

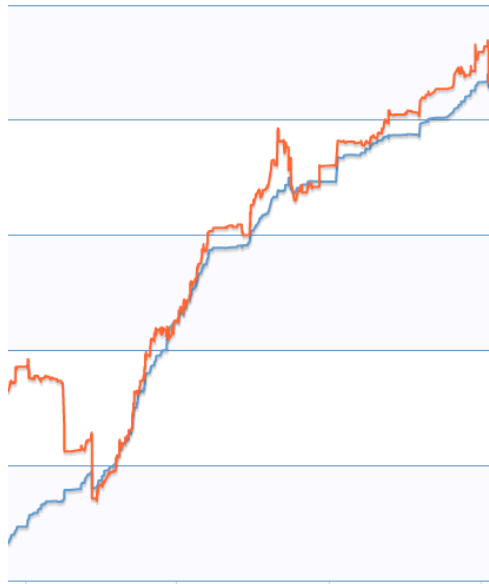
Zeit, Ihr Tool zu wecken

---

# Codeanalyse im Dornröschenschlaf

Ann-Sophie Kracker

■ Anzahl Codezeilen  
■ Anzahl Findings

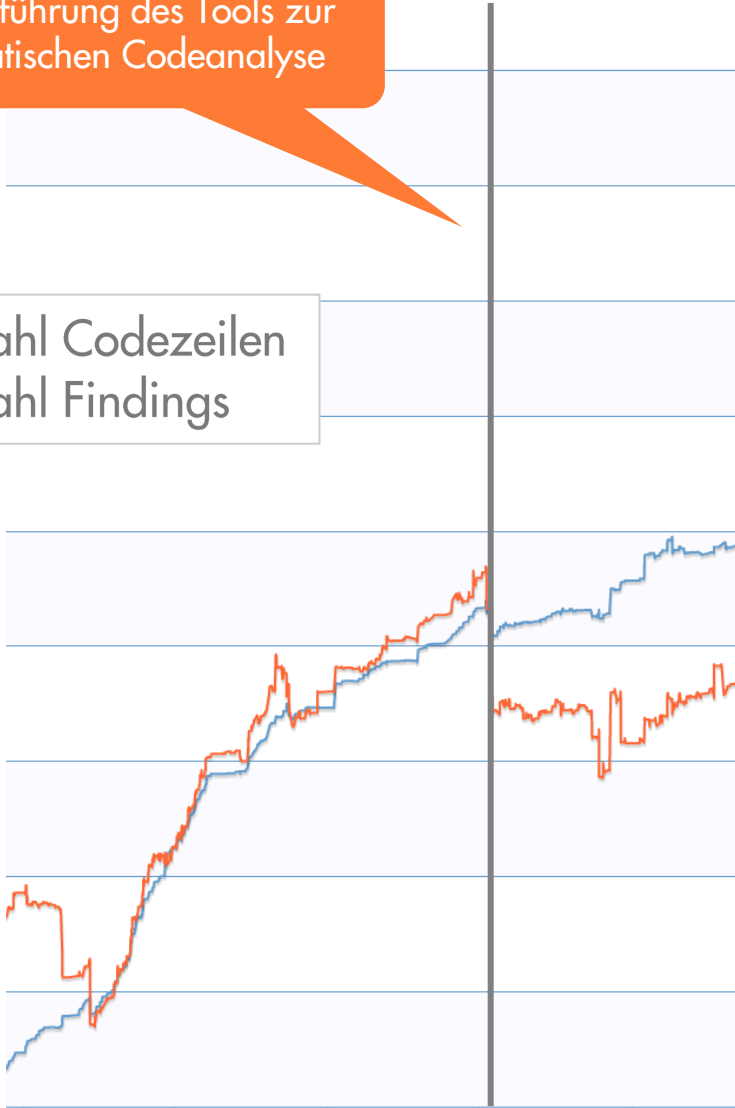


Wir sollten ein Tool für  
Codequalität nutzen.

