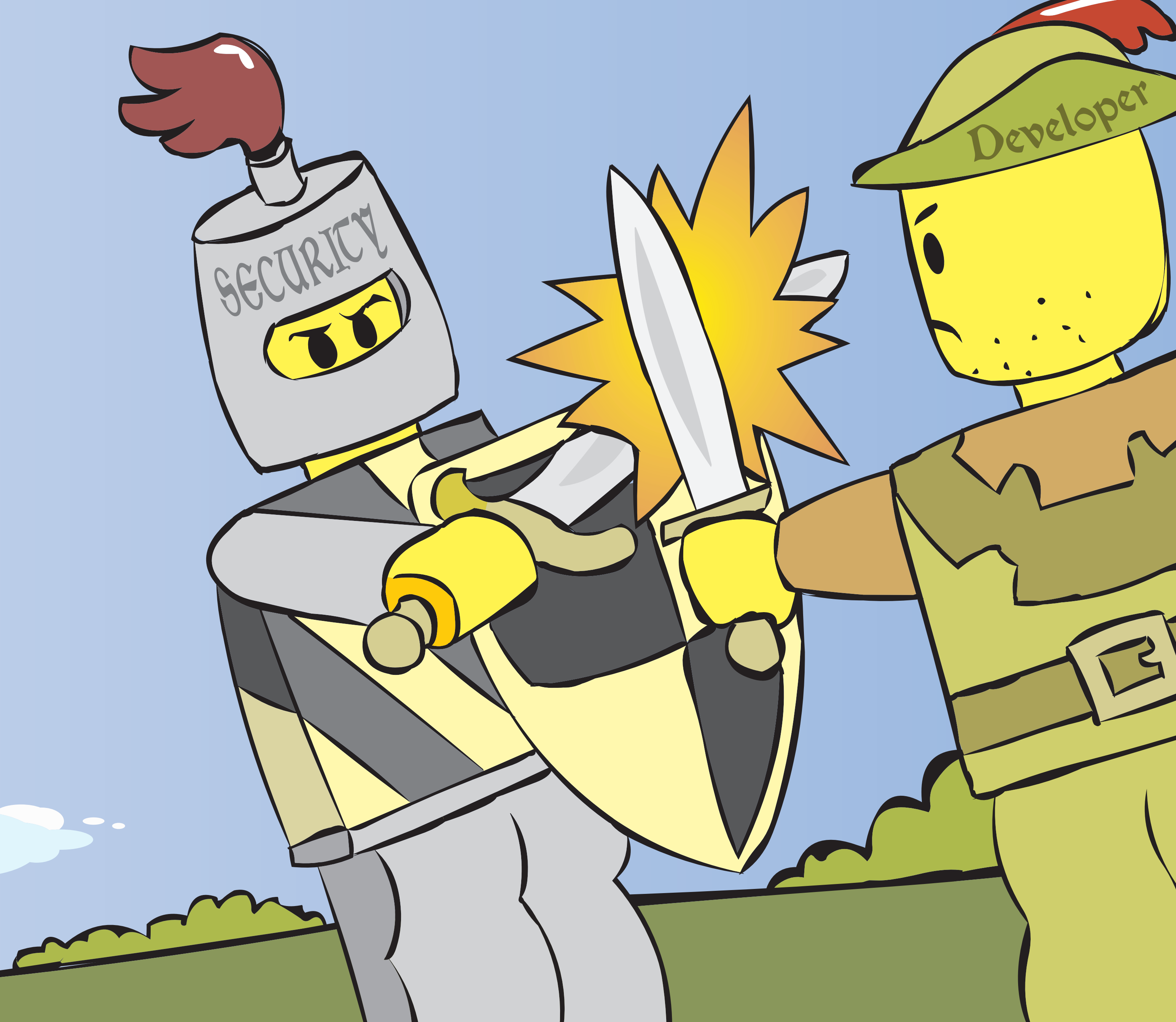
Go Fast. Be Secure.

A true story of how
Development and Security
came together to fix
the risk in open source.

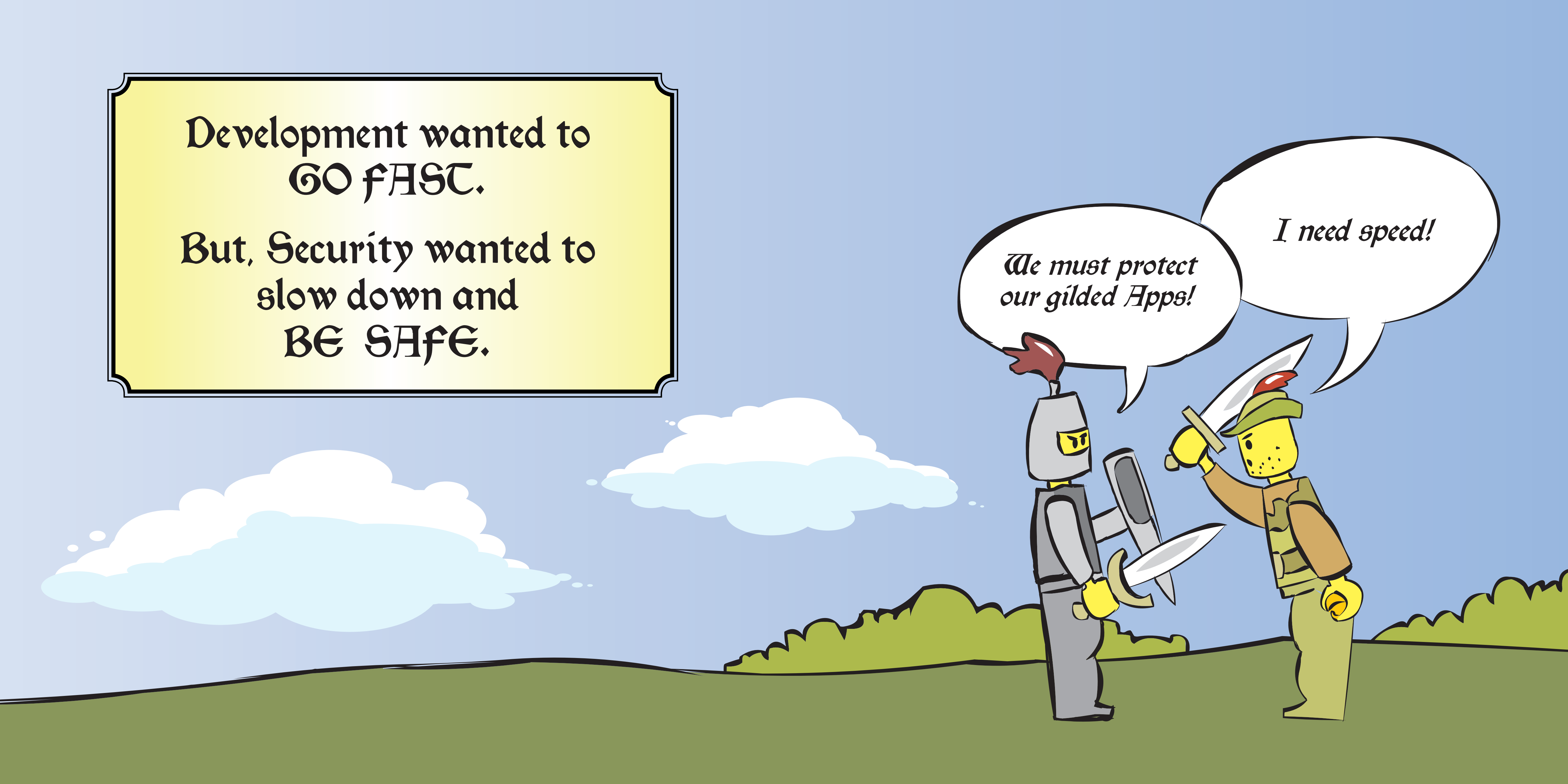
Once upon a time...

There was a great battle
between
SPEED
and
SECURITY.



Development wanted to GO FAST.

