



# Advanced Security Automation in DevOps

Murray Goldschmidt | Chief Operating Officer

Mar-17

Security, it's all we do. Knowledge, Experience & Trust.

**Sense of Security Pty Ltd**  
ABN 14 098 237 908

**Sydney**  
Level 8, 66 King Street  
Sydney NSW 2000

**Melbourne**  
Level 15, 401 Docklands Drive  
Docklands VIC 3008

Tel. 1300 922 923  
Intl. +61 2 9290 4444  
[www.senseofsecurity.com.au](http://www.senseofsecurity.com.au)

  
@ITSecurityAU

 **WIRED** This Robot Barista Makes a Dang Good Latte SUBSCRIBE 

BUSINESS CULTURE DESIGN **GEAR** SCIENCE SECURITY TRANSPORTATION

DAVID PIERCE GEAR 01.30.17 8:00 AM

## THIS ROBOT BARISTA MAKES A DANG GOOD LATTE



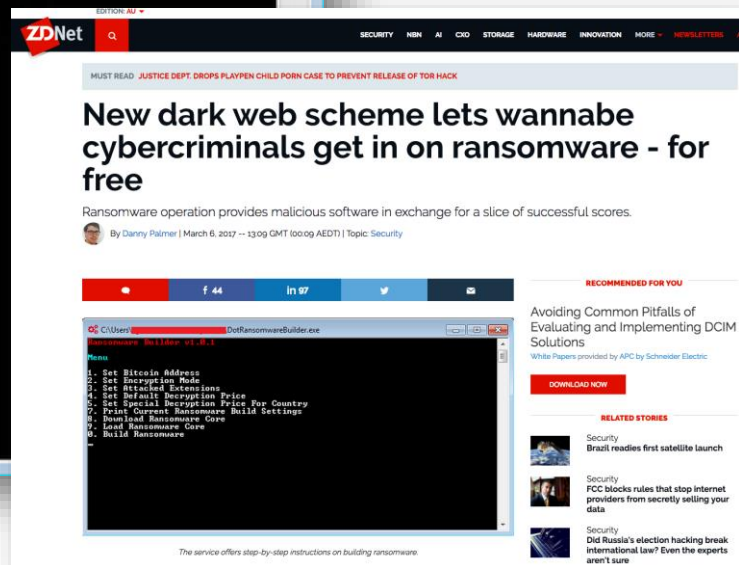
Source: <https://www.wired.com/2017/01/cafe-x-robot-barista/>

# Why does Automation matter?



```

C:\Users\... DotRansomwareBuilder.exe
Ransomware Builder v1.0.1
Menu
1. Set Bitcoin Address
2. Set Encryption Mode
3. Set Attacked Extensions
4. Set Default Decryption Price
5. Set Special Decryption Price For Country
7. Print Current Ransomware Build Settings
8. Download Ransomware Core
9. Load Ransomware Core
0. Build Ransomware
  
```

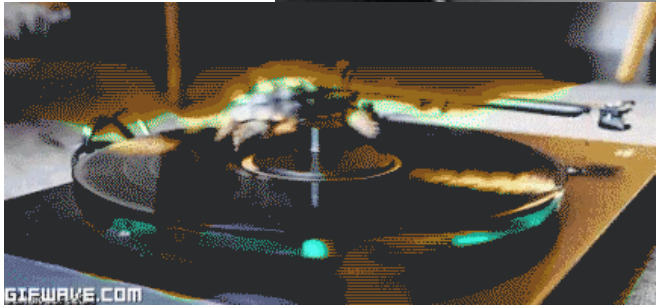
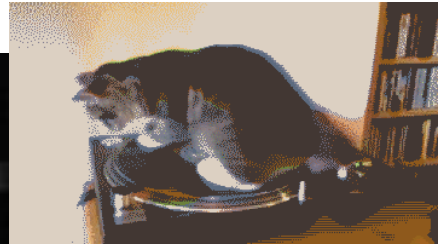


Source: <http://www.zdnet.com/article/new-dark-web-scheme-lets-wannabe-cybercriminals-get-in-on-ransomware-for-free/>

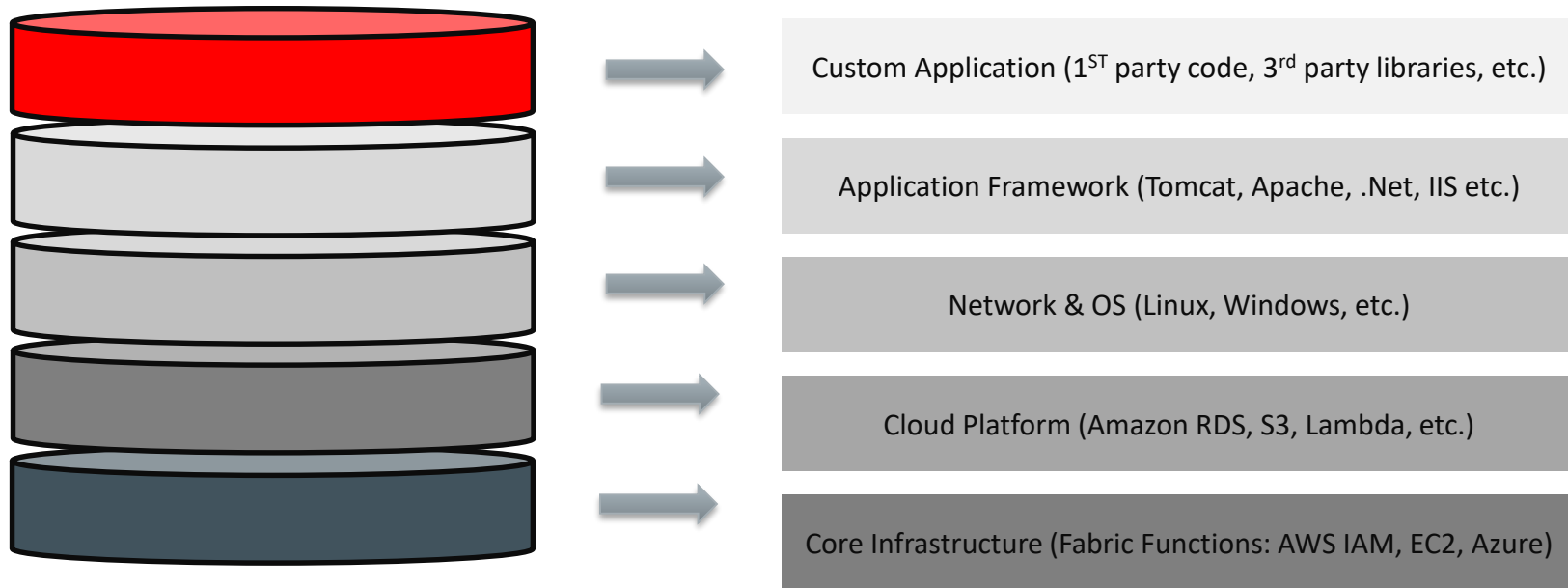


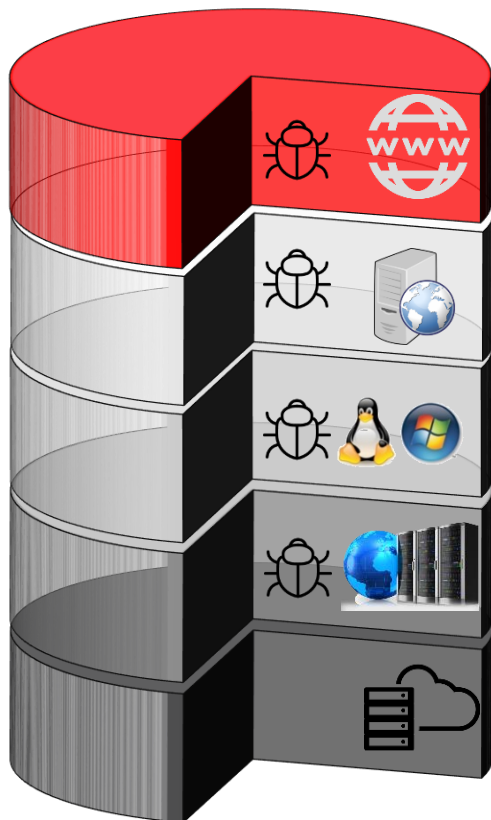












**Custom Application (1<sup>ST</sup> party code, 3<sup>rd</sup> party libraries, etc.)**

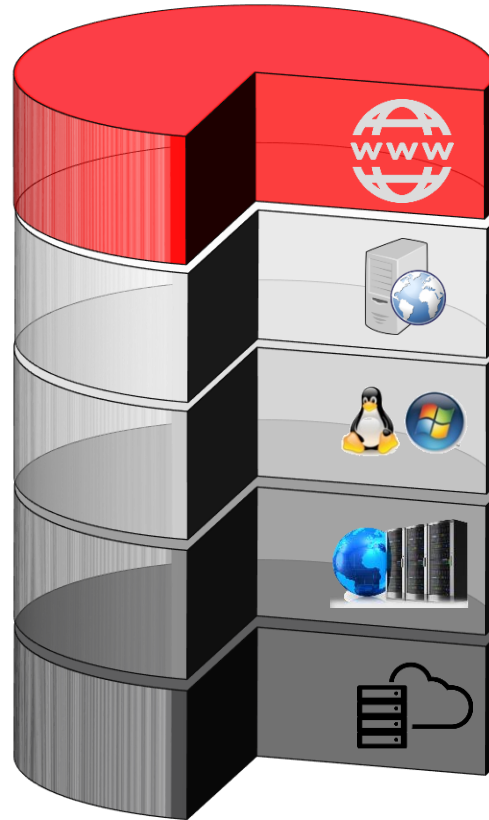
**Application Framework (Tomcat, Nginx, Apache, etc.)**














