Hewlett Packard
Enterprise

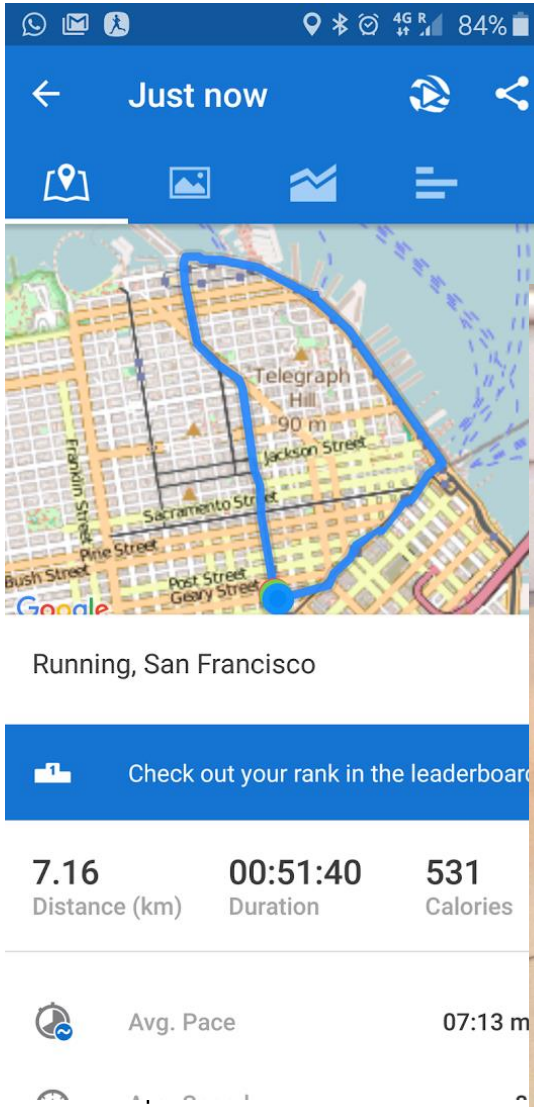
# A day in a life of HPE security architect

## or.. My 3 stairs to security (heaven)

Ori Troyna, Transform Security Lead
ITOM & ADM Cross portfolio Security
Technologies lead

# Who am I?

## Ori Troyna



84% 07:43

Just now

Running, San Francisco

Check out your rank in the leaderboar

| | | |
|---|---|---|
| 7.16<br>Distance (km) | 00:51:40<br>Duration | 531<br>Calories |

Avg. Pace 07:13 m

# My 3 stairs to security

Hewlett Packard
Enterprise

# What we will not discuss today

### Scanners

- Static
- Dynamic
- 3rd party
- Etc..

### Runtime

- WAF
- RASP
- Etc..

### HPE SW

- Product names
- Process
- Etc..

# My daily Challenges

– What are we facing today? **Flood of information**

## Per Year

**60**

**Products**

Across our portfolio.

**450**

**Risk Assessments**

Are conducted and separated to different types: threat modeling, design review, automatic scanning.
manual penetration testing,

**15**

**Operating Roles**

Taking part in the assessments life cycle:
Security team, R&D team, QA team, Product management, Corporate teams, management.

**180**

**Releases**

Required to undergo security assessment.

**12**

**World wide locations**

With dozens of teams requires support across time zones

.

