

ORACLE



Intelligent Application Security

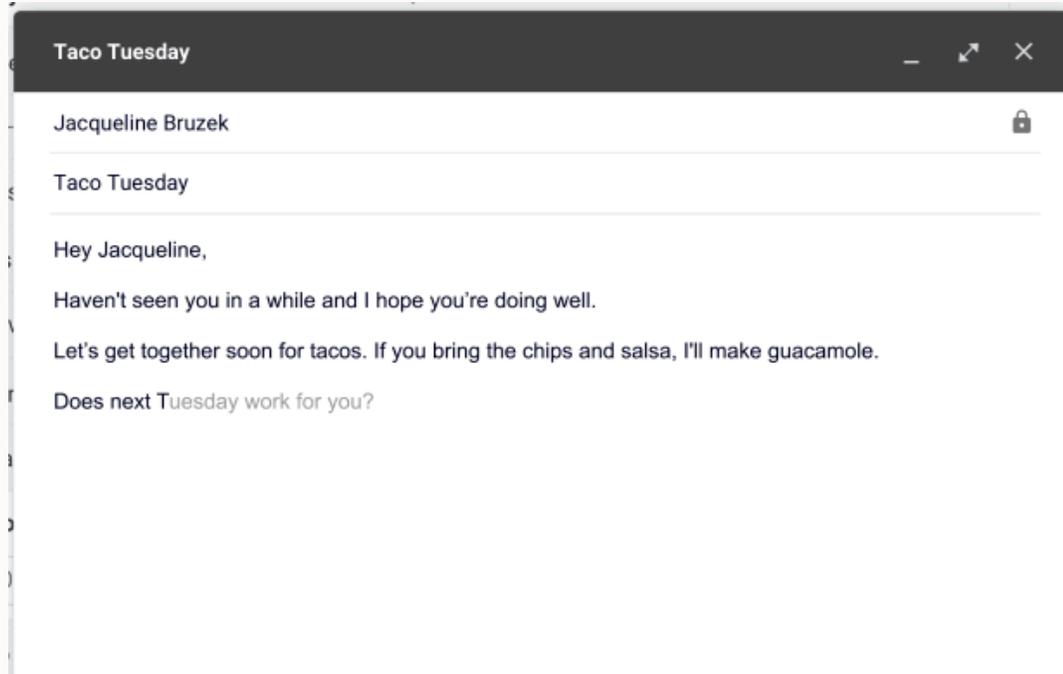
Cristina Cifuentes

Oracle Labs, Australia

May 25th, 2021

We Are Living With Intelligent Applications

Gmail's Smart Compose



iOS's Predictive Text



Microsoft's Visual Studio IntelliCode

Code completion suggestions based on 1,000s of open source projects

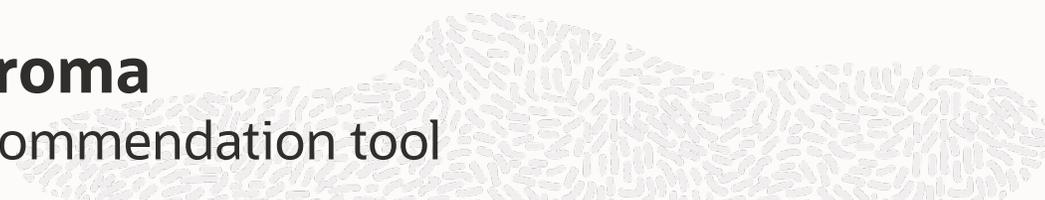
```
127 → // use the code formatter
128 → String lineDelim = TextUtilities.getDefaultLineDelimiter(document);
129 → String replacement = CodeFormatterUtil.format(CodeFormatter.K_CLASS_BODY_DECLARATIONS,
130
131 → // remove line delimiters
132 → if (replacement.endsWith(lineDelim)) {
133 →     int endIndex = replacement.length() - lineDelim.length();
134 →     replacement = replacement.
135 → }
136
137 → return replacement;
138 → }
139 }
140
```

- ★ substring(int beginIndex, int endIndex) : St...
- ★ length() : int
- ★ endsWith(String suffix) : boolean
- ★ charAt(int index) : char
- ★ substring(int beginIndex) : String
- concat(String str) : String
- intern() : String
- replace(CharSequence target, CharSequence replacem...
- replace(char oldChar, char newChar) : String
- replaceAll(String regex, String replacement) : Str...
- replaceFirst(String regex, String replacement) : S...
- toLowerCase() : String



Facebook's Aroma

Code-to-code search and recommendation tool



```
1 final BitmapFactory.Options options = new BitmapFactory.Options();
2 options.inSampleSize = 2;
3 // ...
4 Bitmap bmp = BitmapFactory.decodeStream(is, null, options);
```

```
1 Bitmap bitmap = BitmapFactory.decodeStream(input);
```

```
1 try {
2     InputStream is = am.open(fileName);
3     image = BitmapFactory.decodeStream(is);
4     is.close();
5 } catch (IOException e) {
6     // ...
7 }
```



Amazon's CodeGuru Reviewer

Identifies critical issues and hard-to-find performance bugs and suggests ways to fix them

```
HelloWorldFunction/src/main/java/helloworld/App.java
```

```
56 + item_values.put("location", new AttributeValue(ipv4));
57 + item_values.put("date", new AttributeValue(now));
58 +
59 + final AmazonDynamoDB ddb = AmazonDynamoDBClientBuilder.defaultClient();
```

 **danilop** 3 minutes ago Author Owner 😊 ⋮

Recommendation generated by Amazon CodeGuru Reviewer. Leave feedback on this recommendation by replying to the comment or by reacting to the comment using emoji.

This code is written so that the client cannot be reused across invocations of the Lambda function. To improve the performance of the Lambda function, consider using static initialization/constructor, global/static variables and singletons. It allows to keep alive and reuse HTTP connections that were established during a previous invocation.