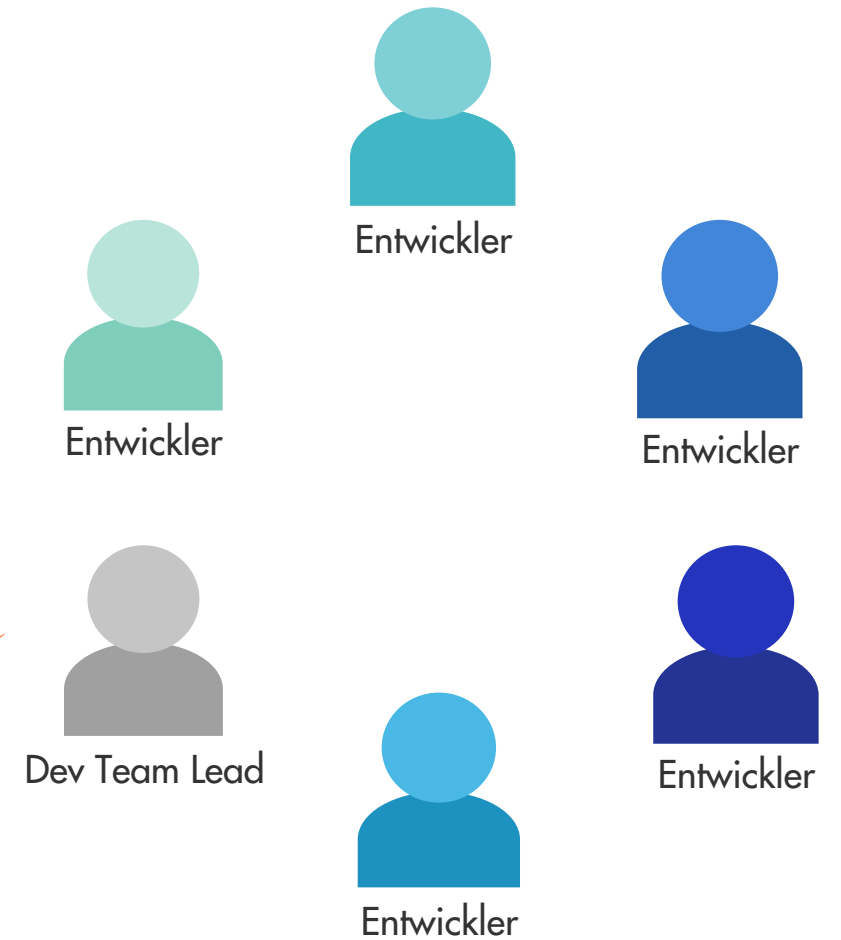


Einführung des Tools zur  
statischen Codeanalyse

■ Anzahl Codezeilen  
■ Anzahl Findings

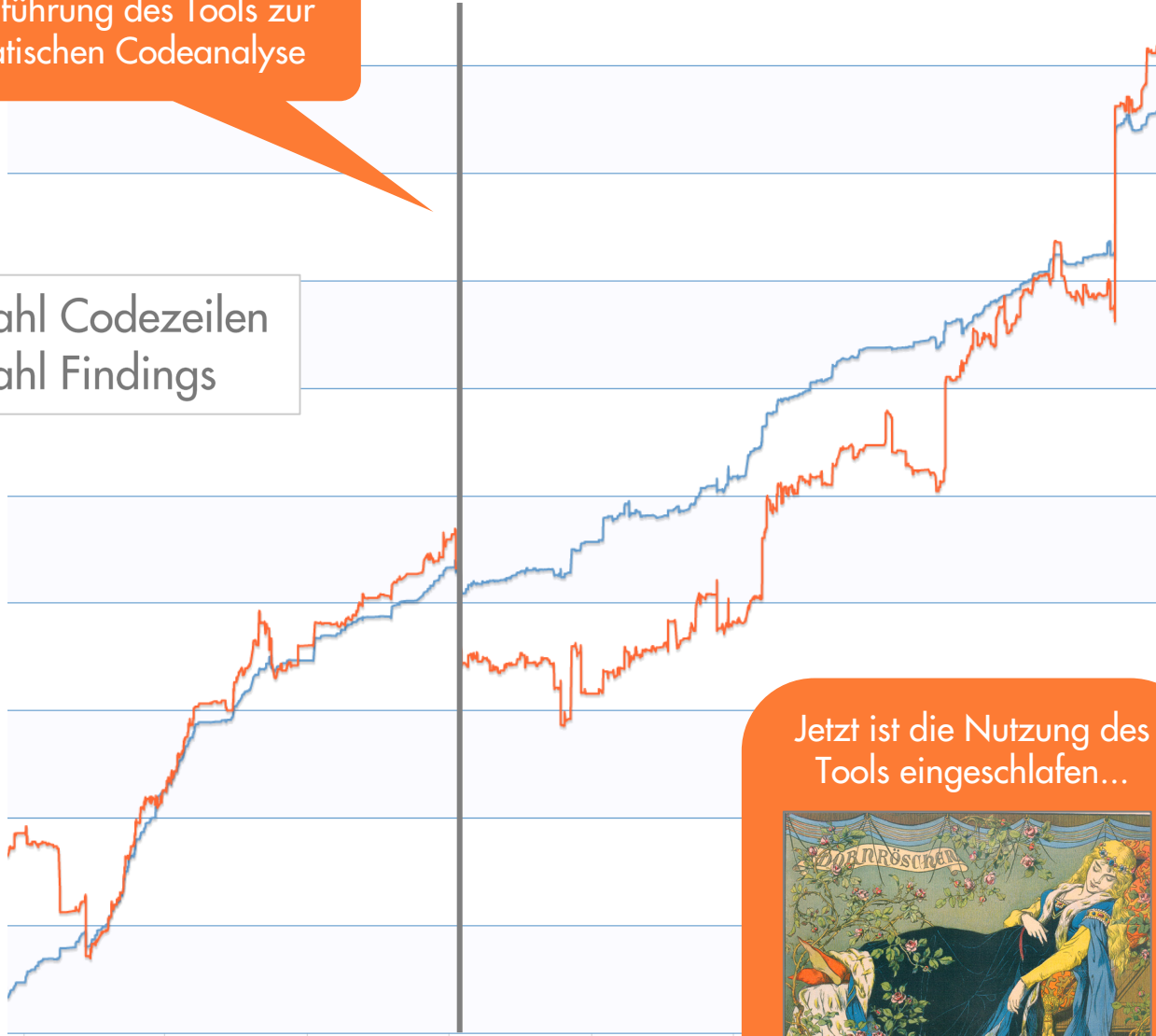


Sehr gut, die Qualität ist  
schon viel besser!