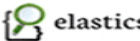





















**Network & OS (Linux, Windows, etc.)**

**Cloud Platform (Amazon RDS, S3, Lambda, etc.)**

**Core Infrastructure (Fabric Functions: AWS IAM, EC2, Azure, etc.)**





|  |   |   |  |   |   |   |
|--|---|---|--|---|---|---|
| <br>Amazon <b>CloudTrail</b><br>Amazon Cloudtrail<br><input checked="" type="checkbox"/> Installed    | <br>Amazon <b>EC2</b><br>Amazon EC2<br><input checked="" type="checkbox"/> Installed | <br>Amazon <b>ElastiCache</b><br>Amazon ElastiCache<br><input checked="" type="checkbox"/> Installed       | <br>Amazon <b>ELB</b><br>Amazon ELB<br><input checked="" type="checkbox"/> Installed         | <br>Amazon <b>Kinesis</b><br>Amazon Kinesis<br><input checked="" type="checkbox"/> Installed | <br>Amazon <b>RDS</b><br>Amazon RDS<br><input checked="" type="checkbox"/> Installed           | <br>Amazon <b>S3</b><br>Amazon S3<br><input checked="" type="checkbox"/> Installed         |
| <br>Amazon <b>Web Services</b><br>Amazon Web Services<br><input checked="" type="checkbox"/> Installed | <br><b>Apache</b><br>Apache<br><input checked="" type="checkbox"/> Installed         | <br>Windows <b>Azure</b><br>Azure<br><input checked="" type="checkbox"/> Installed                         | <br>Atlassian <b>bitbucket</b><br>Bitbucket<br><input checked="" type="checkbox"/> Installed | <br><b>Cassandra</b><br>Cassandra<br><input checked="" type="checkbox"/> Installed           | <br><b>docker</b><br>Docker<br><input checked="" type="checkbox"/> Installed                   | <br><b>elasticsearch</b><br>Elasticsearch<br><input checked="" type="checkbox"/> Installed |
| <br>Microsoft <b>Event Viewer</b><br>Event Viewer<br><input checked="" type="checkbox"/> Installed     | <br><b>Go</b><br>Go Expvar<br><input checked="" type="checkbox"/> Installed          | <br>Google <b>Cloud Platform</b><br>Google Cloud Platform<br><input checked="" type="checkbox"/> Installed | <br>Atlassian <b>HipChat</b><br>Hipchat<br><input checked="" type="checkbox"/> Installed     | <br>Microsoft <b>IIS</b><br>IIS<br><input checked="" type="checkbox"/> Installed             | <br><b>Java</b><br>Java<br><input checked="" type="checkbox"/> Installed                       | <br><b>MySQL</b><br>MySQL<br><input checked="" type="checkbox"/> Installed                 |
| <br><b>NGINX</b><br>Nginx<br><input checked="" type="checkbox"/> Installed                             | <br><b>pagerduty</b><br>Pagerduty<br><input checked="" type="checkbox"/> Installed   | <br><b>PostgreSQL</b><br>Postgres<br><input checked="" type="checkbox"/> Installed                         | <br><b>redis</b><br>Redis<br><input checked="" type="checkbox"/> Installed                   | <br><b>slack</b><br>Slack<br><input checked="" type="checkbox"/> Installed                   | <br>Microsoft <b>SQL Server</b><br>SQL Server<br><input checked="" type="checkbox"/> Installed | <br><b>salesforce</b><br>Desk<br><input checked="" type="checkbox"/> Installed             |
| <br><b>ActiveMQ</b>  | <br><b>Airbrake</b>  | <br><b>btrabbit</b>   | <br><b>cacti</b>  | <br><b>Campfire</b>   | <br><b>Canistrano</b>   | <br><b>chatwork</b>  |