Learn more about [best practices for working with AWS Lambda functions](#).

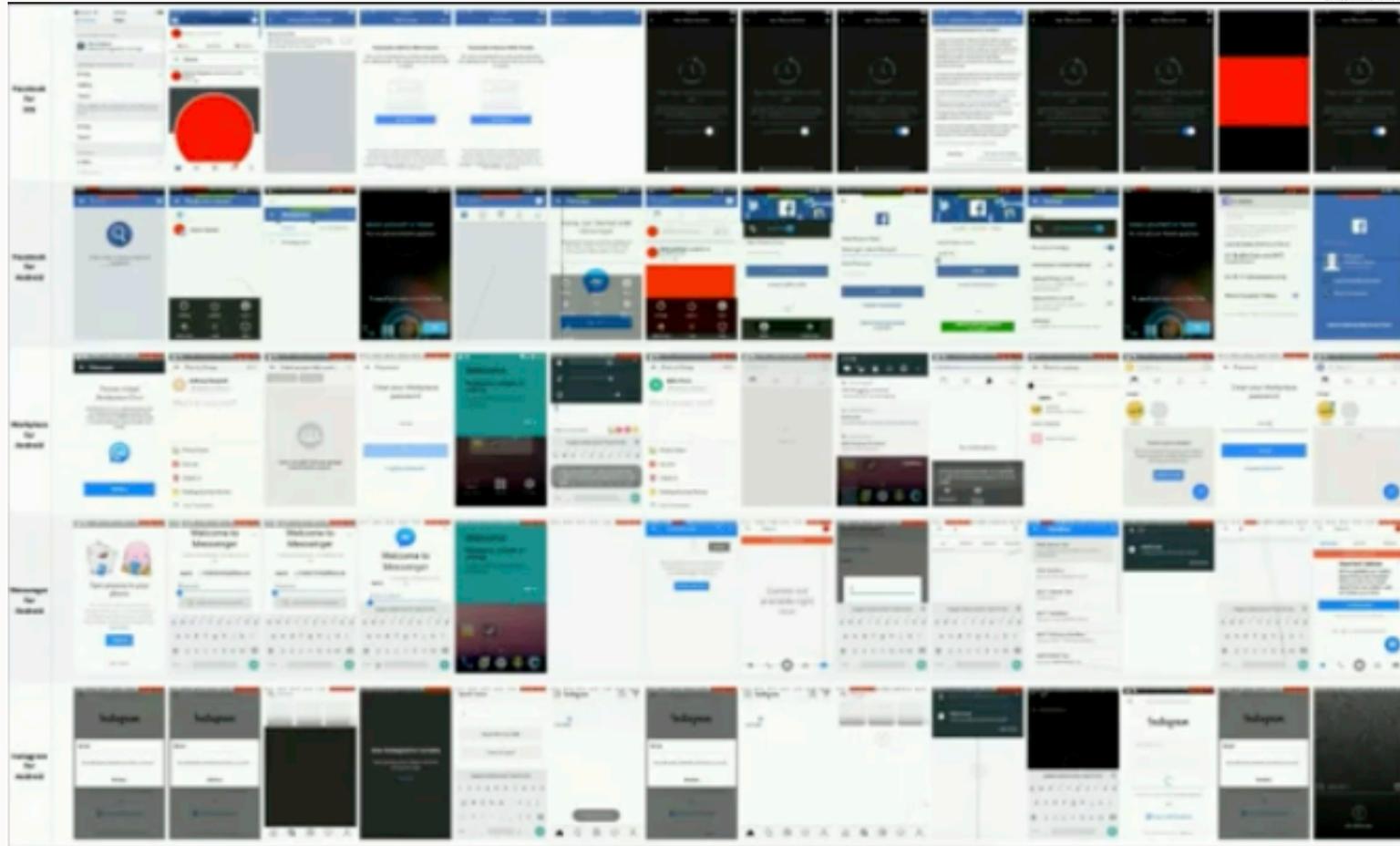
 Reply...

Resolve conversation



Facebook's Sapienz

Automatic generation of tests for Android applications based on system testing



Facebook's GetAFix

Finds fixes for bugs and offers them to engineers

```
20 public boolean onBackPressed() {
21     ApplicationContext ctx = this.getContext();
22     return ctx.onBackPressed();
23 }
24
```

 **phabricatorlinter** suggested changes to line 22

The value of `ctx` in the call to `onBackPressed()` could be null. (Origin: call to `getContext()` at line 21).
Questions about this suggested fix? Post in [Getafix Feedback](#)
Lint code: INFER
Lint name: Null Method Call

```
+   if (ctx == null) {
+       return false;
+   }
    return ctx.onBackPressed();
```