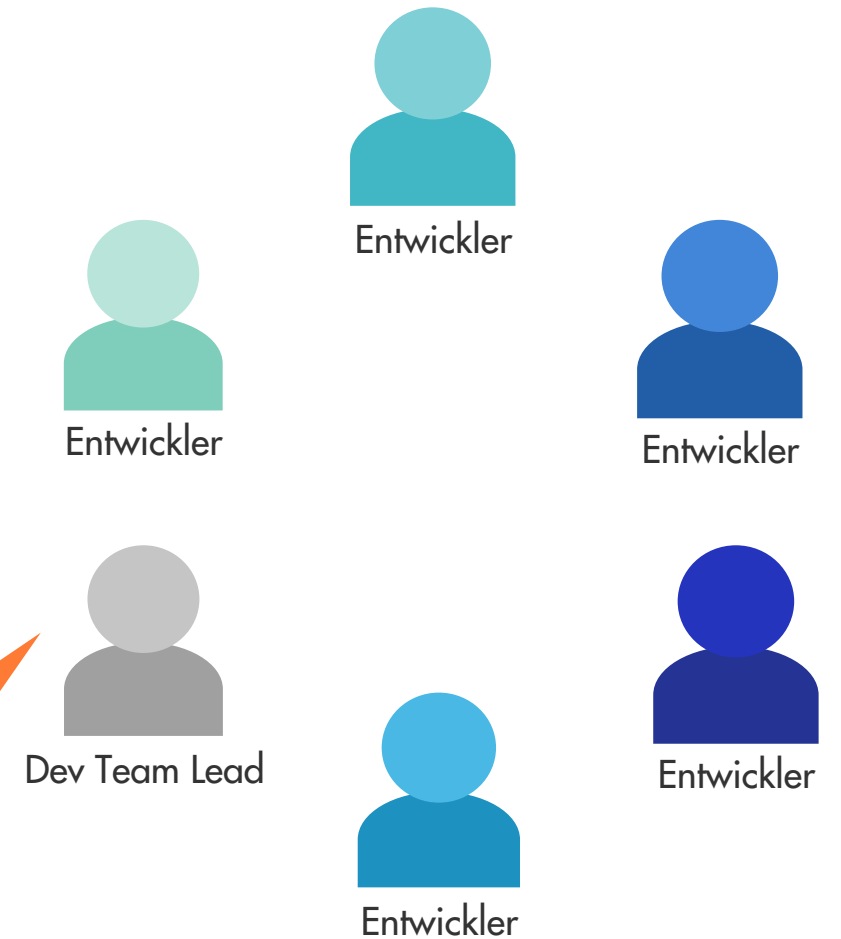


Einführung des Tools zur  
statischen Codeanalyse

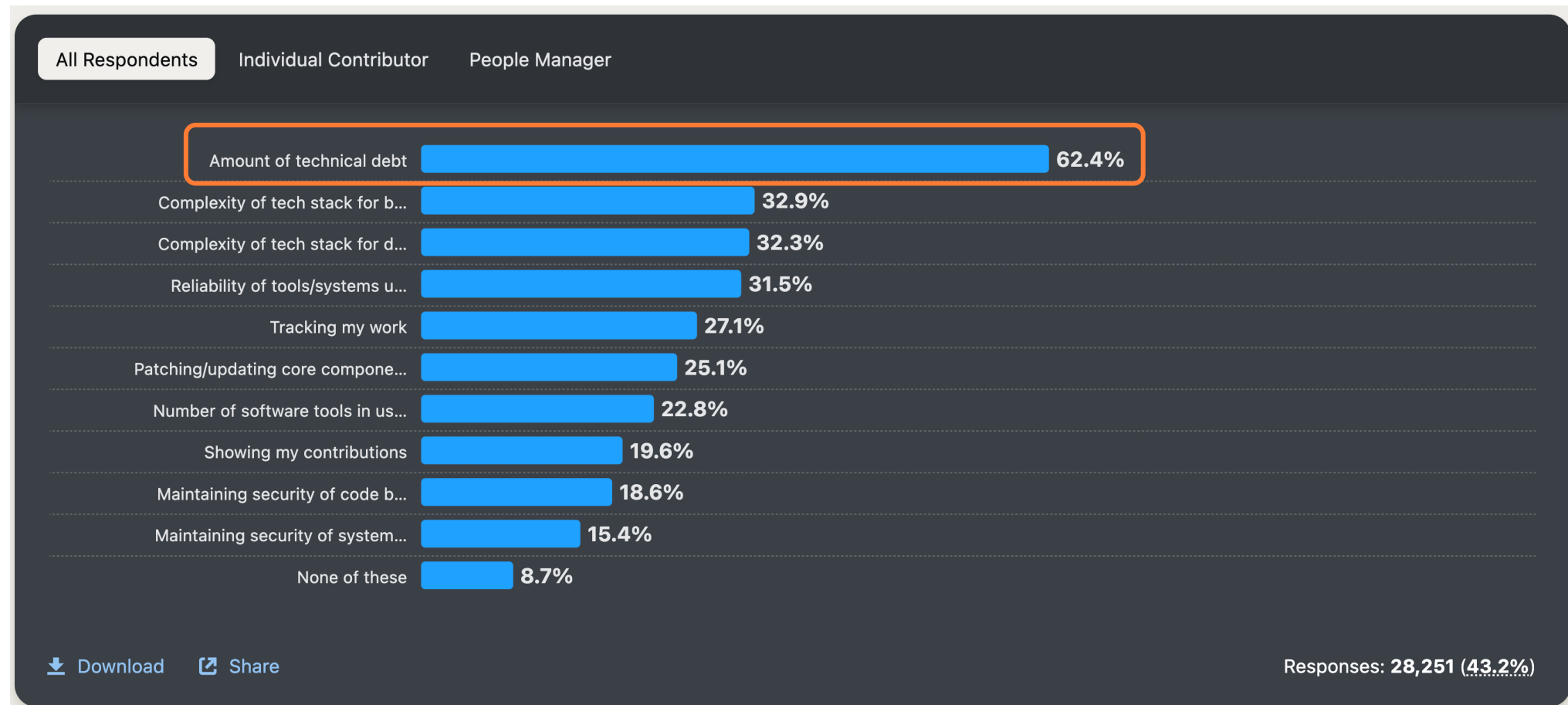
■ Anzahl Codezeilen  
■ Anzahl Findings



Jetzt ist die Nutzung des  
Tools eingeschlafen...



# Hauptursache für Frustrationen



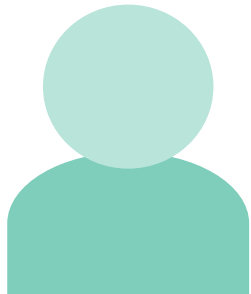
Schon wieder bekomme ich neue Vorgaben von oben auferlegt...



Das Feature muss schnell fertig werden. Ich habe keine Zeit zum Beheben der Findings



Ich werde immer erst auf die Findings aufmerksam gemacht, wenn ich das Ticket schon abgeschlossen habe



Das Finding ist total unwichtig. Warum soll ich das beheben?



# Tatsächliche Gründe



Mangelhafte Konfiguration



Tool-Feedback an falscher Stelle

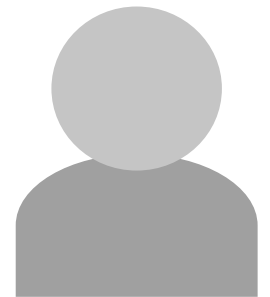


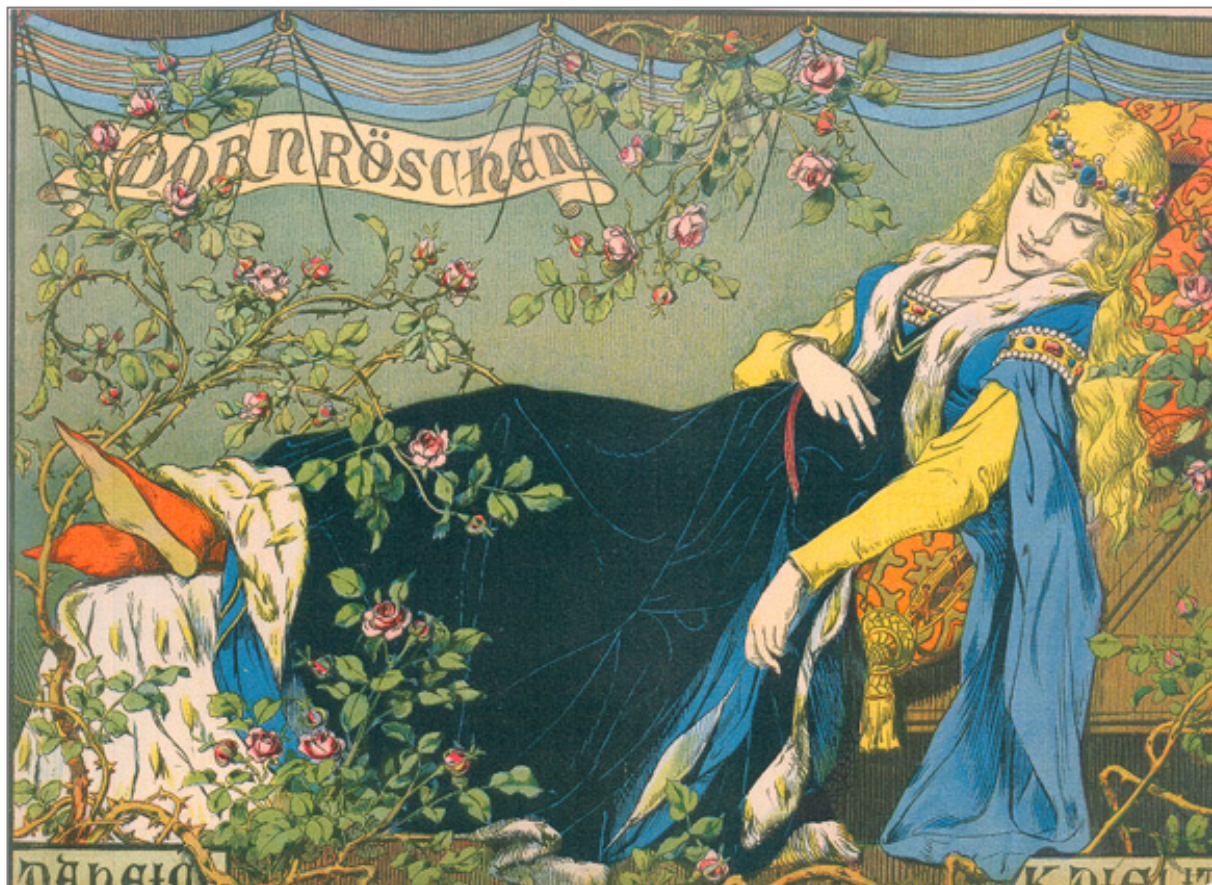
Keine Schulung bzw. Einbeziehung des Entwicklungsteam



Keine Zeit für die Einführung eingeplant

Wie lässt sich das lösen?





Tool

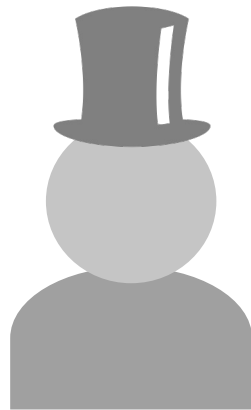


Prozess

# Lösungsansätze



Zeit für die Einführung einplanen - anfangs ca. halber Tag pro Woche



Tool-Verantwortlicher



Teil des Entwicklungsteams



Entwicklungserfahrung



Motiviert, die Codequalität zu verbessern

# Lösungsansätze



Zeit für die Einführung einplanen



Konfiguration anpassen

# Anpassung an Programmierrichtlinien

## C# Coding Guidelines

### 5 Structure Limits

- Files must be no larger than **400 lines**.
- Statement lists (e.g. methods) must not be longer than **40 lines**.
- The nesting depth must not exceed **3** (counting from the method level).