## Infrastructure Security

**Network Firewall**

**Network Monitoring**

**Intrusion Prevention**

**Unified Threat Management**

## Endpoint Security

**Endpoint Protection & Anti-Virus**

## Application Security

**WAF & Application Security**

## Application Security

**WAF & Application Security**

## Vulnerability Assessment

**Vulnerability Assessment**

## IoT Security

## Security

## Transaction Security

## Risk & Compliance

## Mobile Security

## Cloud Security

## Data Security

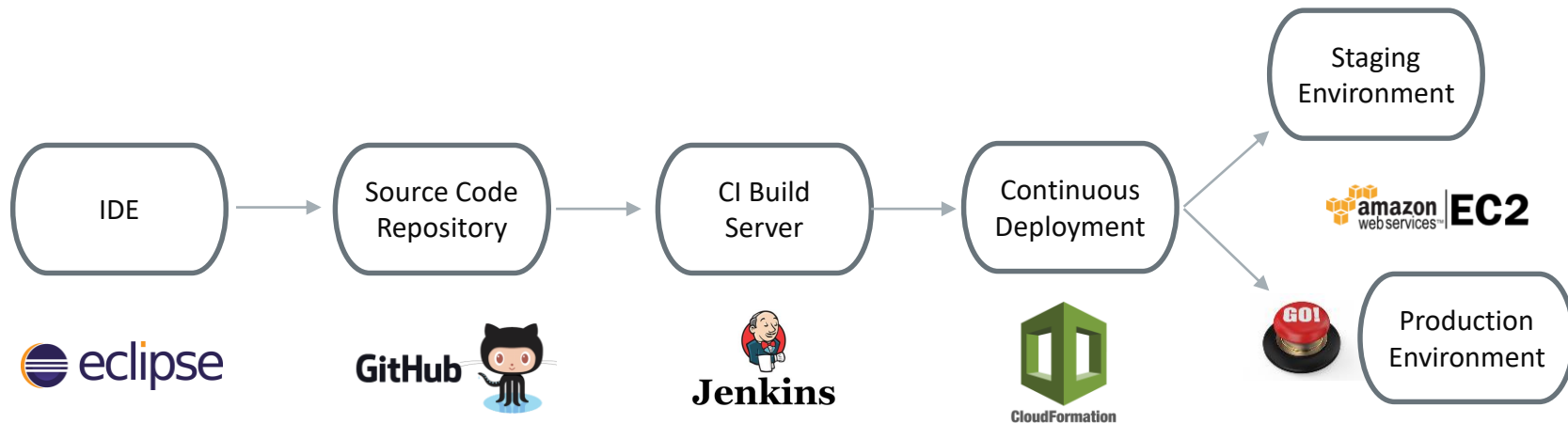
## Data Security

## Cloud Security

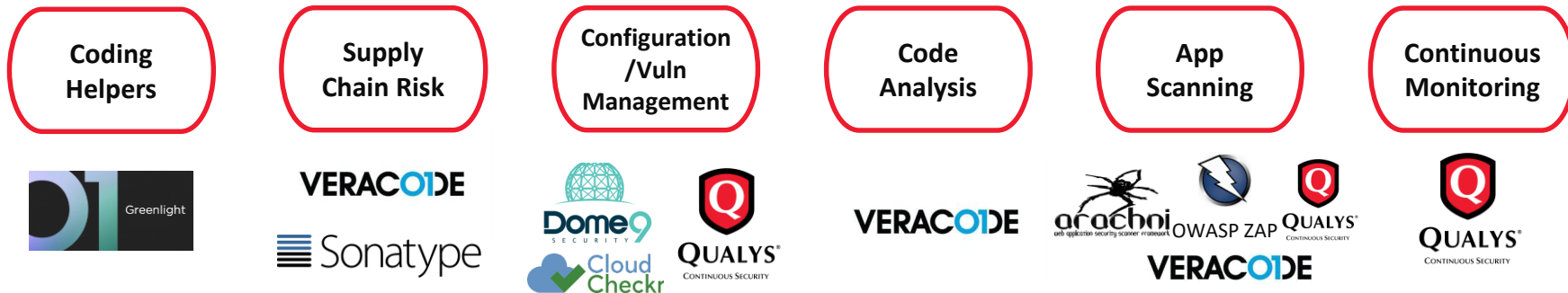
## Assessment

## WAF & Application Security

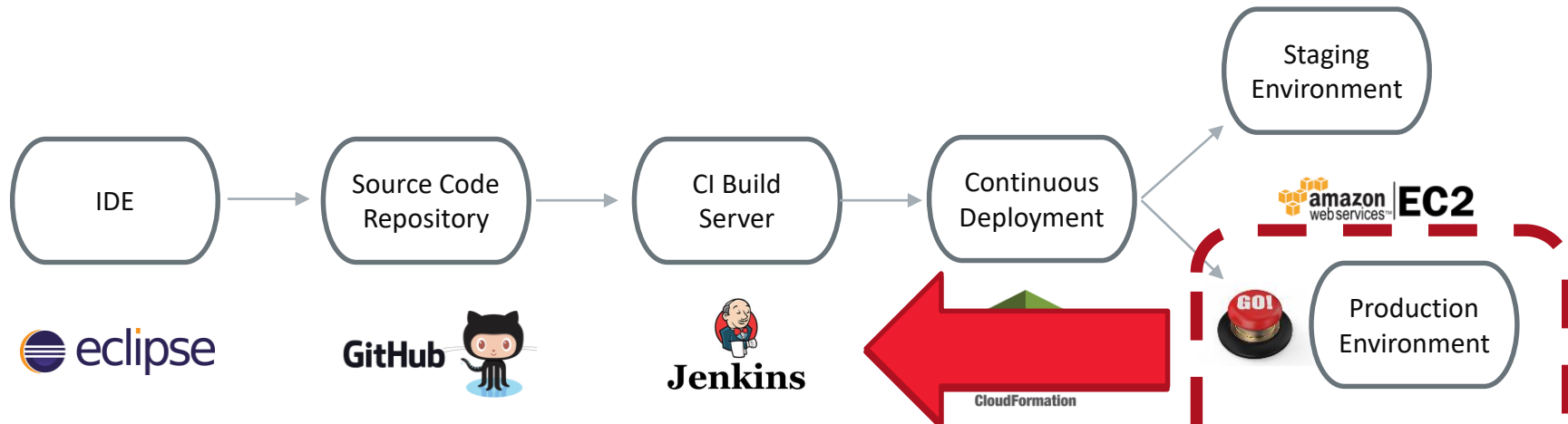




## Advanced Security Automation

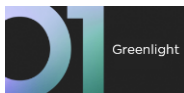


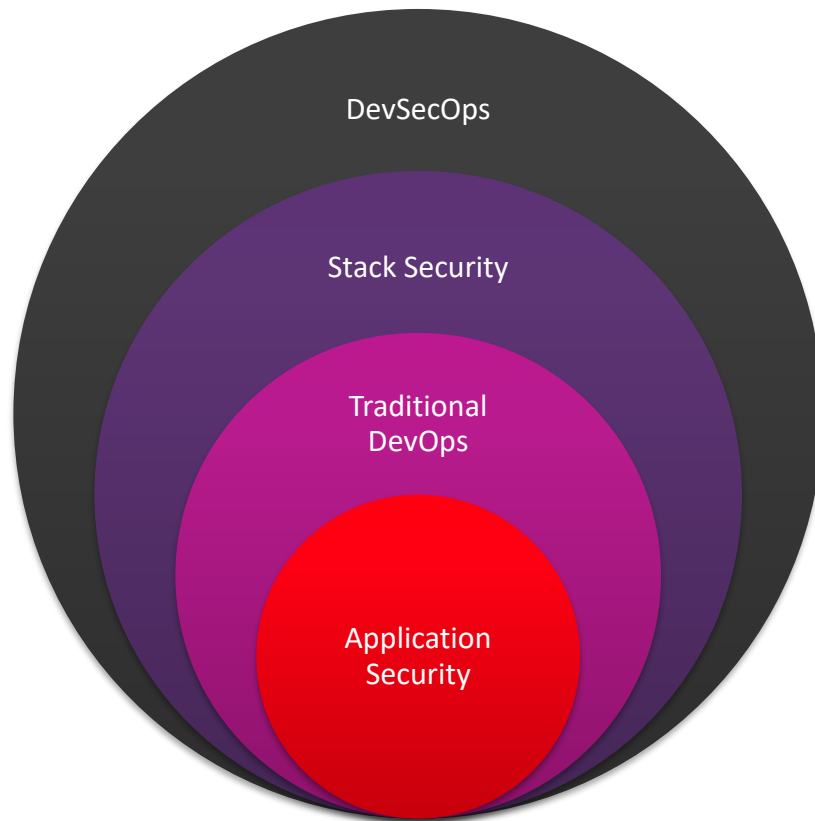




## Advanced Security Automation

- Coding Helpers
- Supply Chain Risk
- Configuration /Vuln Management
- Code Analysis
- App Scanning
- Continuous Monitoring



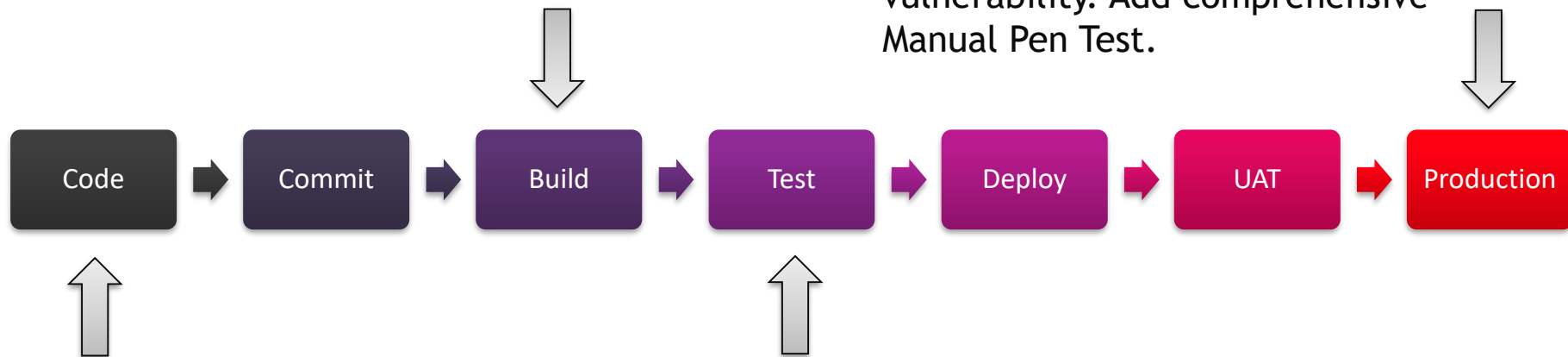




**Per Developer IDE Integration**  
**Per Developer Sandbox Testing**  
**Combined Project Static Analysis**  
**Dynamic Testing**  
**Continuous Monitoring (Public)**

**Layer #2** - Static code analysis triggered by the code commit action identifies the vulnerability - build fails.

**Layer #4** - Continuous Monitoring through Vulnerability Management Program detects the exposed vulnerability. Add comprehensive Manual Pen Test.

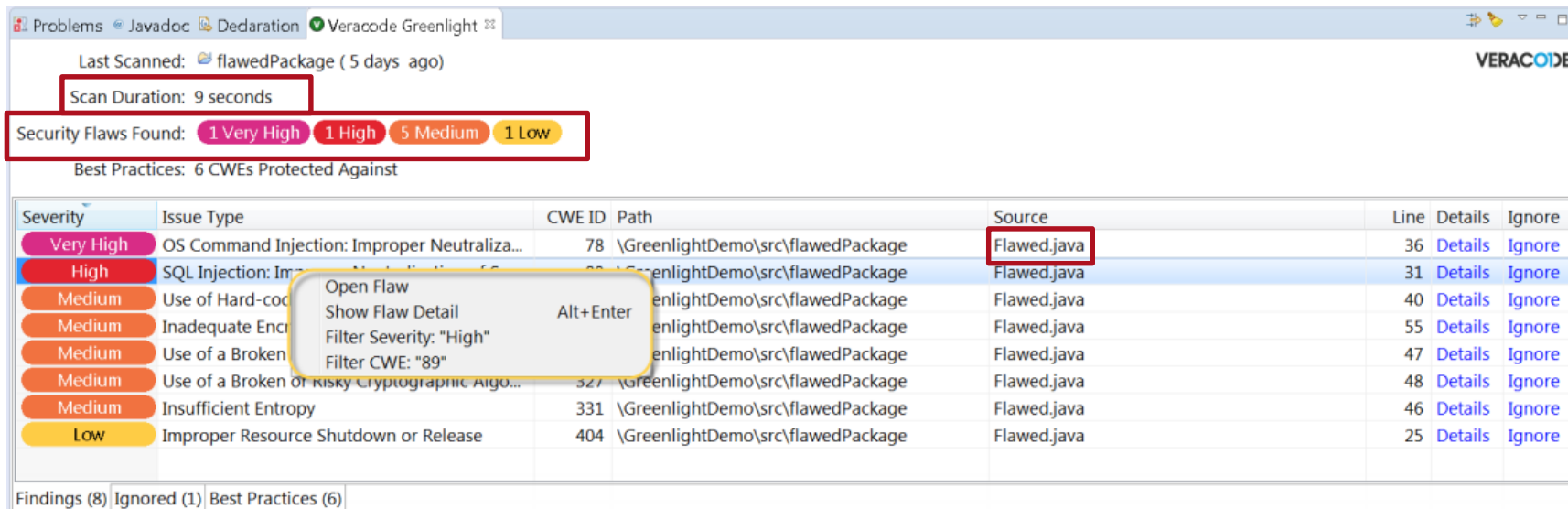


**Layer #1** - The developer has an opportunity to avoid introducing a security vulnerability in their IDE.

**Layer #3** - Automated dynamic scanning of the application detects the same vulnerability if it gets this far.

- Veracode Greenlight

- Eclipse
- Visual Studio



Last Scanned: flawedPackage ( 5 days ago)

