The **Highway Model** of **DevSecOps**

CI/CD security – New **cornerstone** of the **Information System?**

Arnaud PETITCOL
Manager

Jeanne GRENIER
Senior Consultant

WAVESTONE

Wavestone Insight Day 2024

CI/CD security: Spotlight on difficulties encountered by our clients

Clients' challenges

Overloaded security teams
Security teams face high workloads and often need to deprioritize security concerns.

Increasing pipeline complexity
Lack of standardization and scalability in pipelines make risk management and incident response more complex.

Insufficient trainings
Squads lack security expertise and a rigorous training on CI/CD security best practices.

Low traceability
Lack of monitoring and logging causes issues with visibility, accountability and slows incident response.

Insights from Wavestone's audit & incident response teams

CI/CD pipelines

	VLN / Helped to compromise	**Led** to **total** compromise
CI/CD audits	N/A	85%
Cloud audits	100%	60%
CERT & RedTeam	75%	20%*

**An easier path was used*

Introduction to the **Highway model of DevSecOps**

Let's **prepare** our **DevSecOps Journey**

The **Product Team** (squad)

- Used to Agile methodology
- Business oriented: « security must not impact planning »
- Little or no security awareness & training

Software Development LifeCycle (SDLC)

- Control before deployment in production or during RUN phase
- Security blocking position increasing time to deliver
- Manual controls increasing time to deliver and overloading security teams

The **CI/CD pipeline**

(Continuous Integration & Continuous Delivery / Deployment)

- A heterogenous toolchain
- An existing CI/CD pipeline built without security

What are we talking about?
Let's have a look at the **CI/CD Tooling Landscape**

- **CI/CD**: stands for "continuous integration" and "continuous delivery" – the development and delivery/deployment process.
- **DevSecOps**: extension of the DevOps paradigm, adding security tools, governance & practices to the development lifecycle with a *shift-left approach* and aiming at promoting collaboration between developers, operationals and security teams.

Collaborate | **Code & Build** | **Deliver to stage** | **Test** | **Deploy & Release** | **Operate & Monitor**

Communication & ChatOps
slack, Mattermost, Microsoft Teams

Source Code Management
Bitbucket, GitLab, GitHub

Continuous Integration Orchestrator
Jenkins, CI/CD

Tests
squash, JMeter, Selenium, POSTMAN, cucumber

Deployment
argo, Octopus Deploy, Spinnaker

Monitoring tools
ELK Stack, PagerDuty, DATADOG, dynatrace

Application Lifecycle Management.
Trello, Jira, asana

Build tools
npm, Maven, docker, gradle

Provisioning
puppet, Terraform, ANSIBLE

App stores

Cloud / IaaS / CaaS
Azure, aws

Knowledge Sharing
Confluence, Notion

Unit tests & regression tests
Jest, JUnit, MOCHA

Artifact Management
nexus repository, JFrog ARTIFACTORY, GitLab

Containerization & Scheduling
kubernetes, docker SWARM, RED HAT OPENSHIFT

Integrated Development Environment
eclipse, WS, Visual Studio Code

Templating
HELM, Packer, Kustomize.io

Which components interest us the most?

What are we talking about?
Let's have a look at the **CI/CD Tooling Landscape**

- **CI/CD**: stands for "continuous integration" and "continuous delivery" – the development and delivery/deployment process.
- **DevSecOps**: extension of the DevOps paradigm, adding security tools, governance & practices to the development lifecycle with a *shift-left approach* and aiming at promoting collaboration between developers, operationals and security teams.

Source Code Management

Bitbucket, GitLab, GitHub

Platforms for **source code** hosting**, version control** and **collaborative development.**

Continuous Integration Orchestrator

Jenkins, CI/CD

Orchestrates reliable and fast code **integration,** triggers **automated builds** and **tests**.

Provisioning

puppet, Terraform, ANSIBLE

Automates the creation and configuration of infrastructure in **repeatable deployment processes**.

Artifact Management

nexus repository, JFrog ARTIFACTORY, GitLab

Centralizes the storage and management of **artifacts**, and ensures **versioning** across the pipeline.

Containerization & Scheduling

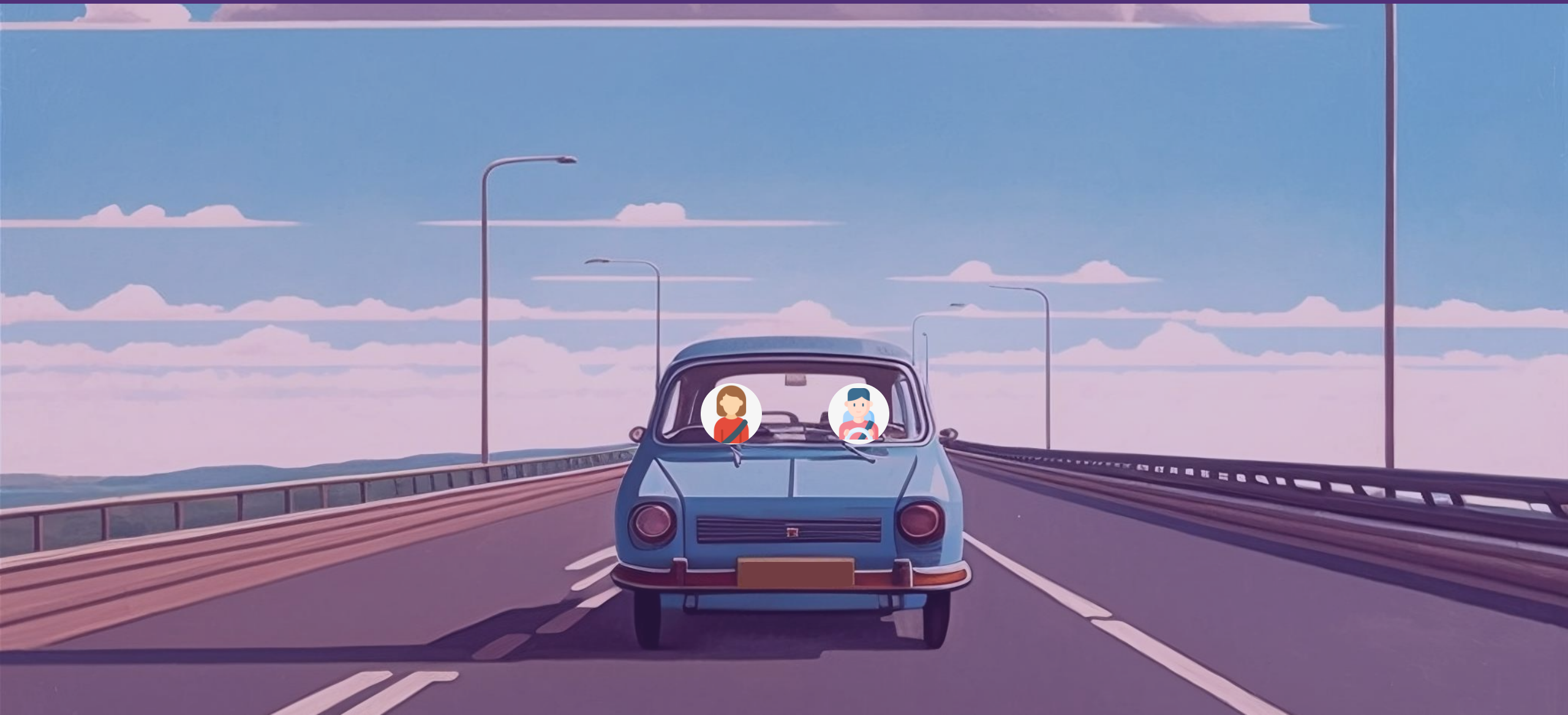
kubernetes, docker SWARM, RED HAT OPENSHIFT

Manages containerized **workloads** and **services**, optimizing deployment and **runtime** operations.

Which components interest us the most?

