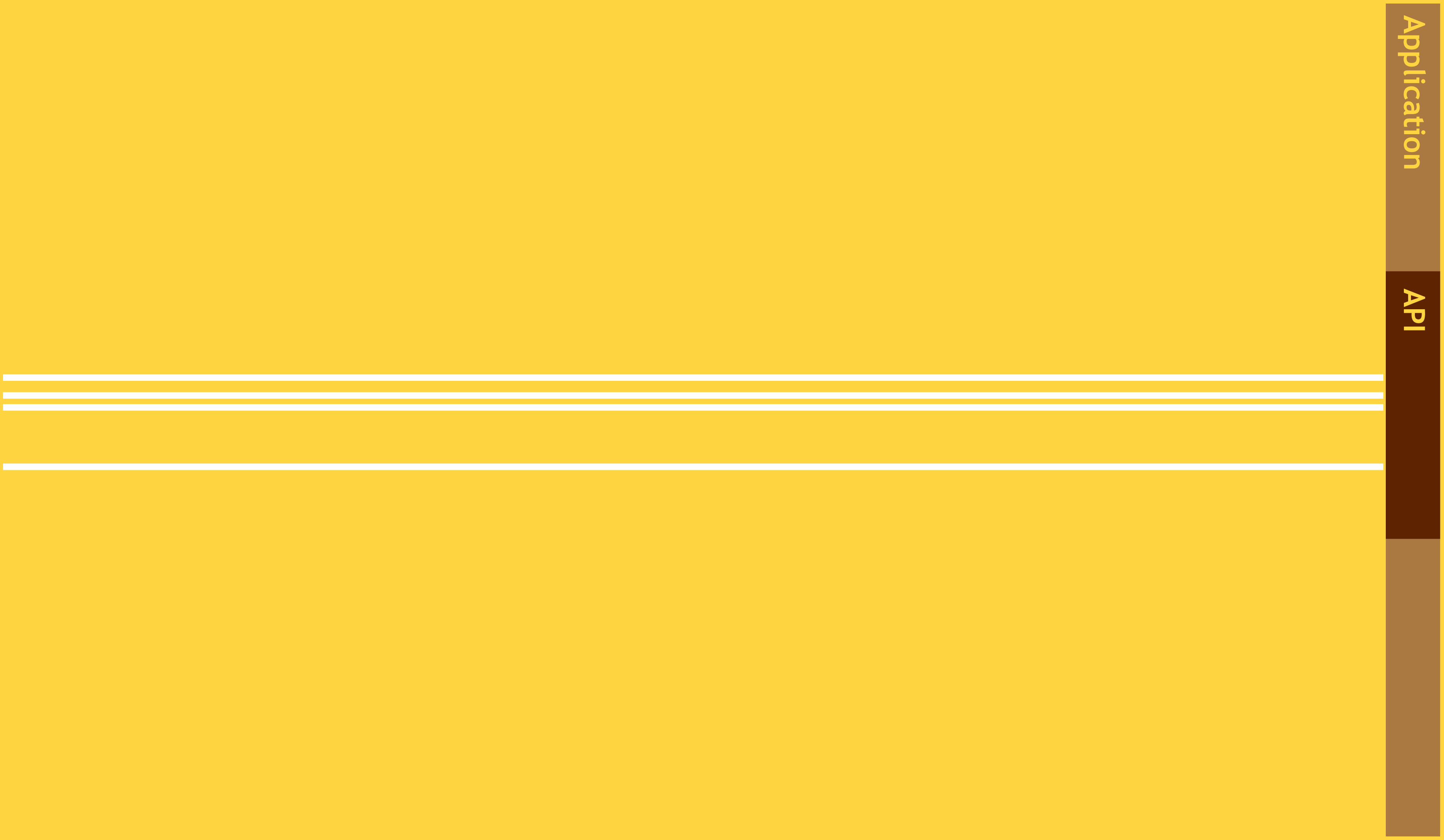
London API Group

Detecting and Responding to Malice in API Use

Colin Watson

17th September 2014

Nice users



Application

API

Naughty users

Application
API

What are indicators of naughty users?

Request with insufficient privileges	Authorisation failures
Invalid data type or length/range	Input validation failures
Incorrect credentials	Authentication failures
Malicious XML or SQL	Blatant code injection
Using the API to fast	Suspicious rate of use
Using the API too frequently	Suspicious pattern of use

What can we do to naughty users?

