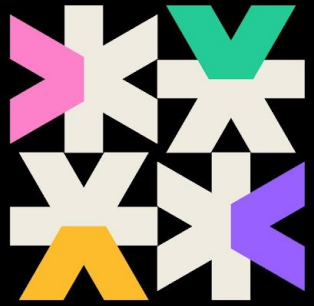


fintech_ devcon

PRESENTED BY moov

Secure Your Data Computations Efficiently

VERY GOOD SECURITY

Mohamad El Hajj

Very Good Security

Security Software Engineer

Talk Outline

- Data Security Overview
- Attack Surface
- State of the Art Solutions
- Starlarky

Data Security

Importance of Data Security

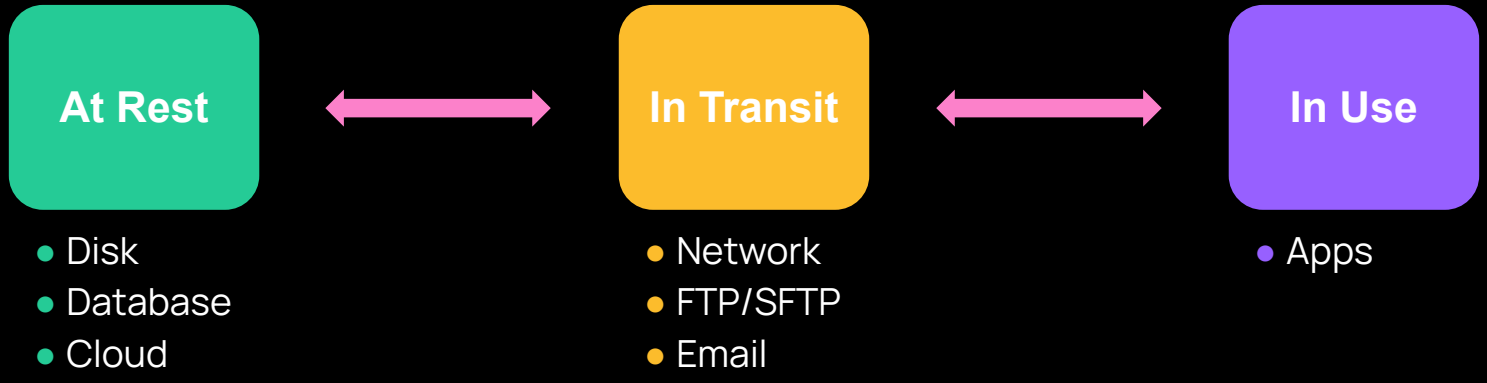
Data is…

- An asset
- A commodity
- Fuel for the economy
- Of high value

Data is also a liability, leaks lead to:

- Identity theft
- Loss of customer trust
- Reputation (brand) damage
- Financial loss
- Loss of business

The 3 States of Data



The 3 States of Data

At Rest

- Disk
- Database
- Cloud

In Transit

- Network
- FTP/SFTP
- Email

In Use

- Apps

Data In Use

When data is consumed for value extraction

- Decrypted / Plaintext
- Transformed by (untrusted) code
- Exposed in shared environment

How can we compute on data securely using untrusted code?

Attack Surface

Adversary Model

The adversary can **write code**...

- To transform data
- That executes on company infrastructure

Attack Surface

Vulnerable Code

- Buffer overflows
- System calls

System Access

- File system
- Network stack
- Timers / Clock
- DB
- Logs

Hardware

- Side channels

Resource Usage

- Memory
- CPU
- RNG

SoA Solutions

How can we compute on data securely using untrusted code?