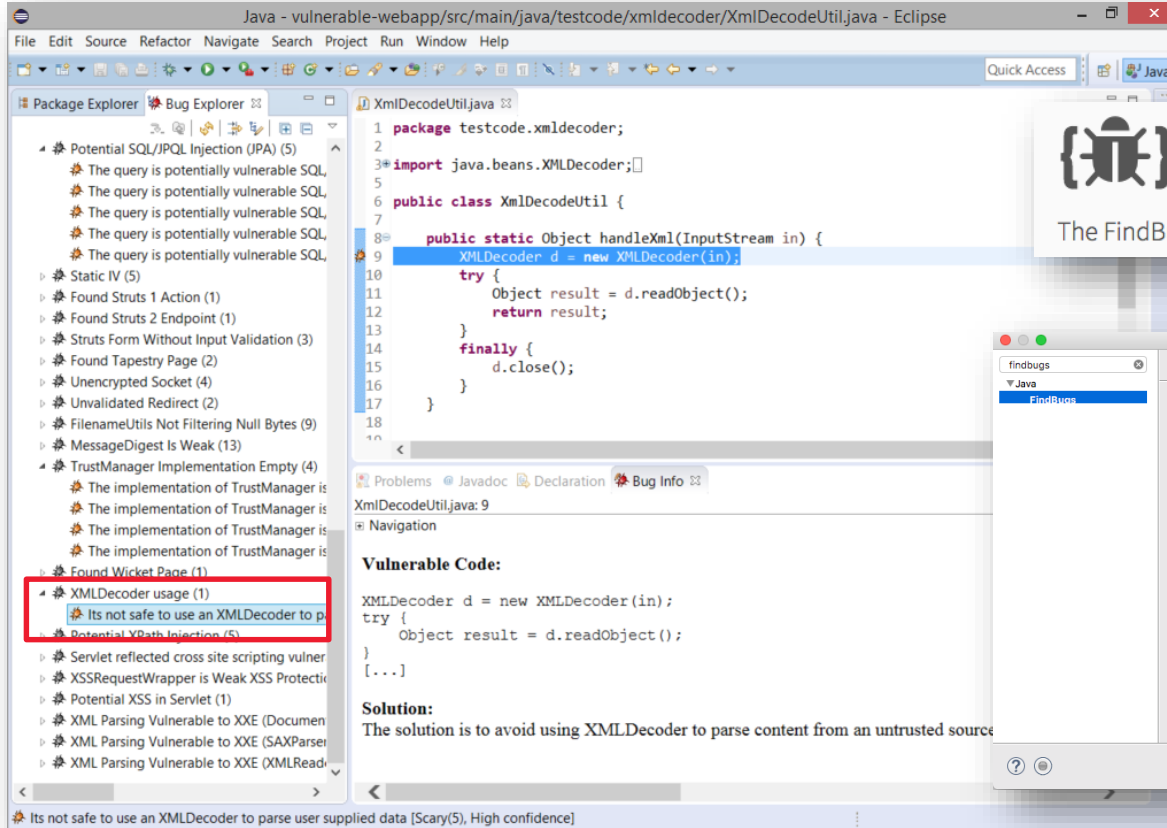
Scan Duration: 9 seconds

Security Flaws Found: 1 Very High 1 High 5 Medium 1 Low

Best Practices: 6 CWEs Protected Against

| Severity  | Issue Type                                     | CWE ID | Path                              | Source      | Line | Details                 | Ignore                 |
|-----------|--|--------|-----------------------------------|-------------|------|-------------------------|------------------------|
| Very High | OS Command Injection: Improper Neutraliza...   | 78     | \GreenlightDemo\src\flawedPackage | Flawed.java | 36   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| High      | SQL Injection: Improper Neutralization of S... | 88     | \GreenlightDemo\src\flawedPackage | Flawed.java | 31   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| Medium    | Use of Hard-coded                              |        | \GreenlightDemo\src\flawedPackage | Flawed.java | 40   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| Medium    | Inadequate Encr...                             |        | \GreenlightDemo\src\flawedPackage | Flawed.java | 55   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| Medium    | Use of a Broken                                |        | \GreenlightDemo\src\flawedPackage | Flawed.java | 47   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| Medium    | Use of a Broken or Risky Cryptographic Algo... | 327    | \GreenlightDemo\src\flawedPackage | Flawed.java | 48   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| Medium    | Insufficient Entropy                           | 331    | \GreenlightDemo\src\flawedPackage | Flawed.java | 46   | <a href="#">Details</a> | <a href="#">Ignore</a> |
| Low       | Improper Resource Shutdown or Release          | 404    | \GreenlightDemo\src\flawedPackage | Flawed.java | 25   | <a href="#">Details</a> | <a href="#">Ignore</a> |

Findings (8) Ignored (1) Best Practices (6)



Java - vulnerable-webapp/src/main/java/testcode/xmldecoder/XmlDecodeUtil.java - Eclipse

```

1 package testcode.xmldecoder;
2
3 import java.beans.XMLDecoder;
4
5 public class XmlDecodeUtil {
6
7
8     public static Object handleXml(InputStream in) {
9         XMLDecoder d = new XMLDecoder(in);
10        try {
11            Object result = d.readObject();
12            return result;
13        }
14        finally {
15            d.close();
16        }
17    }
18
19 }

```

**Problems** | Javadoc | Declaration | Bug Info

XmlDecodeUtil.java: 9

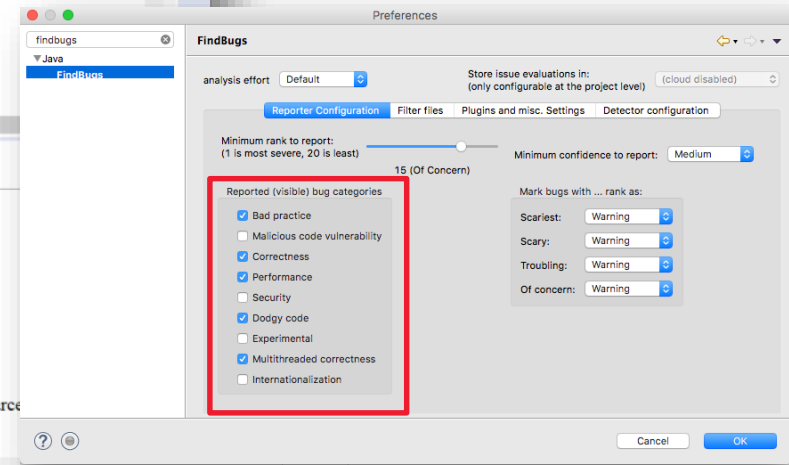
**Vulnerable Code:**

```
XMLDecoder d = new XMLDecoder(in);
try {
    Object result = d.readObject();
}
[...]
```

**Solution:**  
The solution is to avoid using XMLDecoder to parse content from an untrusted source

Its not safe to use an XMLDecoder to parse user supplied data [Scary(5), High confidence]

 **Find Security Bugs**  
The FindBugs plugin for security audits of Java web applications.



Preferences

findbugs

▼ Java

FindBugs

analysis effort: Default

Store issue evaluations in: (only configurable at the project level) (cloud disabled)

Reporter Configuration | Filter files | Plugins and misc. Settings | Detector configuration

Minimum rank to report: (1 is most severe, 20 is least)

15 (Of Concern)

Minimum confidence to report: Medium

Mark bugs with ... rank as:

