Security is an API:
Evolving to a decentralised security culture

Roger Wang
Senior Solutions Architect | AWS

SECURITY IS AN API

Thank You to Our Sponsors and Hosts!

AppSec NZ
appsec.org.nz

OWASP NEW ZEALAND
owasp.org.nz

AUT UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

BASTION SECURITY GROUP

DATACOM

aws

84.

PentesterLab

plexure

VERACODE

Without them, this Conference couldn't happen.

What is an API? Technology

1. A way for two or more computer programs to communicate with each other
2. This communication uses a structured software interface, which offers a service to other pieces of software
3. This simplifies programming by abstracting the underlying implementation and only exposing the actions the developer needs
4. A standard that describes how to build or use such an interface is called an API specification
5. A computer system that meets this standard is said to implement or expose an API

What is an API? Teams

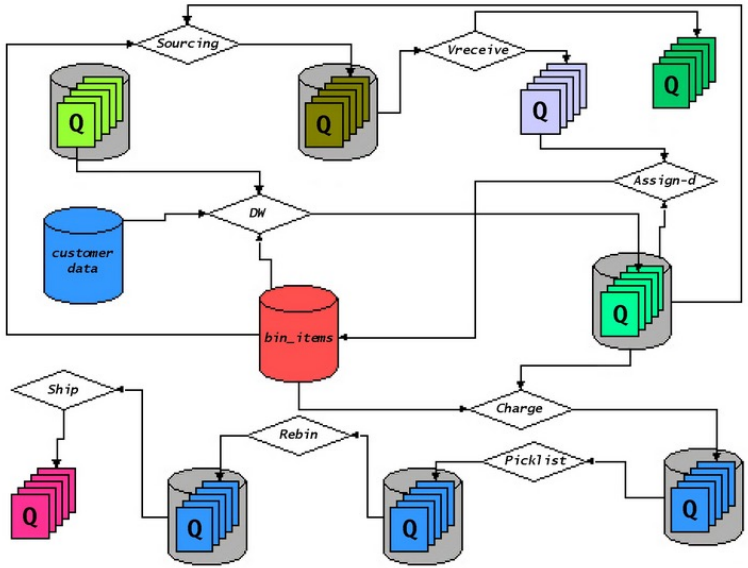
1. A way for two or more humans or teams to communicate with each other
2. This communication uses a structured process, which offers a service to other teams
3. This simplifies interactions by abstracting the specific team process and only requiring humans to interact in predefined ways
4. A standard that describes how to build or use such a process is called an API specification
5. A team that meets this standard is said to implement or expose an API