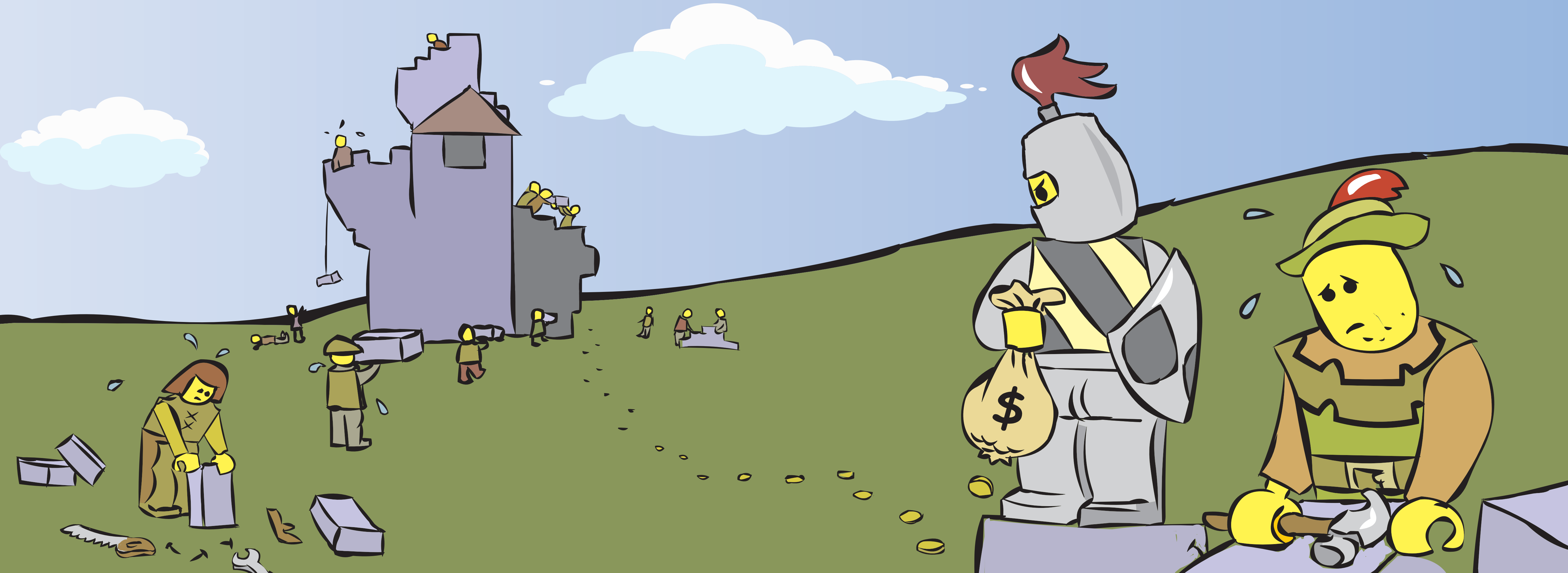
But, Security wanted to slow down and BE SAFE.

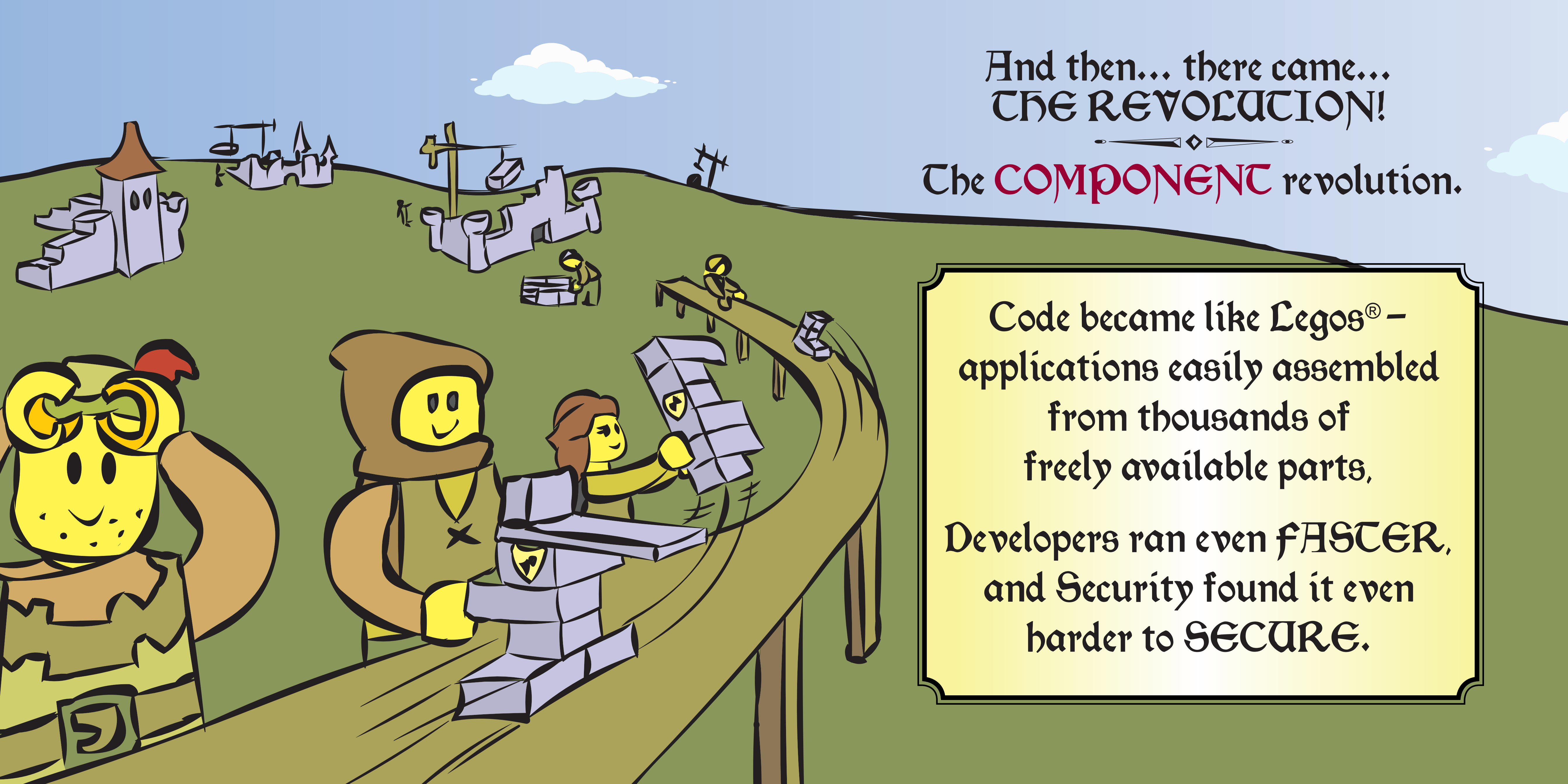


For years...
they endured the pain of late testing,
false positives...

and the added costs of getting
the bad stuff out.

There HAD to be a better way!





And then... there came... THE REVOLUTION!

The COMPONENT revolution.