Increase logging

Alert administrator

Proxy request

Change user's status

User notification

Timing change

Function amended

Function disabled

Log out

Lock account

API disabled

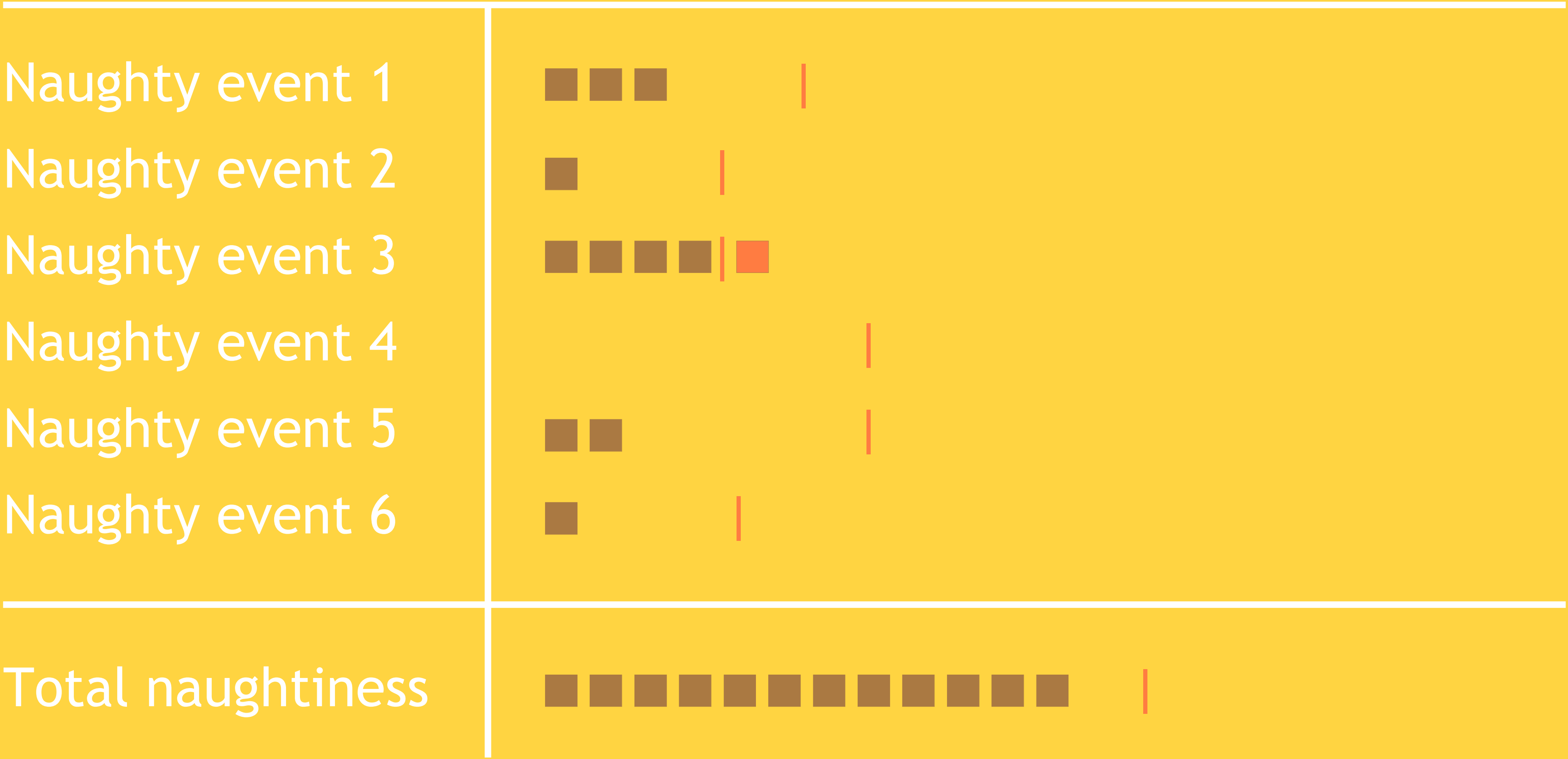
Groups of users

Thresholds

Time periods

Continuous monitoring

Define thresholds and maintain a record for each API user



Naughty event 1

Naughty event 2

Naughty event 3

Naughty event 4

Naughty event 5

Naughty event 6

Total naughtiness

OWASP AppSensor

OWASP

https://www.owasp.org

AppSensor

http://appsensor.org

https://www.owasp.org/index.php/OWASP_AppSensor_Project
https://github.com/jtmelton/appsensor

Guide (v2.0.1, May 2014)

Creative Commons Attribution-ShareAlike 3.0 license

AppSensor Guide v2.0

Application-Specific Real Time Attack Detection and Response

Code (v2.0.0 beta, Sep 2014)

MIT open-source license

We have an API for that

Maven

```
<repositories>
    <repository>
       <id>sonatype-snapshots</id>
       <name>Snapshot repository for Sonatype dependencies</name>
       <url>https://oss.sonatype.org/content/repositories/snapshots/</url>
    </repository>
</repositories>

<dependency>
    <groupId>org.owasp.appsensor</groupId>
    <artifactId>appsensor-core</artifactId>
    <version>2.0.0-RC1</version>
</dependency>
```

Gradle

```
'org.owasp.appsensor:appsensor-core:2.0.0'
```

Binary

```
http://mvnrepository.com/artifact/org.owasp.appsensor
```

Instrument the code

```
if ( accno.length > 10 )
{
    api_errors.add ( "The account number entered is too long." )

    # -----------------------------
    #  start new code for AppSensor

    # "AE4" is the identifier for this specific detection point
    appSensor.addEvent ( api_user, "AE4" )

    #  end new code for AppSensor
    # -----------------------------
}
```

Your presenter

Colin Watson

https://www.clerkendweller.uk

https://twitter.com/clerkendweller

https://www.linkedin.com/in/clerkendweller

https://www.watsonhall.uk