Structure > Method Length > Long Method

### Violation of method length threshold (source lines of code) of 30: 31

```
public override MembershipUser GetUser (string username, bool userIsOnline)
{
    SqlConnection cn = GetDBConnectionForMembership ();
    try {
        using (SqlCommand cmd = cn.CreateCommand()) {
            cmd.CommandText = "SELECT UserId, Username, Email, PasswordQuestion,"
                + " Comment, IsApproved, IsLockedOut, CreateDate, LastLoginDate,"
                + " LastActivityDate, LastPasswordChangedDate, LastLockoutDate"
                + " FROM " + USER_TB_NAME + " WHERE LoweredUsername = $Username AND ApplicationId = $ApplicationId";

            cmd.Parameters.AddWithValue ("$Username", username.ToLowerInvariant ());
            cmd.Parameters.AddWithValue ("$ApplicationId", _applicationId);

            MembershipUser user = null;

            if (cn.State == ConnectionState.Closed)
                cn.Open ();

            using (SqlDataReader dr = cmd.ExecuteReader()) {
                if (dr.HasRows) {
                    dr.Read ();
                    user = GetUserFromReader (dr);
                }
            }

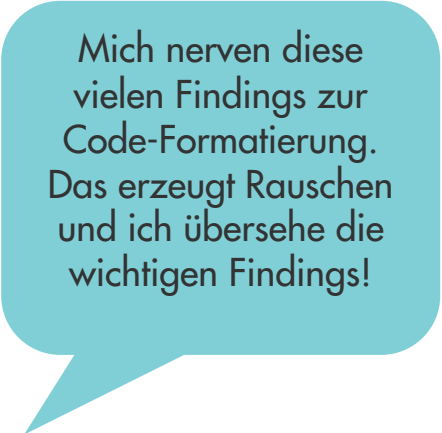
            if (userIsOnline) {
                cmd.CommandText = "UPDATE " + USER_TB_NAME
                    + " SET LastActivityDate = $LastActivityDate"
                    + " WHERE LoweredUsername = $Username AND ApplicationId = $ApplicationId";

                cmd.Parameters.AddWithValue ("$LastActivityDate", DateTime.UtcNow);

                cmd.ExecuteNonQuery ();
            }

            return user;
        }
    } finally {
        if (!IsTransactionInProgress ())
            cn.Dispose ();
    }
}
```

# Quick Win: Auto-Formatter einführen



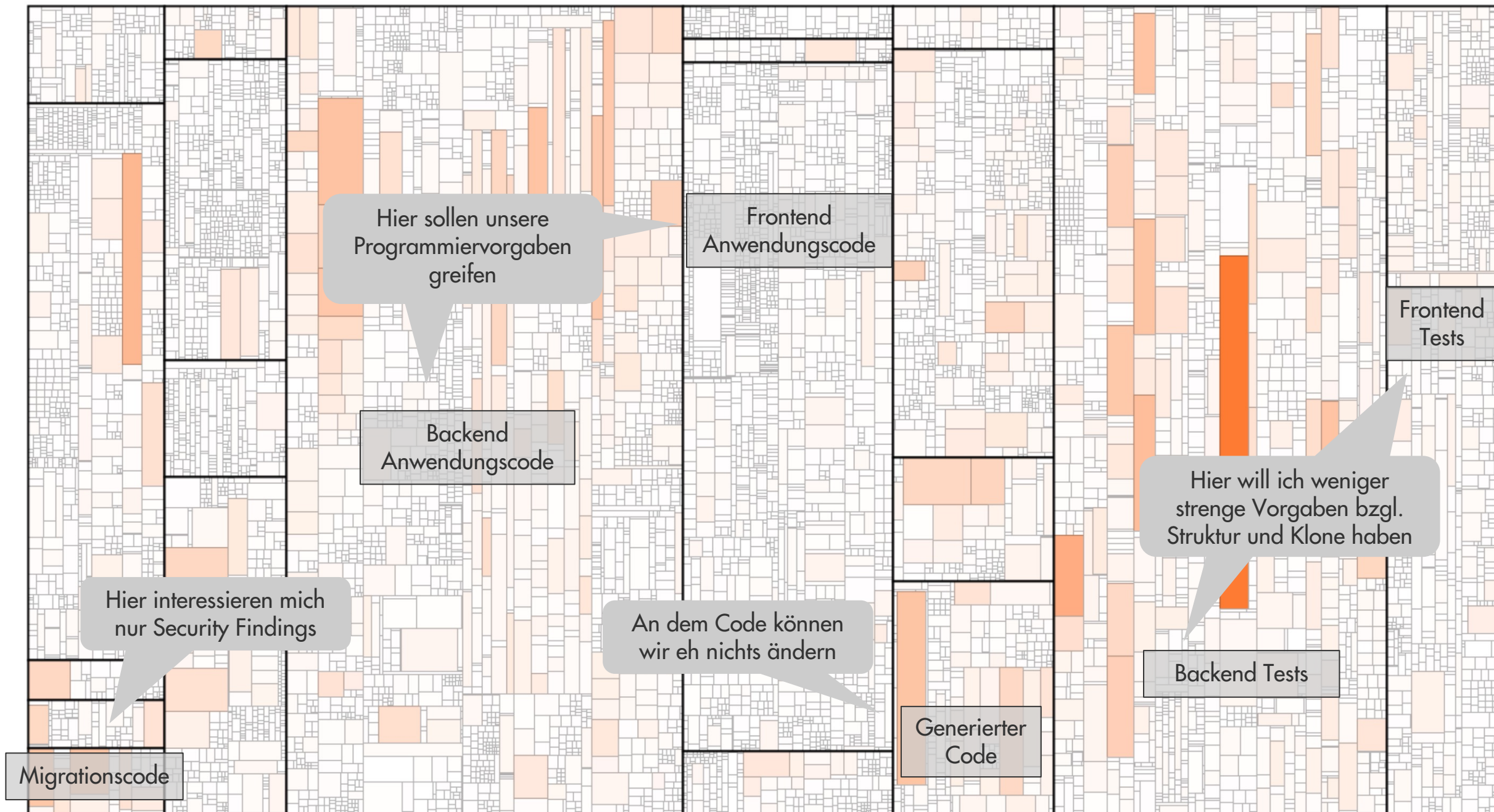
Mich nerven diese vielen Findings zur Code-Formatierung. Das erzeugt Rauschen und ich übersehe die wichtigen Findings!



[Comprehensibility](#) > [Formatting](#) > [Elements should have the same indentation \(SA1137\)](#)

## Elements should have the same indentation

```
91 |  
92 |  
93 |  
94 |  
95 |  
96 |  
97 |  
98 |  
99 |  
100 |  
101 |  
102 |  
103 |  
    private void UpdateConfigFile(ConfigFile configFile)  
    {  
        if (string.IsNullOrEmpty(txtServer.Text))  
            configFile.Remove(DbConstants.KEY_HOST);  
        else  
            configFile.Set(DbConstants.KEY_HOST, txtServer.Text);  
  
        if (string.IsNullOrEmpty(txtFilePath.Text))  
            configFile.Remove(DbConstants.KEY_FILE_NAME);  
        else  
            configFile.Set(DbConstants.KEY_FILE_NAME, txtFilePath.Text);  
    }  
}
```