Software evolution

SECURITY IS AN API

System architecture, 1998

amazon.com
EARTH'S BIGGEST BOOKSTORE

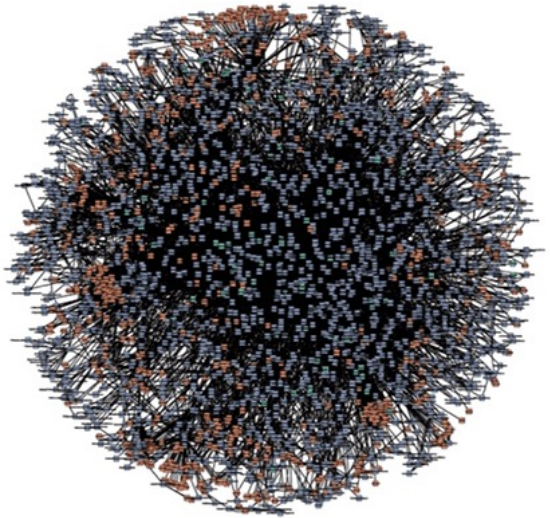


The Distributed Computing Manifesto

bit.ly/3UaT6dP

SECURITY IS AN API

20 years later

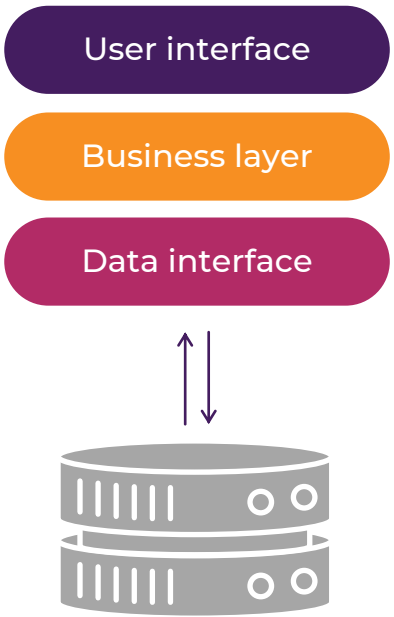


amazon

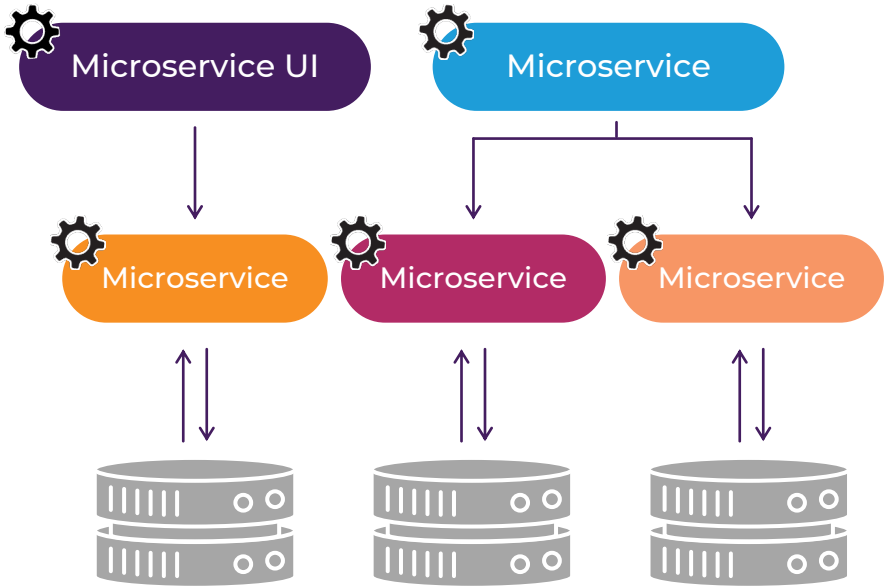
NETFLIX

Software evolution: Monolith to microservices

Monolithic architecture
Centralised / organised



Microservices architecture
Decentralised / organised