Introduction to the **Highway model of DevSecOps**

Life in the Fast Lane: Building a **Secure SDLC** with DevSecOps



Introduction to the **Highway model of DevSecOps**

The **new product squad** ready for the **DevSecOps Journey**

1

A **Product Owner**

- Setting the route, taking into account security objectives

2

Some **Developers & Ops**

- Building a secure and reliable engine with robust coding practices
- Deploying & maintaining it thanks to automation and monitoring

3

and a **Security Champion**

Leading the team through security best practices and teamwork

Role

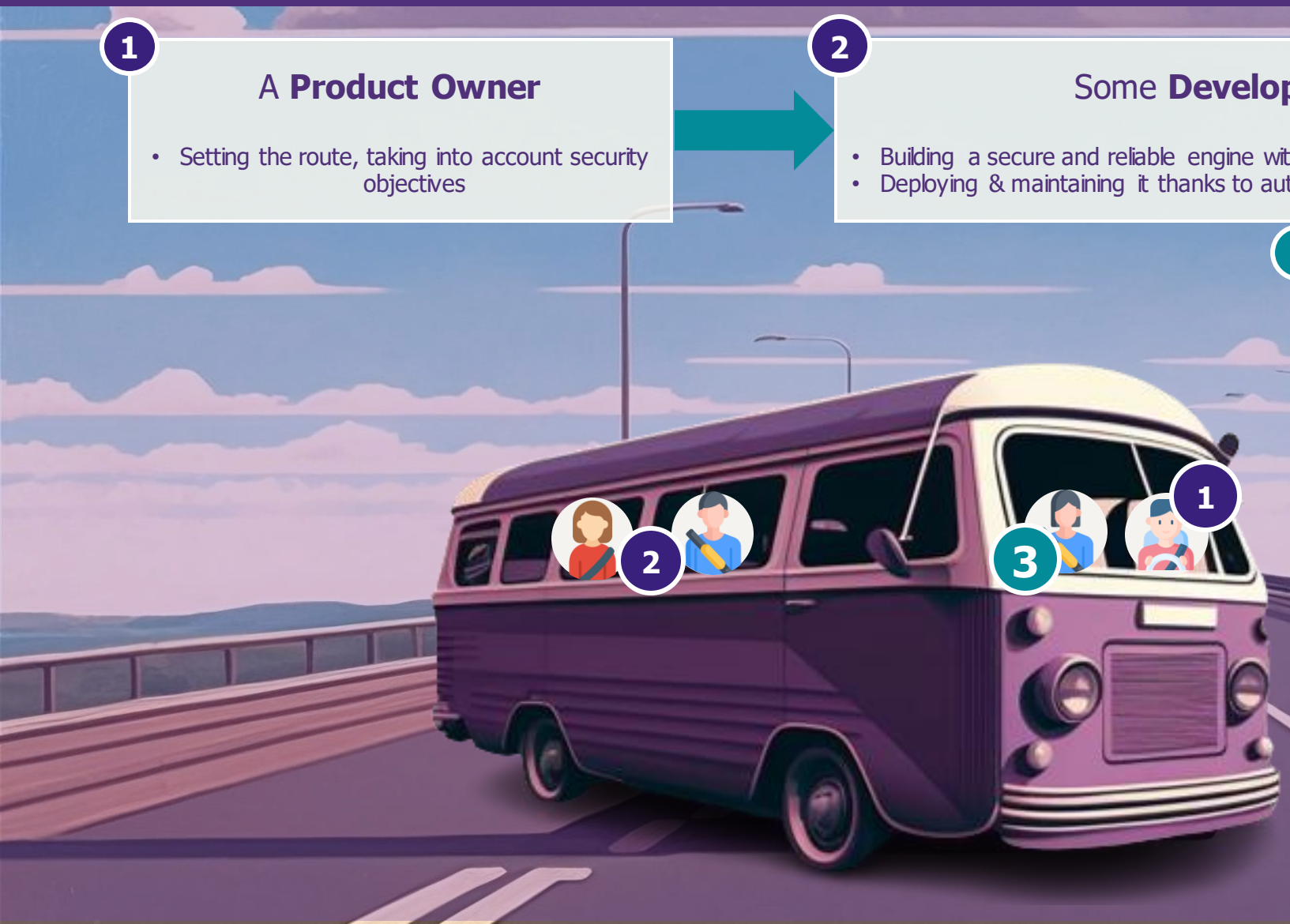
Acts as a local security relay, ensuring the liaison between his squad and security teams, fostering a security culture

Missions

/ Promote security best practices
/ Address threats
/ Help the team mitigate threats & remediate vulnerabilities
/ Validate security of deployed code
/ Collaborate with other Security Champions and security teams

Who?

/ An existing Dev with this additional role
/ A person with technical background dedicated to this role



Introduction to the **Highway model of DevSecOps**

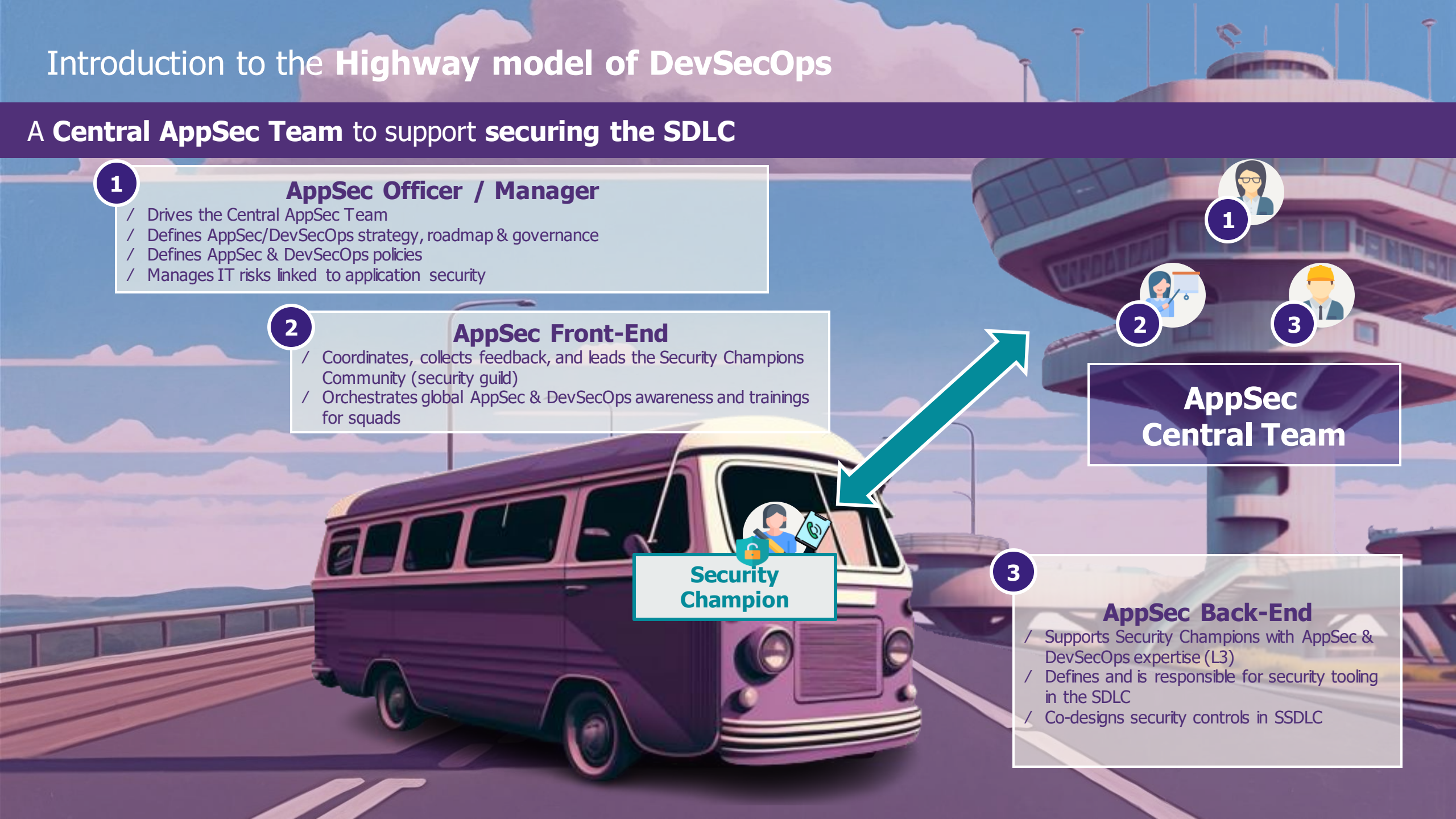
A **Central AppSec Team** to support **securing the SDLC**

1 AppSec Officer / Manager

- Drives the Central AppSec Team
- Defines AppSec/DevSecOps strategy, roadmap & governance
- Defines AppSec & DevSecOps policies
- Manages IT risks linked to application security

2 AppSec Front-End

- Coordinates, collects feedback, and leads the Security Champions Community (security guild)
- Orchestrates global AppSec & DevSecOps awareness and trainings for squads



3 AppSec Back-End

- Supports Security Champions with AppSec & DevSecOps expertise (L3)
- Defines and is responsible for security tooling in the SDLC
- Co-designs security controls in SSDLC

Co-building

A TRANSVERSAL FRAMEWORK

to be used by any squad

A **DevSecOps Framework** as **security policies, rules** and **standards**...

