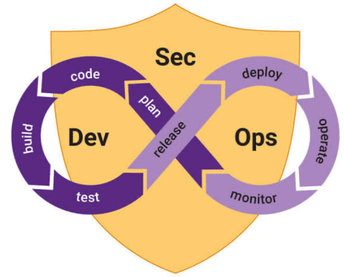
- 1 of 2 **large research groups** (other being AI) within the **Departement of Computer Science** (DINF) at **Vrije Universiteit Brussel** (VUB) in the capital of Belgium
- originating from the **2008 merger** of SSEL and PROG, both **founded in 1987** by Prof. emeriti V. Jonckers and T. D'Hondt
- currently counting about **20 pre-doctoral researchers, 8 post-docs, and 1 valorisation manager –led by 6 full-time faculty members**
- supported by portfolio covering entire **spectrum from fundamental over strategic basic to applied research**

Research scope



Research Diversity Dimensions at SOFT

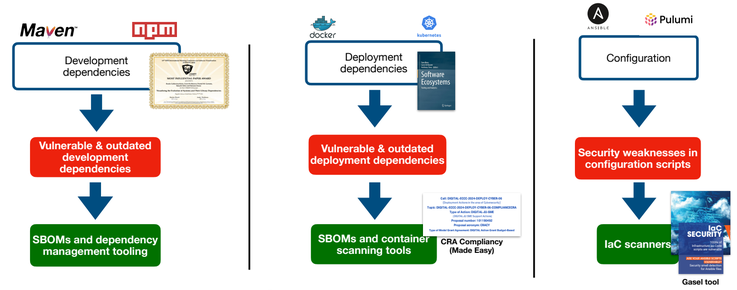
" SOFT researches **theories**, **technologies** and **methods** that are at the basis of, or help to improve, the **construction** **of** **software** at all layers of the **software stack** that **begins** where **computer engineering ends** and **goes up** to and includes **application construction**. "



- empirical research into **secure practices**
- **reactive security** & incident management
- dynamic and static program **analyses**
- **tools** for SCA, SAST, DAST, IAST, RASP
- secure programming **abstractions**
- secure programming **languages**

SOFT Research highlights

Managing the software supply chain



On the Impact of Security Vulnerabilities in the npm and RubyGems Dependency Networks
Ahmed Zerouali, Tom Mens, Alexandre Decan, Coen De Roover
In Empirical Software Engineering (EMSE), 2022

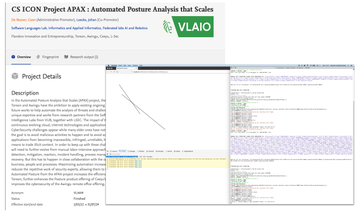
The Docker Hub Image Inheritance Network: Construction and Empirical Insights
Ruben Opdebeeck, Jonas Lety, Ahmed Zerouali, Coen De Roover – SCAM 2023

Helm Charts for Kubernetes Applications: Evolution, Outdatedness and Security Risks
Ahmed Zerouali, Ruben Opdebeeck and Coen De Roover – MSR 2023

Control and Data Flow in Security Smell Detection for Infrastructure as Code: Is It Worth the Effort?
Ruben Opdebeeck, Ahmed Zerouali and Coen De Roover - MSR 2023

SOFT Research highlights

Dynamic application security testing



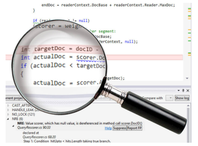
concolic testing for event-driven systems

resilience testing through fault injection

fault reproduction through fuzzing

SOFT Research highlights

Static application security testing

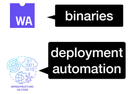


"to boldy go where no SAST tool has gone before"

Static Slack-Preserving Intra-Procedural Slicing of WebAssembly Binaries
Quentin Stiévenart, Dave Binkley and Coen De Roover – ICSE 2022

Compositional Information Flow Analysis for WebAssembly Programs
Quentin Stiévenart and Coen De Roover – SCAM 2020

Control and Data Flow in Security Smell Detection for Infrastructure as Code: Is It Worth the Effort?
Ruben Opdebeeck, Ahmed Zerouali and Coen De Roover - MSR 2023



analysis designs for "shift left"

Result Invalidation for Incremental Modular Analyses
Jens Van der Plas, Quentin Stiévenart and Coen De Roover – VMCAI 2023

Change Pattern Detection for Optimizing Incremental Static Analysis
Cindy Wauters, Jens Van der Plas, Quentin Stiévenart and Coen De Roover – SCAM 2023

A Parallel Worklist Algorithm and Its Exploration Heuristics for Static Modular Analyses
Quentin Stiévenart, Noah Van Es, Jens Van der Plas, and Coen De Roover - In JSS 2021