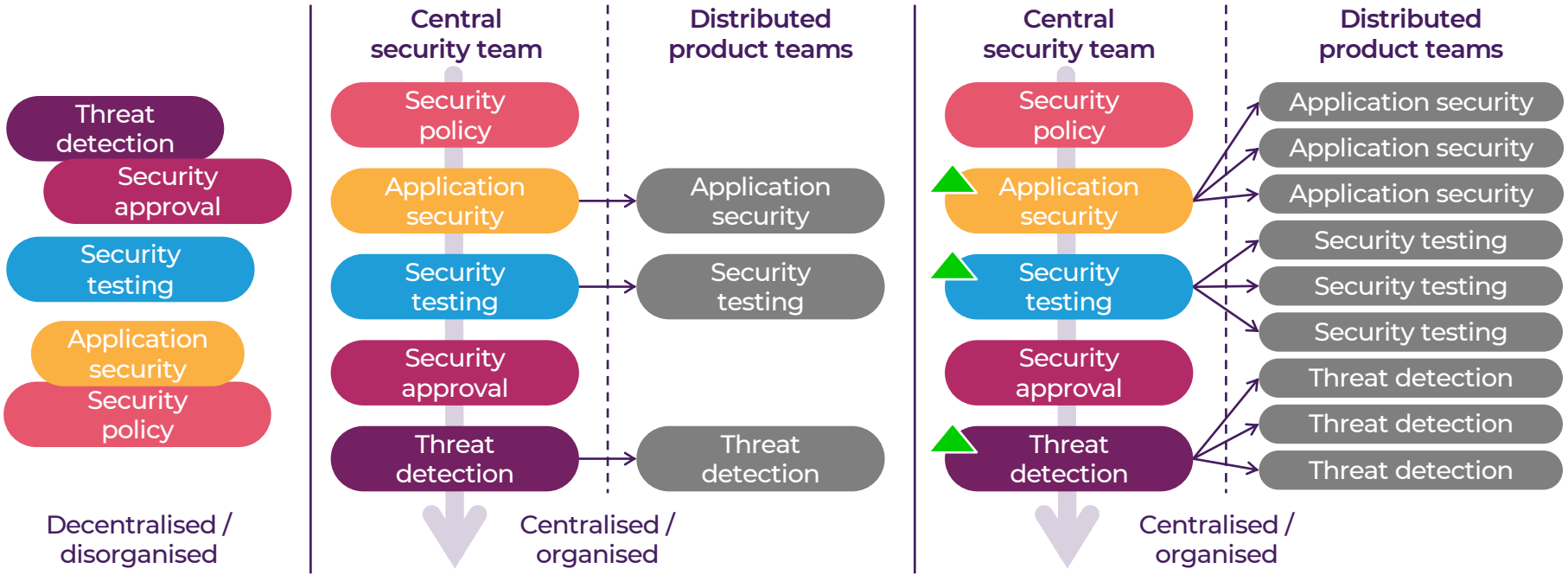


SECURITY IS AN API

Security evolution

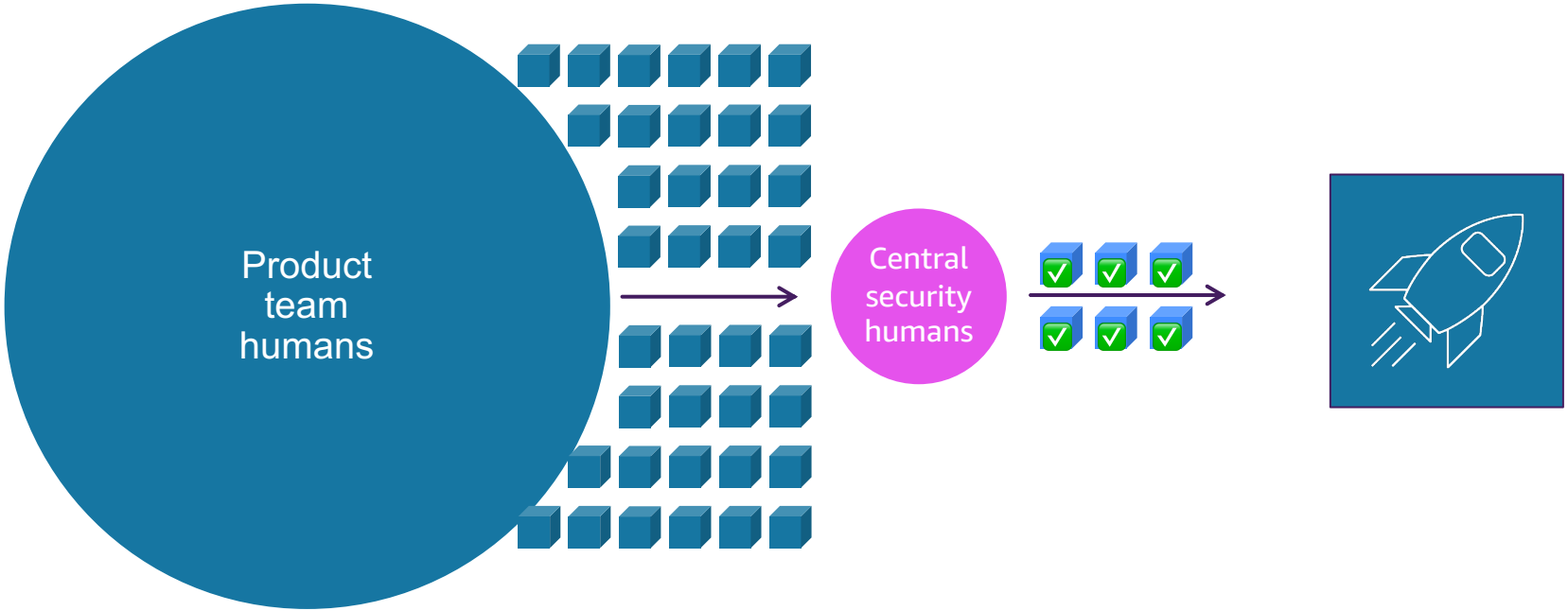
SECURITY IS AN API

Security evolution



SECURITY IS AN API

Builders : Security ratio disparity



Security evolution: APIs are everywhere

One: APIs underpin modern tech, and your modern business likely runs on APIs

Level one

Security evolution: APIs need to be secure

Two: You need to make sure these APIs are secure. This is “Security of the API”