...with different **tools and services** to **enforce** it.

GOVERNANCE

/ Security Target Operating Model
/ Security Champion Role playbook
/ AppSec & DevSecOps Community

PROCESSES

/ Global Security Engineering process
/ Security code reviews framework
/ Threat modeling framework
/ Security controls & guardrails

KNOWLEDGE MANAGEMENT

/ Ad-hoc AppSec training
/ AppSec Knowledge Base

ON-DEMAND SERVICES

/ AppSec expertise
/ Security audits & pentests
/ Bug Bounty

TOOLING

/ DevSecOps security tools
/ Security workflow templates

...and **IMPROVING** the framework **CONTINUOUSLY**

4 strategic areas *and associated* DevSecOps security tools

SAST
(Static App. Security Testing)

DAST
(Dynamic App. Security Testing)

SCA
(Softw are Composition Analysis)

IAST
(Interactive App. Security Testing)

Infrastructure-as-Code scanner

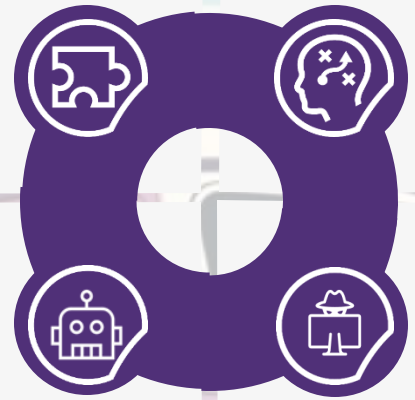
Artifacts scanner

Extend & enhance detection capabilities in your SDLC

Secrets detector

Secrets manager

Securely manage your secrets from the development phase



Standardize and automate the security process

Threat modeling

Vulnerability manager

ASOC
(Application Security Orchestration & Correlation)

Improve AppSec knowledge of your teams

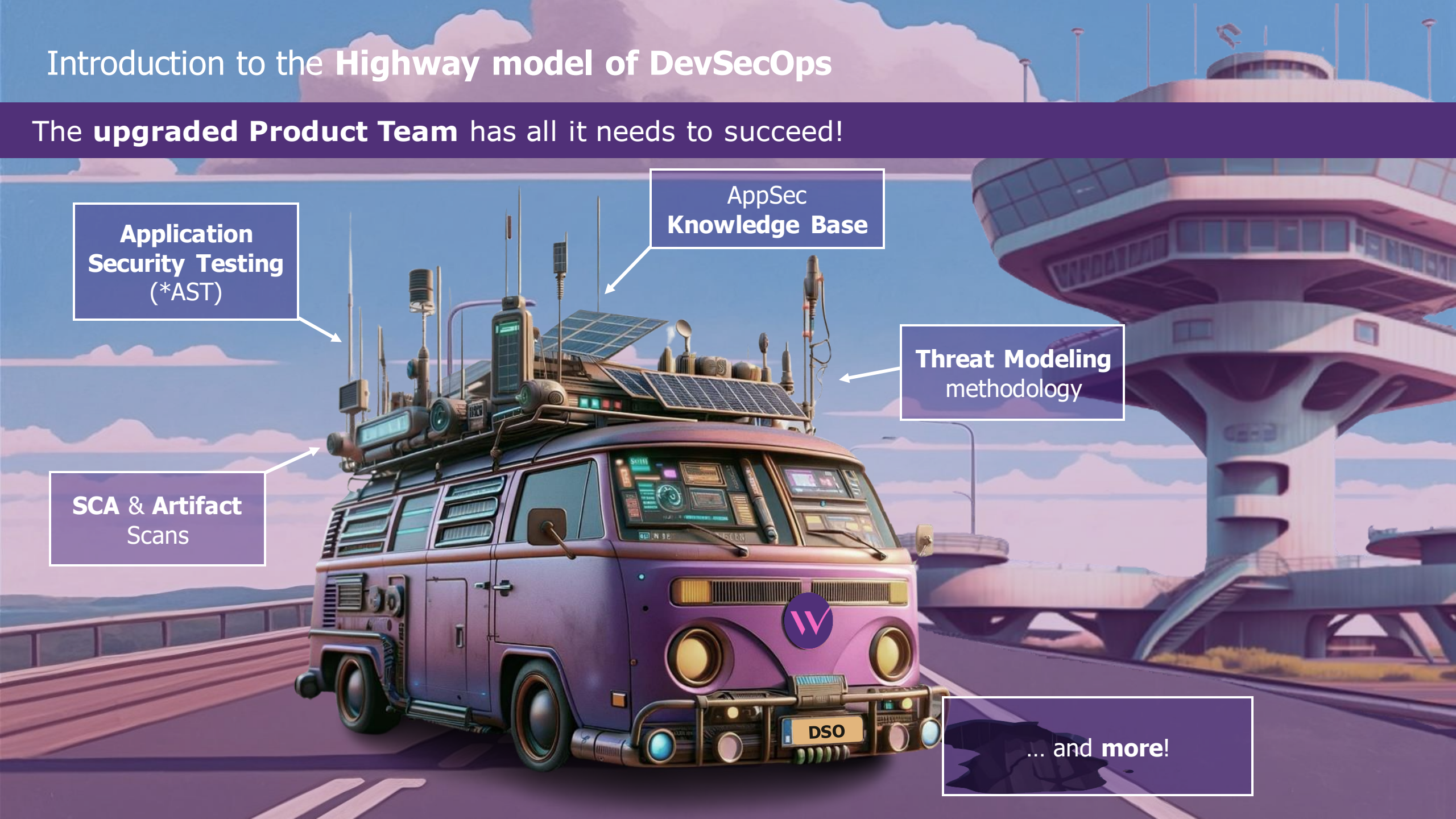
AppSec Knowledge Base

Training platforms

*And don't forget **RUN tools** (WAF, RASP, APIM, CWPP, SIEM...)*

Introduction to the **Highway model of DevSecOps**

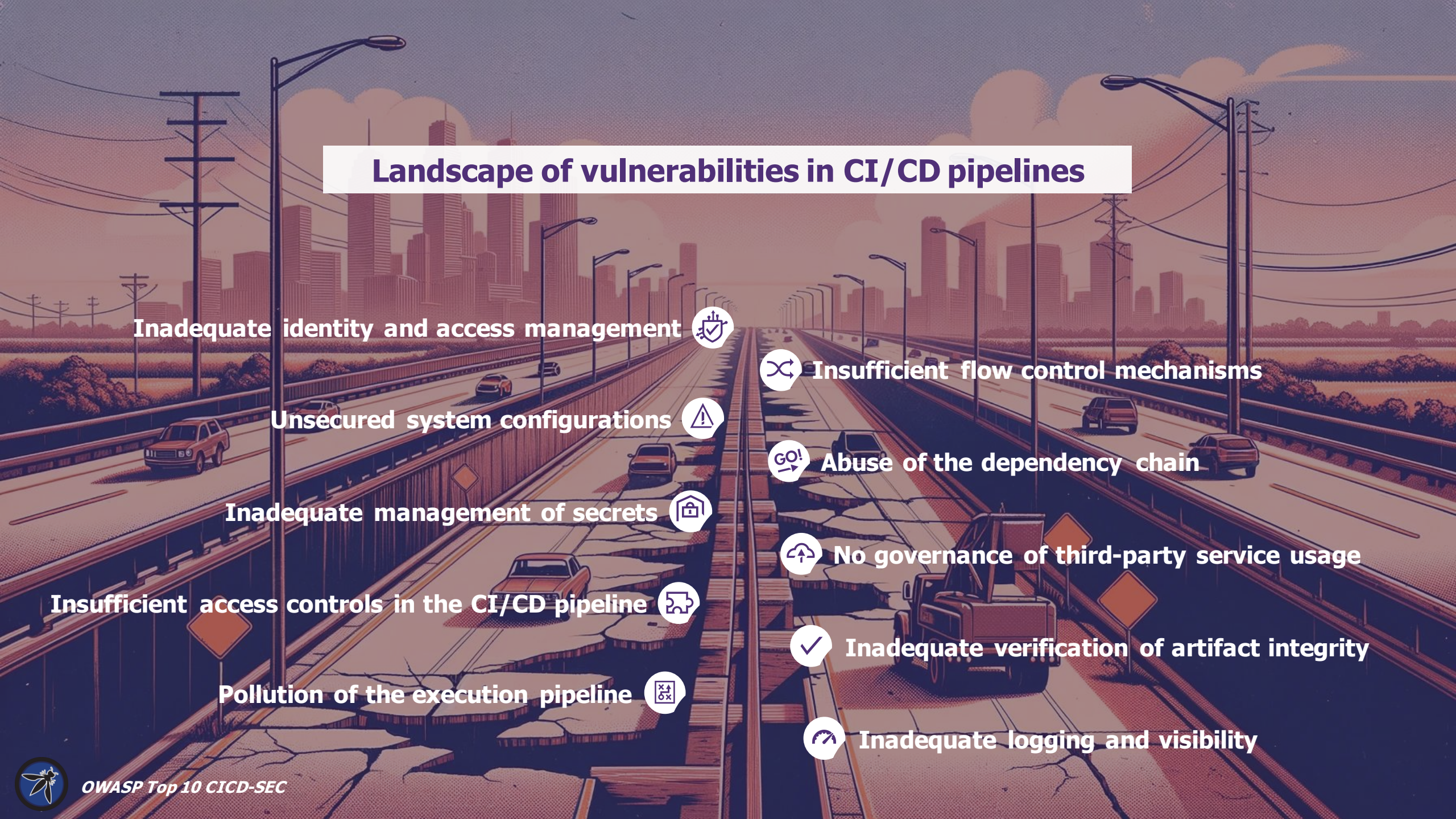
The **upgraded Product Team** has all it needs to succeed!