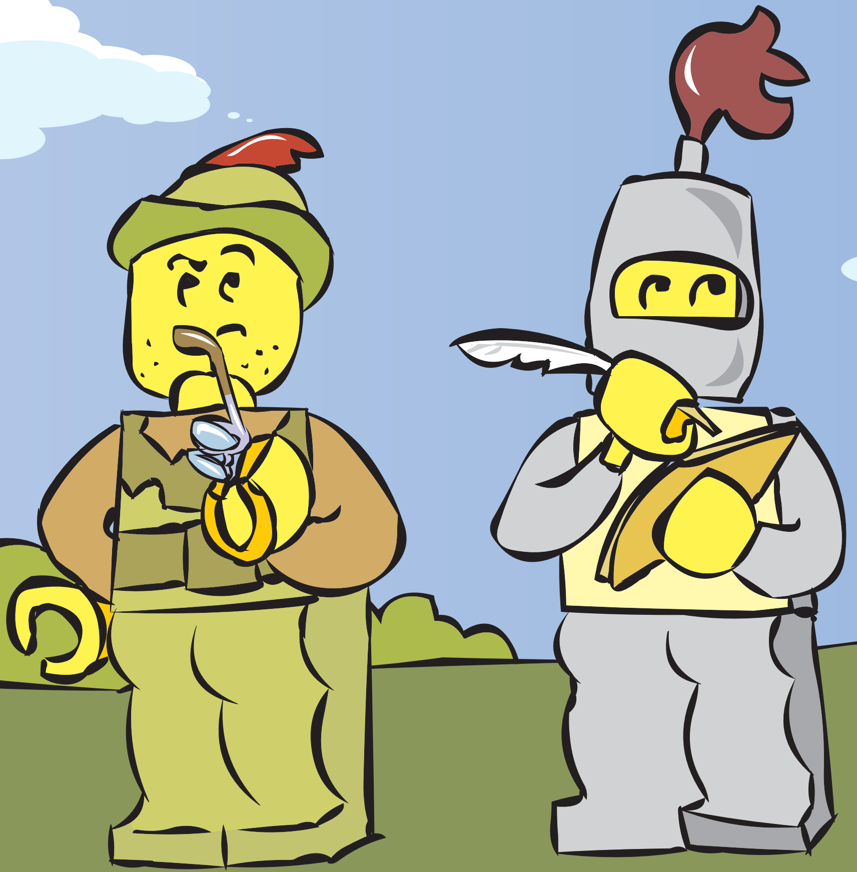
Code became like Legos® – applications easily assembled from thousands of freely available parts.

Developers ran even FASTER, and Security found it even harder to SECURE.

Together, they pondered...

"How can we keep SAFE
at this even FASTER
speed of development?"

"How can we SECURE
this new Lego®
'software supply chain'?"

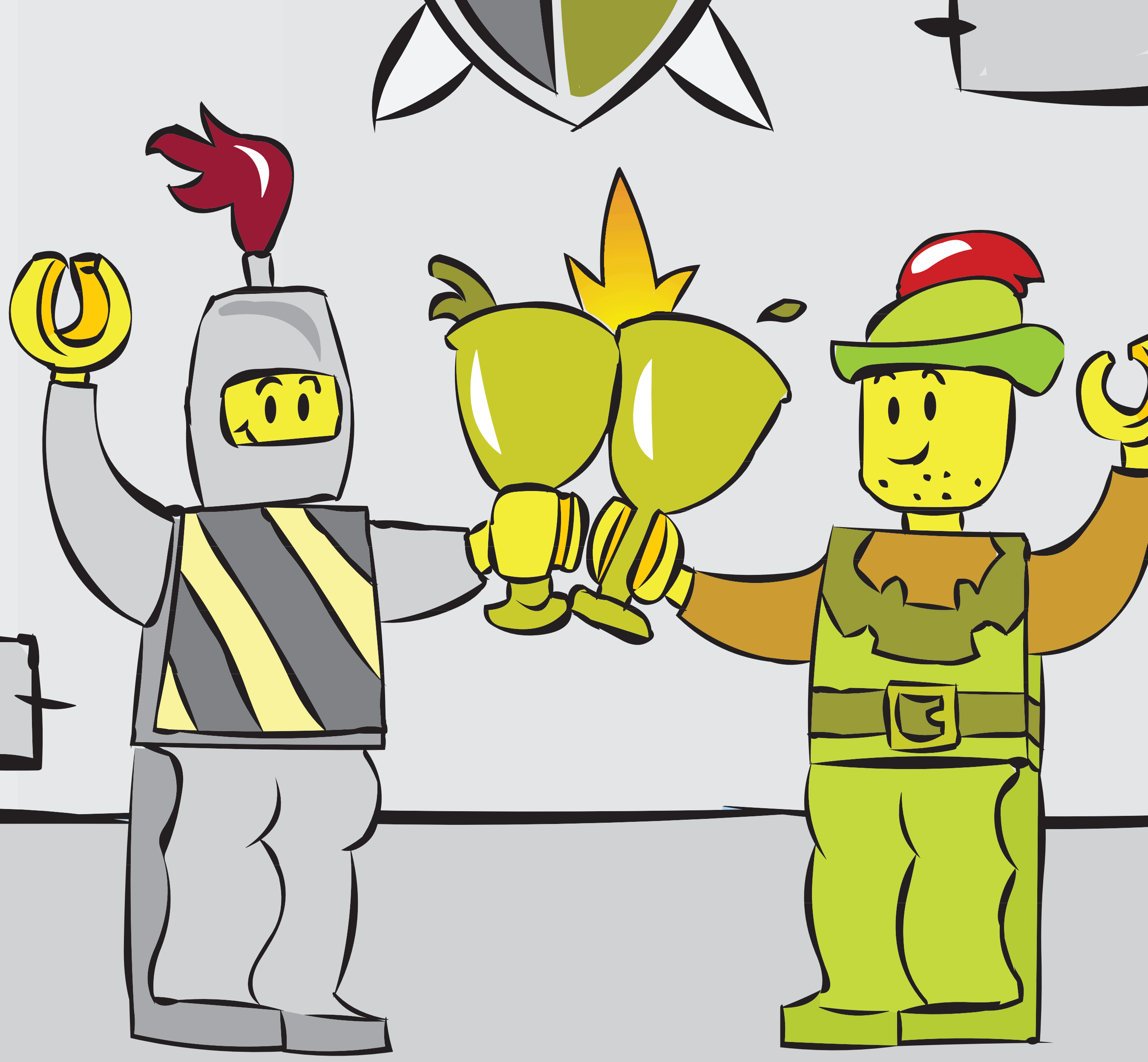


After much self – reflection...
the ANSWER
revealed itself:

Bring SECURITY
and SPEED together

by building component
intelligence and governance
in from the START...

using all the tools
developers love to use today!



And so it was.

The birth of a new way to secure the software supply chain...

where developers went FAST and applications were SAFE.

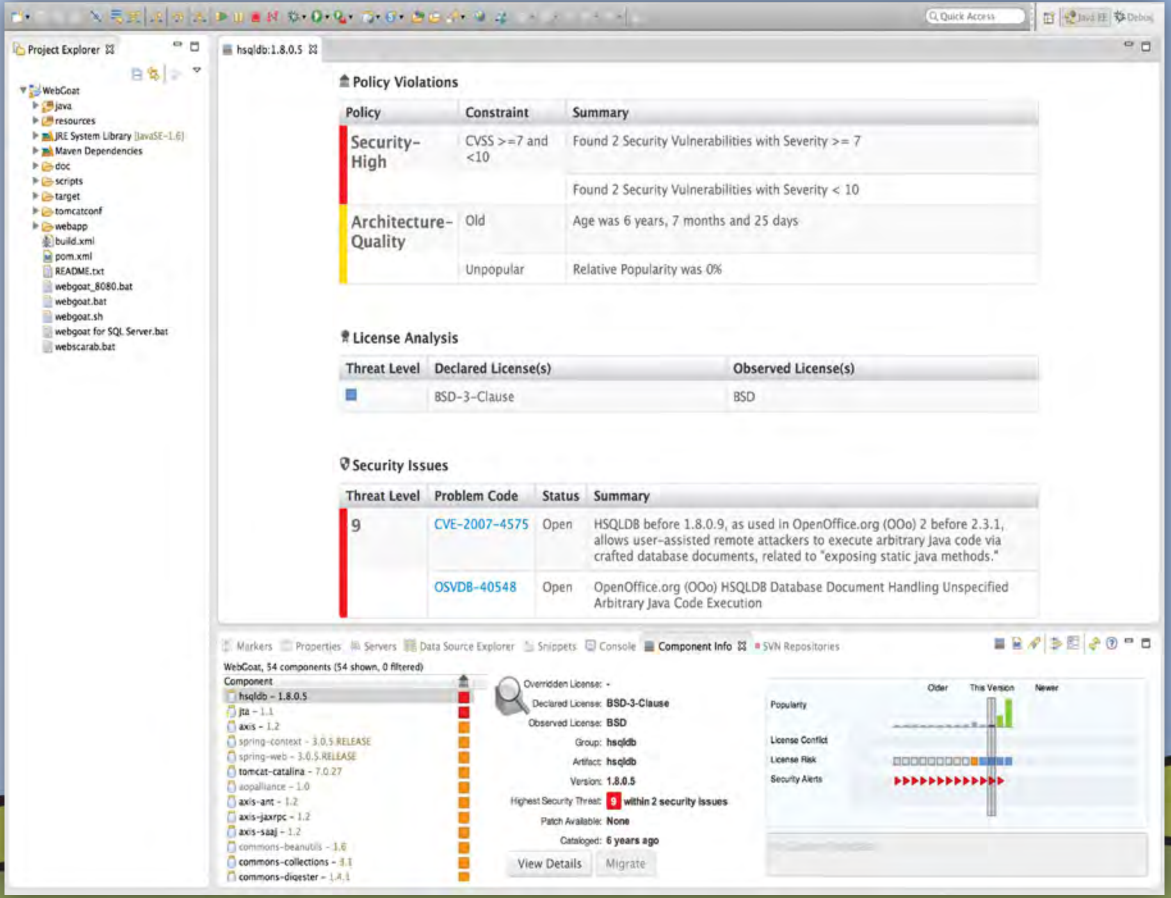
And this REVOLUTIONARY, yet SIMPLE approach came to be called...