# Lösungsansätze



Zeit für die Einführung einplanen



Konfiguration anpassen



Tool-Feedback an passender Stelle

# Feedback beim Entwickeln

```
49  /**
50   * Returns the end index of the text area within the initial html text that should be attributed to the given text node.
51   * This includes all (nested) (self-)closing tags that end directly after the given text.
52   */
53  function getAreaEndIndex(node: AnyNode) : number | null { Show usages
54      let currentNode : AnyNode = node;
55      while (true) {
56          // Last child is a closing tag -> Incorporate the characters into the text area
57          if (
58              currentNode.nextSibling === null &&
59              currentNode.parentNode !== null &&
60              !isDocument(currentNode.parentNode)
61          ) {
62              currentNode = currentNode.parentNode;
63          } else if (
64              // The next sibling is a self-closing tag e.g. <br /> or an HTML comment -> Incorporate the characters into the text area
65              currentNode.nextSibling !== null &&
```

**Findings**

| Findings                           | Category    | Group                 | Lines |
|------------------------------------|-------------|-----------------------|-------|
| webapp/src/perspectives/requiremen |             |                       |       |
| ! Unexpected constant condition.   | Correctness | Error-prone Practices | 55    |

Check Descriptions

no-constant-condition x

A constant expression (for example, a literal) as a test condition might be a typo or development trigger for a specific behavior. For example, the following code looks as if it is not ready for production.

```
if (false) {
    doSomethingUnfinished();
}
```

Rule Details

# Feedback in relevanten Tools

## TS-42507 centralize check explorer filtering

Open requested to merge `ts/42507_fix_findings` into `master` 15 hours ago

Overview 3

Commits 5

Pipelines 2

Changes 6

3 open threads ^ v ⋮ Add a to-do item

Teamscale

Findings 3 1 2 0 Test Gaps (0%)

Edited 14 hours ago by CQSE Teamscale IO

👍 0

👎 0

😊

✓ Merge request pipeline #2322356577 passed

Merge request pipeline passed for `d94478b8` 15 hours ago ?

8v Approve Approval is optional ?

Assign reviewers v

Teamscale / TS-21692

## Merge Request View: Introduce common data classes

Edit

Comment

Assign

More v

Back to New

Details

Type: Feature

Priority: Normal

Component/s: Backend

Labels: user-guide-checked

Merge Request: [https://git.cqse.eu/cqse/teamscale/merge\\_requests/7106](https://git.cqse.eu/cqse/teamscale/merge_requests/7106)

Customer:

PDash Task: #7310

Epic Link: better-review

Change Log: -

Teamscale: v Teamscale Info

| Project name | Findings balance | Test Gap |
|--------------|------------------|----------|
| CQSE All     | 23 1 1           | 100.00%  |

```
44 + @Override
45 + public void execute() throws CheckException {
46 +     SimulinkModel model = context.getSimulinkModel();
47 +     for (SimulinkBlock block : SimulinkUtils.listBlocksDepthFirst(model)) {
48 +         if (block.getType().equals(SimulinkConstants.TYPE_REFERENCE)) {
49 +             if (prohibitedBlockTypes.contains(block.getParameter(SimulinkConstants.PARAM_SOURCE_TYPE))) {
```

build @build · 1 day ago

! [New] Calling `contains()` on lists is inefficient

view in Teamscale)

Maintainer

✓

😊

💬

✎

⋮

# Lösungsansätze



Zeit für die Einführung einplanen



Konfiguration anpassen



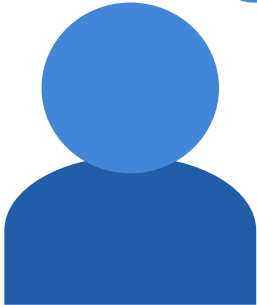
Tool-Feedback an passender Stelle



Schulung bzw. Einbeziehung des Entwicklungsteam



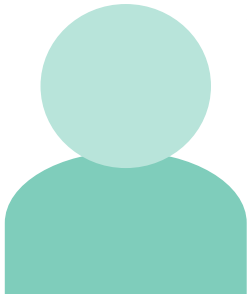
Ich würde gerne eine Liste mit allen Findings sehen, die ich eingebaut habe. Ist das möglich?



Die Konfiguration ist schon viel besser, aber es gibt noch den einen Check, den ich deaktivieren würde.

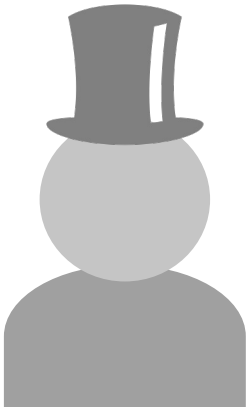


Funktioniert die Arbeit mit dem Tool für euch, inkl. IDE Plugin und Merge Request Annotationen?



Das IDE Plugin für Rider schaut gut aus. Aber gibt es das auch für Visual Studio?

## Codequalität als Teamsport verstehen



# Lob für das Beheben von Findings

|    |                                                                                                                        |          |
|----|------------------------------------------------------------------------------------------------------------------------|----------|
| TT | IB: Refaktoring nach Teamscale<br>Feb 09 2026 14:19 by [redacted] (10989df7   /  Feature/[redacted]  )                 | 1        |
| TT | IB: Refaktoring nach Teamscale<br>Feb 09 2026 14:15 by [redacted] (d4c90fb9   /  Feature/[redacted]  )                 | 3        |
| SS | Merged PR 88588: Bugfix InvalidOperationException [redacted]<br>Feb 09 2026 14:01 by [redacted] (12e84ff9   /  main  ) | 3  67  1 |
| TT | IB: Refaktoring nach Teamscale<br>Feb 09 2026 13:34 by [redacted] (2be92427   /  Feature/[redacted]  )                 | 29       |

# Mögliche Division durch Null

```
public Task<ActionResult> ExecuteActionsAsync(IPackage package,  
    IEnumerable<ActionElement> actions,
```

```
    IEnumerable<ActionElement> actionElements = actions as ActionElement[] ?? actions.ToArray();  
  
    //Gesamtgewichtung der Actions für Fortschritt bestimmen  
    int totalProgressWeight = 0;  
    foreach (ActionElement ae in actionElements)  
    {  
        totalProgressWeight += ae.ProgressWeight;  
    }
```

```
    //gewichtete Anzahl Prozente dazu addieren  
    int addPercentage = 100 * action.ProgressWeight / totalProgressWeight;  
    progressPercent = Math.Min(progressPercent + addPercentage, 100); //auf max. 100 Begrenzen  
    lastActionSeqPos = action.SequencePosition;
```

## Zu kurze Schlüssellänge für RSA

```
/// <summary>
/// Erzeugt eine RSA-Signatur über den Inhalt einer Hash-Datei.
/// </summary>
public static class RsaSignature
{
    /// <summary>
    /// Erzeugt für die angegebene Hash-Datei eine RSA-Signatur und trägt diese in die HashDatei ein.
    /// </summary>
    /// <param name="hashFile"></param>
    public static void Calculate(IIntegrityCheckHashFile hashFile)
    {
        hashFile = hashFile ?? new IntegrityCheckHashFile();
        RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
        try
        {
            rsa.ImportParameters(RsaParametersCodec.GetRsaParameters(hashFile.PrivateKey));
            hashFile.Signature = rsa.SignHash(CalculateHash(hashFile), null);
        }
        catch (CryptographicException)
        {}
        finally
        {
            rsa.Dispose();
        }
    }
}
```

# Kurze Schulung zu Verschlüsselungsalgorithmen

When selecting encryption algorithms, tools, or combinations, you should also consider two things:

1. No encryption is unbreakable.
2. The strength of an encryption algorithm is usually measured by the effort required to crack it within a reasonable time frame.