CI/CD security – New **cornerstone** of the **Information System?**

But what about the **security** of the CI/CD **pipeline** itself?


HIGHWAY TO HELL?
Is the CI/CD pipeline
a new "Active Directory"?
CI/CD is the new systemic component of the IT system,
that can lead to a complete compromise.


Landscape of vulnerabilities in CI/CD pipelines
Inadequate identity and access management
Unsecured system configurations
Inadequate management of secrets
Insufficient access controls in the CI/CD pipeline
Pollution of the execution pipeline
Insufficient flow control mechanisms
Abuse of the dependency chain
No governance of third-party service usage
Inadequate verification of artifact integrity
Inadequate logging and visibility
OWASP Top 10 CICD-SEC

Back to the **CI/CD tooling landscape…**

What can happen in case of an attack?

Source Code Management

Platforms for source code hosting, **version control** and **collaborative development.**

Artifact Management

Centralizes the storage and management of **artifacts**, and ensures **versioning** across the pipeline.

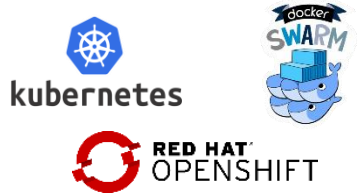
Continuous Integration Orchestrator

Orchestrates reliable and fast code integration, triggers **automated builds** and **tests**.

Provisioning

Automates the creation and configuration of infrastructure in repeatable **deployment processes**.

Containerization & Scheduling



Manages containerized **workloads** and **services**, optimizing deployment and **runtime** operations.

Intellectual property loss or theft

Service operation disruption or **IS compromise**

Supply-chain poisoning

Infrastructure drift

Intellectual property theft

Supply-chain poisoning

SolarWinds

C2 Beacon (backdoor) hidden in software update

FTP **credentials on GitHub** into **CI poisoning**

14 months before the attack was discovered post-deployment

100 organizations and more than **18 000 customers** affected

$26 millions paid in a resulting lawsuit

Intellectual property theft

Supply-chain poisoning

Codecov

Exfiltration of customer **CI env variables** (and secrets)

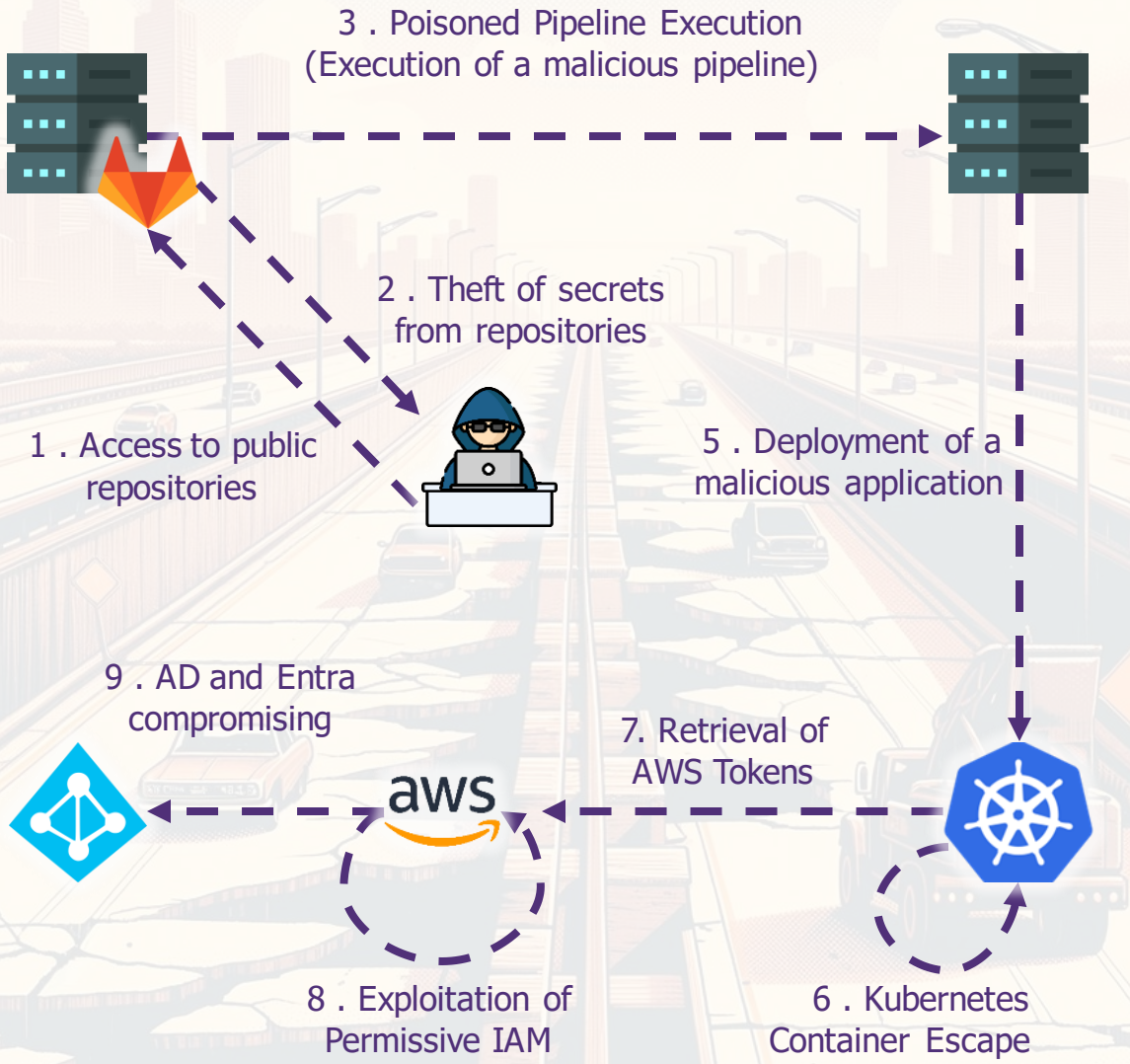
Artefact storage token exfiltration into **artefact poisoning**