Scariest: Warning

Scary: Warning

Troubling: Warning

Of concern: Warning

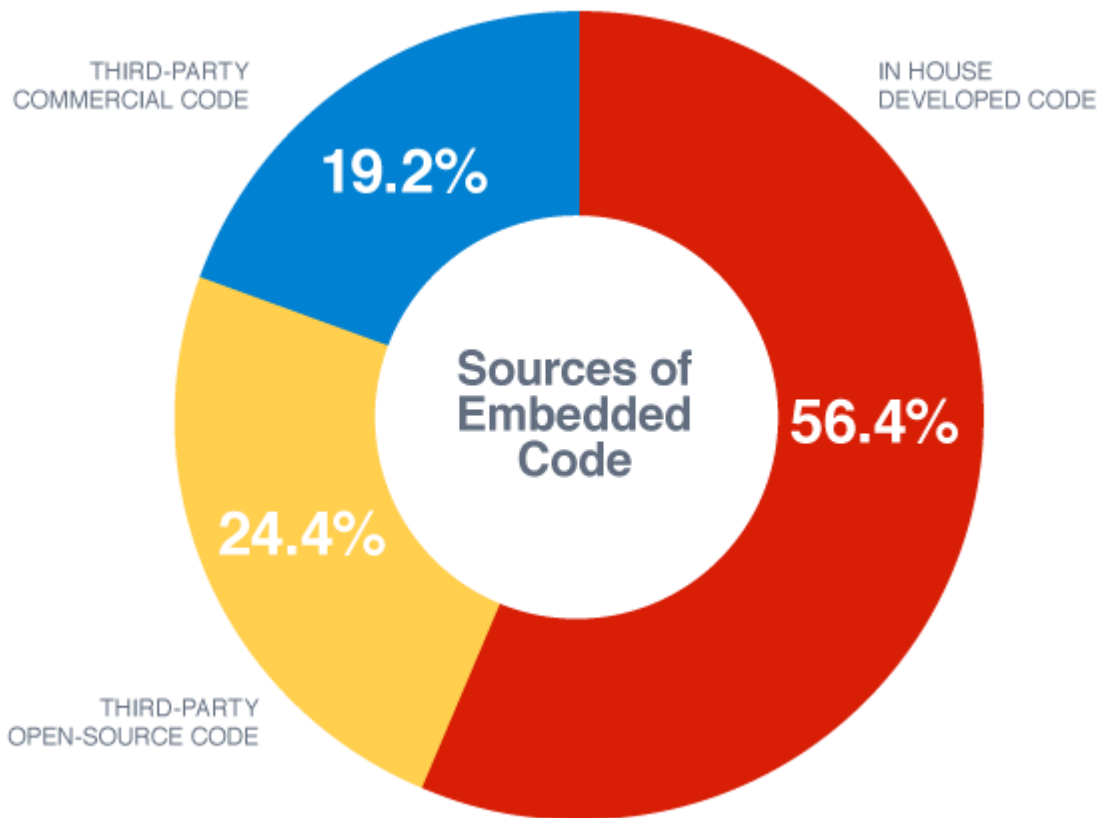
**Reported (visible) bug categories**

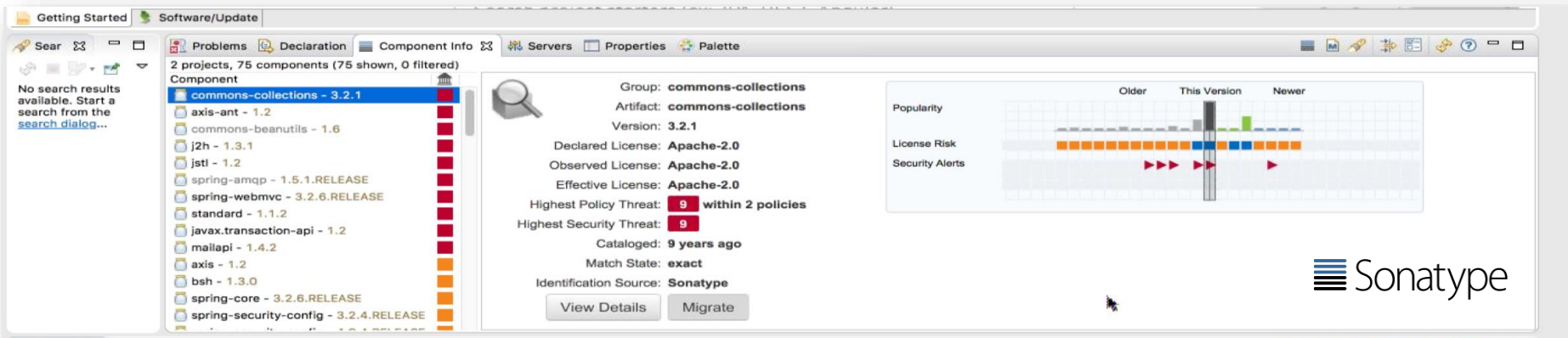
- Bad practice
- Malicious code vulnerability
- Correctness
- Performance
- Security
- Dodgy code
- Experimental
- Multithreaded correctness
- Internationalization

Cancel OK

*44% of applications contain critical vulnerabilities in an open source component.*

*~ Veracode*





- Advanced binary fingerprinting identifies all open source and proprietary components and dependencies.
- Categories: exact, similar or unknown.
- Configure policy actions to automatically prevent applications from moving forward with unwanted or unapproved components.
- Setup automated notifications when unwanted components are being used in your applications.



## APPLICATION

Profile

Metadata

## SANDBOXES

## SCANS

In Progress

Completed

## RESULTS

### Results

Latest

View Report

**Software Composition Analysis**

Flaw Sources

Triage Flaws

Mitigated Flaws

Static Scan

6 Oct 2015 Static

## Third-Party Components

## Vulnerabilities

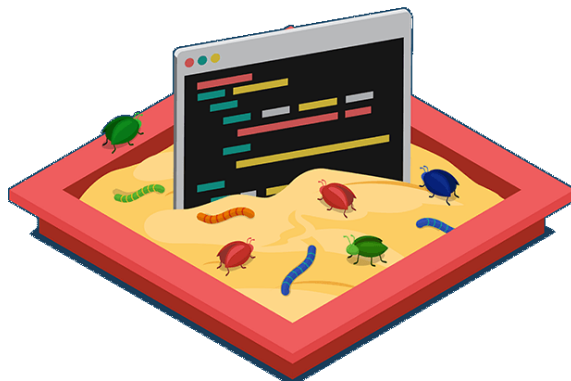
View all components in your application by version, count, or number of known vulnerabilities.

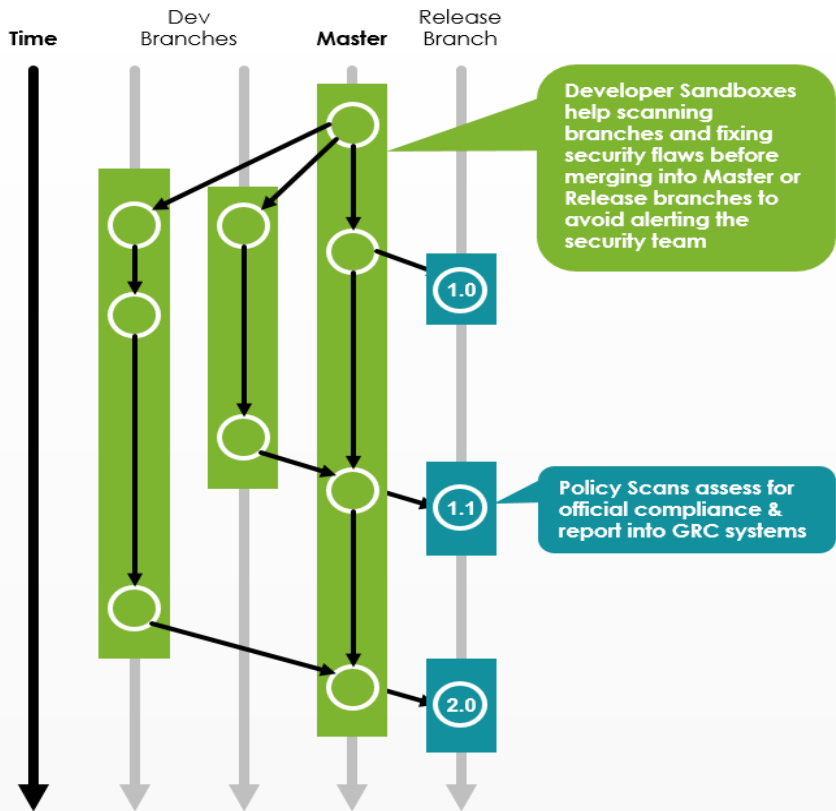
## Third-Party Components

CVE ID

1 of 1

| Policy Violations | Component Filename           | Version | Number of Known Vulnerabilities by Severity |      |        |     |        |      |
|-------------------|------------------------------|---------|---|------|--------|-----|--------|------|
|                   |                              |         | V. High                                     | High | Medium | Low | V. Low | Info |
| ✓                 | commons-beanutils-1.8.0.jar  | 1.8.0   |   |      |        |     |        |      |
| ✓                 | commons-collections-2.1.jar  | 2.1     |   |      |        |     |        |      |
| ✓                 | portal-service.jar           | 6.2.2   |   |      |        |     |        |      |
| ✓                 | portlet-api_2.0_spec-1.0.jar | 1.0     |   |      |        |     |        |      |
| ✓                 | util-taglib.jar              | 6.2.3   |   |      |        |     |        |      |





Applications that used sandbox had an average fix rate of 59%, or a 2x improvement in fix rate

- Veracode
  - Static Code Analysis
  - Dynamic Code Analysis

**VERACODE** Veracode Detailed Report prepared for Sense of Security Pty Ltd - 09-Mar-2017

---

**Veracode Detailed Report**  
**Application Security Report**  
 As of 6 Mar 2017

**Veracode Level: VL2**  
 Rated: 06-Mar-2017

---

Application: testjenkins  
 Target Level: VL3

Business Criticality: Medium  
 Published Rating: A

---

| Scans Included in Report                              | Static Scan            | Dynamic Scan           | Manual Scan            |
|---|------------------------|------------------------|------------------------|
| 5 Mar 2017 Static<br>Score: 92<br>Completed: 06/03/17 | Not Included in Report | Not Included in Report | Not Included in Report |

---

**Executive Summary**

This report contains a summary of the security flaws identified in the application using automated static, automated dynamic and/or manual security analysis techniques. This is useful for understanding the overall security quality of an individual application or for comparisons between applications.