OWASP
API Top Ten

bit.ly/4aDl9Yx

SECURITY IS AN API

Security evolution: Security tools and APIs

Three (A): Your security tools need to understand APIs

Three (B): Your security tools should expose their own APIs

SECURITY IS AN API

Security evolution: Security is an API

Four: Redefine your security process & culture to use the structure of APIs

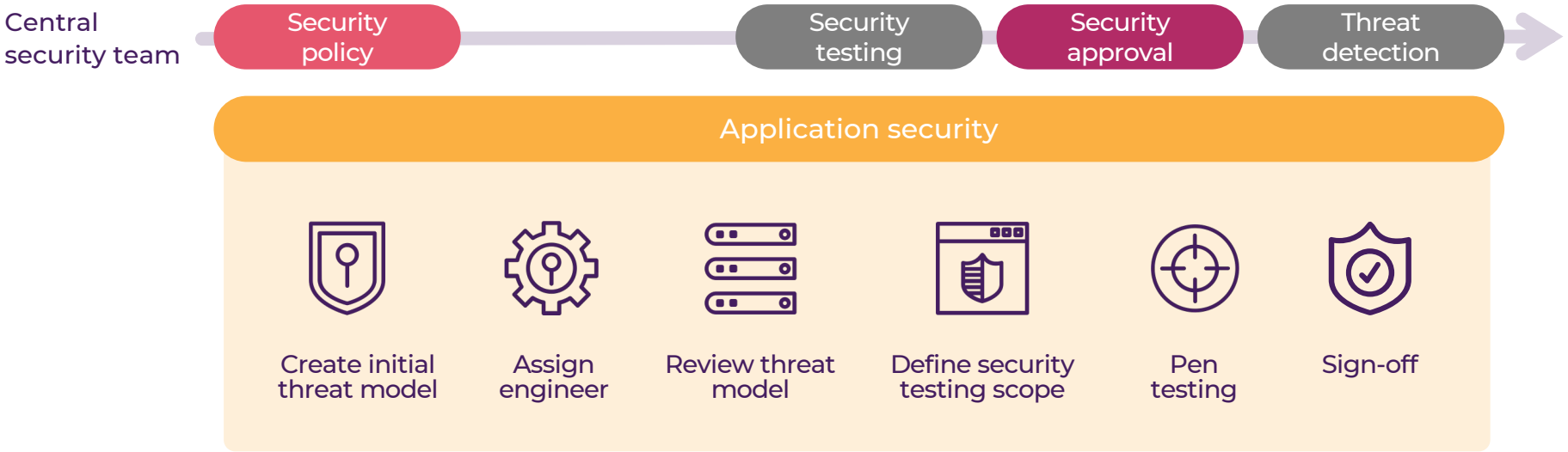
SECURITY IS AN
API

What is an API? Teams

1. A way for two or more humans or teams to communicate with each other
2. This communication uses a structured process, which offers a service to other teams
3. This simplifies interactions by abstracting the specific team process and only requiring humans to interact in predefined ways
4. A standard that describes how to build or use such a process is called an API specification
5. A team that meets this standard is said to implement or expose an API