2 months before the attack was discovered by a customer

29 000 customers possibly affected

One single injected line of code was enough to exfiltrate secrets

Concrete scenario of compromise of a CI/CD pipeline, based on real audit cases



D3FCON

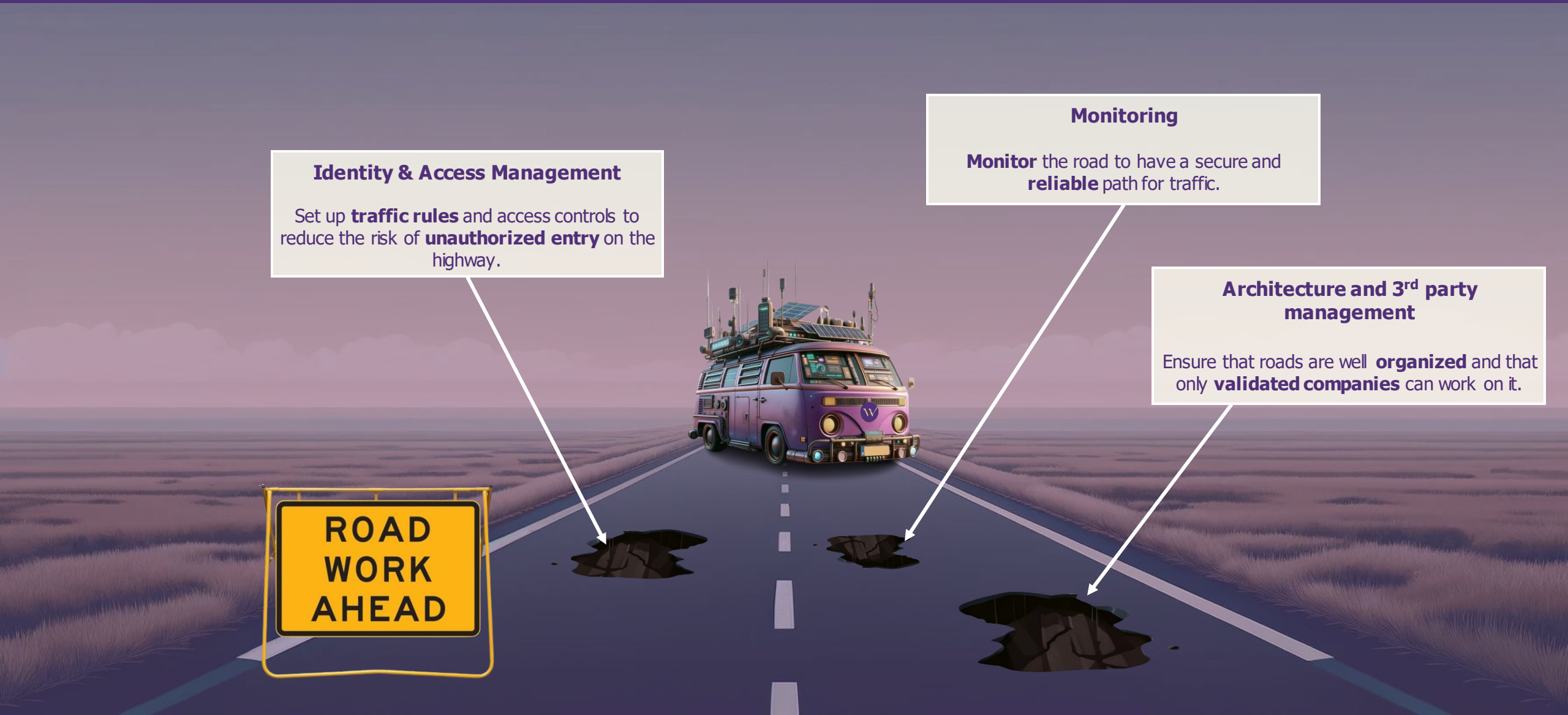
BSIDES LAS VEGAS

** Presented in 2022 on the International scene*

To what extent can a compromise in your CI/CD breach your organization?

CI/CD security – New **cornerstone** of the **Information System?**

Let's work on making the road **secure**.



Identity & Access Management

Set up **traffic rules** and access controls to reduce the risk of **unauthorized entry** on the highway.

Monitoring

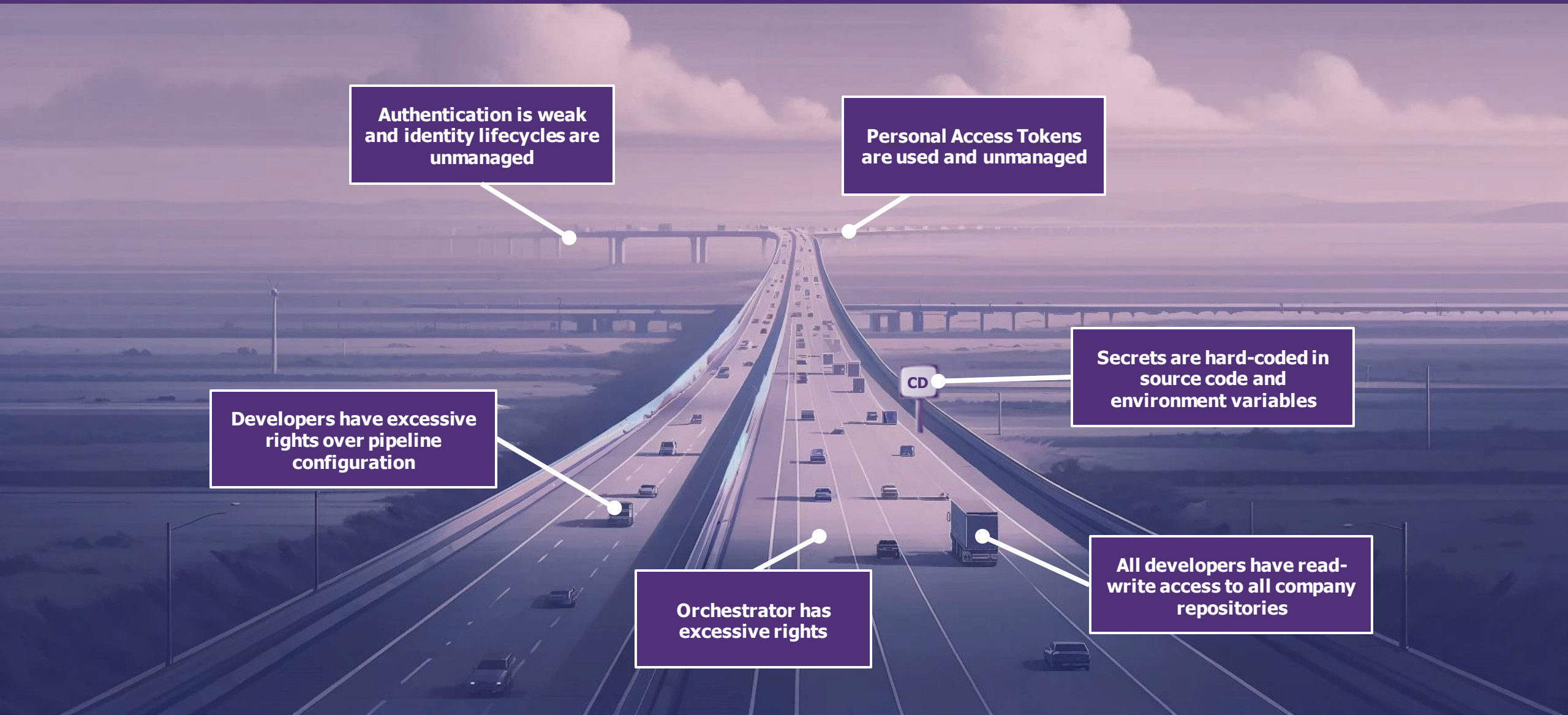
Monitor the road to have a secure and **reliable** path for traffic.

Architecture and 3rd party management

Ensure that roads are well **organized** and that only **validated companies** can work on it.