**$$$**

**Working hours**

Are spent to manage the entire lifecycle by the different roles assigned

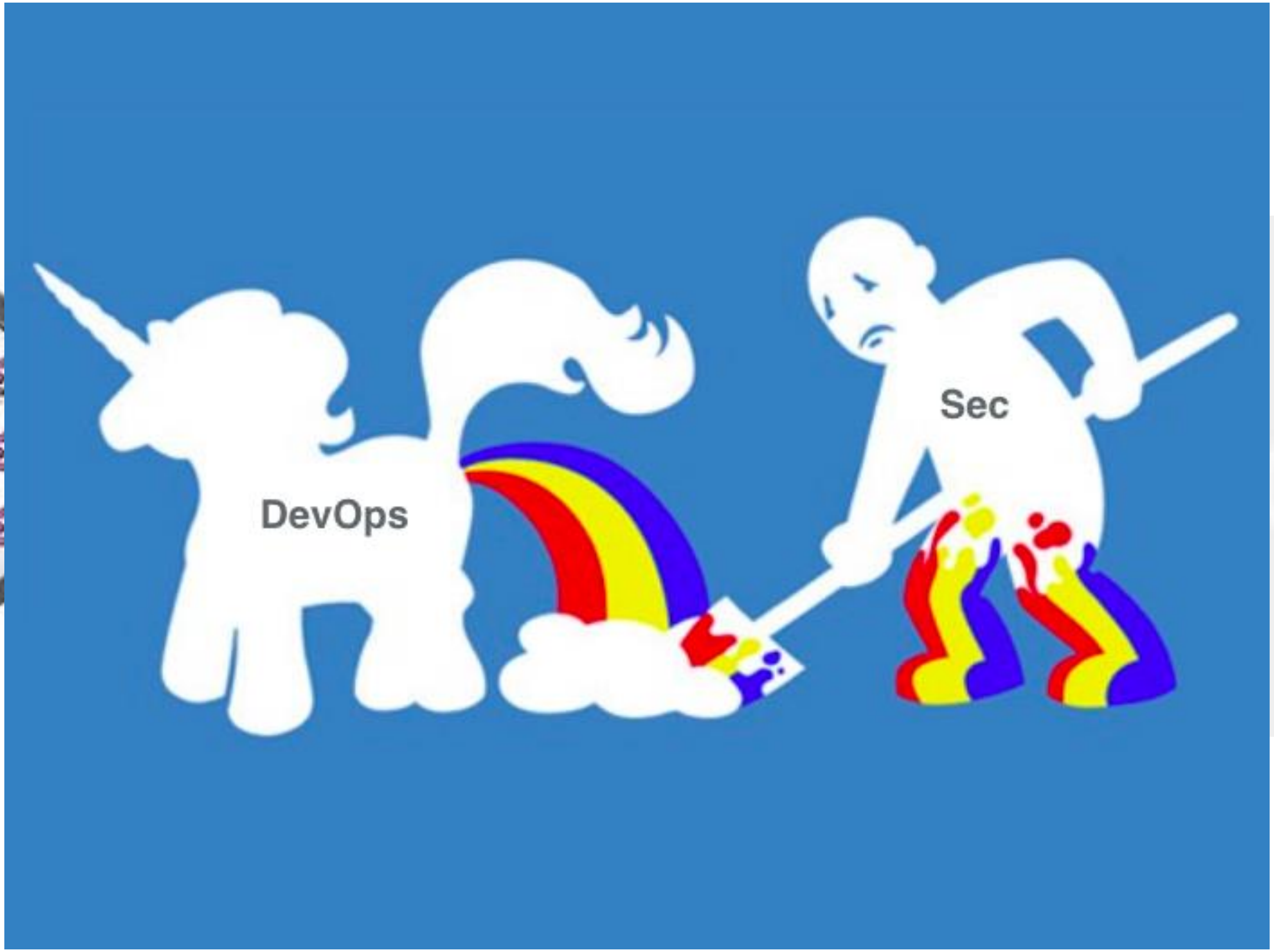
# Product teams challenge

## Products Teams

## Security Architect

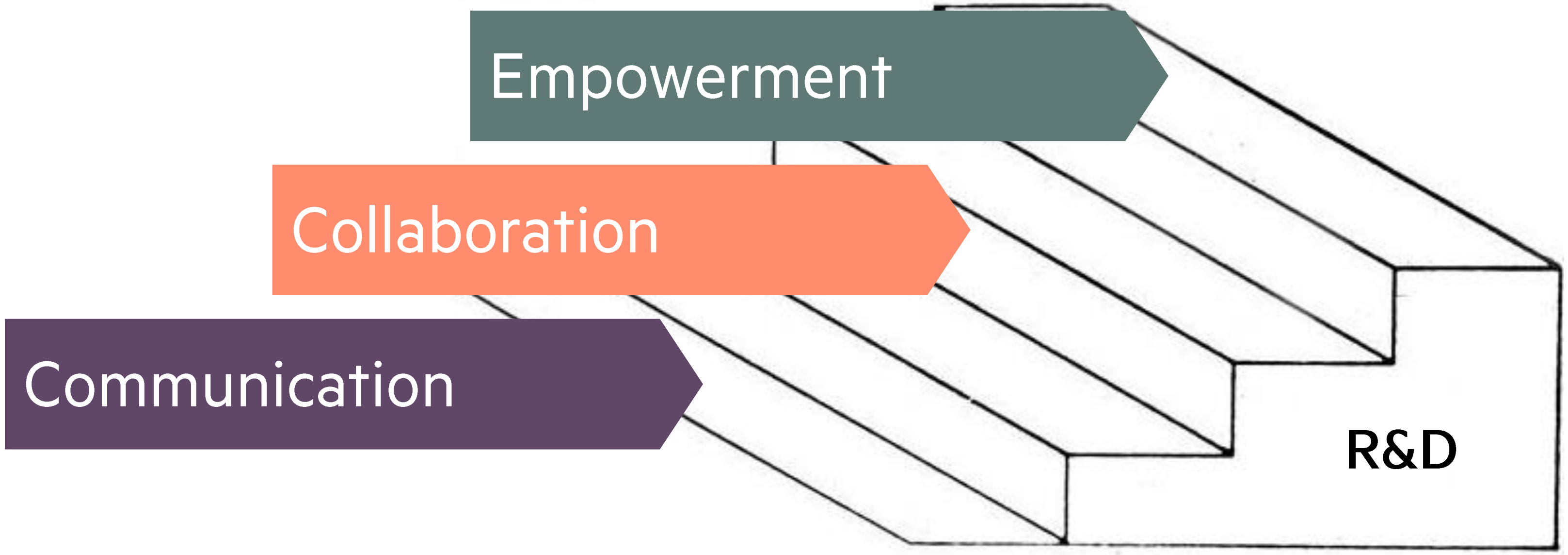
VS

# Development challenges



# My stairs to security

Three key steps for successfully embedding security in SW products



Empowerment

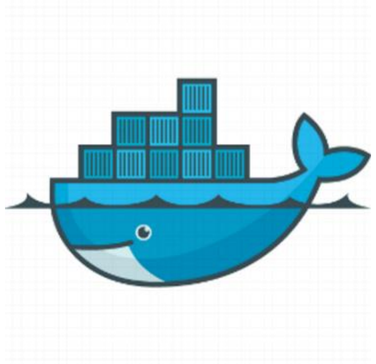
Collaboration

Communication

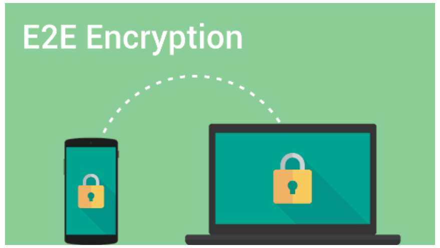
# User stories & what we learned?

redis

Docker

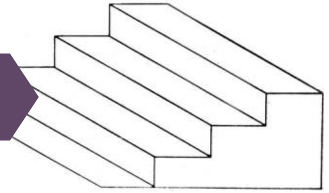


E2E encryption



# redis

Communication



– Open source (BSD licensed), in-memory **data structure store**

– "It's good to get reports, …… ,

in a software which is designed to be totally insecure if exposed to the outside world."