Component Lifecycle Management

A new way to secure the modern software supply chain

A new way to...

AUTOMATE and
enforce GOVERNANCE
in the tools
you use today.



Policy Violations

Policy	Constraint	Summary
Security-High	CVSS >=7 and <10	Found 2 Security Vulnerabilities with Severity >= 7
		Found 2 Security Vulnerabilities with Severity < 10
Architecture-Quality	Old	Age was 6 years, 7 months and 25 days
	Unpopular	Relative Popularity was 0%

License Analysis

Threat Level	Declared License(s)	Observed License(s)
🟦	BSD-3-Clause	BSD

Security Issues

Threat Level	Problem Code	Status	Summary
9	CVE-2007-4575	Open	HSQLDB before 1.8.0.9, as used in OpenOffice.org (OOo) 2 before 2.3.1, allows user-assisted remote attackers to execute arbitrary Java code via crafted database documents, related to "exposing static java methods."
	OSVDB-40548	Open	OpenOffice.org (OOo) HSQLDB Database Document Handling Unspecified Arbitrary Java Code Execution

WebGoat, 54 components (54 shown, 0 filtered)

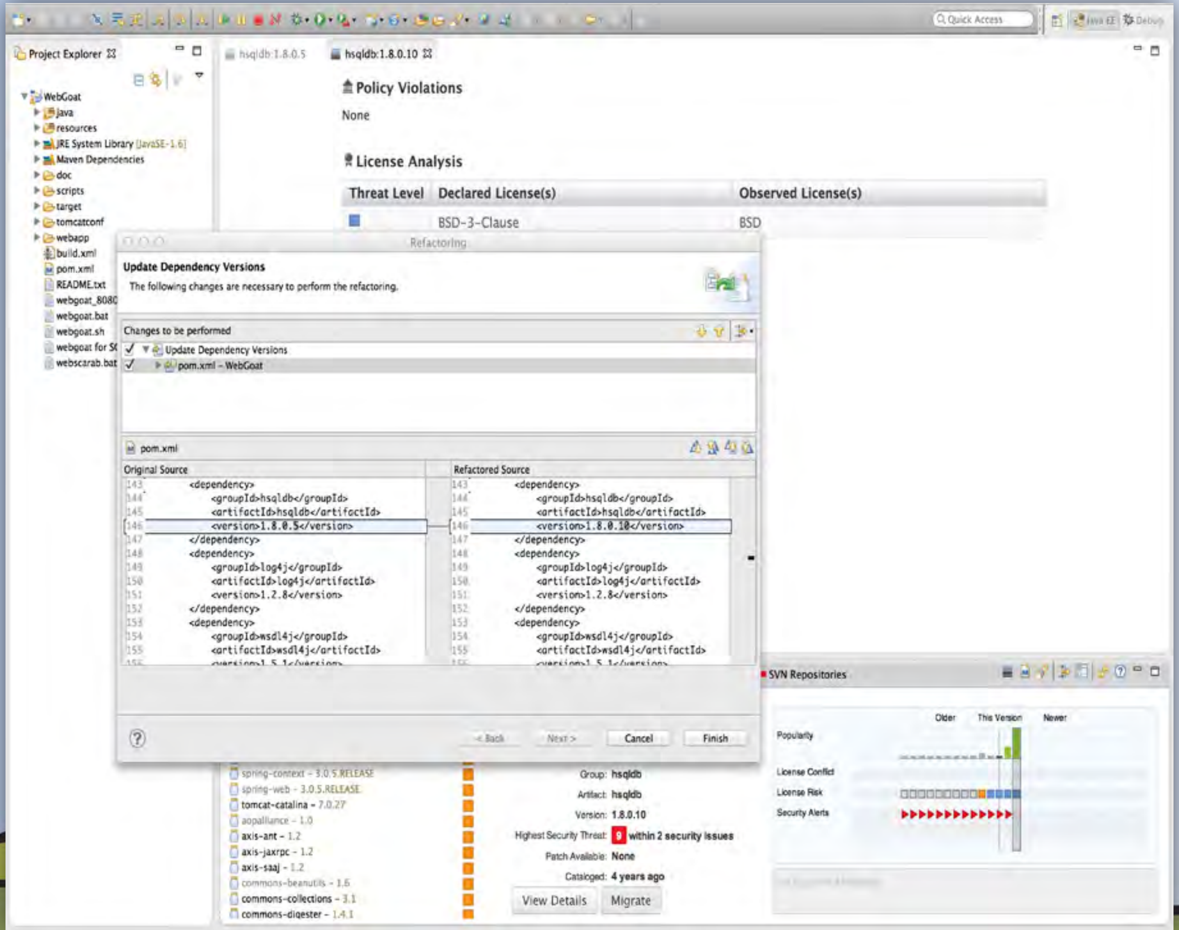
Component	
hsqldb - 1.8.0.5	🟥
jta - 1.1	🟥
axis - 1.2	🟧
spring-context - 3.0.5.RELEASE	🟧
spring-web - 3.0.5.RELEASE	🟧
tomcat-catalina - 7.0.27	🟧
aopalliance - 1.0	🟧
axis-ant - 1.2	🟧
axis-jaxrpc - 1.2	🟧
axis-saaj - 1.2	🟧
commons-beanutils - 1.6	🟧
commons-collections - 3.1	🟧
commons-digester - 1.4.1	🟧

Overridden License: -
Declared License: BSD-3-Clause
Observed License: BSD
Group: hsqldb
Artifact: hsqldb
Version: 1.8.0.5
Highest Security Threat: 9 within 2 security issues
Patch Available: None
Cataloged: 6 years ago

▲ **Policy, security and licensing information guides developers to select the best components in their development environment.**

A new way to...

REMEDIATE RISK
early in the process
to reduce risk and cost.



Policy Violations

None

License Analysis

Threat Level	Declared License(s)	Observed License(s)
🟦	BSD-3-Clause	BSD

Update Dependency Versions

The following changes are necessary to perform the refactoring.