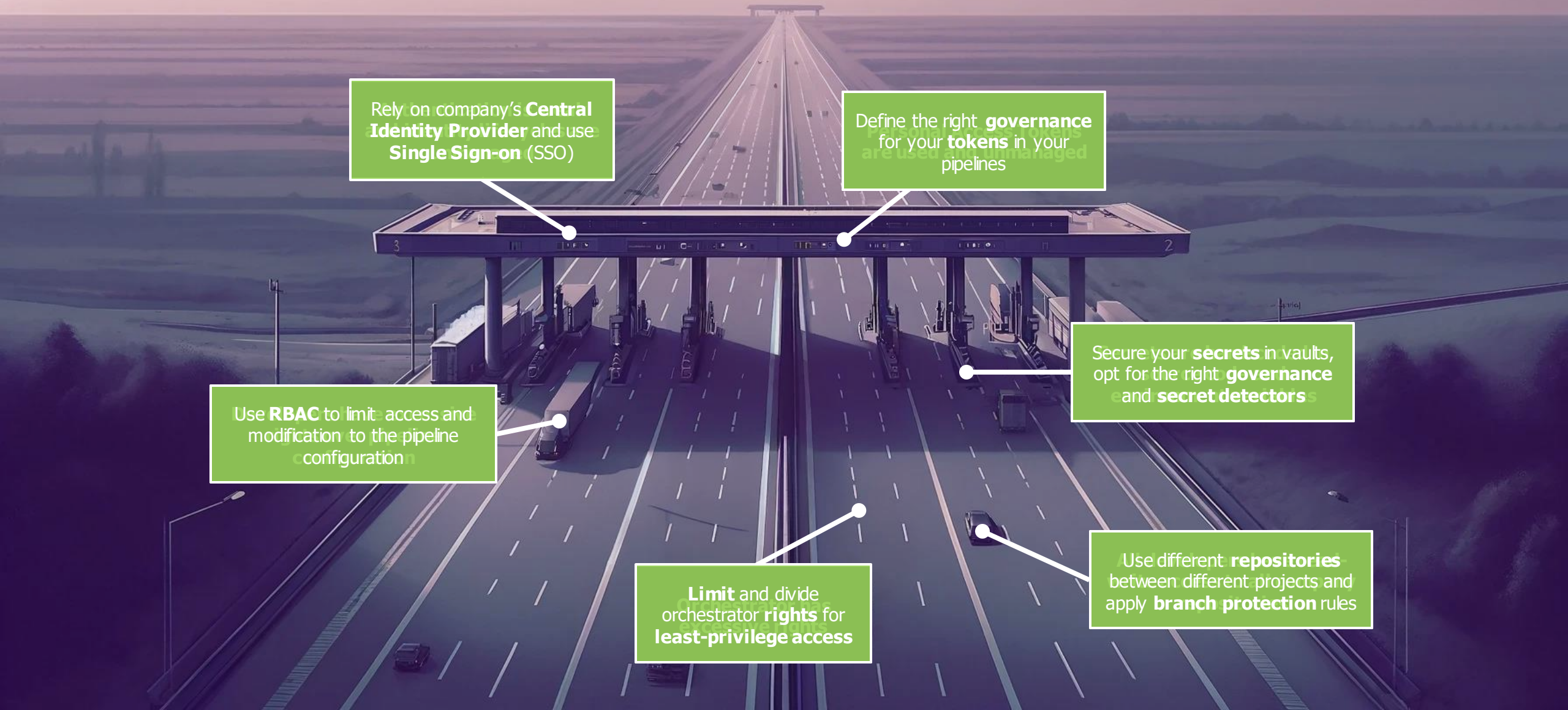
CI/CD security – New **cornerstone** of the **Information System?**

Let’s consider a pipeline with weak **Identity & Access Management.**



CI/CD security – New **cornerstone** of the **Information System?**

How to enable a **secure access** to the highway?



CI/CD security – New cornerstone of the Information System?

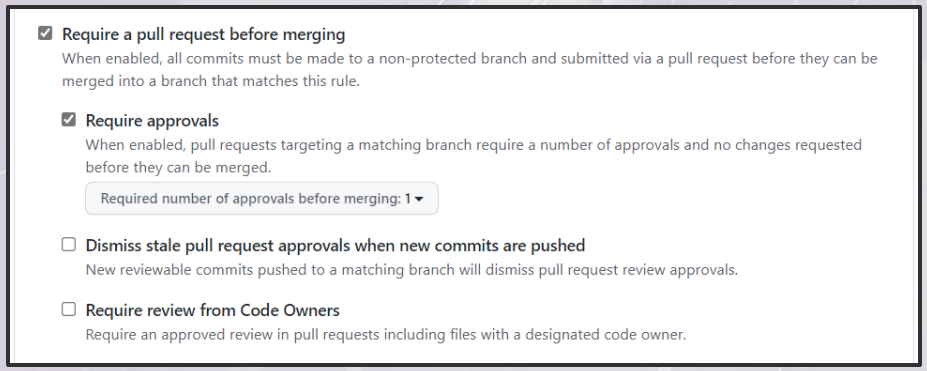
Implementing better **access controls.**

Use **RBAC** to limit access and modification to the pipeline configuration and apply **branch** protection rules.

GitHub GitLab

Use branch protection rules to manage access in Git repositories

Branch protection rules enforce constraints by limiting who can push changes on a critical branch.



Secure your yaml files with CODEOWNERS

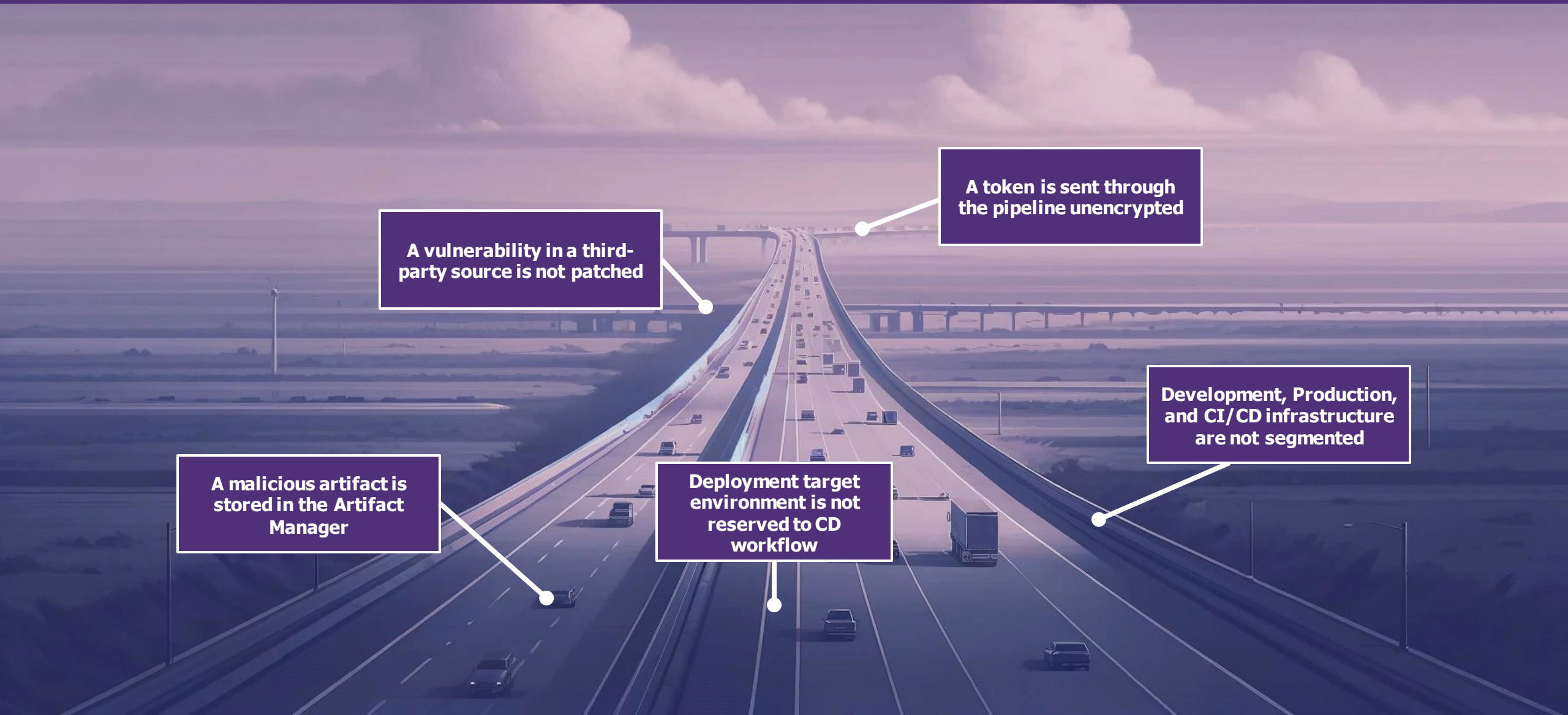
Specify individuals or teams responsible for reviewing and approving changes of high risk code.

```
1  # Default owners:
2  *                                       @all-developers
3
4  # Require security review for high-risk code changes:
5  /Web/Controllers/AccountController.cs   @security
6  /Shared/Services/Cryptography/          @security
7  /LICENSE                                @legal
8
9  # Workflow definitions for yaml files and GitHub Actions
10 /.github/workflows/                     @sec-champion
11
12 CODEOWNERS                              @admin
```