In today's cryptography, the length of the **key** directly affects the security level of cryptographic algorithms

Note that depending on the algorithm, the term **key** refers to a different mathematical property. For example:

- For RSA, the key is the product of two large prime numbers, also called the **modulus**.
- For AES and Elliptic Curve Cryptography (ECC), the key is only a sequence of randomly generated bytes.
  - In some cases, AES keys are derived from a master key or a passphrase using a Key Derivation Function (KDF) like PBKDF2 (Password-Based Key Derivation Function 2)

If an application uses a key that is considered short and **insecure**, the encrypted data is exposed to attacks aimed at getting at the plaintext.

## Compliant solution

```
using System;
using System.Security.Cryptography;

public void encrypt()
{
    var RsaCsp = new RSACryptoServiceProvider(2048);
}
```

## Schwerpunkt duplizierter Code

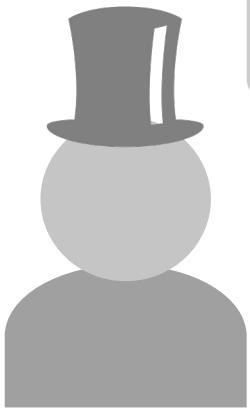
## Clone Coverage

# 15.4%

## Clone Findings

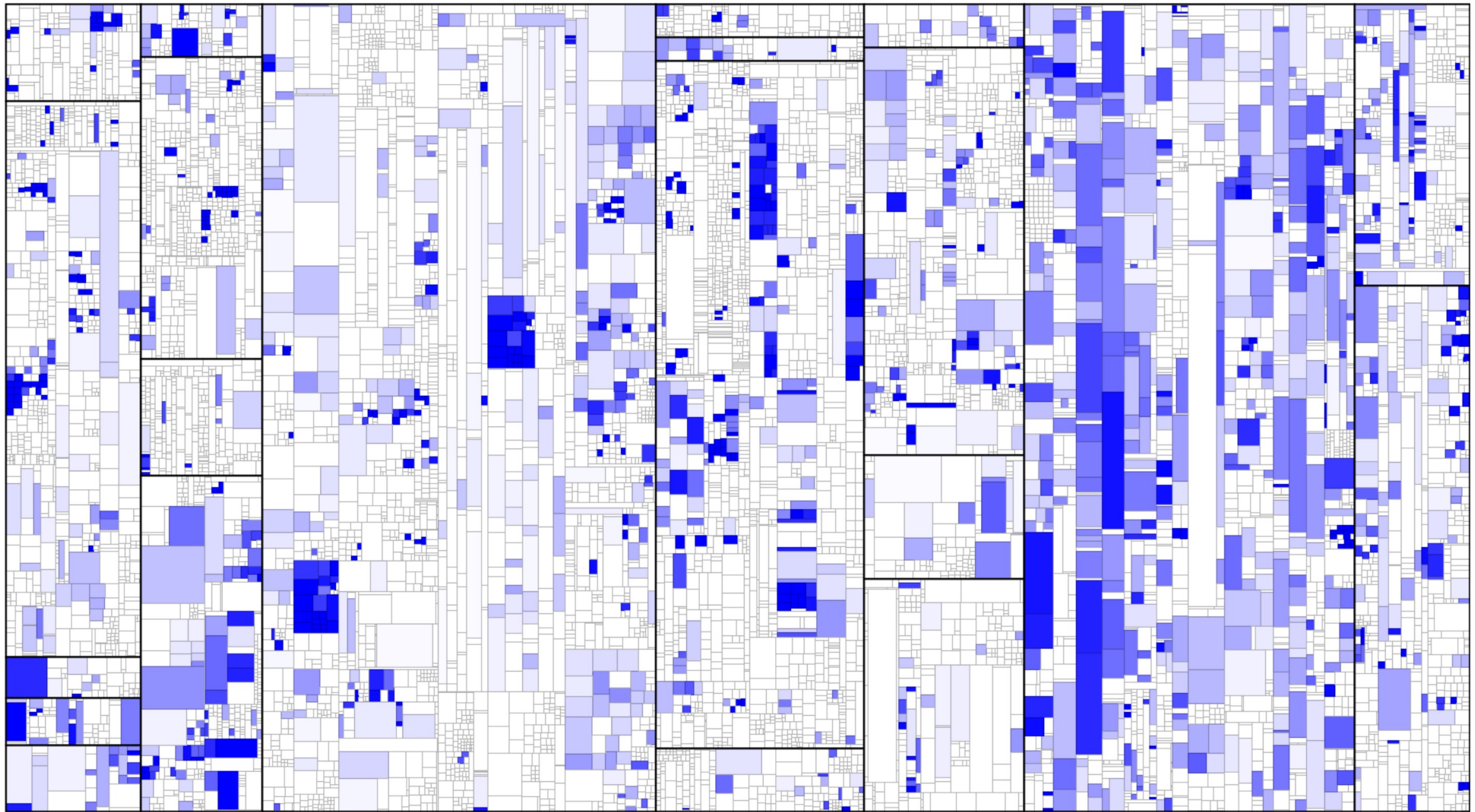
4.2k  
+22

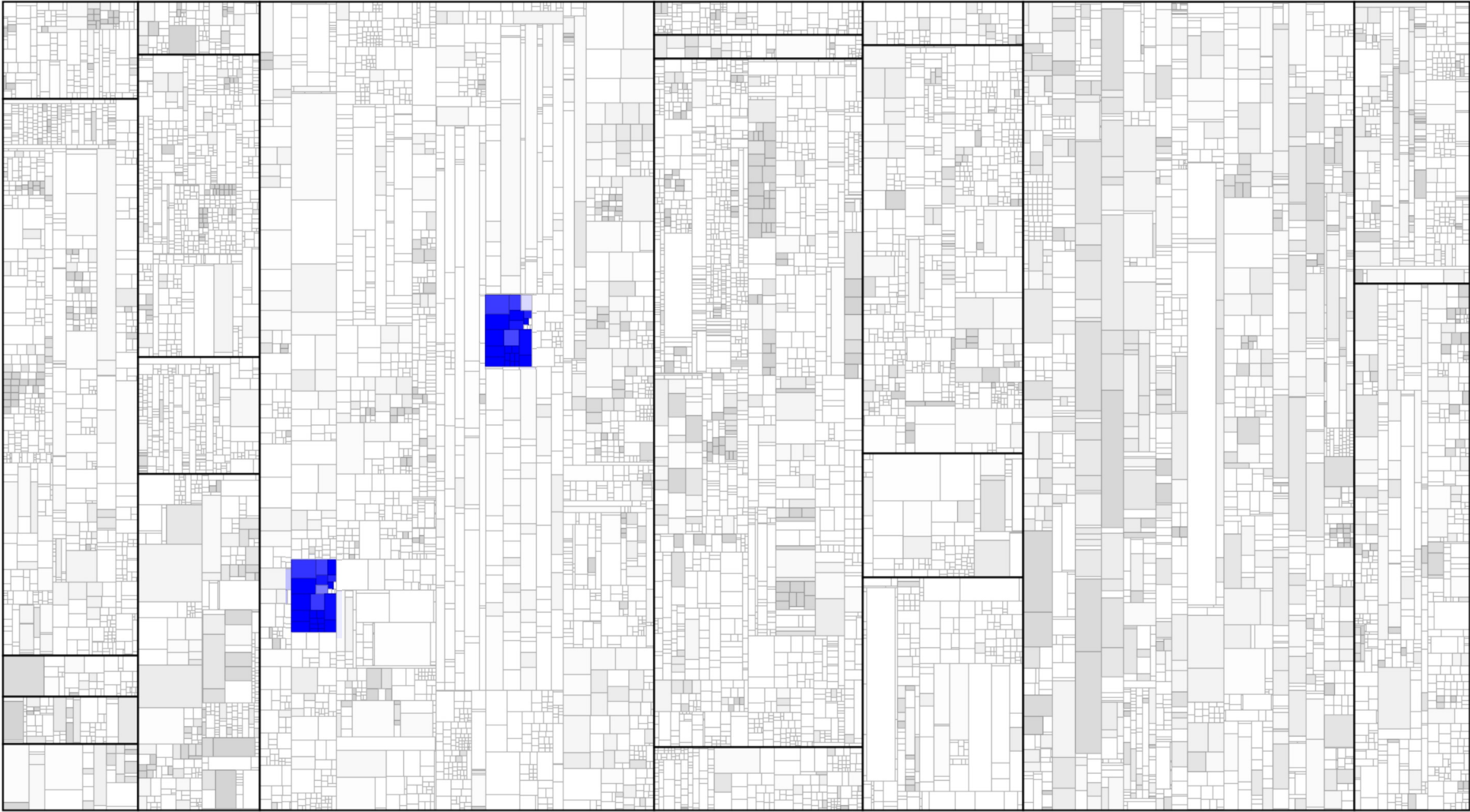
Das Thema sollten wir  
genauer anschauen