Changes to be performed

- ✓ Update Dependency Versions
  - ✓ pom.xml - WebGoat

Original Source

```
        <dependency>
            <groupId>hsqldb</groupId>
            <artifactId>hsqldb</artifactId>
            <version>1.8.0.5</version>
        </dependency>
        <dependency>
            <groupId>log4j</groupId>
            <artifactId>log4j</artifactId>
            <version>1.2.8</version>
        </dependency>
        <dependency>
            <groupId>wsdl4j</groupId>
            <artifactId>wsdl4j</artifactId>
            <version>1.5.1</version>
```

Refactored Source

```
        <dependency>
            <groupId>hsqldb</groupId>
            <artifactId>hsqldb</artifactId>
            <version>1.8.0.10</version>
        </dependency>
        <dependency>
            <groupId>log4j</groupId>
            <artifactId>log4j</artifactId>
            <version>1.2.8</version>
        </dependency>
        <dependency>
            <groupId>wsdl4j</groupId>
            <artifactId>wsdl4j</artifactId>
            <version>1.5.1</version>
```

- spring-context - 3.0.5.RELEASE
- spring-web - 3.0.5.RELEASE
- tomcat-catalina - 7.0.27
- aopalliance - 1.0
- axis-ant - 1.2
- axis-jaxrpc - 1.2
- axis-saaj - 1.2
- commons-beanutils - 1.6
- commons-collections - 3.1
- commons-digester - 1.4.1

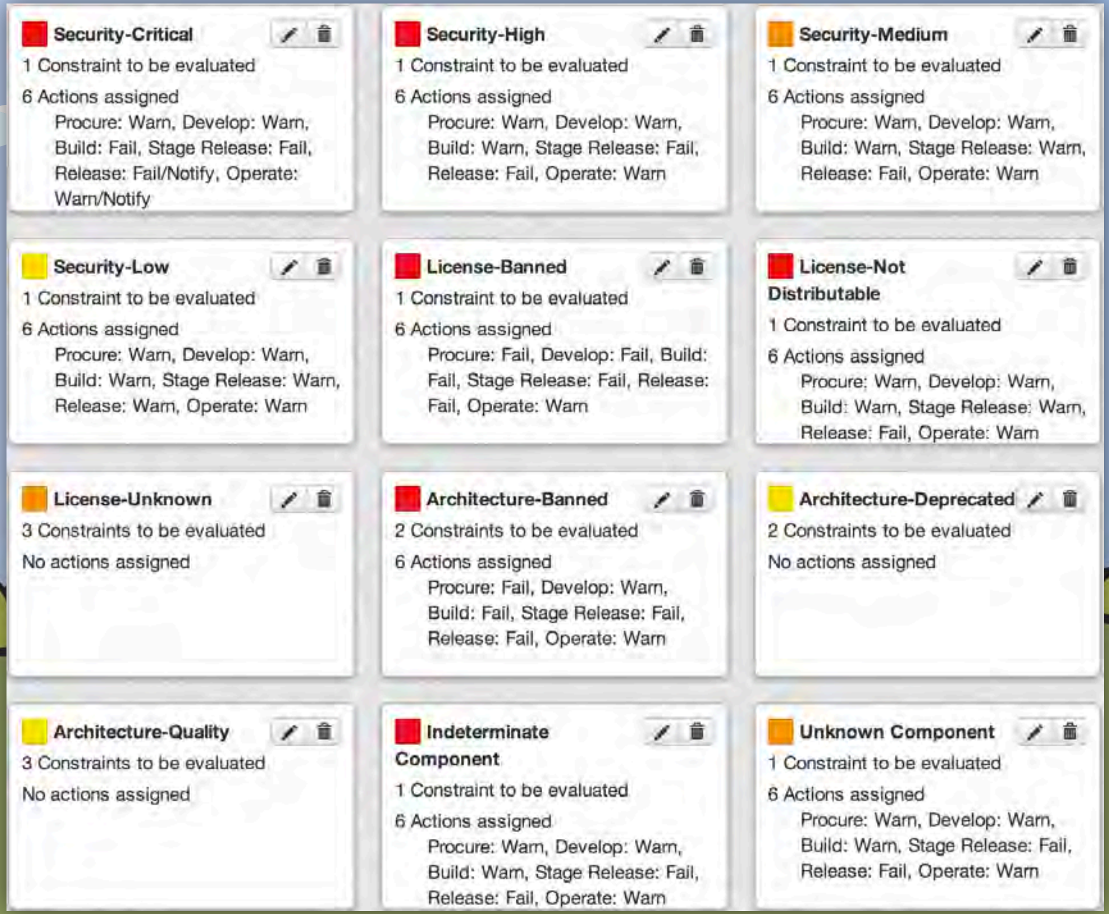
Group: hsqldb
Artifact: hsqldb
Version: 1.8.0.10
Highest Security Threat: 9 within 2 security issues
Patch Available: None
Cataloged: 4 years ago

▲ Optimal components can be selected and application flaws can be remediated with a single click.

A new way to...

CENTRALIZE POLICIES

that ensure license and security risks are managed throughout the software lifecycle.



🟥 **Security-Critical**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Fail, Stage Release: Fail, Release: Fail/Notify, Operate: Warn/Notify

🟥 **Security-High**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Fail, Release: Fail, Operate: Warn

🟧 **Security-Medium**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Warn, Release: Fail, Operate: Warn

🟨 **Security-Low**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Warn, Release: Warn, Operate: Warn

🟥 **License-Banned**
1 Constraint to be evaluated
6 Actions assigned
Procure: Fail, Develop: Fail, Build: Fail, Stage Release: Fail, Release: Fail, Operate: Warn

🟥 **License-Not Distributable**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Warn, Release: Fail, Operate: Warn

🟧 **License-Unknown**
3 Constraints to be evaluated
No actions assigned

🟥 **Architecture-Banned**
2 Constraints to be evaluated
6 Actions assigned
Procure: Fail, Develop: Warn, Build: Fail, Stage Release: Fail, Release: Fail, Operate: Warn

🟨 **Architecture-Deprecated**
2 Constraints to be evaluated
No actions assigned

🟨 **Architecture-Quality**
3 Constraints to be evaluated
No actions assigned

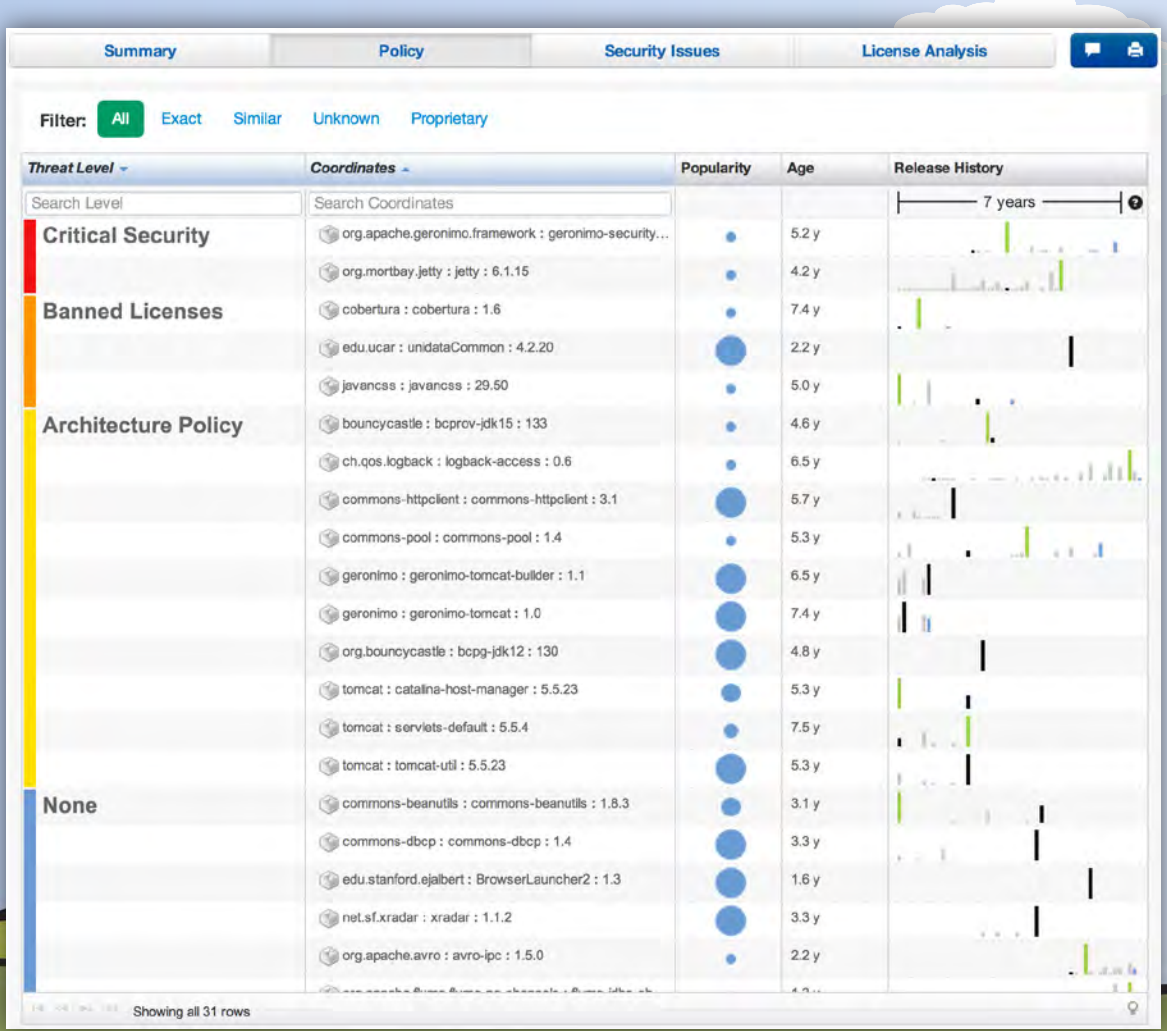
🟥 **Indeterminate Component**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Fail, Release: Fail, Operate: Warn