10 minutes ago • Like • Reply • Resolve

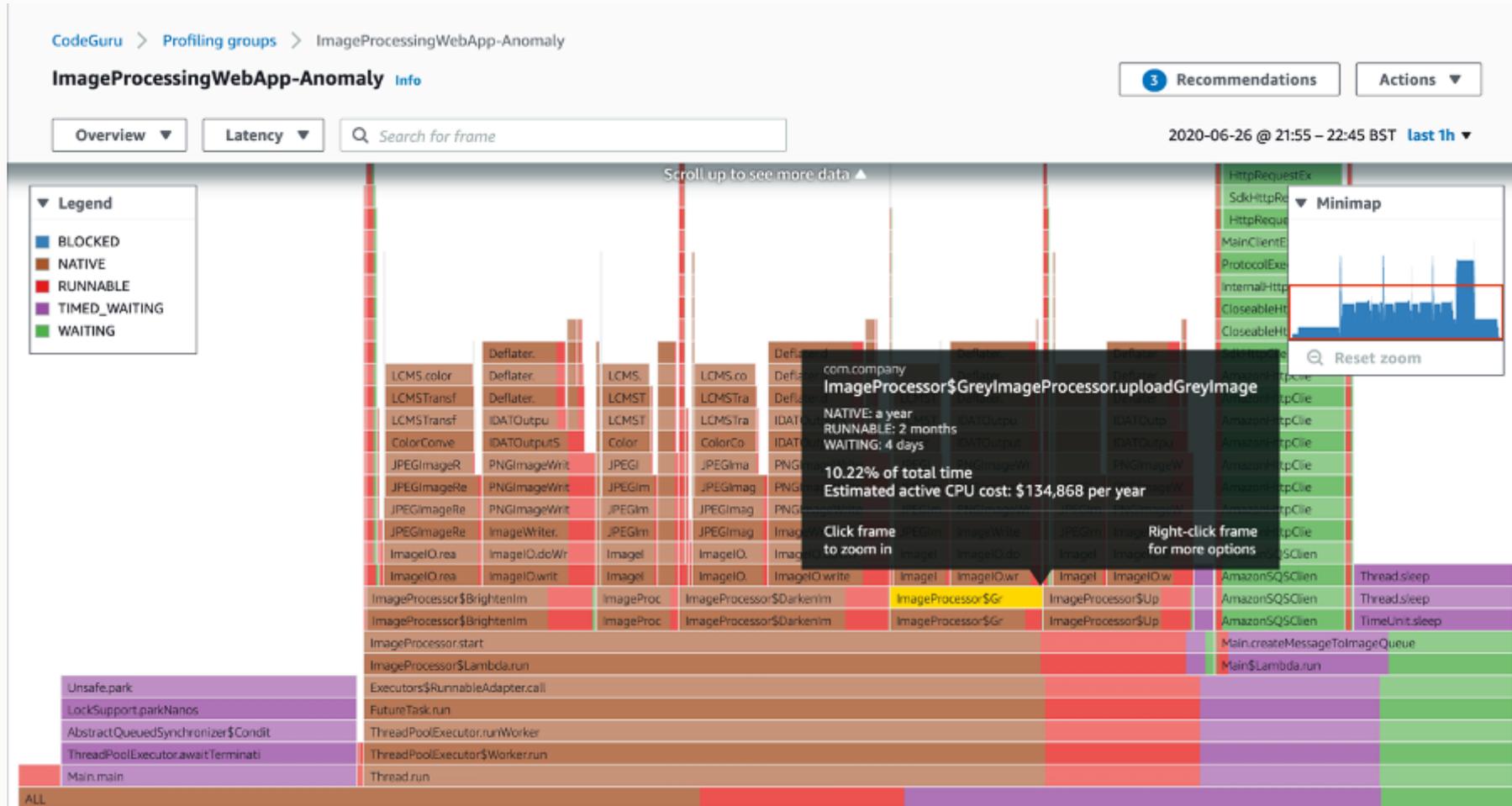
[Accept](#) • [Reject](#)

A code fix to a **lint** error



Amazon's CodeGuru Profiler

Finds most expensive lines of code and recommends improvements



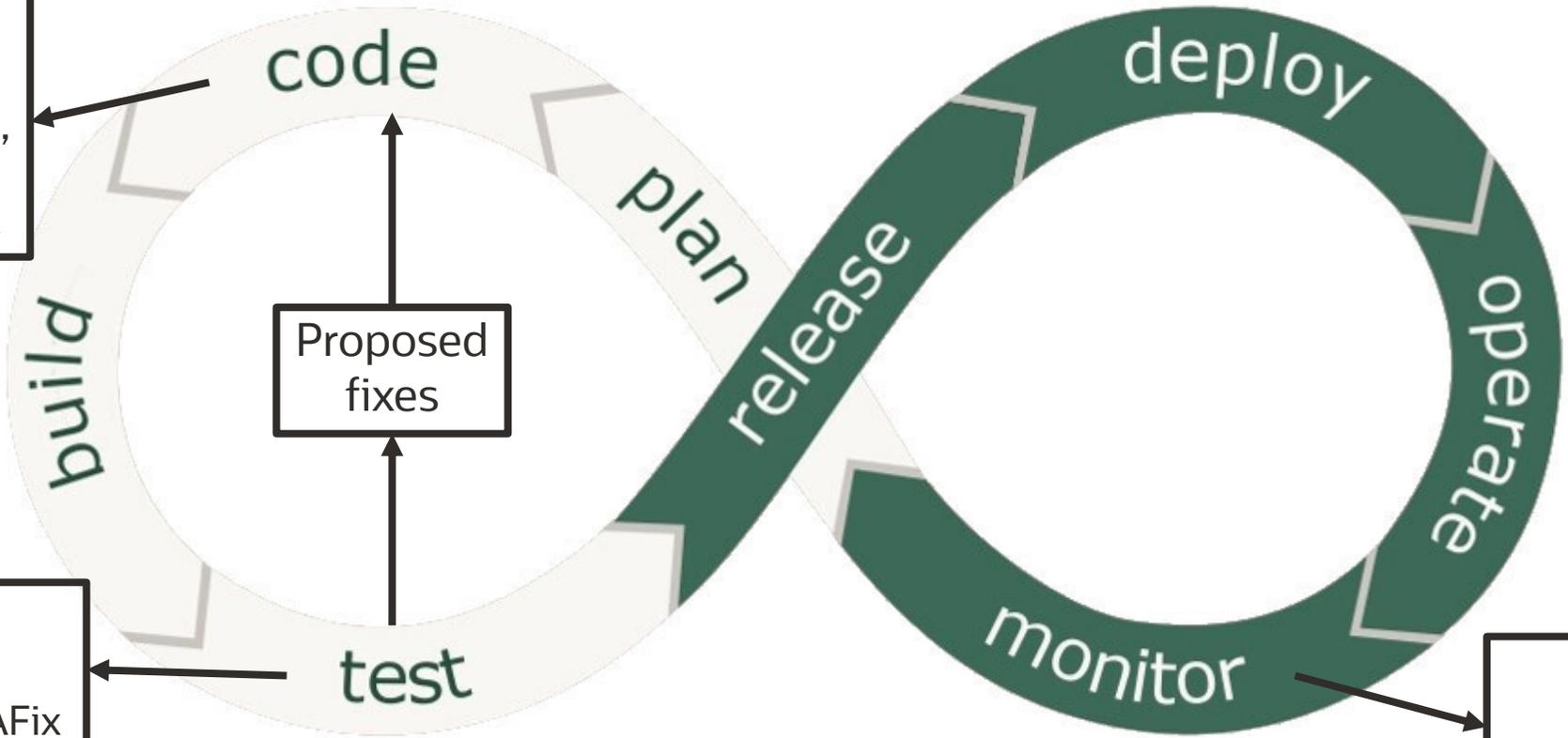
These Examples Help Developers, Testers and Operations Staff