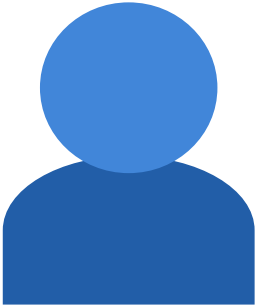


| Findings                                                                              | 7420                                  | Tolerated | 68     | False Positives | 6 |
|---------------------------------------------------------------------------------------|---------------------------------------|-----------|--------|-----------------|---|
|                                                                                       | Message                               | Instances | Length |                 |   |
|    | Clone with 2 instances of length 670  | 2         | 670    |                 |   |
|    | Clone with 2 instances of length 670  | 2         | 670    |                 |   |
|    | Clone with 2 instances of length 578  | 2         | 578    |                 |   |
|    | Clone with 2 instances of length 578  | 2         | 578    |                 |   |
|    | Clone with 2 instances of length 564  | 2         | 564    |                 |   |
|    | Clone with 2 instances of length 564  | 2         | 564    |                 |   |
|    | Clone with 2 instances of length 331  | 2         | 331    |                 |   |
|    | Clone with 2 instances of length 331  | 2         | 331    |                 |   |
|    | Clone with 2 instances of length 275  | 2         | 275    |                 |   |
|    | Clone with 2 instances of length 275  | 2         | 275    |                 |   |
|    | Clone with 2 instances of length 218  | 2         | 218    |                 |   |
|    | Clone with 2 instances of length 218  | 2         | 218    |                 |   |
|    | Clone with 2 instances of length 204  | 2         | 204    |                 |   |
|    | Clone with 2 instances of length 204  | 2         | 204    |                 |   |
|    | Clone with 2 instances of length 180  | 2         | 180    |                 |   |
|    | Clone with 2 instances of length 180  | 2         | 180    |                 |   |
|    | Clone with 2 instances of length 169  | 2         | 169    |                 |   |
|    | Clone with 2 instances of length 169  | 2         | 169    |                 |   |
|    | Clone with 2 instances of length 133  | 2         | 133    |                 |   |
|    | Clone with 2 instances of length 133  | 2         | 133    |                 |   |
|    | Clone with 2 instances of length 133  | 2         | 133    |                 |   |
|    | Clone with 2 instances of length 133  | 2         | 133    |                 |   |
|    | Clone with 3 instances of length 131  | 3         | 131    |                 |   |
|    | Clone with 3 instances of length 131  | 3         | 131    |                 |   |
|    | Clone with 3 instances of length 131  | 3         | 131    |                 |   |
|    | Clone with 2 instances of length 126  | 2         | 126    |                 |   |
|    | Clone with 2 instances of length 126  | 2         | 126    |                 |   |
|    | Clone with 2 instances of length 120  | 2         | 120    |                 |   |
|    | Clone with 2 instances of length 120  | 2         | 120    |                 |   |
|    | Clone with 2 instances of length 116  | 2         | 116    |                 |   |
|    | Clone with 2 instances of length 116  | 2         | 116    |                 |   |
|   | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |
|  | Clone with 11 instances of length 115 | 11        | 115    |                 |   |

[illegible]







Ich habe den Code  
im Kontext von  
Feature A kopiert.

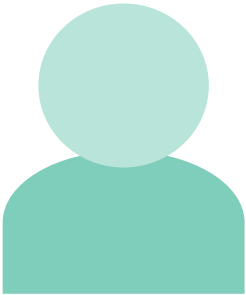
Dafür hätte ich einige  
Änderungen machen  
müssen.

Ich wollte die anderen Stellen  
nicht anfassen. Ich habe  
keine Zeit, alle potenziellen  
Änderungen zu testen.



Mir fällt noch was auf.

Ich habe an der ursprünglichen  
Stelle einen Bug gefixt. Das  
sollten wir an der neuen Stelle  
noch nachziehen.



Wie kann man das  
wiederverwenden?  
Was genau wollen wir  
auslagern?

Sollen wir das über  
Vererbung lösen oder  
wollen wir eine Util-  
Klasse anlegen?



Warum hast du den  
bestehenden Code nicht  
wiederverwendet?

# Beschluss des Teams



## Erstellen eines Tasks

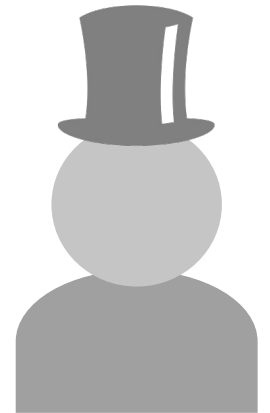
- Auslagern des wiederverwendbaren Codes in eine Util-Klasse
- Sicherstellen, dass der Bug an allen Stellen behoben ist
- Abdeckung durch automatisierte Tests sicherstellen



