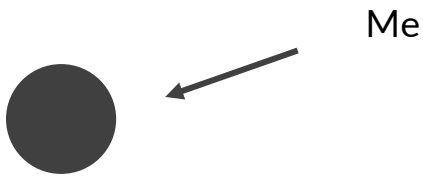
KEY NOTE

SECURING THE SOFTWARE THAT WILL SAVE THE WORLD

Laura Bell Main
CEO and Founder, SafeStack


Me

2000 to 2022

Apprentice Software Developer

AI and Robotics

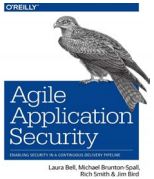
CERN

Counter Terrorism

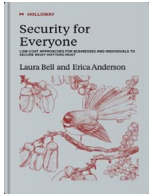
Penetration Tester

Security Consultant

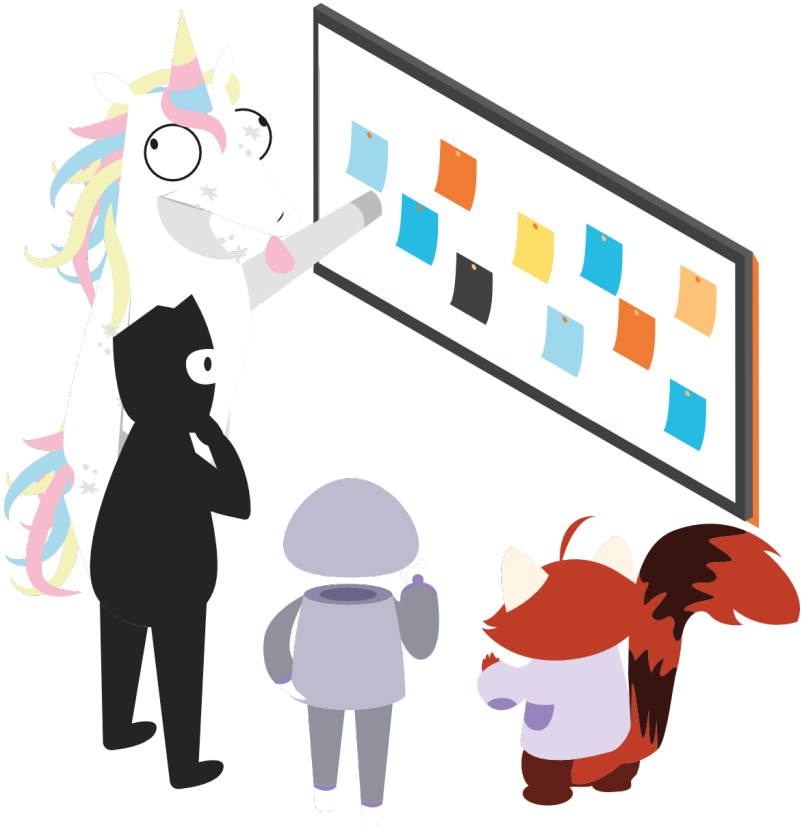
Founder



CEO



Finding the “Why”



The one about the **vineyard**

challenge

How healthy are my grapes and when are they ready to harvest?

FENDT
FENDT

the why

Vineyards are a just in time business.

