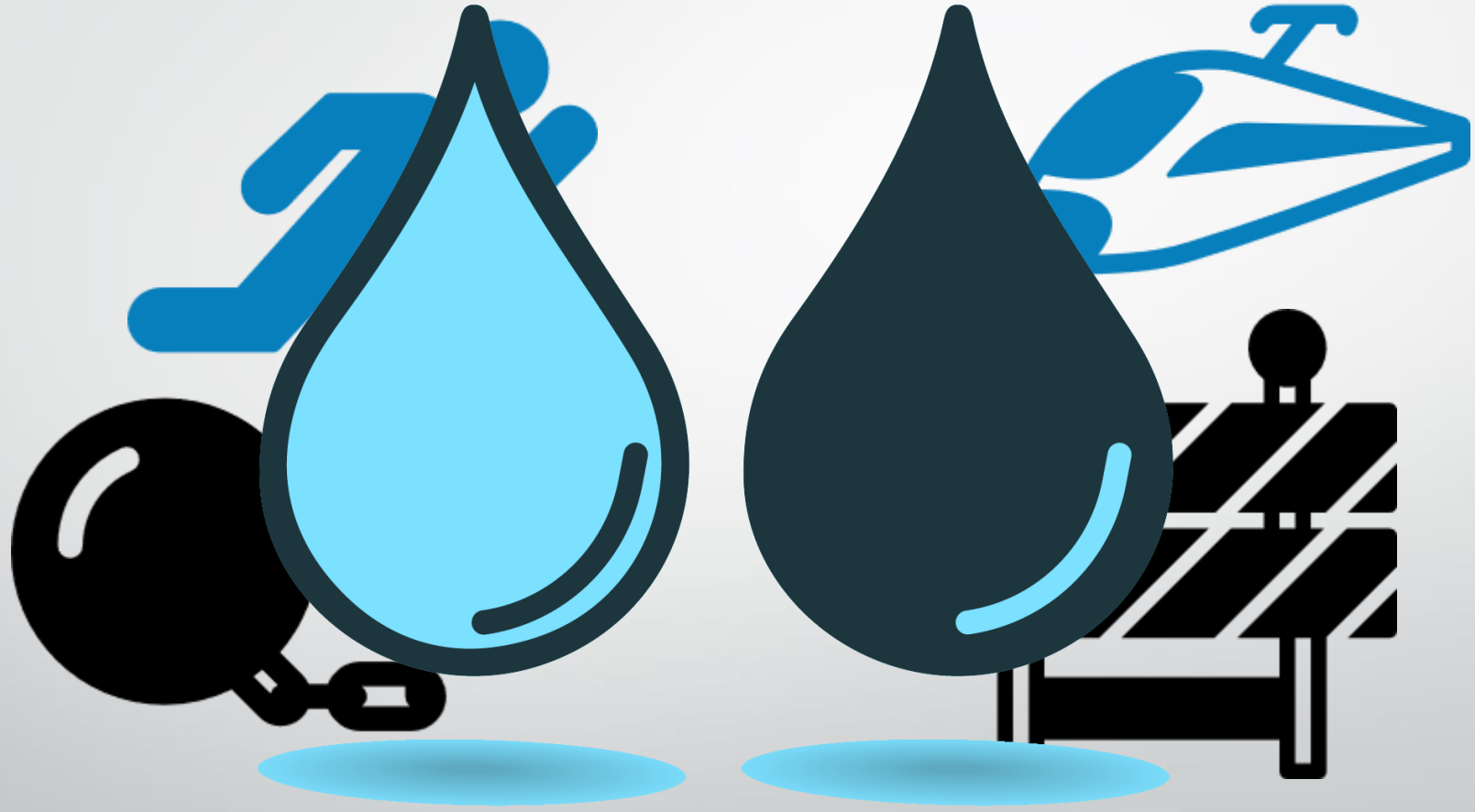
# Infusing Security Awareness into Agile Product Management

**Elena Kravchenko, Security Lead**
**Efrat Wasserman, Product Manager & Agile Coach**

# Secure Development vs. Agile Development



# Secure Agile Development


We believe **Agile** and **Security** are on the same **Team**!