🟧 **Unknown Component**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Fail, Release: Fail, Operate: Warn

▲ **Security, licensing and architecture policies are easily defined and enforced throughout the software lifecycle.**

A new way to...

PRECISELY IDENTIFY
and track all components
used in your organization,
from consumption to production.



Filter: All Exact Similar Unknown Proprietary

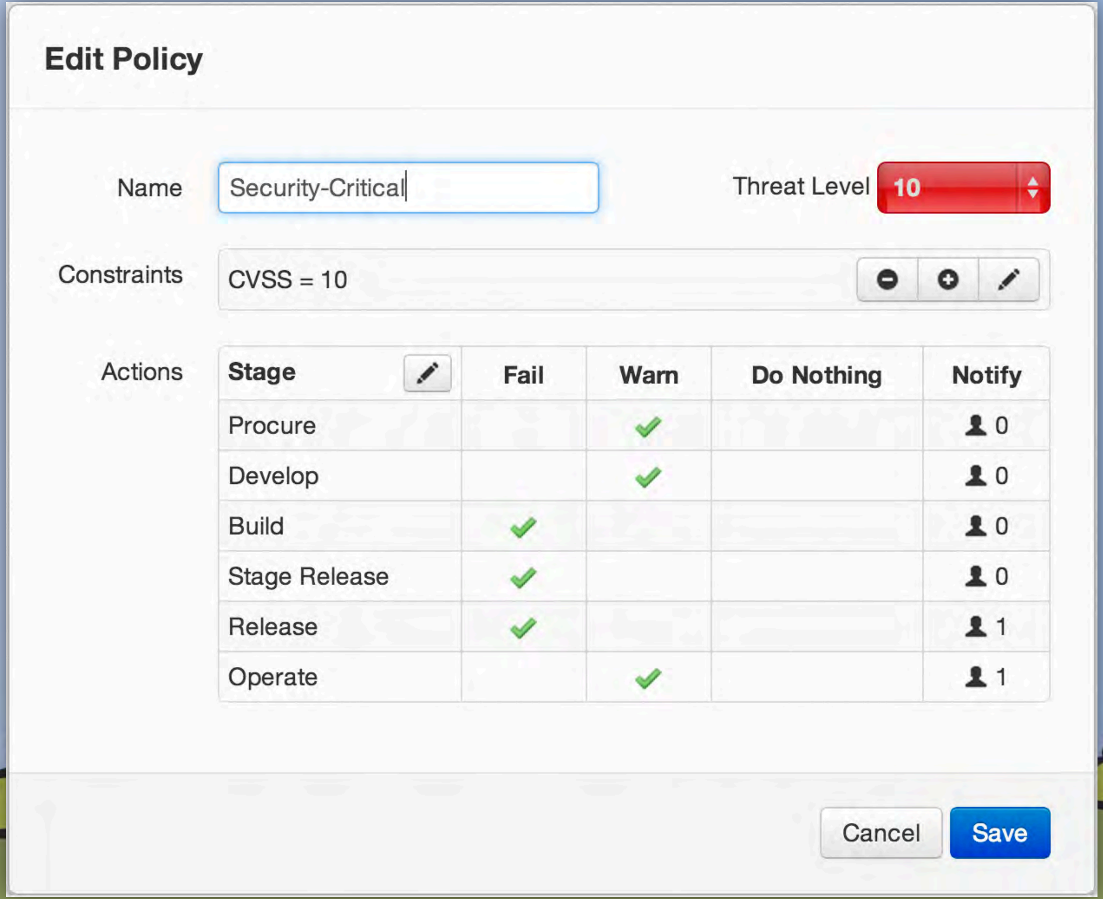
Threat Level	Coordinates	Popularity	Age	Release History
Search Level	Search Coordinates			7 years
Critical Security	org.apache.geronimo.framework : geronimo-security...	•	5.2 y	
	org.mortbay.jetty : jetty : 6.1.15	•	4.2 y	
Banned Licenses	cobertura : cobertura : 1.6	•	7.4 y	
	edu.ucar : unidataCommon : 4.2.20	●	2.2 y	
	javancss : javancss : 29.50	•	5.0 y	
Architecture Policy	bouncycastle : bcprov-jdk15 : 133	•	4.6 y	
	ch.qos.logback : logback-access : 0.6	•	6.5 y	
	commons-httpclient : commons-httpclient : 3.1	●	5.7 y	
	commons-pool : commons-pool : 1.4	•	5.3 y	
	geronimo : geronimo-tomcat-builder : 1.1	●	6.5 y	
	geronimo : geronimo-tomcat : 1.0	●	7.4 y	
	org.bouncycastle : bcpg-jdk12 : 130	●	4.8 y	
	tomcat : catalina-host-manager : 5.5.23	•	5.3 y	
	tomcat : servlets-default : 5.5.4	•	7.5 y	
	tomcat : tomcat-util : 5.5.23	●	5.3 y	
None	commons-beanutils : commons-beanutils : 1.8.3	•	3.1 y	
	commons-dbcp : commons-dbcp : 1.4	●	3.3 y	
	edu.stanford.ejalbert : BrowserLauncher2 : 1.3	●	1.6 y	
	net.sf.xradar : xradar : 1.1.2	●	3.3 y	
	org.apache.avro : avro-ipc : 1.5.0	•	2.2 y	

Showing all 31 rows

▲ Accurate and comprehensive component inventory provides visibility across the software lifecycle.

A new way to...

TRULY ACHIEVE defense-in-depth with enforcement points throughout the software lifecycle.