Intelligent coding
e.g., VS IntelliCode, Aroma, CodeGuru Reviewer, GetAFix

Intelligent testing
e.g., Sapienz, GetAFix

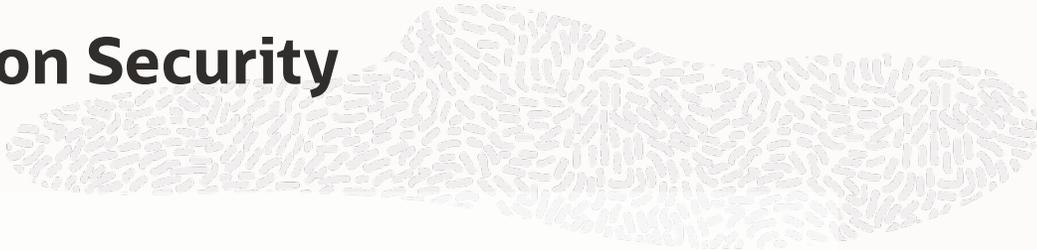
Intelligent monitoring
e.g., CodeGuru Profiler



We Can Build an Intelligent Application Security Future

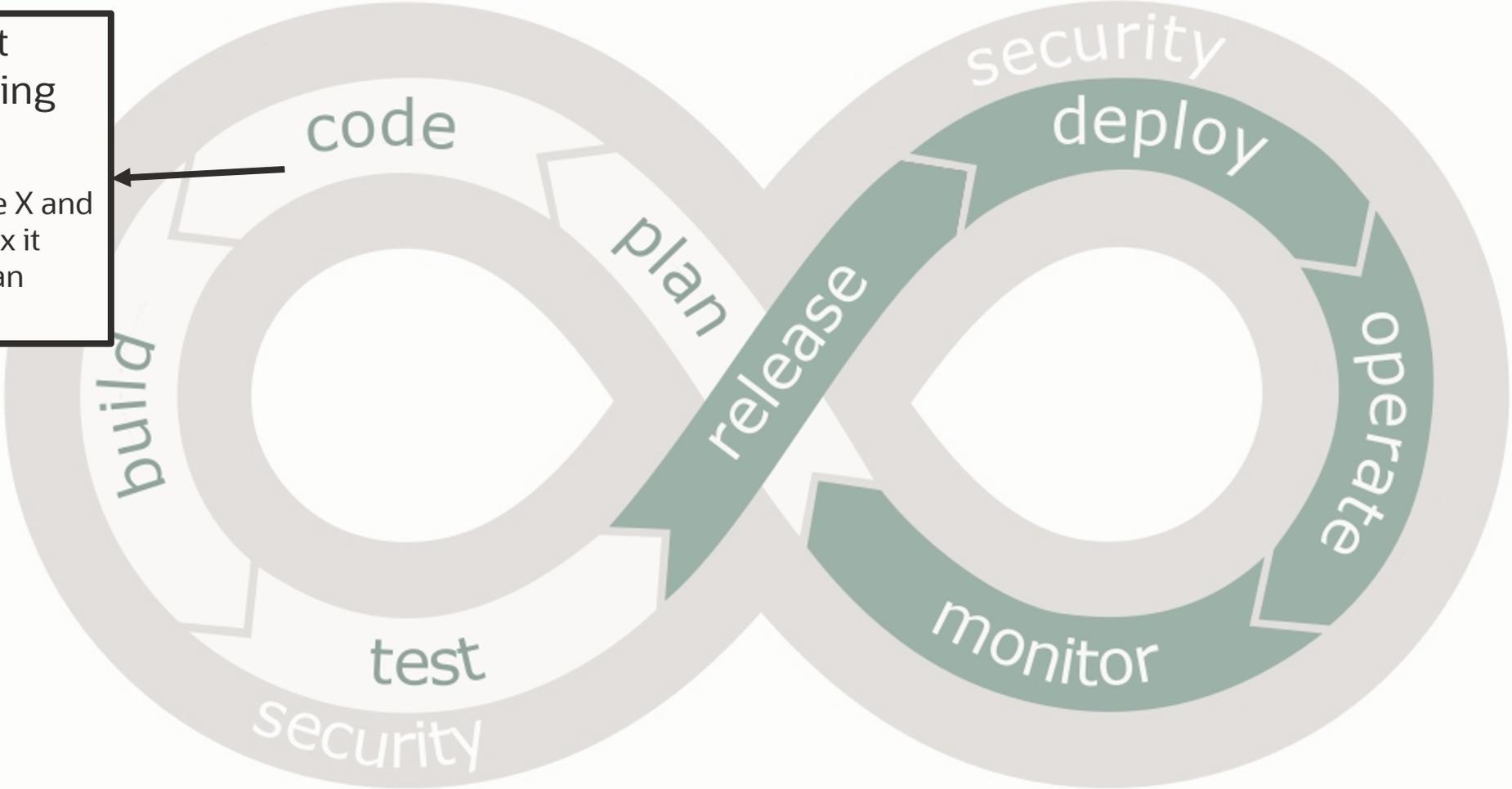
#ias

Intelligent Application Security

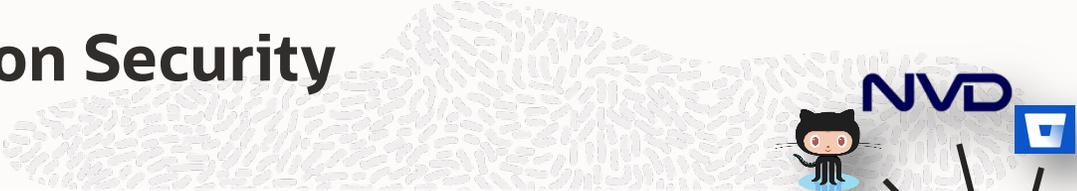


Intelligent security coding

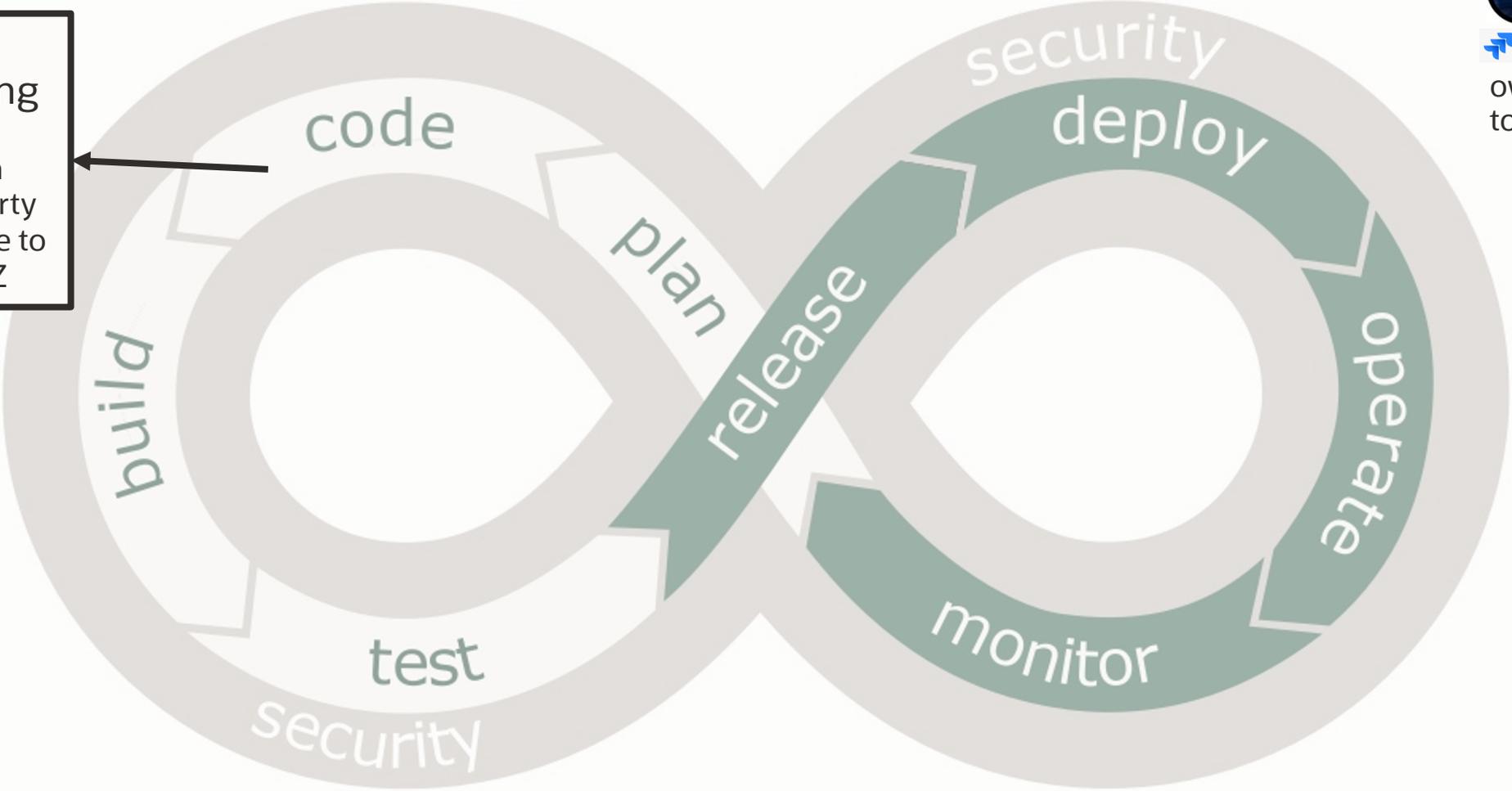
You have a vulnerability at line X and here's how to fix it [before you can commit]