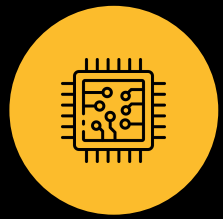
Answer: Isolation, Zero Trust

Different Granularities

Language Runtime

Process / OS
(sandboxing, process isolation)

Hypervisor
(VMs, micro-VMs)



Hardware
(Enclaves)

Isolation Methods

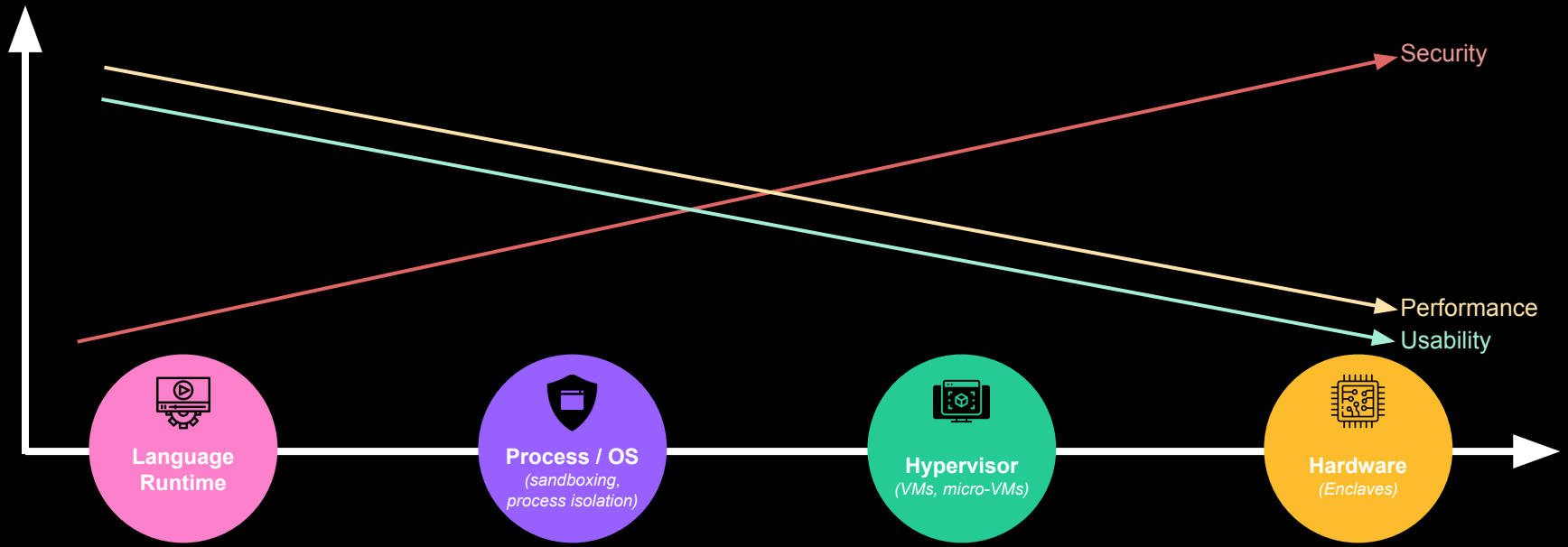
- Limits / disallows access
- Reduce timer precision

- OS virtualization
- Process separation
- System partitioning / overlay
- Reimplements syscalls

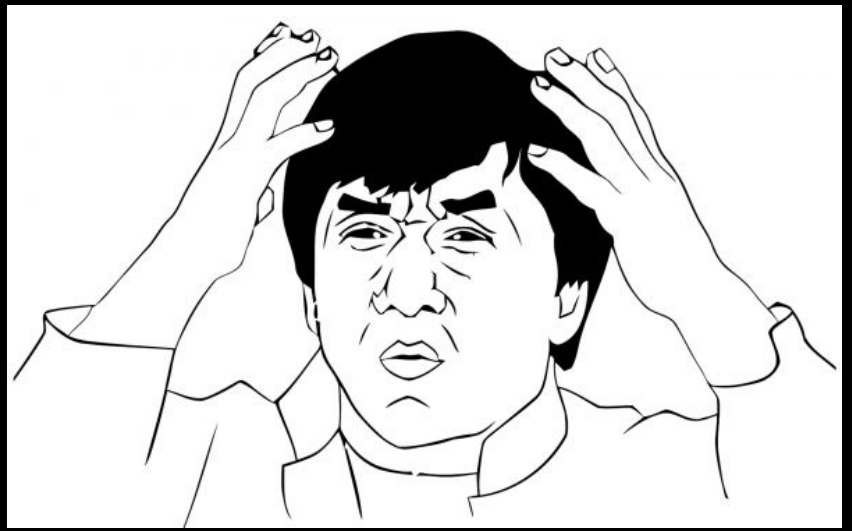
- Hardware & OS simulation
- Host separation
- Strong virtual separation

- Physical separation on chip

Isolation Tradeoffs



General-Purpose Languages?