Edit Policy

Name: Security-Critical

Threat Level: 10

Constraints: CVSS = 10

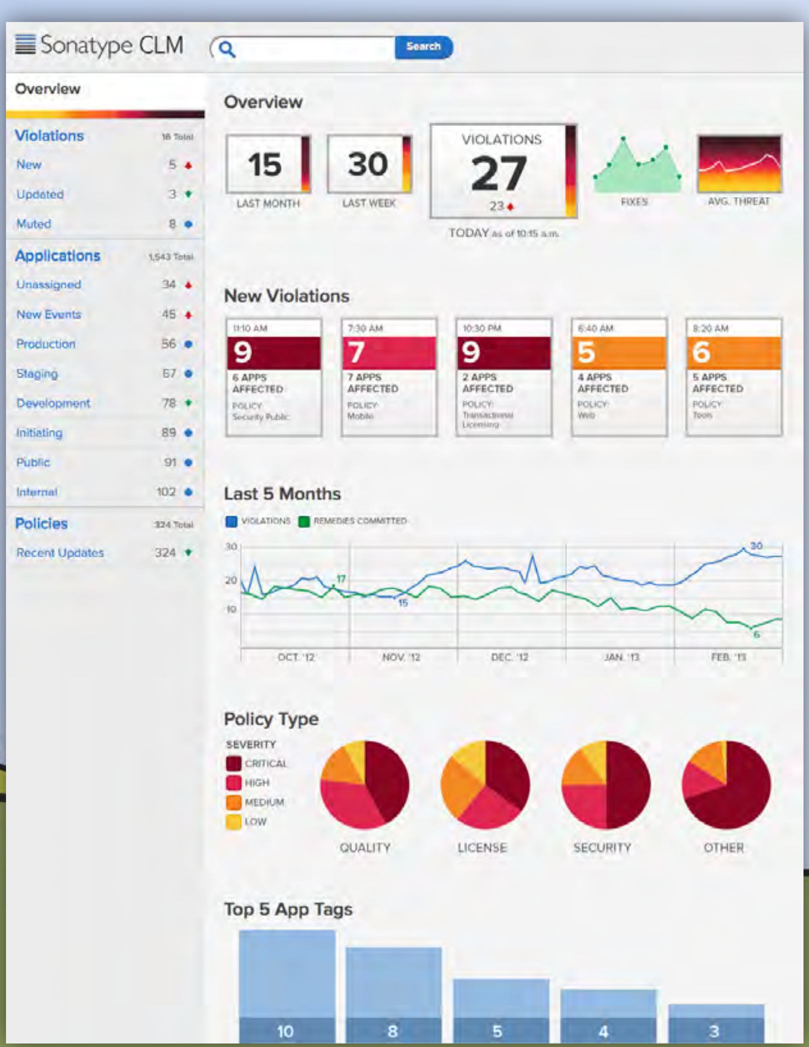
Actions

Stage	Fail	Warn	Do Nothing	Notify
Procure		✓		👤 0
Develop		✓		👤 0
Build	✓			👤 0
Stage Release	✓			👤 0
Release	✓			👤 1
Operate		✓		👤 1

▲ The CLM model for component governance automates policy management and approvals throughout the software lifecycle with enforcement points in the repository, IDE and CI Server.

A new way to...

PROTECT your production applications with proactive alerts for newly discovered vulnerabilities.



Sonatype CLM

Search

Overview

Violations	18 Total
New	5 ▲
Updated	3 ▼
Muted	8 ●
Applications	1,543 Total
Unassigned	34 ▲
New Events	45 ▲
Production	56 ●
Staging	67 ●
Development	78 ▼
Initiating	89 ●
Public	91 ●
Internal	102 ●
Policies	324 Total
Recent Updates	324 ▼

Overview

LAST MONTH	LAST WEEK	VIOLATIONS TODAY as of 10:15 a.m.
15	30	27 23 ▲

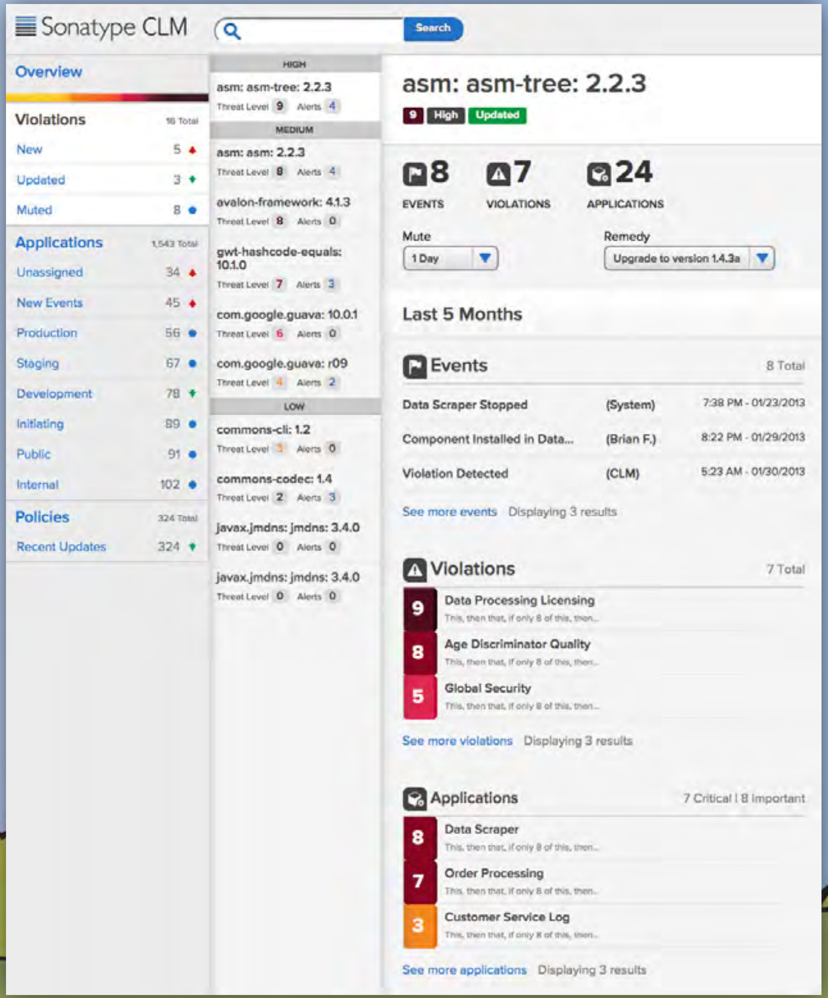
New Violations

11:10 AM	7:30 AM	10:30 PM	6:40 AM	8:20 AM
9	7	9	5	6
6 APPS AFFECTED	7 APPS AFFECTED	2 APPS AFFECTED	4 APPS AFFECTED	5 APPS AFFECTED
POLICY: Security Public	POLICY: Mobile	POLICY: Transactional Licensing	POLICY: Web	POLICY: Tools

▲ Newly discovered threats are continuously reported ensuring trust from design through production.

A new way to...

ASSESS ENTERPRISE RISK and support your compliance and regulatory initiatives.



Sonatype CLM

Overview

Violations	16 Total
New	5 ♦
Updated	3 ♦
Muted	8 ●

Applications	1,543 Total
Unassigned	34 ♦
New Events	45 ♦
Production	56 ●
Staging	67 ●
Development	78 ♦
Initiating	89 ●
Public	91 ●
Internal	102 ●

Policies	324 Total
Recent Updates	324 ♦

HIGH

asm: asm-tree: 2.2.3
Threat Level 9 Alerts 4

MEDIUM

asm: asm: 2.2.3
Threat Level 8 Alerts 4

avalon-framework: 4.1.3
Threat Level 8 Alerts 0

gwt-hashcode-equals: 10.1.0
Threat Level 7 Alerts 3

com.google.guava: 10.0.1
Threat Level 6 Alerts 0

com.google.guava: r09
Threat Level 4 Alerts 2

LOW

commons-cli: 1.2
Threat Level 3 Alerts 0

commons-codec: 1.4
Threat Level 2 Alerts 3

javax.jmdns: jmdns: 3.4.0
Threat Level 0 Alerts 0

javax.jmdns: jmdns: 3.4.0
Threat Level 0 Alerts 0

asm: asm-tree: 2.2.3

9 High Updated

8 EVENTS 7 VIOLATIONS 24 APPLICATIONS

Mute: 1 Day

Remedy: Upgrade to version 1.4.3a

Last 5 Months

Events — 8 Total

Data Scraper Stopped	(System)	7:38 PM - 01/23/2013
Component Installed in Data...	(Brian F.)	8:22 PM - 01/29/2013
Violation Detected	(CLM)	5:23 AM - 01/30/2013