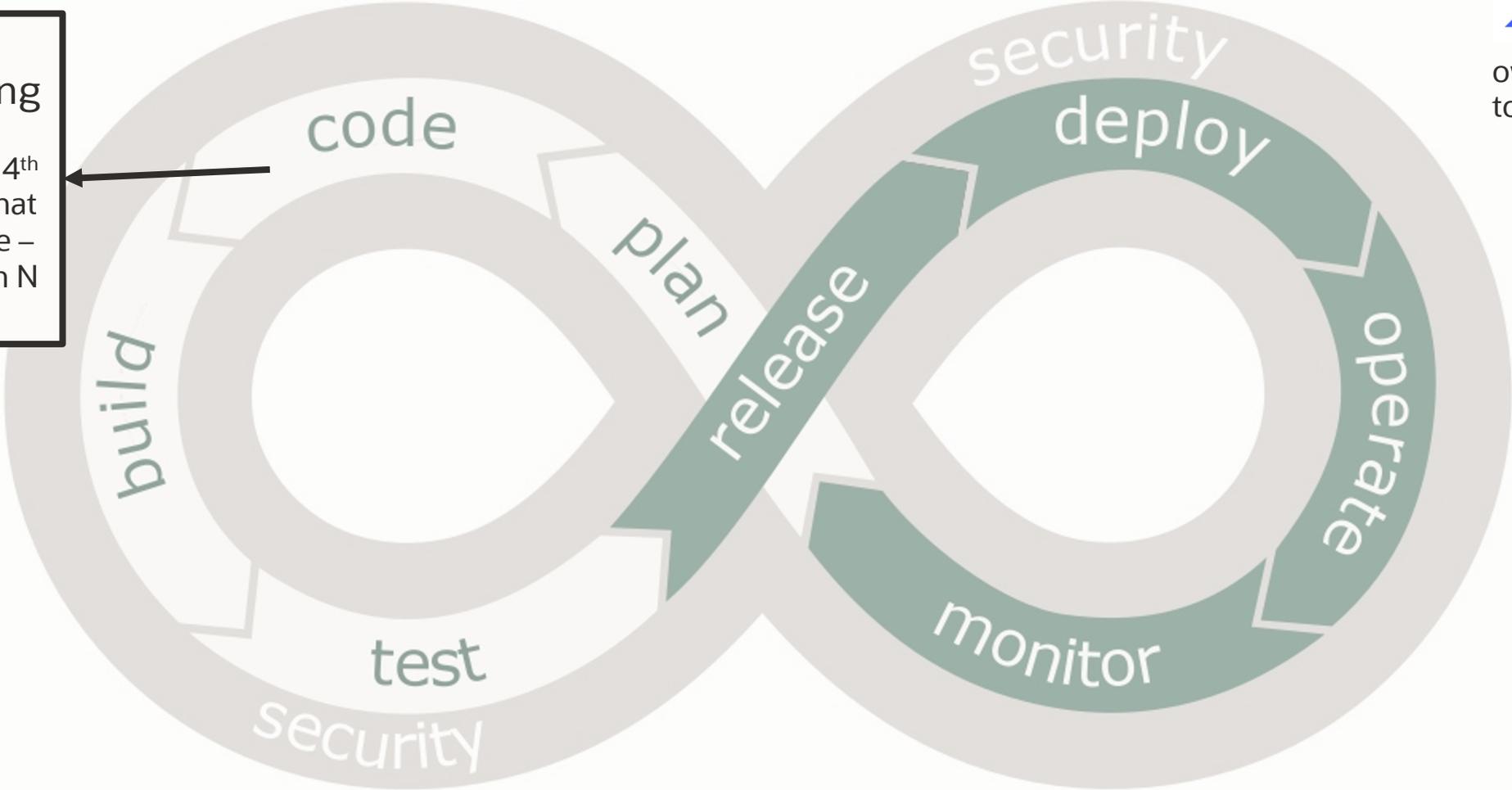
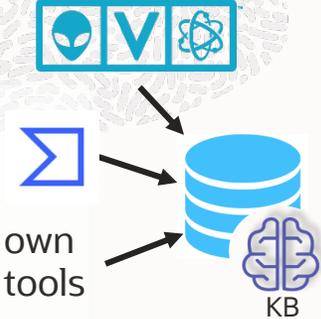
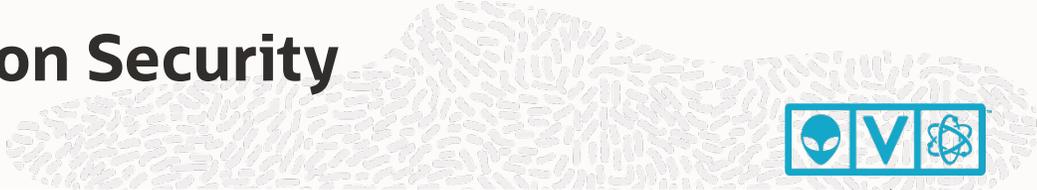
Intelligent Application Security



Intelligent security coding
You depend on vulnerable 3rd party library Y – upgrade to clean version Z