**Application Business Criticality: BC3 (Medium)**  
 Impact: Operational Risk (Low), Financial Loss (Medium)

An application's business criticality is determined by business risk factors such as: reputation damage, financial loss, operational risk, sensitive information disclosure, personal safety, and legal violations. The Veracode Level and required assessment techniques are selected based on the policy assigned to the application.

**Analyses Performed vs. Required**

| Any   | Static                                      | Dynamic                          | Manual                           |
|---|---|----------------------------------|----------------------------------|
| Performed: <input checked="" type="radio"/> | Performed: <input checked="" type="radio"/> | Performed: <input type="radio"/> | Performed: <input type="radio"/> |
| Required: <input type="radio"/>             | Required: <input checked="" type="radio"/>  | Required: <input type="radio"/>  | Required: <input type="radio"/>  |

**Summary of Flaws Found by Severity**



| Severity  | Count |
|-----------|-------|
| Very High | 0     |
| High      | 3     |
| Medium    | 8     |
| Low       | 9     |
| Very Low  | 0     |
| Info      | 0     |

---

**Action Items:**

Veracode recommends the following approaches ranging from the most basic to the strong security measures that a vendor can undertake to increase the overall security level of the application.

**Required Analysis**

- Your policy requires periodic Static Scan. Your next analysis must be completed by 06/06/17. Please submit your application for Static Scan by the deadline and remediate the required detected flaws to conform to your assigned policy.

**Flaws To Fix By Expires Date**

A grace period is specified for any flaw that violates the rules contained in your policy. These include CWE, Rollup Category, Issue Severity, Industry Standards as well as any flaws that prevent an application from achieving a minimum Veracode Level and/or score. To maintain policy compliance you must fix these flaws and resubmit your application for scanning before the grace period expires. The detailed flaw listing will badge the flaws that must be fixed and show the fix by date as well.

- The grace period has expired [06/03/17] for 3 flaws that were found in your Static Scan.

**Flaw Severities**

---

© 2017 Veracode, Inc. Sense of Security Pty Ltd and Veracode Confidential  
 68 Network Drive, Burlington, MA 01803 Tel: +1.338.674.2500 Fax: +1.338.674.2502 URL: http://www.veracode.com

- Remember your DevOps tools too!
- Many don't have out of the box security controls enabled
- E.g. Jenkins default installation -
  - NO access control
  - NO audit of configuration changes.
  - #facepalm



Shodan Developers Book View All...

SHODAN  [Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#)

[Exploits](#) [Maps](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOTAL RESULTS

535

TOP COUNTRIES



Australia 535

TOP CITIES

|             |     |
|-------------|-----|
| Sydney      | 433 |
| Melbourne   | 21  |
| Seven Hills | 6   |
| Research    | 2   |
| Brisbane    | 2   |

TOP SERVICES

|             |     |
|-------------|-----|
| HTTP (8080) | 235 |
| HTTPS       | 150 |
| HTTP        | 110 |



**Amazon.com**  
 Added on 2017-03-14 22:18:23 GMT  
 Australia, Sydney  
[Details](#)

```
HTTP/1.1 403 Forbidden
Date: Tue, 14 Mar 2017 22:14:44 GMT
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID. [blurred] /;HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
X-Hudson: 1.395
```

## Dashboard [Jenkins]



**TPG Internet**  
 Added on 2017-03-14 21:54:56 GMT  
 Australia, Saint Kilda  
[Details](#)

```
HTTP/1.1 200 OK
Date: Tue, 14 Mar 2017 21:53:17 GMT
X-Content-Type-Options: nosniff
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson-Theme: default
Content-Type: text/html;charset=UTF-8
Set-Cookie: JSESSIONID. [blurred]
```

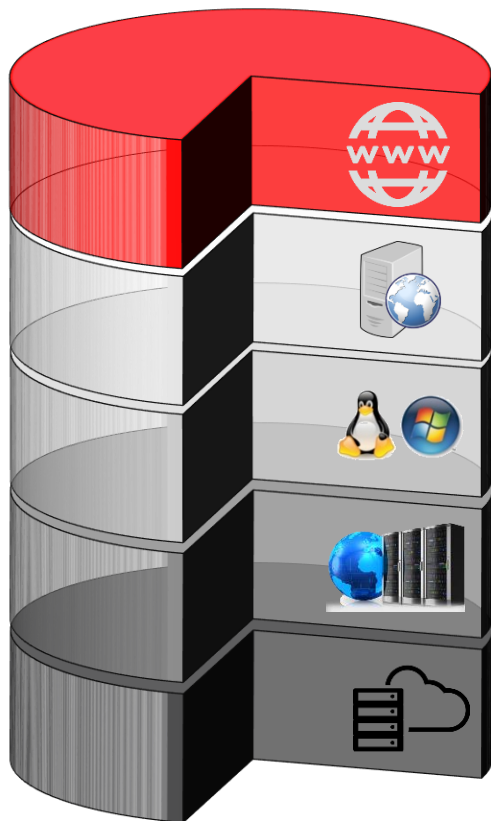


```
HTTP/1.1 403 Forbidden
```

## Preventing a deployment if something fails.

```
Using Scan 1218389  
Checks Failed  
POST BUILD TASK : FAILURE  
END OF POST BUILD TASK: 0  
ESCALATE FAILED POST BUILD TASK  
TO JOB STATUS  
Build step 'Post build task'  
changed build result to FAILURE  
Finished: FAILURE
```





- Vulnerability Management
  - Patch Management
- Configuration Management
  - Hardening of Framework Configurations
  - Hardening of OS & Apps
- Policy Compliance Automated Testing
- Continuous Monitoring - External & Internal



- Automation through Deployment Through Code
- Use Immutable Objects
- Update Source Repo's
- Use Deployment Mgt to focus on StackSec:
  - (a) access control,
  - (b) integrity of configuration
  - (c) auditability of changes.

- Concerns in this layer:
  - Heartbleed
  - Expired SSL Certs
  - Assessed through external continuous scans
  - Unpatched/Vulnerable server apps like Tomcat/Apache
  - Configuration Management issues

Configuration
Monitoring Profiles
Rulesets

Search:

Title: SOSDevSecOp

Ruleset Builder: UpgradedRuleSet
Launch help ✕


Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.


Title\*


Description


This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).


Rule Types


  
Host

  
Vulnerability

  
Certificate

  
Port / Service


  
Software

  
Ticket

▼ Rule 1: Expired or Expiring Certificate Remove ✕

When a certificate is\*  New  Expired

Expiring in 10 days  Expiring in 30 days  Expiring in 90 days

 Add Criteria ▼

> Rule 2: Opened or Changed Port / Service Remove ✕

> Rule 3: New or Updated Host Remove ✕

> Rule 4: Added Software Remove ✕

> Rule 5: New or Active or Reopened Vulnerability Remove ✕

Cancel
Save as..
Save



Alerts Configuration

22 days remaining in trial. Upgrade Now

Alerts

Search...

Profile: (All Monitoring Profiles) Ruleset: (multiple profiles selected) Edit... Start Date: 03/01/2017 End Date: 03/08/2017


Category: **All 5** Host 1 Port 3 Vulnerability 1 Hide graph

Actions (0) 5 alerts


|                          | Alert Message   | Host Impacted | Time                         |
|--------------------------|---|---------------|------------------------------|
| <input type="checkbox"/> | <b>New Open Port</b> : 43345/tcp (ssh)<br>Port found on host ec2-54-...ap-southeast-2.compute.amazonaws.com   | 54            | 08 Mar 2017 10:51AM GMT+1100 |
| <input type="checkbox"/> | <b>New Open Port</b> : 22/tcp (ssh)<br>Port found on host ec2-54-...ap-southeast-2.compute.amazonaws.com  | 54            | 08 Mar 2017 10:51AM GMT+1100 |
| <input type="checkbox"/> | <b>New Open Port</b> : 8080/tcp (http)<br>Port found on host ec2-54-...ap-southeast-2.compute.amazonaws.com   | 54            | 08 Mar 2017 10:51AM GMT+1100 |
| <input type="checkbox"/> | <b>New Vulnerability Found</b> 86728 <span style="color: red;">!!!</span> <span style="color: green;">PCI</span><br>Web Server Uses Plain-Text Form Based Authentication was found on host ec2-54-...ap-southeast-2.compute.amazonaws.com | 54            | 08 Mar 2017 10:51AM GMT+1100 |
| <input type="checkbox"/> | <b>New Host Found</b><br>Host ec2-54-...ap-southeast-2.compute.amazonaws.com with the OS Linux 2.6 was found by the scan ContinuousMonitoring Jenkins   | 54            | 08 Mar 2017 10:51AM GMT+1100 |

- Alert Message


---

-  **New Open Port : 43345/tcp (ssh)**  
Port found on host ec2-██████████.ap-southeast-2.compute.amazonaws.com


---

-  **New Open Port : 22/tcp (ssh)**  
Port found on host ec2-██████████.ap-southeast-2.compute.amazonaws.com


---

-  **New Open Port : 8080/tcp (http)**  
Port found on host ec2-██████████.ap-southeast-2.compute.amazonaws.com