See more events Displaying 3 results

Violations — 7 Total

9 Data Processing Licensing
This, then that, if only 8 of this, then...

8 Age Discriminator Quality
This, then that, if only 8 of this, then...

5 Global Security
This, then that, if only 8 of this, then...

See more violations Displaying 3 results

Applications — 7 Critical | 8 Important

8 Data Scraper
This, then that, if only 8 of this, then...

7 Order Processing
This, then that, if only 8 of this, then...

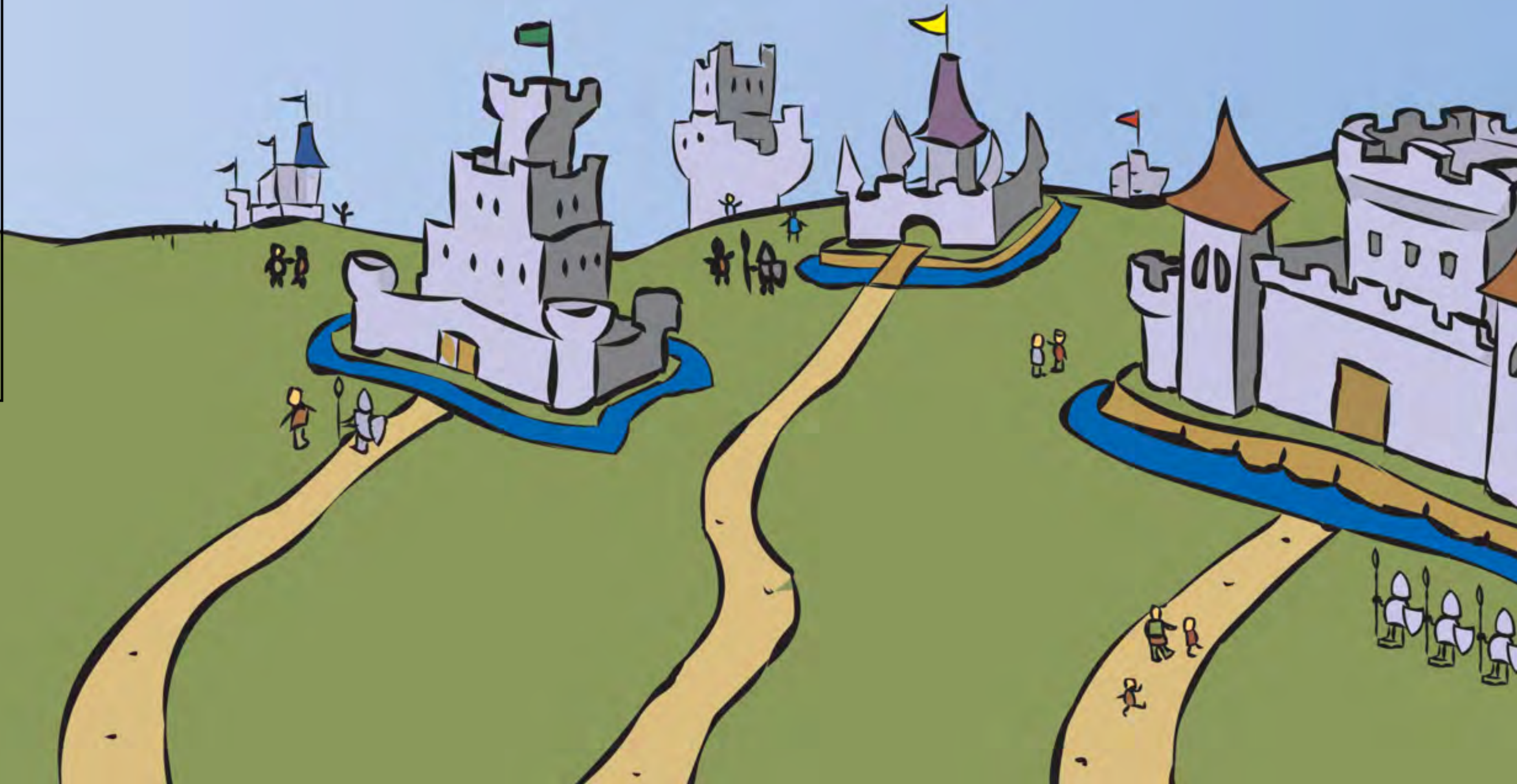
3 Customer Service Log
This, then that, if only 8 of this, then...

See more applications Displaying 3 results

▲ Dashboards and reports provide a complete view of global risk supporting regulatory and compliance initiatives.

And so it came be to...

the people of the kingdom
ushered in a NEW ERA
of application security and
lived in HARMONY
ever more.

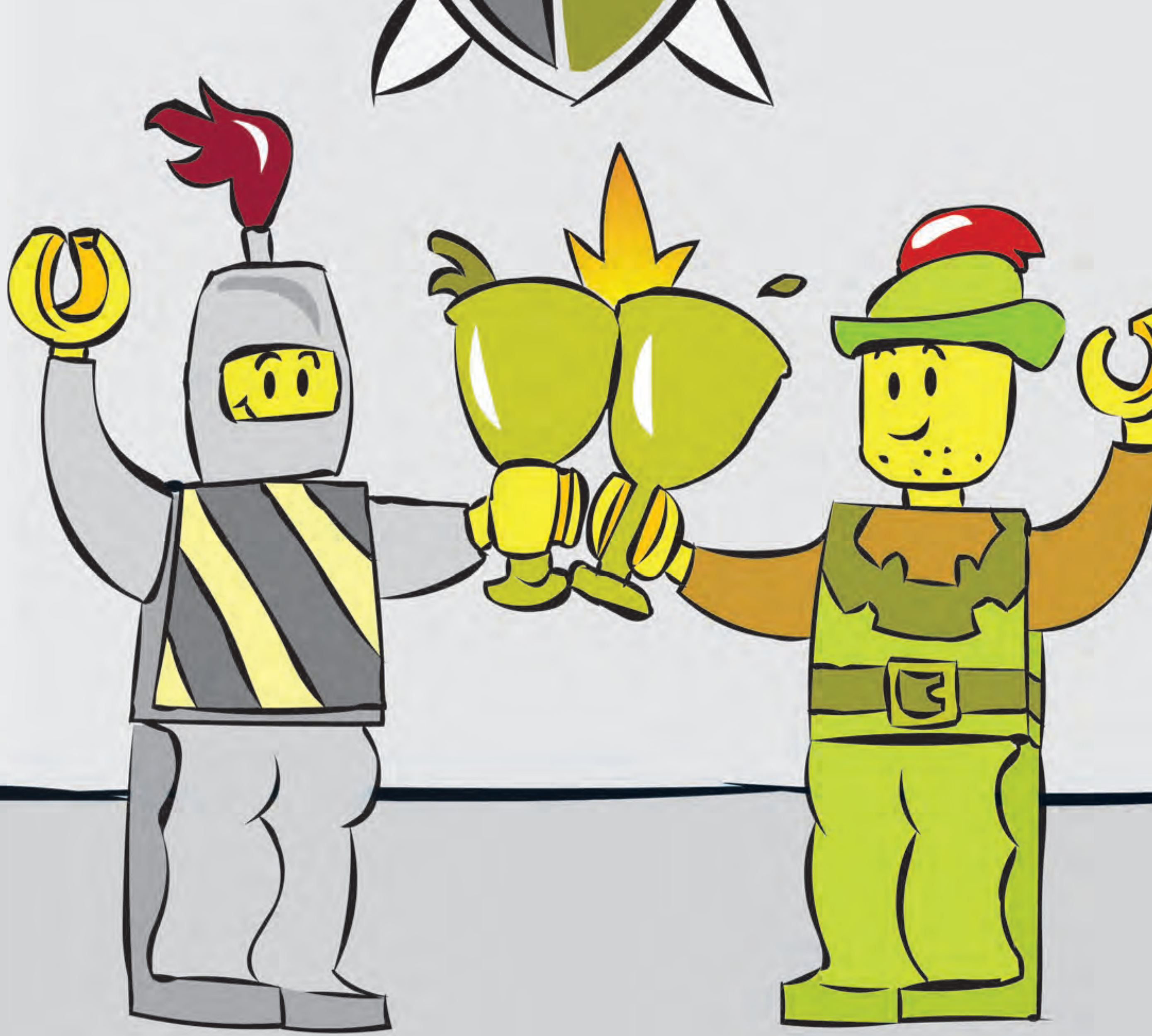


The end.

Revolutionize your approach to software security!

Start with a FREE snapshot of your current application vulnerabilities:
www.sonatype.com/go-fast-be-secure

Or learn more at:
www.sonatype.com/clm/product-tour



Sonatype

12501 Prosperity Drive, Suite 350 · Silver Spring, MD 20904 · 1.877.866.2836 · www.sonatype.com