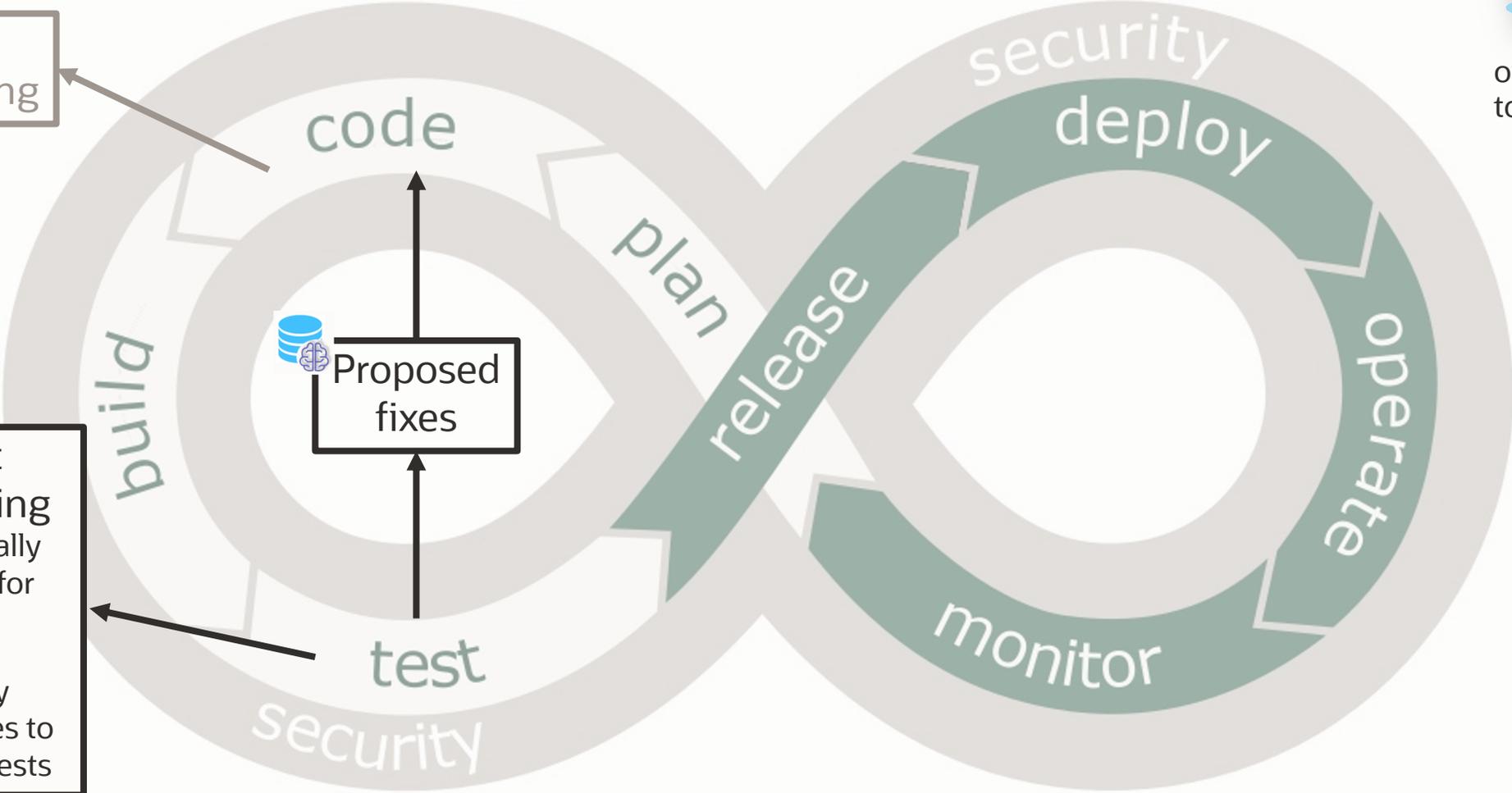
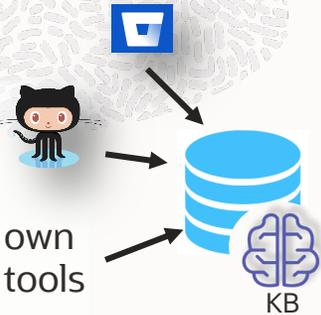
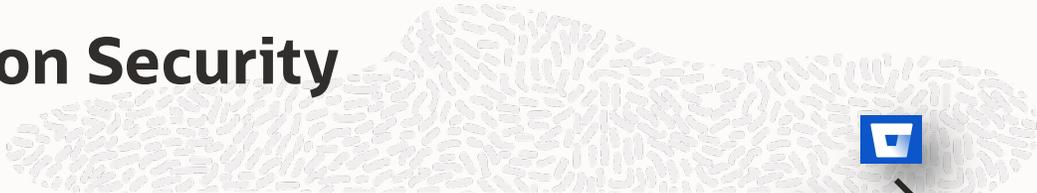
Intelligent Application Security



Intelligent security coding
You depend on a 4th party library M that contains malware – use clean version N instead