Security is an API

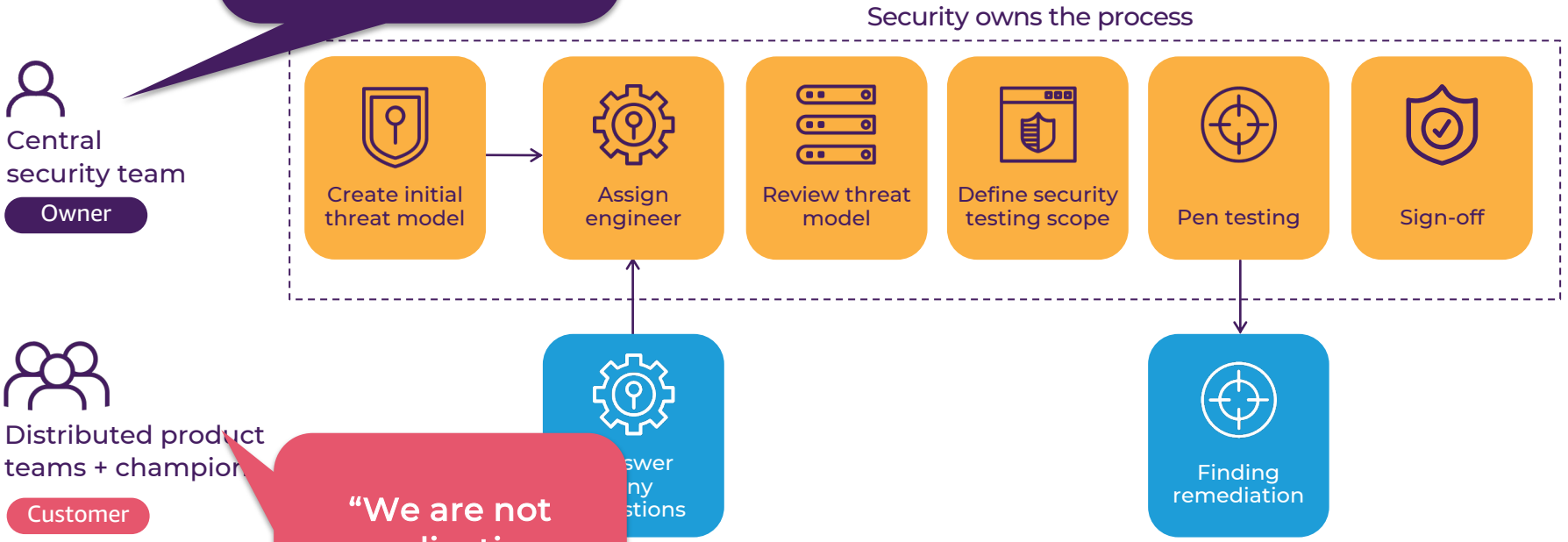
Decentralised / organised



SECURITY IS AN API

Security [illegible]cation security as a monolith

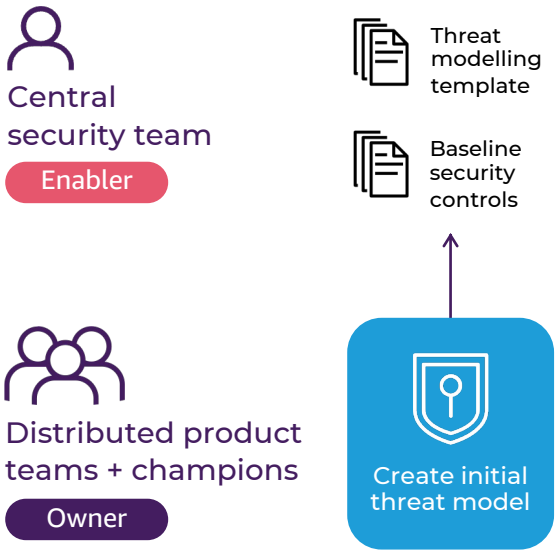
"We are not deep experts in the design of every feature that is currently being built"



"We are not application security experts"