– antirez

– Workaround:

1. Create a secure repository scripts
2. Preapprove any script and create a digest (define a process)
3. Load the scripts from a secure location
4. Use EVALSHA instead (rename the method)

I got an email

"You know we use redis ….. There is a cool method called EVAL that we must use"

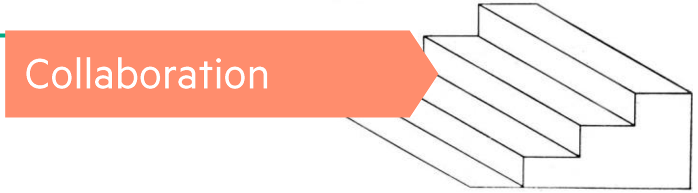
EVAL!!

"Yes based on LUA"

Bottom line: good **communication** prevented new security hole in production and new ground rules

for 3rd parties

# Docker



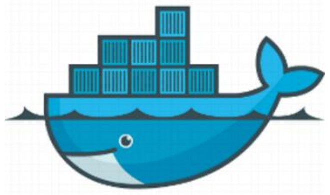
- Open source, Based on tried and tested features of the *Linux kernel – over 15 years*
  - Namespaces, cgroups, etc..
- **“Develop, Ship and Run Any Application, Anywhere”**

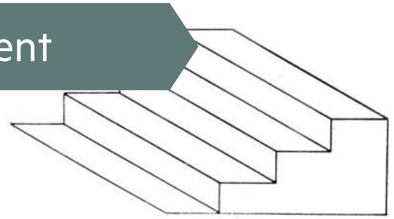
About a year ago, most products teams stated that Docker is the next thing, let’s go for it.

- What is docker ?
  - Is it enterprise ready…?

- Good cooperation with R&D lead to joint research on the different aspects of Docker
  - Result: Docker is not ready for adoption
- Current days
  - Docker security evolve
  - In-depth assessment how to onboard securely and harden

Bottom line: great **collaboration** lead to insights about new technology on boarding and set of hardening





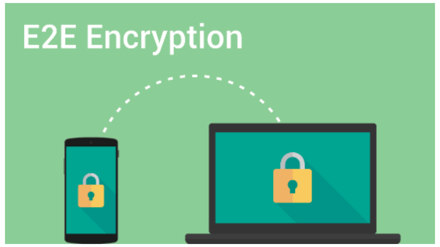
# E2E encryption

- High demand from customers to protect sensitive information found in the cloud
  - Current situation mixed with policies
- Very complex product with global team
  - Pure internal development
  - Stressed timelines to production

From the product point of view, the easy thing was to invent the wheel

- Result: we block the release….
- What actually happened:
  - We created a think tank to get the most of all worlds, security & product
    - Using asymmetric and symmetric cryptography
  - Worked together on every challenge
  - PenTested as soon as we could
  - Released successfully to customers

Bottom line: great **Empowerment** created security standards to the organization



# My stairs to security

## Three key steps for successfully embedding security in SW products

### Communication

1. Security is part of the development team
2. Keep open communication channels
3. Be open for suggestions

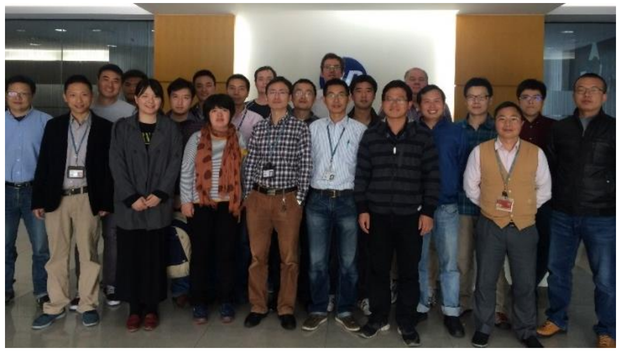
### Collaboration

1. Research together on new subjects

### Empowerment

1. Delegate when possible
2. Create a baseline to hardening guidelines
3. Define ground rules for new 3rd parties
4. Establish Product Security Standards

HP Software IL Academy
Roy Kornvlats



Hewlett Packard
Enterprise

# Thank you