Common Data Transformations

- Extraction
- Parsing
- Mapping
- Filtering / Aggregation
- Tokenization
- Enriching
- Formatting
- Casting
- Encryption

How can we compute on data securely without using expensive isolation?

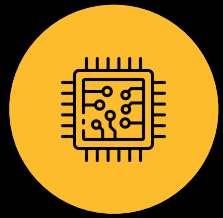
Starlarky

Starlarky at Language Granularity

Language Runtime

Process / OS

Hypervisor



Hardware

Starlarky at Language Granularity

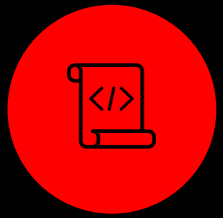
Language Runtime

Process / OS

Hypervisor

Hardware

Starlarky at Language Granularity

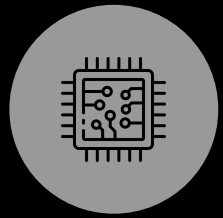


Language

Language Runtime

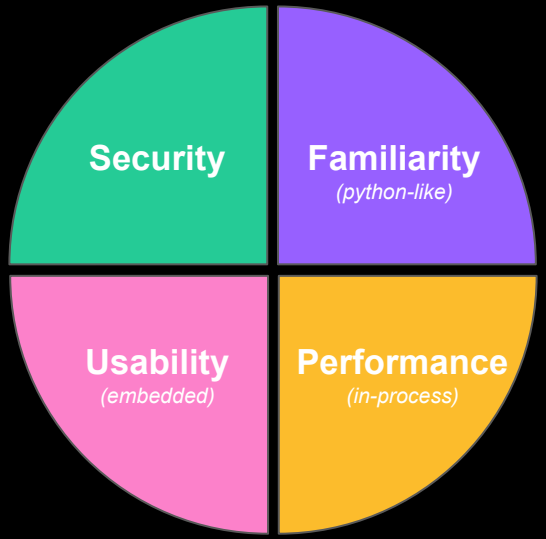
Process / OS

Hypervisor

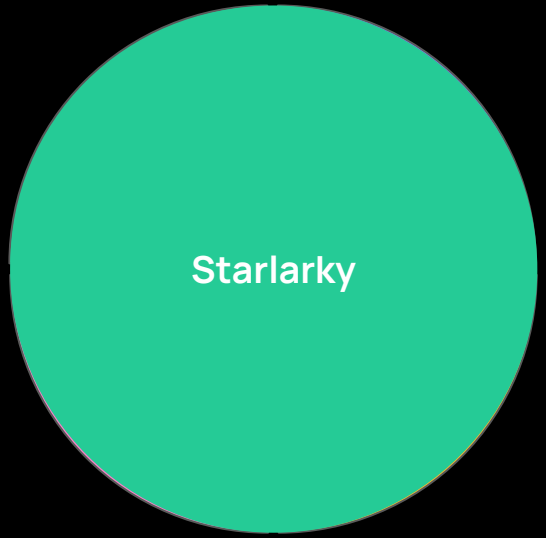


Hardware

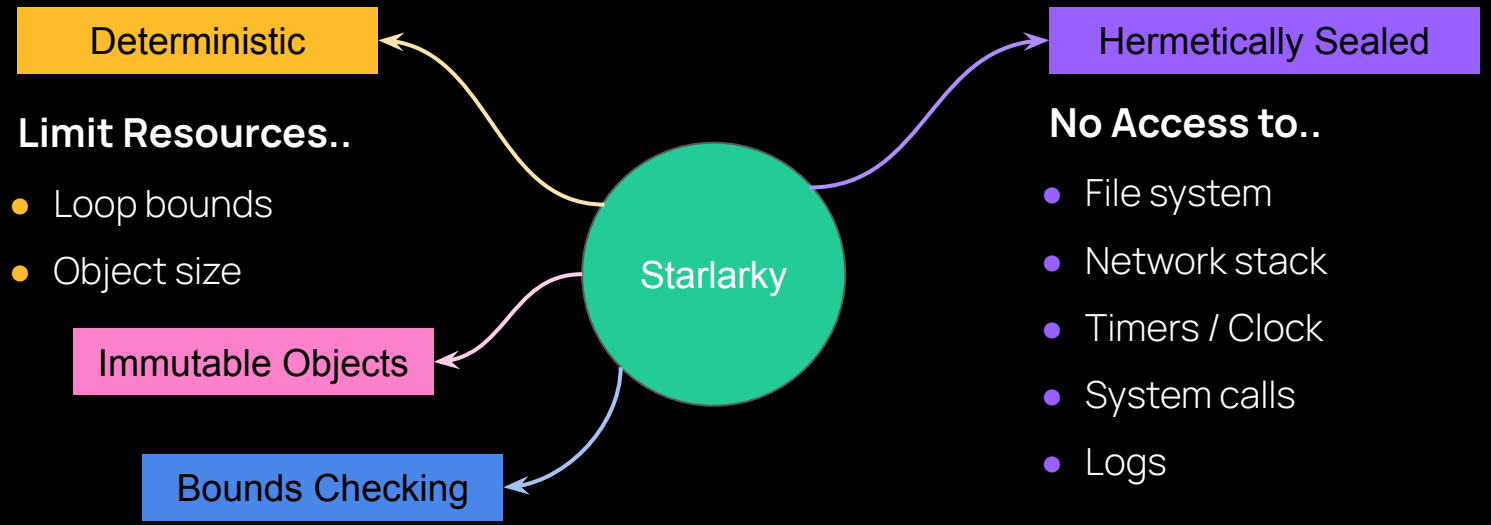
Starlarky Design Components



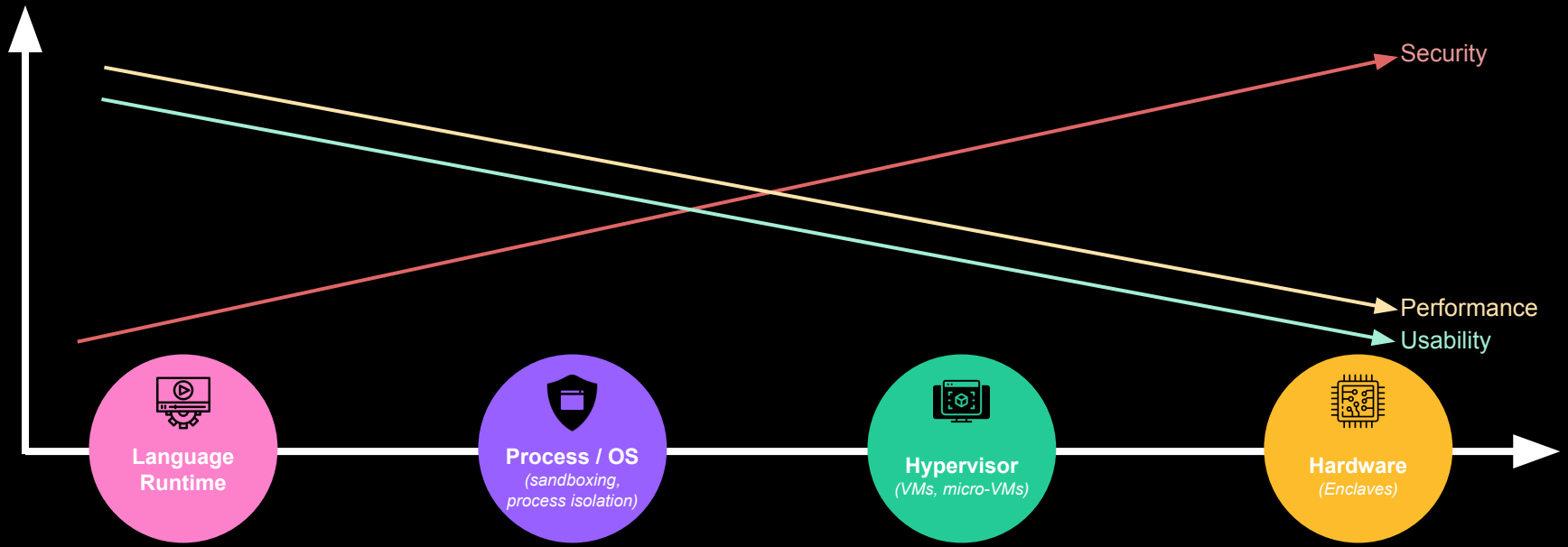
Starlarky Design Components



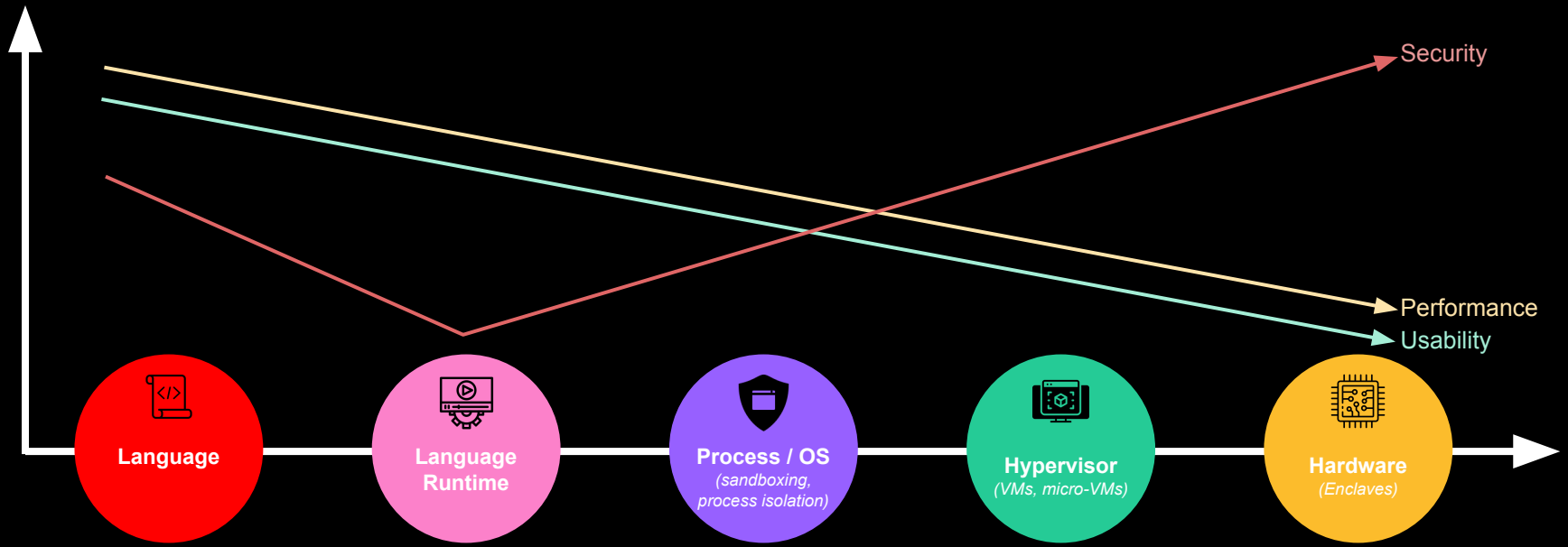
Starlarky Secure by Design



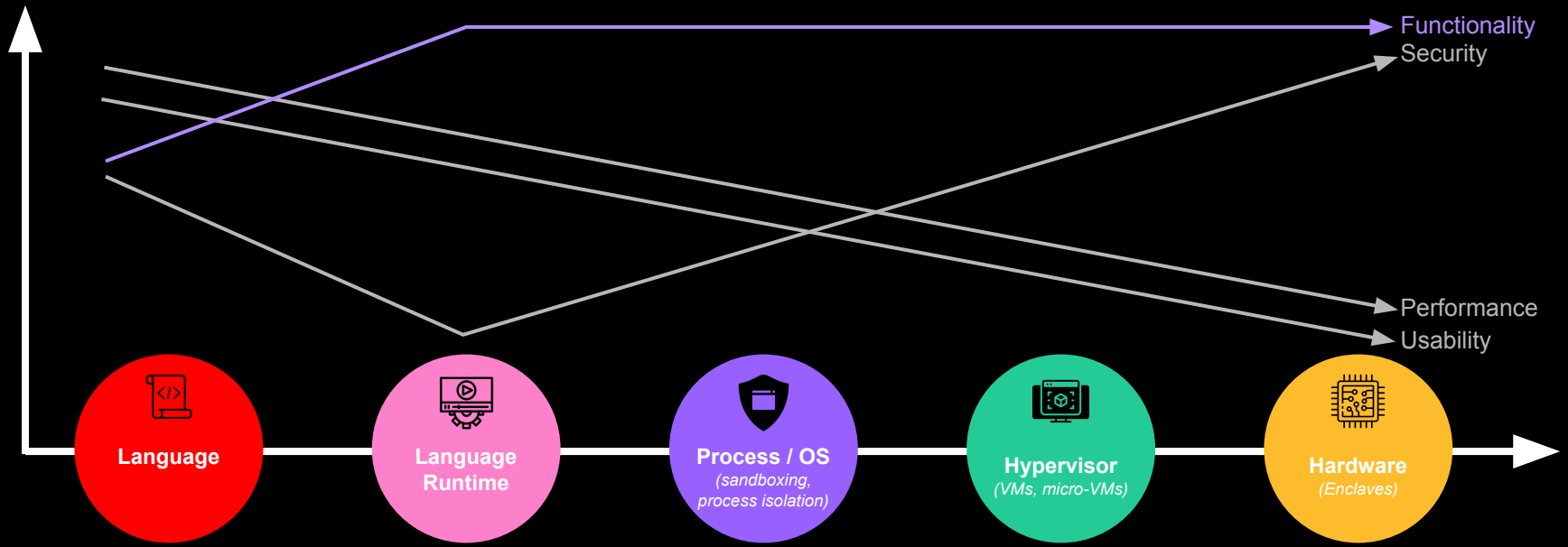
Tradeoff Recall



Minimizing Security Tradeoff



Sacrificing Functionality



Complex Use Cases

- Use Cases: ML, anti-virus scans, etc.
- Need general-purpose languages

Use Complex Isolation!

Demo

Q & A

Find Us