---

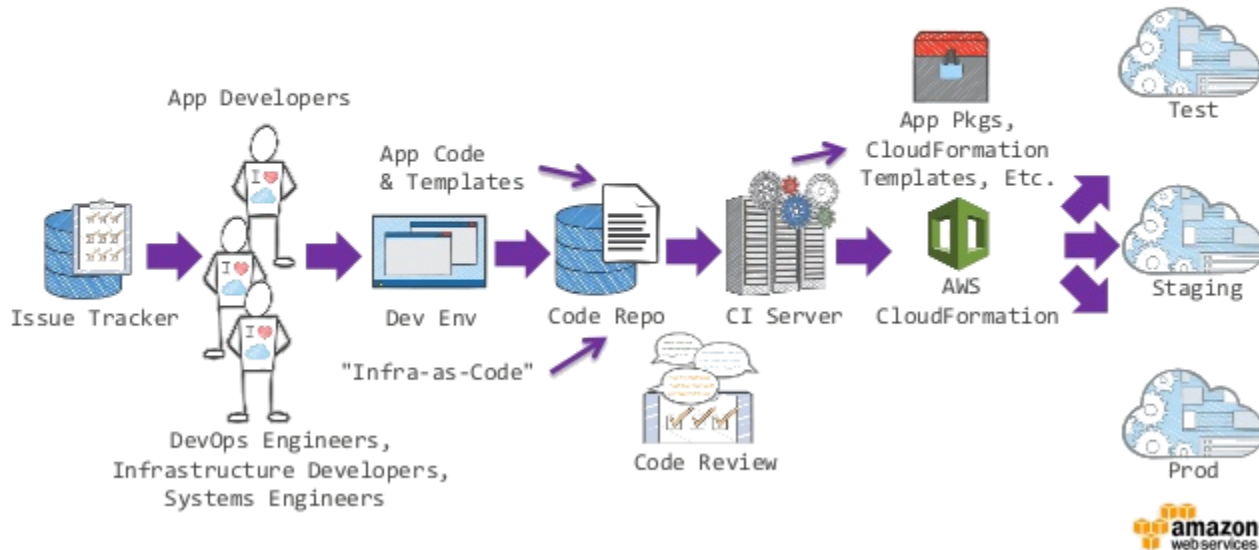
-  **New Vulnerability Found 86728** ■ ■ ■ ■ **PCI**  
Web Server Uses Plain-Text Form Based Authentication was found on host ec2-██████████.ap-southeast-2.compute.amazonaws.com

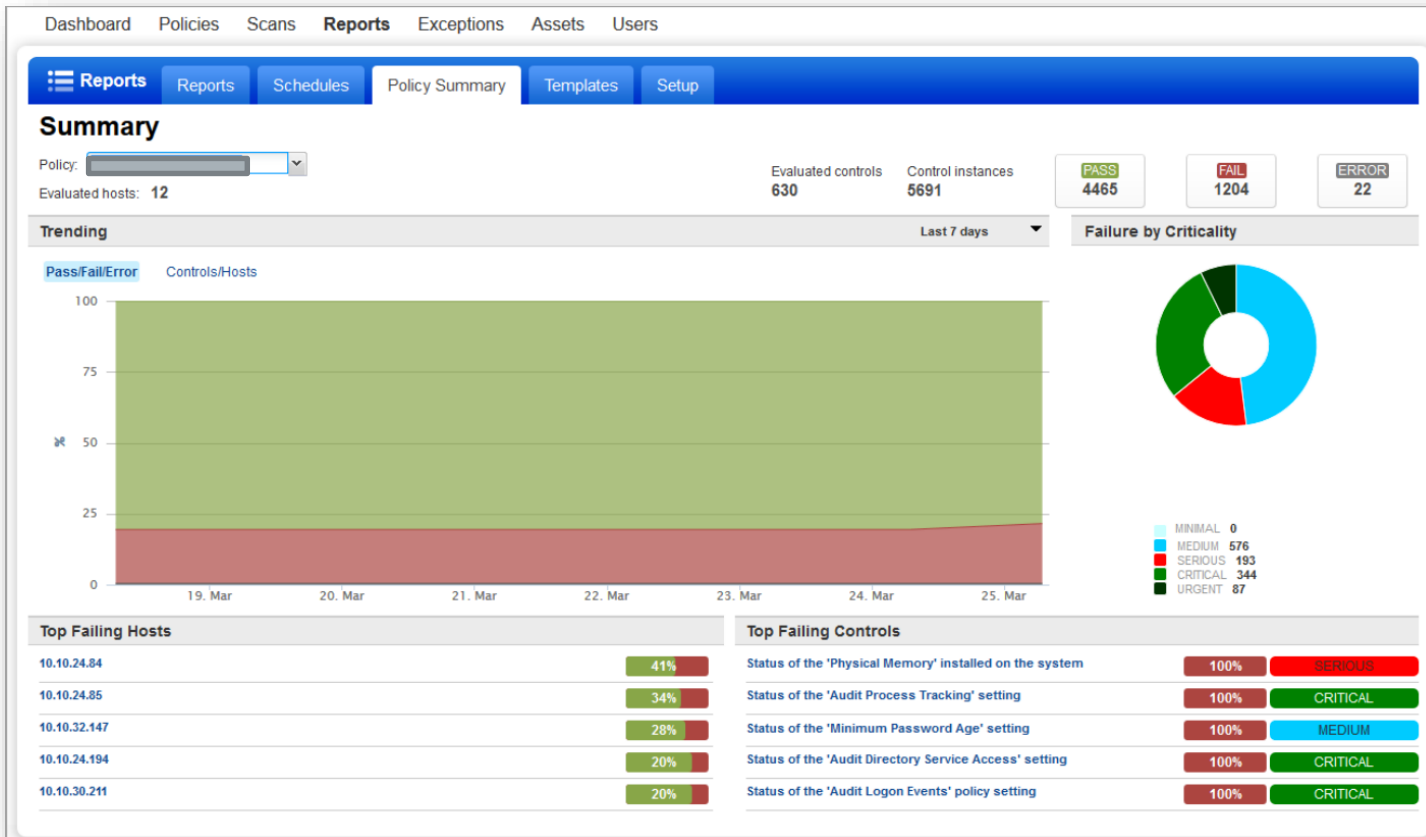
---

-  **New Host Found**  
Host ec2-██████████.ap-southeast-2.compute.amazonaws.com with the OS Linux 2.6 was found by the scan ContinuousMonitoring J

- Coverage across OS & App configs needed
- Combination of FIM & Policy Compliance, Hardening Checks
- SoD for Development, Staging and Prod Environments

## CloudFormation in a CI/CD pipeline





## Preventing a deployment if something fails.

Using Scan 1218389

Checks Failed

**POST BUILD TASK : FAILURE**

**END OF POST BUILD TASK: 0**

ESCALATE FAILED POST BUILD TASK  
TO JOB STATUS

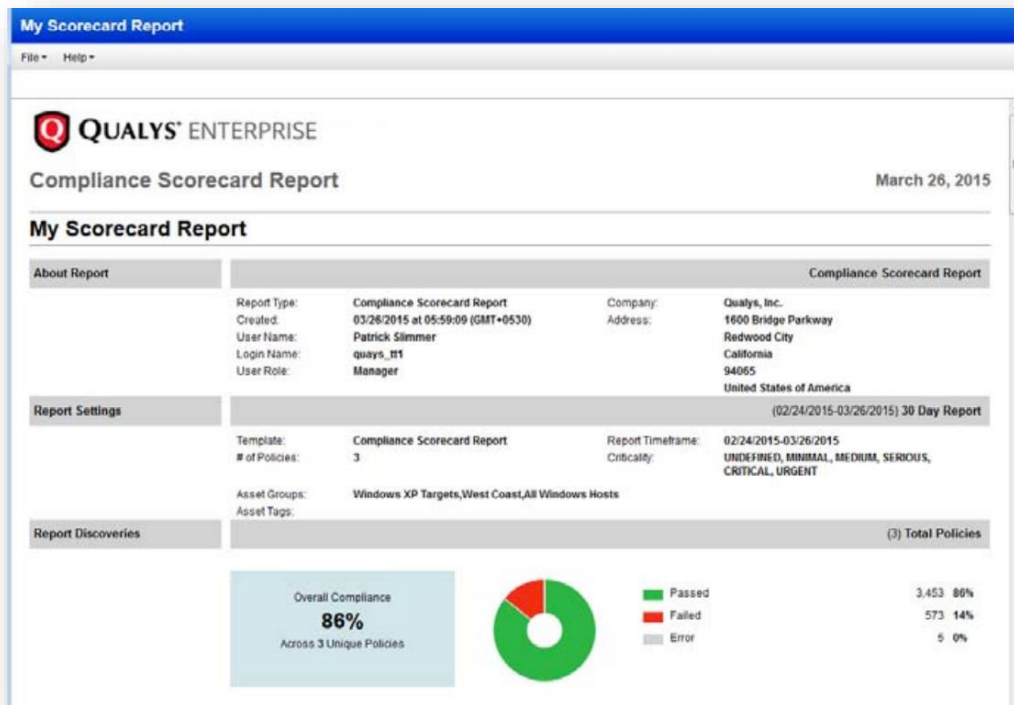
Build step 'Post build task'  
changed build result to FAILURE