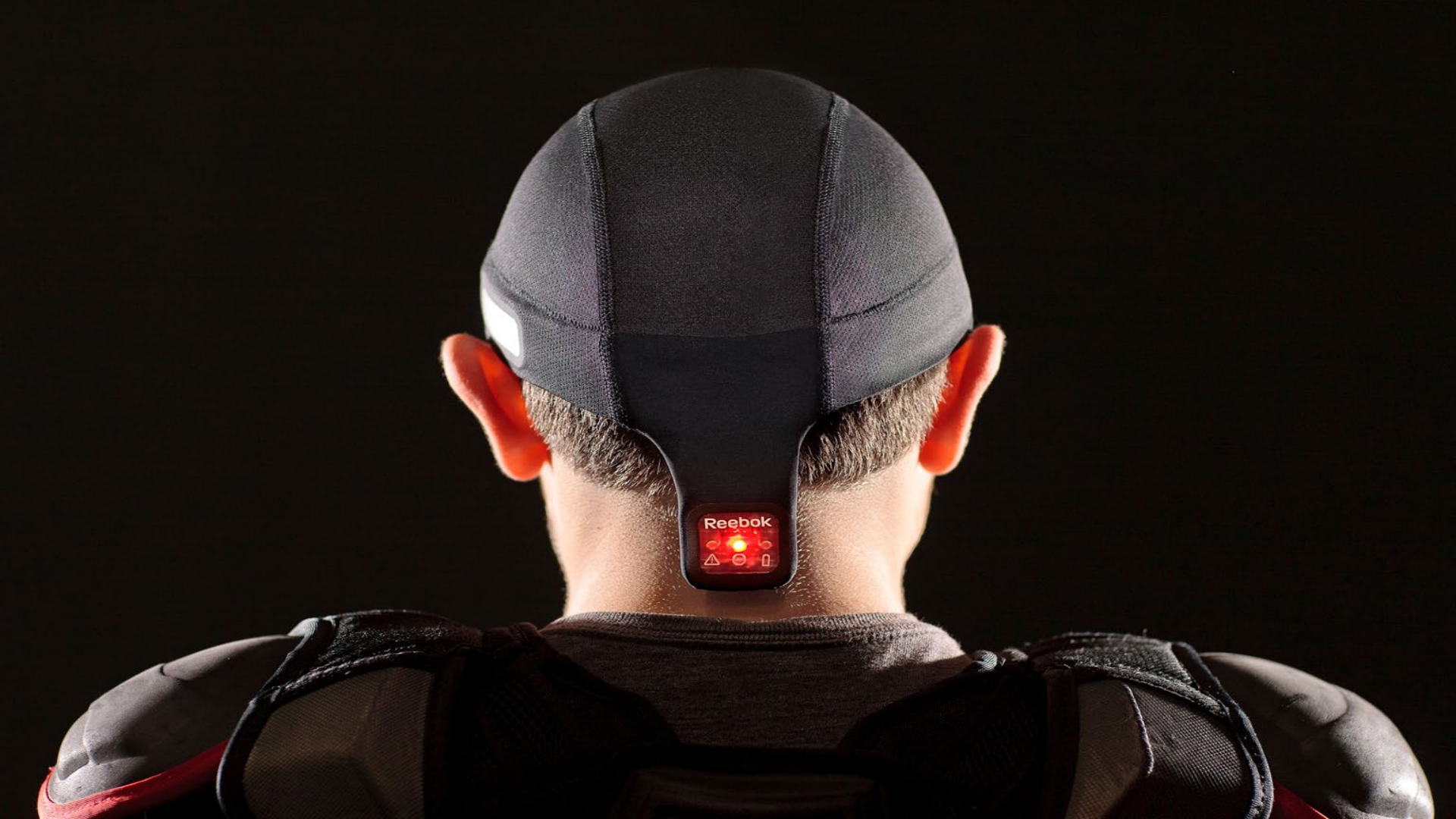
The health and readiness of their crop affects:

Hiring seasonal workers
Purchasing packaging
Selling prices to wholesalers and processors

The one about the **athlete**

challenge

How are my athletes performing?


Reebok

the why

Athletes work in a high risk environment

Understanding physical performance:

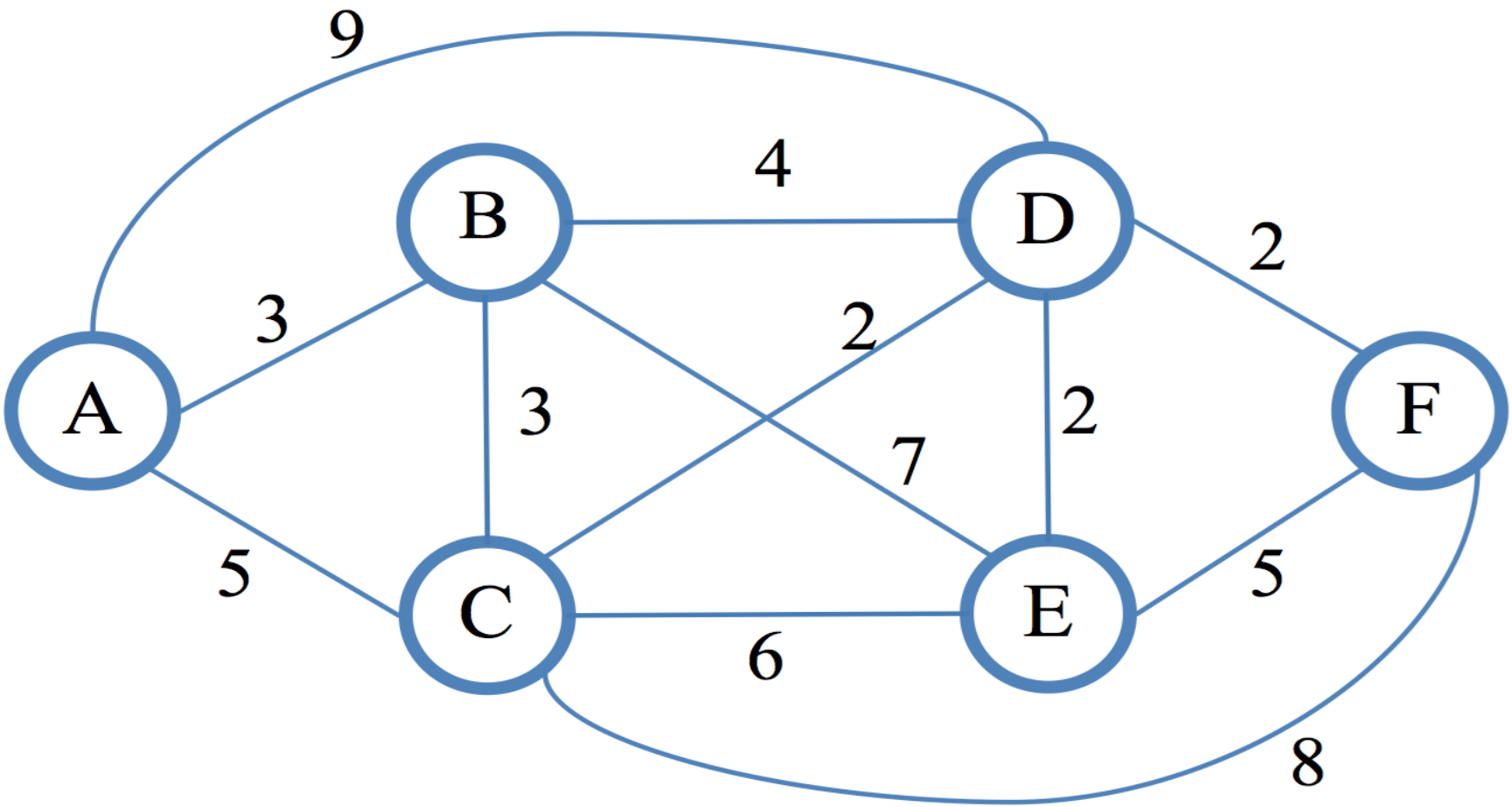
Reduces injury
Increases potential performance
Increases club revenues

The one about the **packages**

MECALUX
MECALUX

challenge

How can I manage my logistics warehouse?
(Where should I put this box?)