Intelligent Application Security



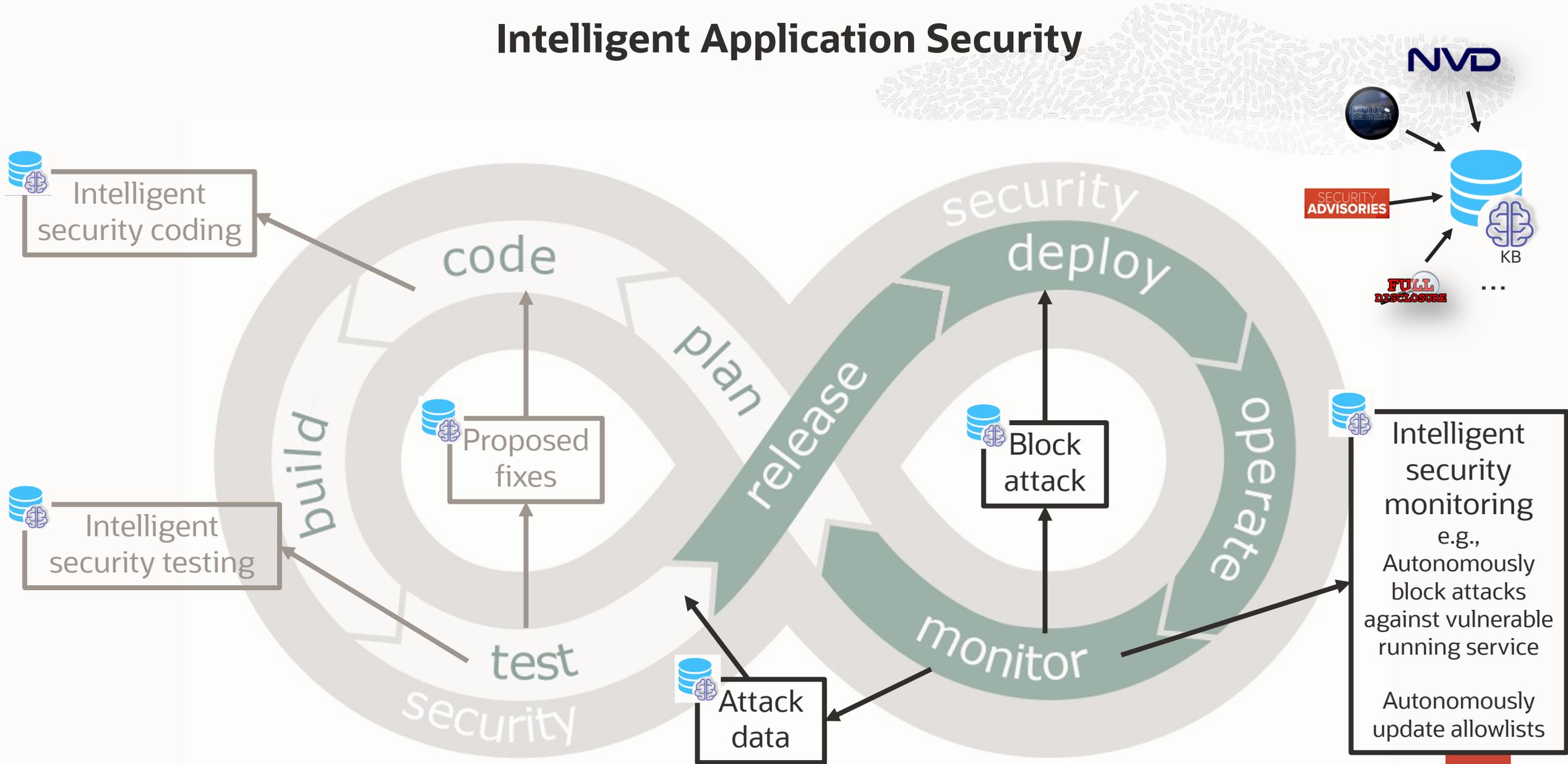
Intelligent security coding

Intelligent security testing
e.g., Automatically generate tests for security

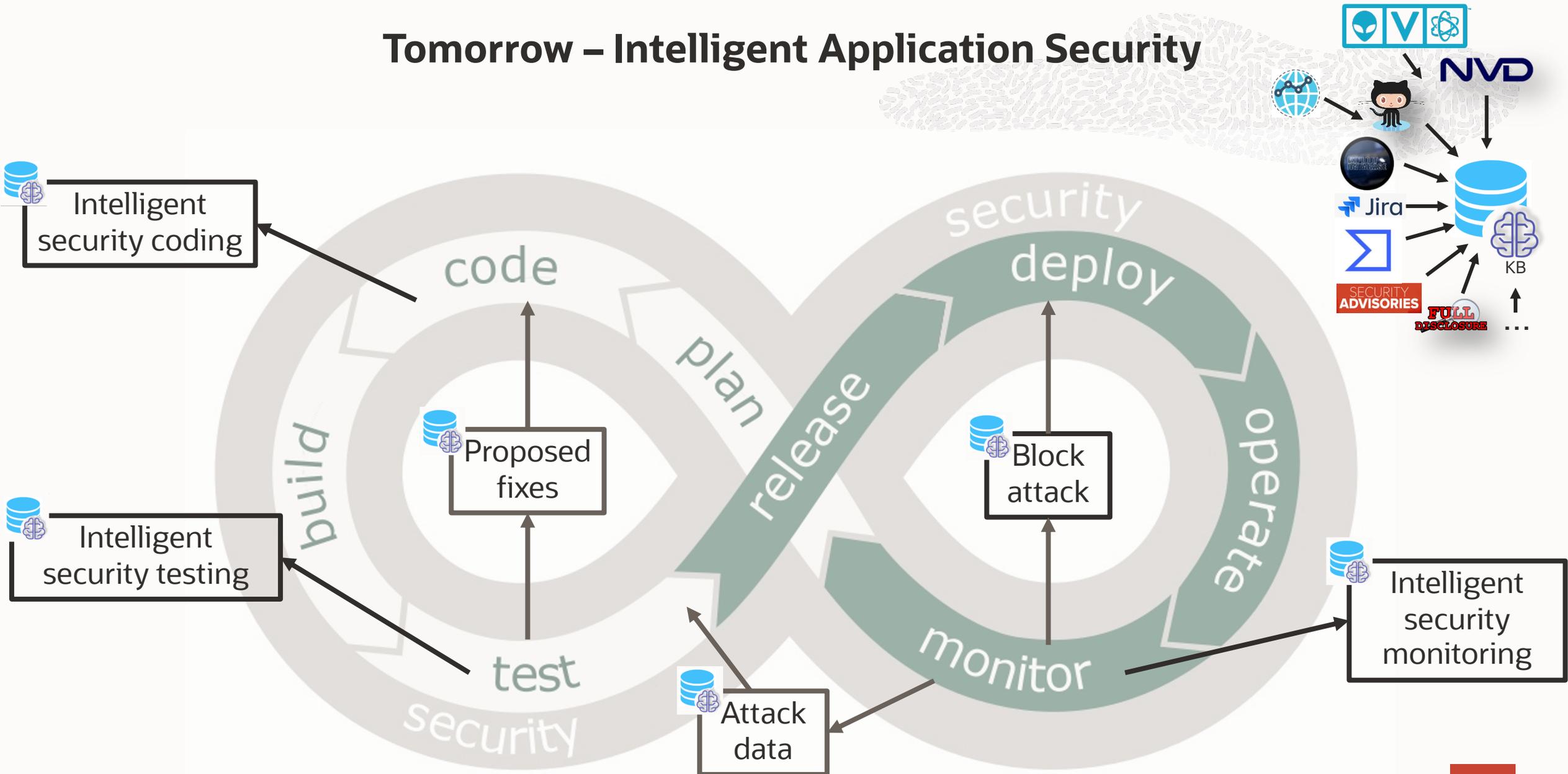
Automatically propose bug fixes to failing security tests



Intelligent Application Security



Tomorrow – Intelligent Application Security



“Intelligent Application Security aims to provide an automated approach to integrate security into all aspects of application development and operations, at scale, using learning techniques that incorporate signals from the code and beyond, to provide actionable intelligence to developers, security analysts, operations staff, and autonomous systems.”

Cristina Cifuentes

October 2020

ORACLE



#ias
cristina.cifuentes@oracle.com

<http://labs.oracle.com>

@criscifuentes