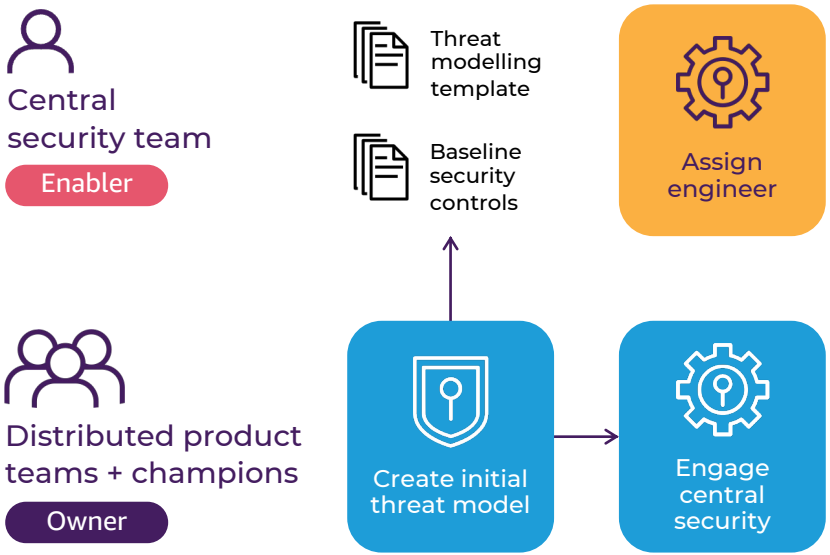
SECURITY IS AN API

Security is an API: Application security as a microservice



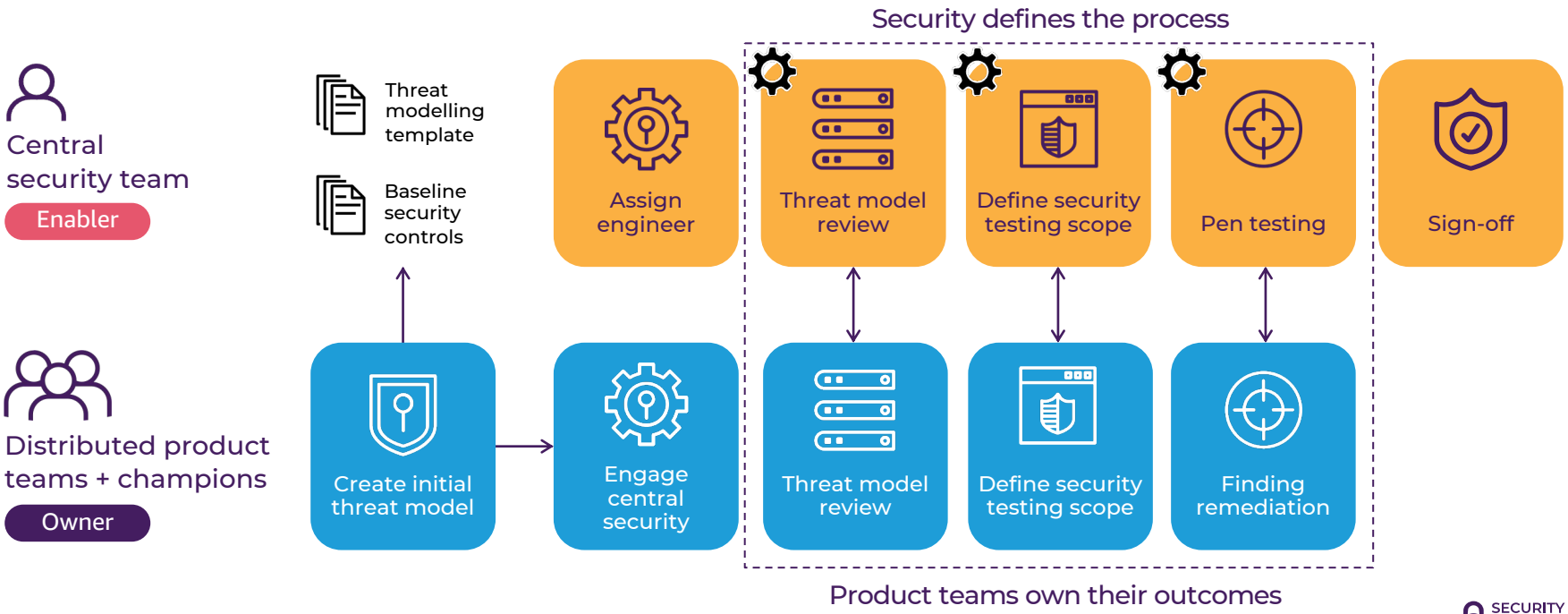
SECURITY IS AN API

Security is an API: Application security as a microservice



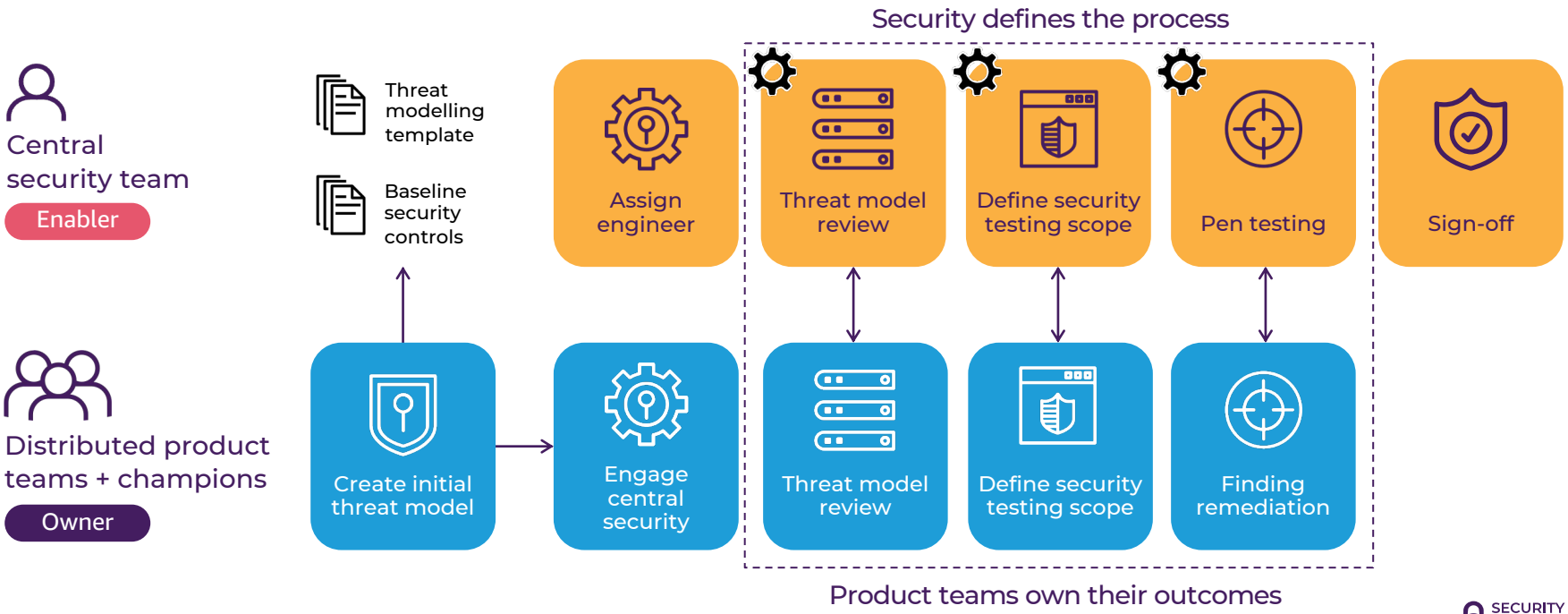
SECURITY IS AN API

Security is an API: Application security as a microservice