# Who are we?

**Elena**:

- Micro Focus (former HPE Software) **Security Lead** of Application Delivery Management (ADM) Business Unit
- 25+ years of software engineering , last 5 years in product security
- MSc in Applied Mathematics from Leningrad State University

**Efrat**:

- **Agile Coach** at Ajimeh
- 7+ years in Software Development, Program management, last 3 years in Product Management
- BSc in Computer Science and Mathematics
- MBA in Business Management and Marketing

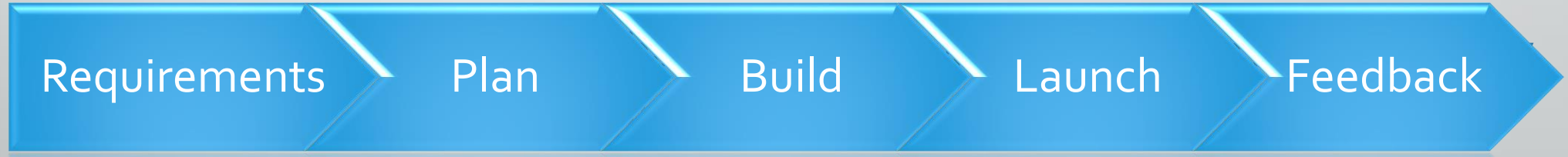
# Anti-pattern

“An anti-pattern is a common response to a recurring problem that is usually ineffective and risks being highly counterproductive. “

Wikipedia

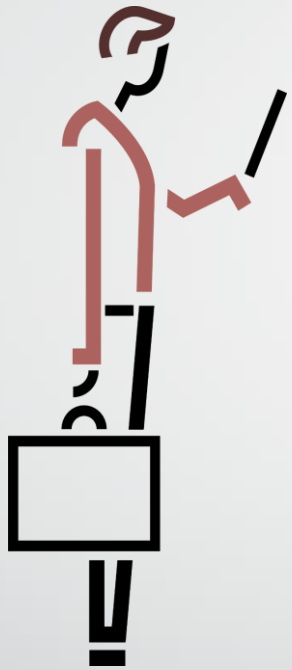
# Best Practices

- Postponing security aspects to later product development life cycle stages is the **anti-pattern**
- The approach "is usually ineffective and risks being highly **counterproductive**"
- We need to start security activities as **early** as possible  in the product development cycle



# The Game of Thrones

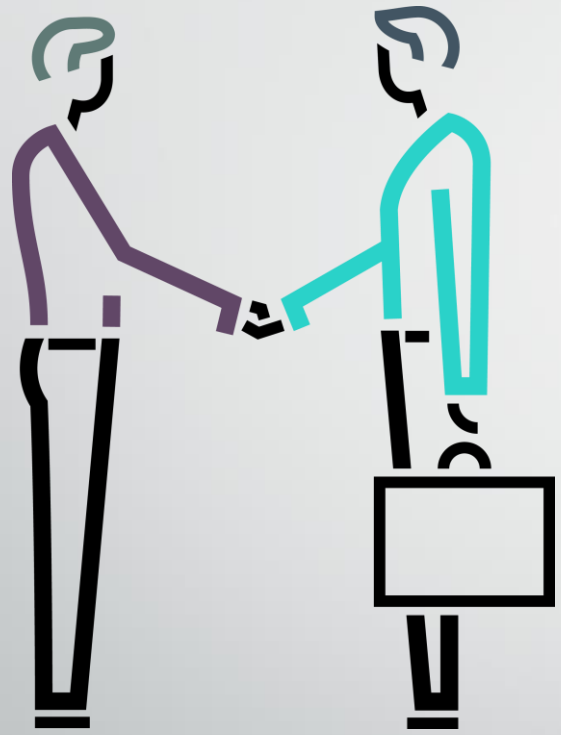
# Is such conversation common?



**Business**

**Security**

# Shared Goals



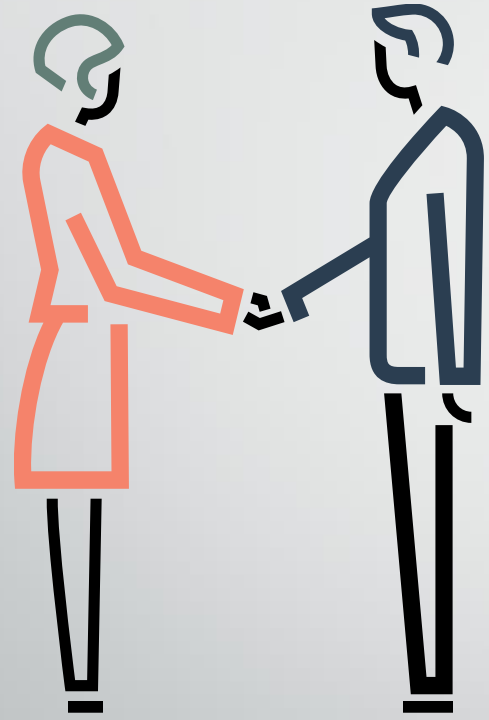
- Protect Customer Data
- Company Reputation And Intellectual Property
- Profit