CODEOWNER file syntax

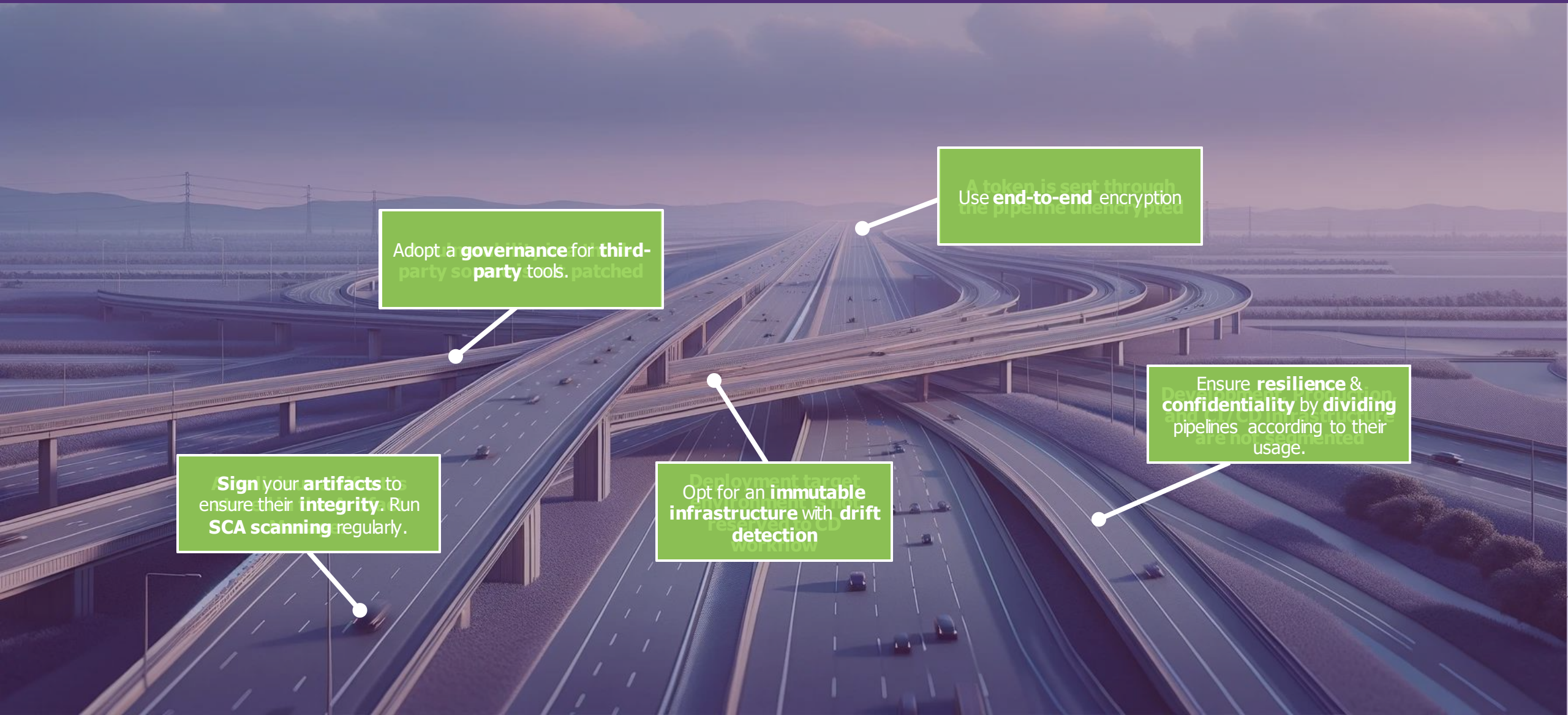
CI/CD security – New **cornerstone** of the **Information System?**

Let’s consider a pipeline with a **poor architecture** and **insufficient 3rd party management**.



CI/CD security – New **cornerstone** of the **Information System?**

How can we ensure that our **highway architecture** is secure?

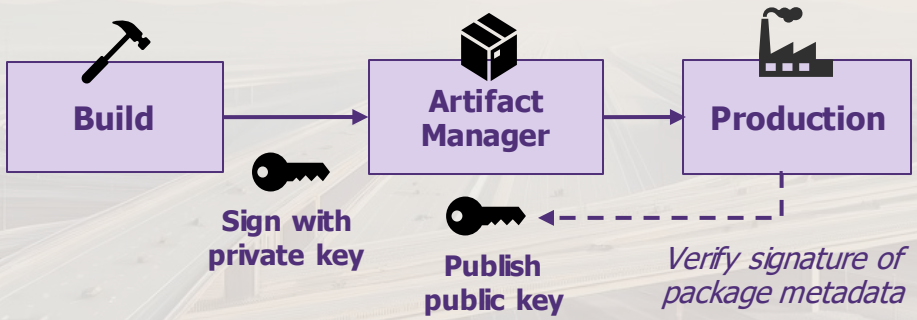


CI/CD security – New **cornerstone** of the **Information System?**

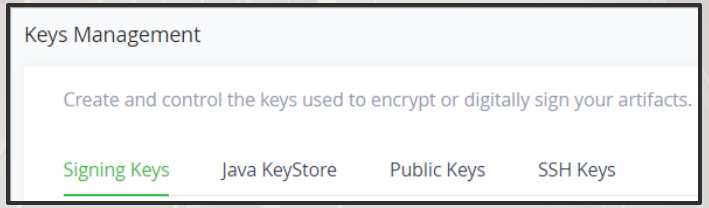
Ensuring the **integrity** of **artifacts.**

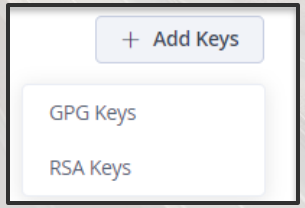
Sign your **artifacts** to ensure their **integrity**. Run **SCA scanning** regularly.

Generate a **GPG** or **RSA** key with a **PKI** on a secure system to get a private and public key. **Safeguard** the private key in a vault.



JFrog ARTIFACTORY





CI/CD security – New **cornerstone** of the **Information System?**

Let’s consider a pipeline with **inefficient monitoring**.

CI/CD security – New **cornerstone** of the **Information System?**

How can we increase **visibility** and **stability** on the highway?

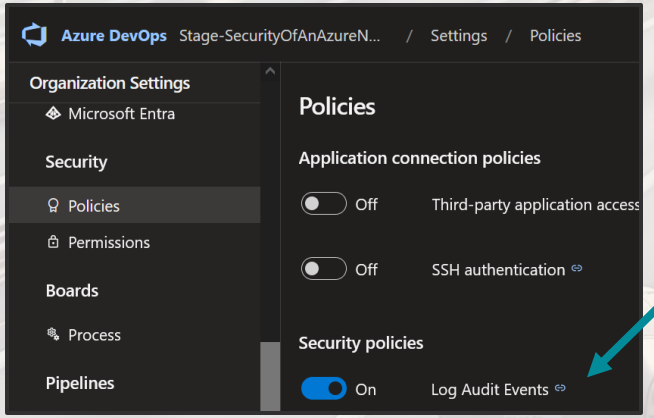
CI/CD security – New **cornerstone** of the **Information System?**

Enabling logs for **incident detection** & **response**.

Maintain **logs** for **traceability** and **accountability**

Azure DevOps

Enable **"Log Audit Events"** and monitor regularly **permissions changes**, **deleted resources** and **branch policy changes**.



Activating Log Audit Events

Actor	Timestamp	Area	Cate...	Details
Jamal 24.16.2	11/4/2019, 1:38:14 PM	Per...	Mo...	3 permissions were modified for [FabrikamFiber]\Project Administrators and [FabrikamFiber]\Project Valid Users
Jamal 24.16.2	11/4/2019, 1:37:43 PM	Per...	Mo...	14 permissions were modified for Project Collection Build Service (fabrikamfiberorg), [FabrikamFiber]\Contributors, [FabrikamFiber]\Readers and 3 other identities

Example of logs

Now that the highway has been secured, it's time to get in the van and hit the road!