SECURITY IS AN API

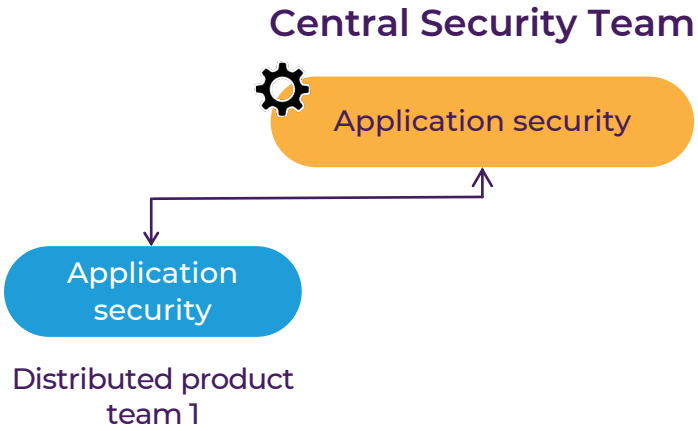
Security is an API: Application security as a microservice



SECURITY IS AN API

Security is an API: Lengthen the lead (leash)

The better the data, the longer the lead

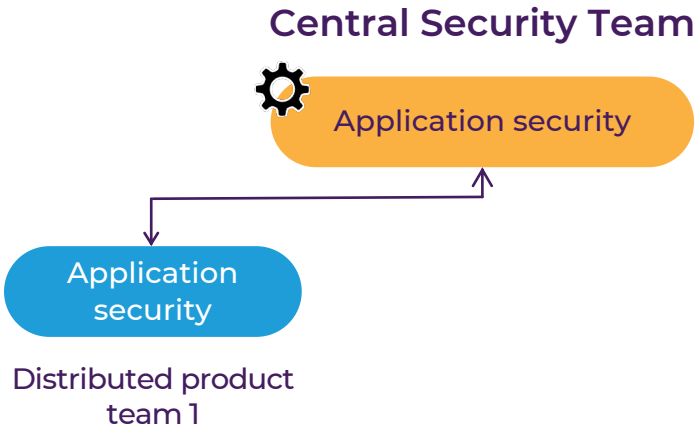


Security is an API: Lengthen the lead (leash)