9
4
B
D
2
3
2
A
3
2
F
7
5
C
E
5
6
8

ARIEL
ARIEL
ARIEL 3in1 PODS

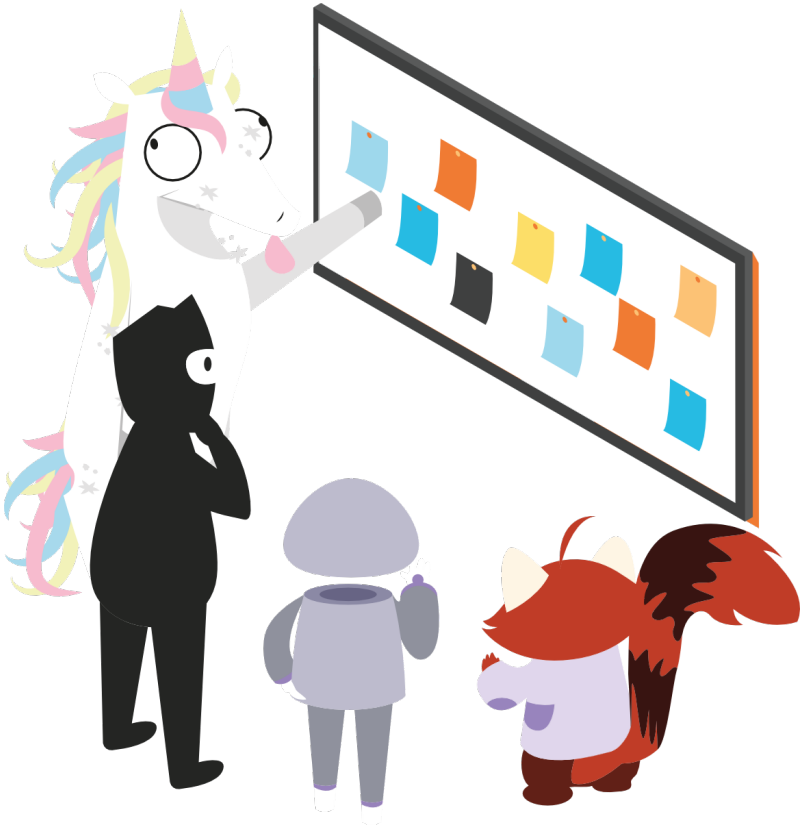
the why

Shipping and haulage is a massive, complex puzzle

Optimal physical placement of goods in a warehouse:

Reduces handling time
Reduces spoilage and theft
Creates a safer working environment
Increases productivity

Working together on the “How?”



our security guidelines **were not built** with the future in mind

OWASP TOP 10 2003

- A1 Unvalidated Input
- A2 Broken Access Control
- A3 Broken Authentication and Session Management
- A4 Cross Site Scripting
- A5 Buffer Overflow
- A6 Injection Flaws
- A7 Improper Error Handling
- A8 Insecure Storage
- A9 Application Denial of Service
- A10 Insecure Configuration Management

Credit: https://www.hahwul.com/cullinan/history-of-owasp-top-10/

OWASP TOP 10 2021

- A1 Broken Access Control
- A2 Cryptographic Failures
- A3 Injection
- A4 Insecure Design
- A5 Security Misconfiguration
- A6 Vulnerable and Outdated Components
- A7 Identification and Authentication Failures
- A8 Software and Data Integrity Failures
- A9 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery

Increased architectural complexity

High use of 3rd party integrations

Larger development community

Non-linear code pathways

Continuous availability

Increased regulation

We have new categories of problems to solve

Natural Language

- Predefined corpus
- Pre-trained models
- No-code and low code
- IP theft and deep fakes

Data Science

- Large, complex data sets
- Sensitive information, privacy and de-identification
- Increased regulation

IOT

- Mass produced commodity devices
- Lifetime support and software liability
- Widespread connectivity and embedded devices

30,000,000

Software developers in full time employment today and growing at 1.2 million per year

The world is not as mature as we like to think

Cutting Edge

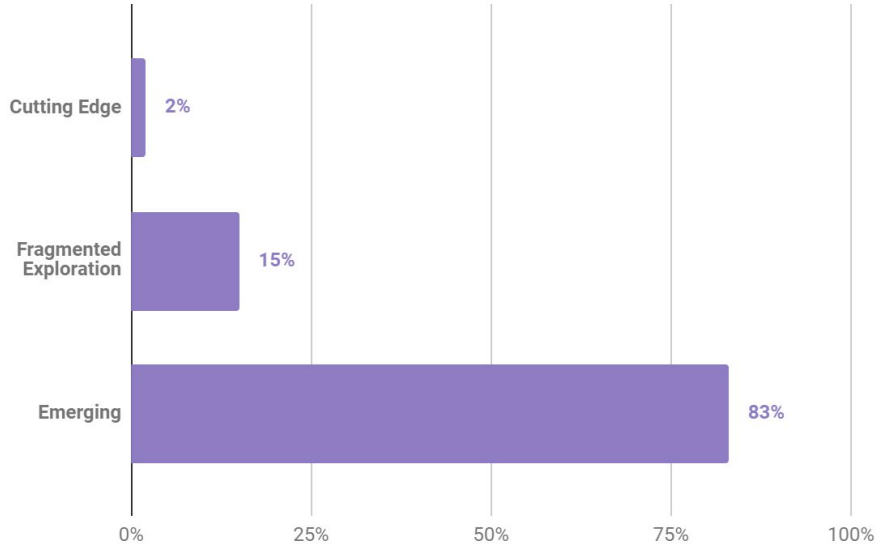
Bleeding edge of application security, DevOps, actively building application security teams