# How to infuse…

Proactively infusing security into product life cycle:

- **Identify** the connection points
- **Align activities**, responsibilities and deliverables
- Define relevant **ceremonies**
- Follow **agile principles**

# Checkpoints



| Release | Sprint |
| --- | --- |
| Kickoff | Pre Planning |
| Design | Implementation |
| Signoff | Demo |

# Kickoff\Pre Planning

| PM activities | Security activities | Agile principles |
| --- | --- | --- |
| • Content<br>• Timeline<br>• Release criteria<br>• Commitment | • Content<br>• Commitments<br>• Timeline<br>• Security Grade gate | • Cooperation<br>• Joint Risk<br>• Transparency<br>• Sync Ceremonies<br>• Early detection |

# Design\Implementation

| PM activities | Security activities | Agile principles |
| --- | --- | --- |
| • Feature definition<br>• Feature review<br>• User story breakdown<br>• Prioritization<br>• DoD | • Security **review**<br>• Threat modelling<br>• Security assessment<br>• Secure **code review** | • Rapid Response<br>• Collaboration |

# Signoff\Demo

| PM activities | Security activities | Agile principles |
| --- | --- | --- |
| • Release\EOS Signoff<br>• Demo | • Security Gate<br>• Demo | • Protect the Customer<br>• Meet Customer real needs<br>• Product reliability & quality<br>• Competitive advantage |

# Kickoff example

## Security Plan

| | |
|---|---|
| **Product name** | Click here to enter text. |
| **Release name** | Click here to enter text. |
| **Release number** | Click here to enter text. |

3. Provide security activities timelines as scheduled with SL and S&TO PMO:

| Security activity | Date |
|---|---|
| STAT kick-off session | Click here to enter a date. |
| Threat Modelling kick-off (Content review) * | Click here to enter a date. |
| Lab assessments starting date ** | Click here to enter a date. |

# User View

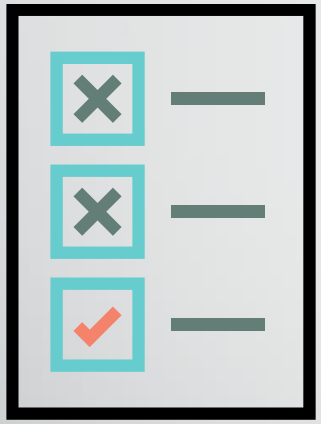

User Name
Password
Financial
transaction table
Budget diagram

# Developer View

# Attacker View

# Defender View

# Signoff Example



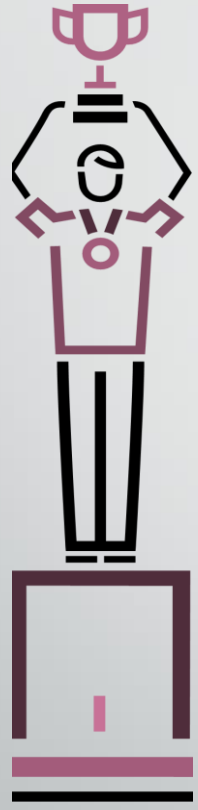
Sprint:

- Participate in **sprint demo** for finalized features
- Confirm **final security status** as feature DoD

Release:

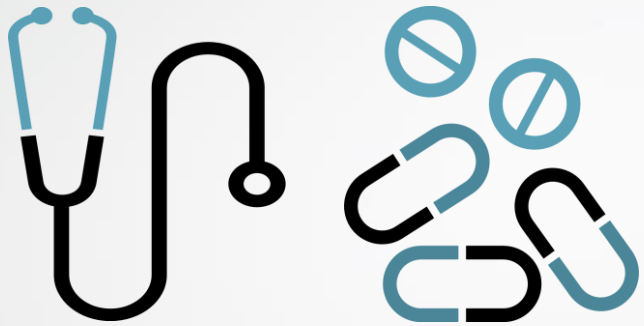
- **Release Criteria** Compliance
- **Planned activities** status
- **Follow-up** actions
- **Retrospective** – Security Trends, Challenges

# WIFM - What's In It For Me?



| Security Lead | PM/PO |
| --- | --- |
| Information | Plan Properly – cost effective |
| Commitment | Agility |
| Compliance | Time |
| Understanding of scope | Risk management |
| Security status and risks | Unblind decision |
| Influence | Alignment |

# Summary



"An ounce of prevention is worth a pound of cure"

# Q&A

elena.kravchenko@microfocus.com
www.linkedin.com/in/elena-kravchenko
efrat@ajimeh.com
www.linkedin.com/in/efrat-wasserman