The better the data, the longer the lead

Product Team 1

- does not share telemetry
- does not have a champion
- does not maintain a threat model
- more manual / human interactions
- result: they go slower

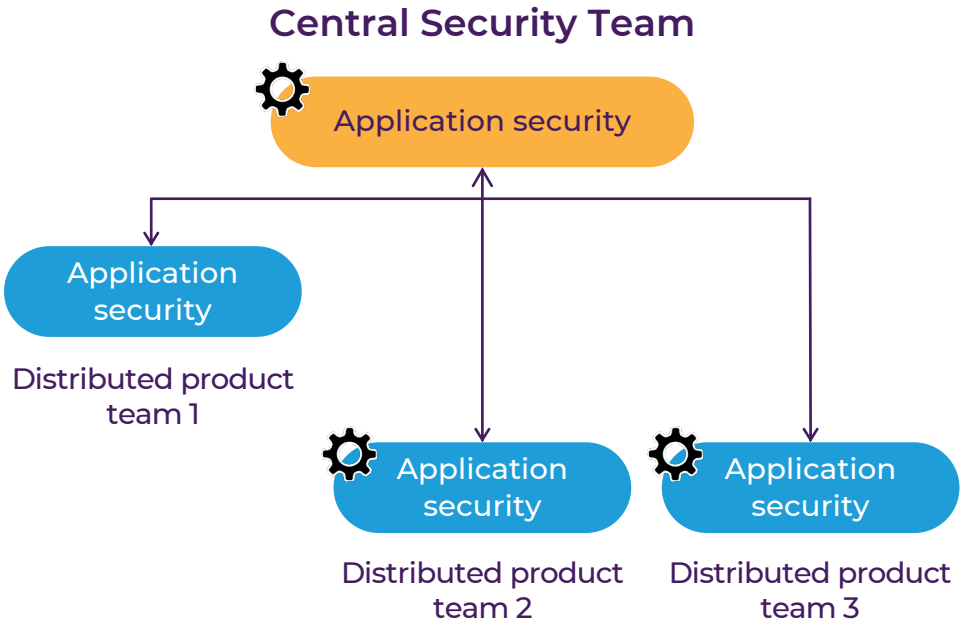


Security is an API: Lengthen the lead (leash)

The better the data, the longer the lead

Product Team 1
- does not share telemetry
- does not have a champion
- does not maintain a threat model
- more manual / human interactions
- result: they go slower

Product Teams 2 & 3
- share telemetry
- have champions
- maintain their threat models
- minimal manual / human interactions
- result: they go faster



SECURITY IS AN API

Security is an API: Inception levels

Level one
In your modern business, developers build APIs

Level two
Your security team publishes the standard for how product teams should build APIs securely

Level three
(A) The security tools used by product teams validate that the APIs they build are secure and
(B) The security tools expose an API so they can be queried remotely

Level four
The AppSec process for new APIs follows an “API-like” structure: well defined process interfaces enable teams to be decentralized and scalable - machines test data while humans review threat models

SECURITY IS AN API

Your next steps

Technology

- Follow best practices for API security
- Use security tools that understand APIs
- Use security tools that are APIs and/or expose APIs

OWASP
API Top Ten

bit.ly/4aDl9Yx

SECURITY IS AN API

Your next steps

Process

- Re-define your process to make distributed product teams accountable for their security
- Have specific teams build granular threat models
- Embrace security champions

OWASP
Security Culture

bit.ly/49pPZCW

SECURITY IS AN API

Your next steps

People

- Identify, train and maintain security champions
- Train developers how to do threat modeling
- Have your leaders talk about security – from the CEO down

Threat Modeling for Builders Workshop

bit.ly/3TJE8ty

SECURITY IS AN API

Feedback

bit.ly/4e1gqSf

Thank you

Roger Wang

yibowang@amazon.com

roger-nz

SECURITY IS AN API