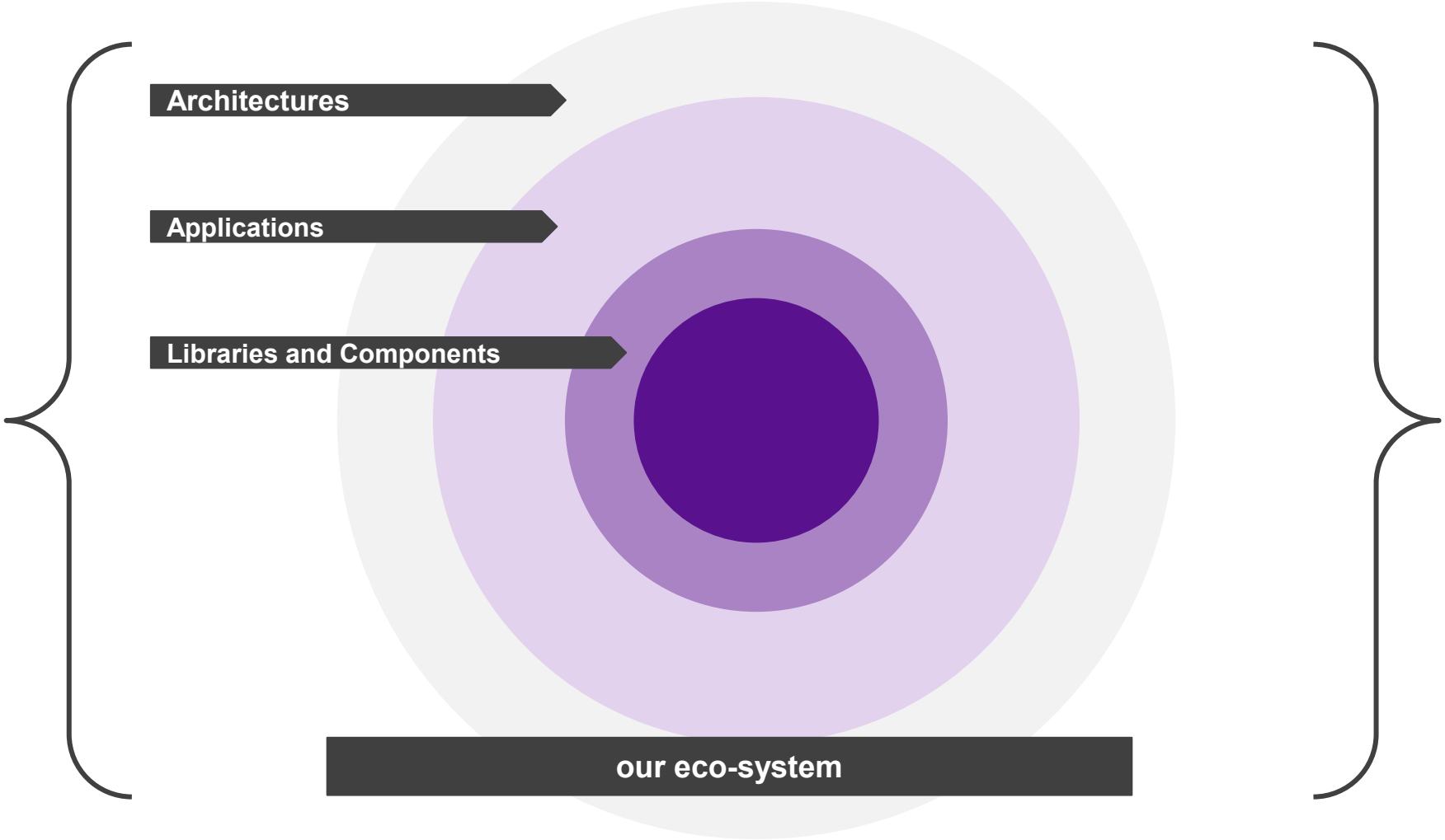
Fragmented Exploration

Fragmented approach to all security domains, looking for guidance and coherence

Emerging

Immature or traditional security practices only.




Architectures
Applications
Libraries and Components
our eco-system

To protect **one** of us
We must protect **all** of us

We need to find the **why**
for securing every technology and then we need
to **work together** to secure it

Laura Bell Main

laura@safestack.io
@lady_nerd
www.safestack.io

Free training