The Positive Way

WAVESTONE

Alexandre GUY
Manager

M +33 (0)6 20 02 63 50
alexandre.guy@wavestone.com

Arnaud PETITCOL
Manager

M +33 (0)7 61 78 24 79
arnaud.petitcol@wavestone.com

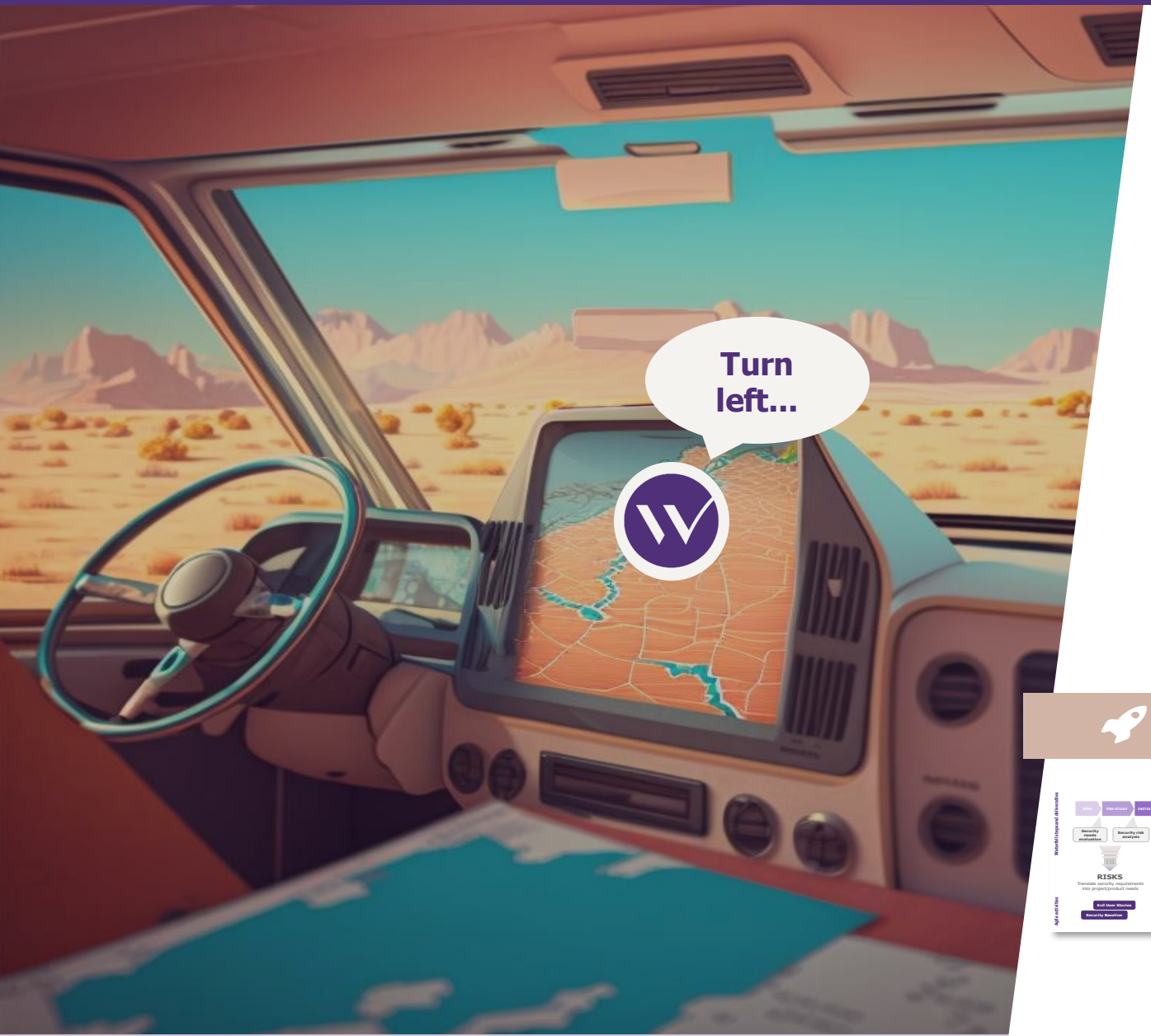
Jeanne GRENIER
Senior Consultant

M +33 (0)6 67 79 46 39
jeanne.grenier@wavestone.com

Thomas JOUBERT
Analyst

M +33 (0)6 51 17 92 14
thomas.joubert@wavestone.com

How does **Wavestone** *guide its clients in this journey?*



Our Capabilities

/ Co-construction of the **DevSecOps Model** / **Transversal Framework** (governance, tooling, processes, services...)

/ **Embody or assist** AppSec Manager, AppSec Back-End, AppSec Front-End or Security Champion roles

/ **Framing & follow-up** of DevSecOps projects / programs (RFPs, DevSecOps strategy & roadmap, deployments)

/ **Maturity assessment** and DevSecOps **recommendations**

/ Technical **POCs & Benchmarks** of DevSecOps solutions

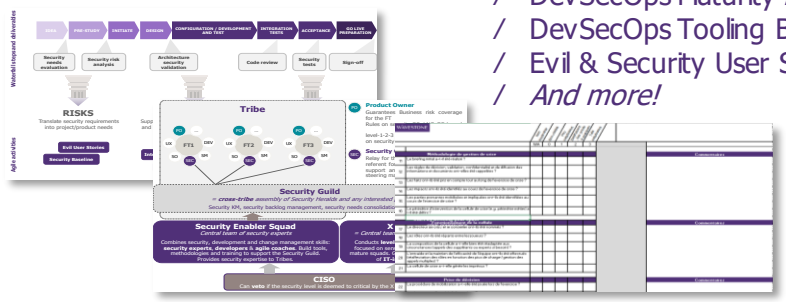
/ Definition of **DevSecOps policies**, rules & standards

/ Design of **Security Guardrails** (Security/Policy-as-Code)

/ **Threat Modeling and Rapid Risk Assessments**

/ AppSec & DevSecOps **Training & Awareness**

Our Boosters



/ DevSecOps Maturity Assessment Framework
/ DevSecOps Tooling Benchmarks
/ Evil & Security User Stories for Agile Security
/ *And more!*

MAJOR PROJECTS *to be carried out as part of a* DevSecOps PROGRAM

Organization and Skills

/ Security Champions
/ Creation of the AppSec Central Team
/ Operating Model
/ AppSec Community

Training & Culture

/ Training Security Champions
/ AppSec Knowledge Sharing
/ Creation of DevSecOps Knowledge Base
/ Animation of the Community

Threat Modelling & Security Baseline

/ Threat Modelling Framework Definition with STRIDE Methodology
/ Threat Modelling Tools
/ Definition of Done

Application Detection

/ SAST, DAST, *AST
/ SCA
/ IaC Scanning

Secret Management

/ Secret Manager
/ Secret Detector

Vulnerability Management

/ Vulnerability Manager
/ Qualification Modalities
/ Patching Process

Guardrails Automation

/ Automated guardrails design
/ Threshold Definition
/ CI/CD Configuration

Metrics & dashboards

/ Correction Speed (MTTD/R)
/ Acceptable Limits per Squad/Entities
/ Maturity-Based Approach
/ Tolerance Rate

Secure your Software Development Lifecycle with **DevSecOps**

Whether hosted in the Cloud or on-premises, get an end-to-end support for your development lifecycle

9 in 10 CISOs

are concerned about threat actors engaging in software supply chain attacks*.

98%
of software developers are not satisfied with their security tools*.

88%
of organizations experienced an AppSec breach in the past 12 months*.

Fixing a vulnerability** in production rather than in development phase costs

4 times more

*according to Checkmarx (2023)
**according to NIST (2023)

WAVESTONE

Your partner to secure your development lifecycle

Our Capabilities

ASSESS & REMEDIATE

- **AppSec & DevSecOps Maturity assessment**
- **Audits 360°** (white box): governance, architecture and implementation review
- **Pentest** and **redteam**: black and grey box
- Incident Response (CERT)

TRANSFORM

- Co-construction of the **DevSecOps Model** (governance, tooling, processes, services…)
- **Framing & follow-up** of projects / programs (RFPs, strategy & roadmap, deployments)
- **Training & Awareness** (Application Secure Development, DevSecOps, Get started with SAST/DAST/SCA…)
- Setting up **AppSec & DevSecOps Communities**

ENGINEER

- **Embody or assist** DevSecOps, AppSec Manager, AppSec Engineers or Security Champion roles
- Technical **POCs & Benchmarks** of DevSecOps solutions (SAST, DAST, SCA, IAST…)
- Define **policies**, rules & standards
- Design **Security Guardrails** (Security/Policy-as-Code)
- **Threat Modeling** and **Rapid Risk Assessments**

Our Boosters

Maturity Assessment Framework

CI/CD **Technical Audits** Methodology

Evil & security **user stories** for Agile Security

Training decks

Animation of **DevSecOps Communities**

The **Highway Model** of DevSecOps

Benchmarks of AppSec/DevSecOps solutions