Workshop

Workshop Outline

- Build a Starlarky FaaS Server
- Build & Inject a Custom Module
- Contribute to Starlarky

Build a Starlarky FaaS Server

1. Download the project skeleton
   github.com/moehajj/starlarky-workshop-fintech-devcon
2. Setup your environment (install & configure tools)
3. Complete the code to integrate Starlarky Engine
   src/main/java/com/moehajj/spring/boot/grpc/example/StarlarkyService.java
4. Build, Run, Test, and Iterate

Implement a Custom Java Module

1. Implement a Custom Starlarky Java Module
   src/main/java/com/moehajj/spring/boot/grpc/example/modules/CustomModule.java
2. Inject it into the engine via bindings
   Example: `bindings.put("custom", new CustomModule());`
3. Invoke custom module from script (no need to import)
   Example: `custom.method(arg1, arg2, argName=arg3)`
4. Build, Run, Test, and Iterate

Contribute to Starlarky

1. Download the repository
   github.com/verygoodsecurity/starlarky
2. Contribute via a Starlarky Module
   larky/src/main/resources
3. (Extra) Try Py2Star
   github.com/mahmoudimus/py2star
4. Contribute via a Java Module
   larky/src/main/java/com/verygood/security/larky/modules

Contact

Mohamad El Hajj

mohamadelhajj