## Best Practice festgelegt

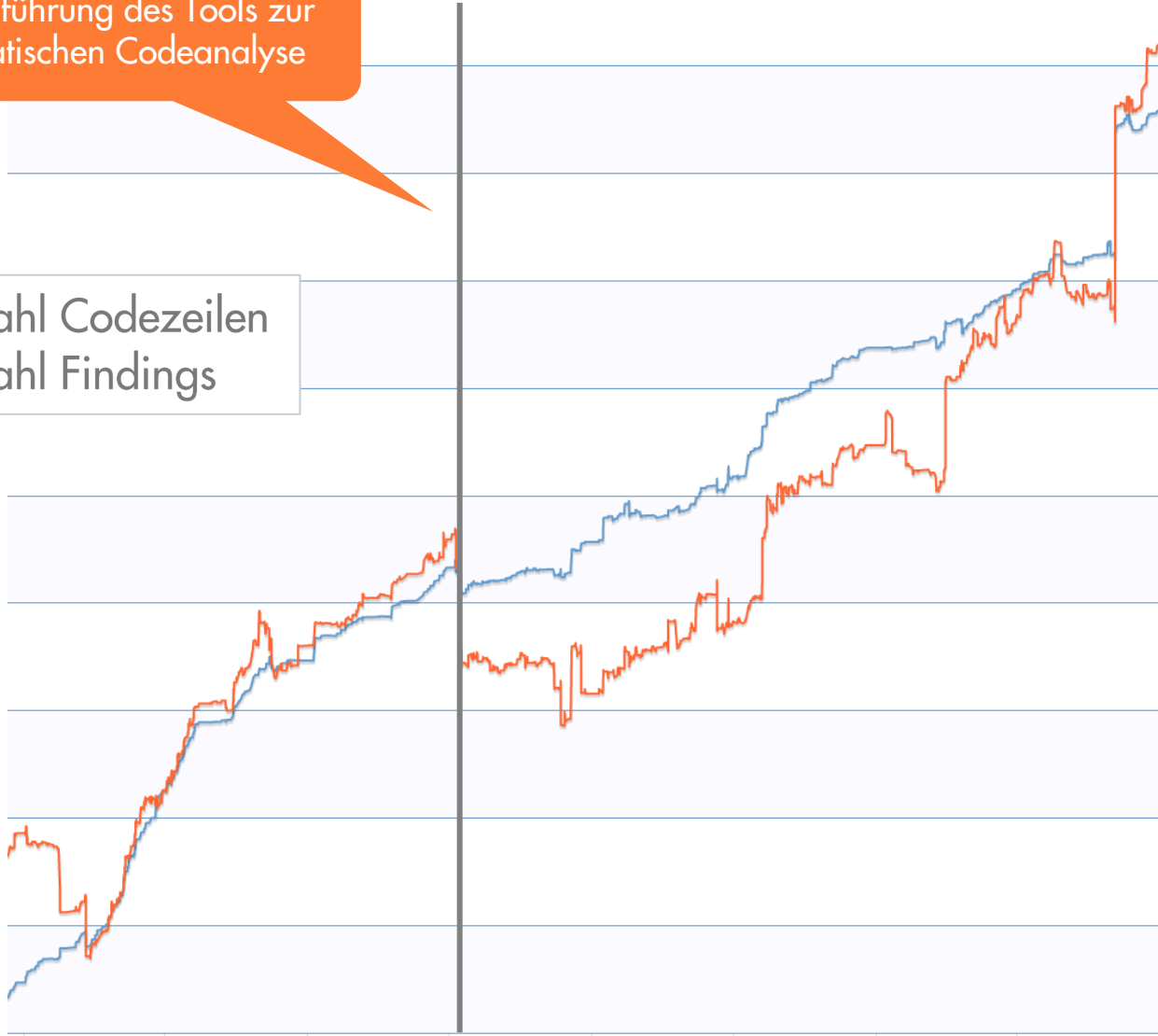
- In Zukunft Klone vermeiden
- Die zusätzliche Zeit ist gut investiert

Termine regelmäßig durchführen!



Einführung des Tools zur  
statischen Codeanalyse

■ Anzahl Codezeilen  
■ Anzahl Findings



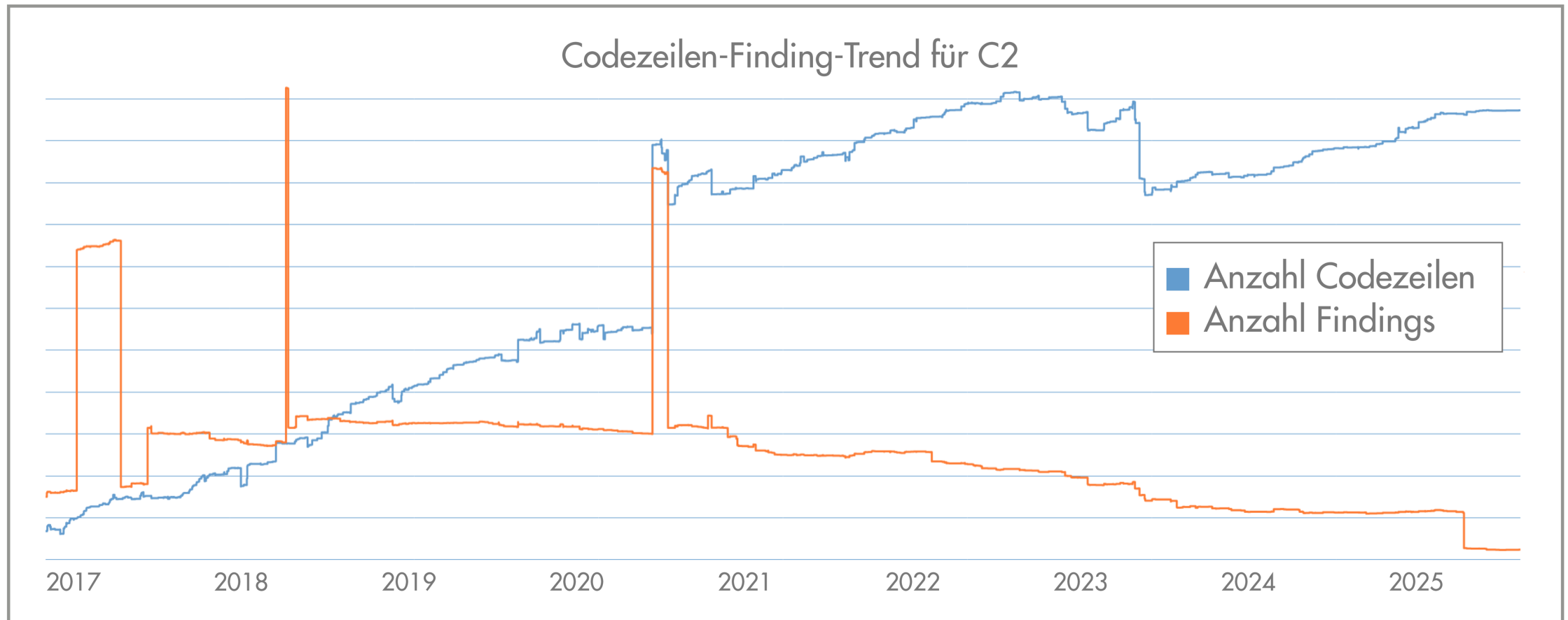
Einführung des Tools zur  
statischen Codeanalyse

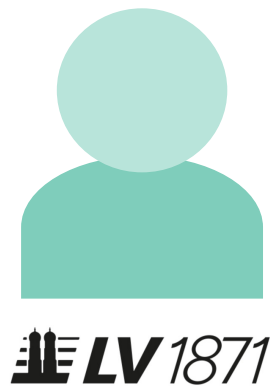
■ Anzahl Codezeilen  
■ Anzahl Findings



Start der regelmäßigen  
Termine

## Stabile Verbesserung über viele Jahre





» ... regelmäßige Qualitätsretrospektiven ...  
helfen uns, eine hohe **Softwarequalität**  
sicherzustellen, **Wissen im Team** zu verteilen  
und einen systematischen Umgang bezüglich  
**Softwaresicherheit** gegenüber  
Aufsichtsbehörden **nachzuweisen**«



**SEW**  
EURODRIVE

»Der Weg zu einer nachhaltigen **Qualitätsverbesserung** geht nicht über ein Werkzeug, sondern über den **Prozess**.«



VER | SICHER | UNGS  
KAMMER  
BAYERN

»Jeder **lernt** dabei.«



— **EnBW**

»Seit wir in Retros **über Codequalität sprechen**, gehen die Kurven deutlich stärker auseinander!«

## Regelmäßige Meetings



Zufriedenheit abklopfen



Lob für schönes Coding



Findings und Verbesserungsvorschläge



Schwerpunkt / Deep-Dive



## Konfiguration anpassen

An Programmierrichtlinie anpassen



Quick Win: IDE Auto-Formatter



Quick Win: Code-Bereiche definieren



## Verantwortlichkeit festlegen



Teil des Entwicklungsteams



Entwicklungserfahrung



Motiviert, die Codequalität zu verbessern



## Tool-Feedback an passender Stelle

Feedback bei der Entwicklung



Feedback für den Reviewer



Der Weg von der bloßen Anschaffung zur effektiven Nutzung ist essenziell und geht nicht von allein