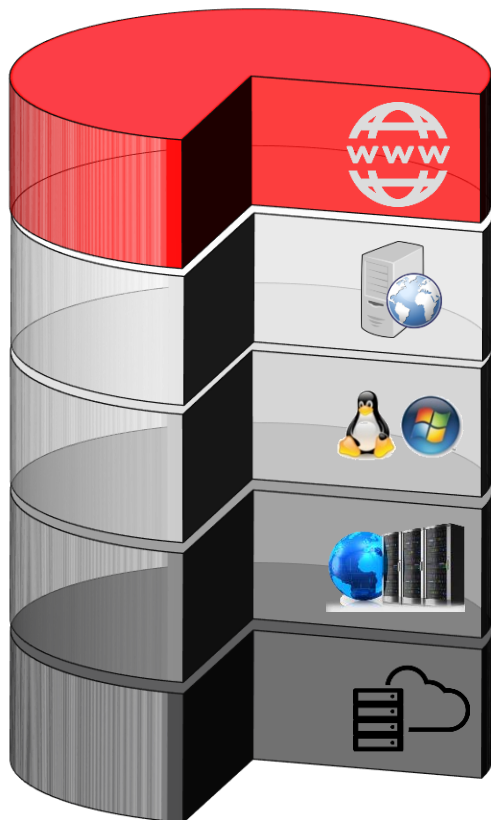
Finished: FAILURE





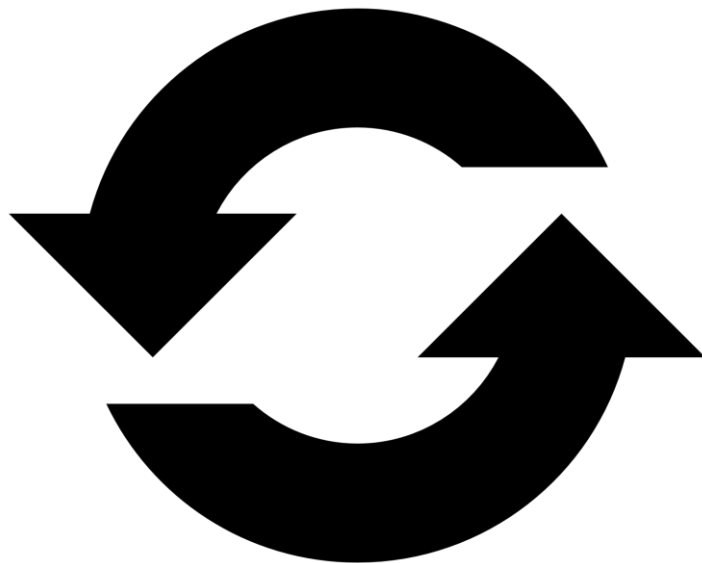
- Ensuring that production environments are verifiably hardened before deployment.
- Can be automated to prevent a production deployment.



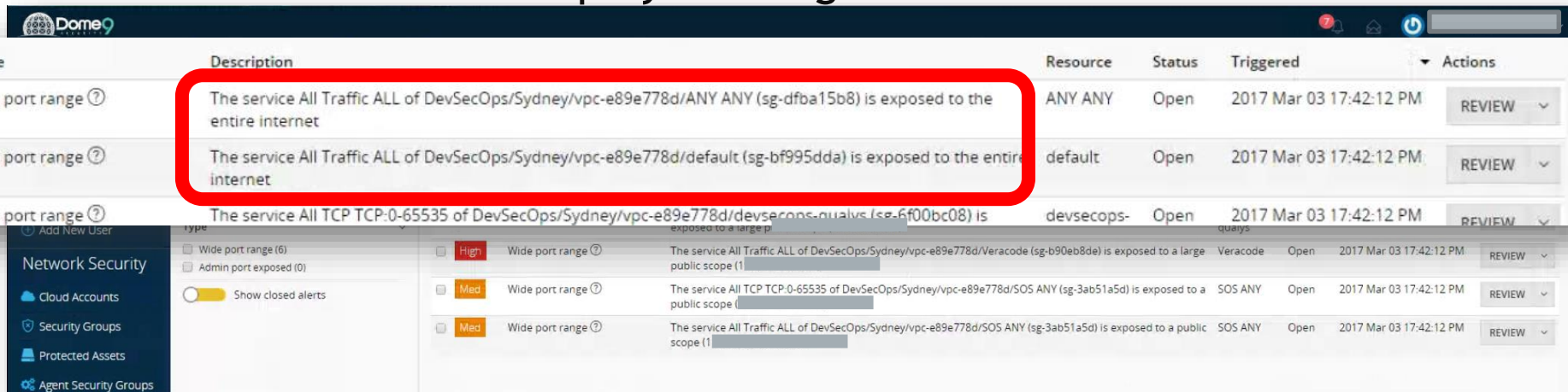


- Cloud Platform Configuration Scanning
- Best Practice & Policy Compliance Tests
- Access & Network Control Auditing (ACLs)
  - Visualisation of Tenancy
  - Self Healing of Defined Controls
  - AWS IAM Config Checks

- Automation to detect any change as it occurs
- Self Healing for API Bind with R/W Permissions
- Cut Your Own Code (Lambda) or use Commercial Products
- Setting policies for Best Practice and/or PCI/ISM etc compliance



- Dome9
  - Detecting configuration issues
  - Automated Fixes thru “Self Healing” of defined Mandatory Controls
  - Extension to API for Deployment Mgt Jenkins



| Name              | Description   | Resource   | Status | Triggered               | Actions |
|-------------------|---|------------|--------|-------------------------|---------|
| Wide port range ? | The service All Traffic ALL of DevSecOps/Sydney/vpc-e89e778d/ANY ANY (sg-dfba15b8) is exposed to the entire internet      | ANY ANY    | Open   | 2017 Mar 03 17:42:12 PM | REVIEW  |
| Wide port range ? | The service All Traffic ALL of DevSecOps/Sydney/vpc-e89e778d/default (sg-bf995dda) is exposed to the entire internet      | default    | Open   | 2017 Mar 03 17:42:12 PM | REVIEW  |
| Wide port range ? | The service All TCP TCP:0-65535 of DevSecOps/Sydney/vpc-e89e778d/devsecops-quals (sg-6f00bc08) is exposed to a large p    | devsecops- | Open   | 2017 Mar 03 17:42:12 PM | REVIEW  |
| Wide port range ? | The service All Traffic ALL of DevSecOps/Sydney/vpc-e89e778d/Veracode (sg-b90eb8de) is exposed to a large public scope (1 | Veracode   | Open   | 2017 Mar 03 17:42:12 PM | REVIEW  |
| Wide port range ? | The service All TCP TCP:0-65535 of DevSecOps/Sydney/vpc-e89e778d/SOS ANY (sg-3ab51a5d) is exposed to a public scope (1    | SOS ANY    | Open   | 2017 Mar 03 17:42:12 PM | REVIEW  |
| Wide port range ? | The service All Traffic ALL of DevSecOps/Sydney/vpc-e89e778d/SOS ANY (sg-3ab51a5d) is exposed to a public scope (1        | SOS ANY    | Open   | 2017 Mar 03 17:42:12 PM | REVIEW  |

Clarity / AWS Prod / us\_west\_2 / vpc-89e113ec / DB servers

VPC: **VPC-89E113EC** View: Security Groups

room: 1:1 Layout: Compact Orientation: Landscape Group IP: No Grouping Hide Empty SG

Show VPC Flow Logs (Private Beta)

External DMZ Partially Open Internal Zone

Grouping the elements based on the exposure level: DMZ vs. Internal

Ranking the elements based on the amount of rejected traffic

DB servers

sg-bde455d8 [Internal]  
sg for RDS, MySQL and Oracle  
Open in Central

Instances (3)  
• DB1  
• DB2  
• DB3

Rules (3)  
• DB Sync - All TCP  
  • DB servers  
• SSH - TCP 22  
• MySQL - TCP 3306  
  • App1 Servers

Sources (2)  
• DB servers  
• App1 Servers

Targets (2)  
• DB servers  
• monitoring

DB servers

Search logs APPLY Show: ALL ACCEPT REJECT Show: since 10/01/2015 12:02:17 PM UTC LOCAL

|                 |       |       |     |     |   |    |                        |        |
|-----------------|-------|-------|-----|-----|---|----|------------------------|--------|
| 50.62.129.199   | 53    | 53120 | DB1 | UDP | 1 | 76 | 10/01/2015 12:07:06 PM | REJECT |
| 111.72.252.91   | 27254 | 8080  | DB1 | TCP | 1 | 40 | 10/01/2015 12:07:06 PM | REJECT |
| 109.234.37.95   | 31894 | 8888  | DB2 | TCP | 1 | 40 | 10/01/2015 12:07:07 PM | REJECT |
| 192.129.223.106 | 58617 | 123   | DB2 | UDP | 1 | 37 | 10/01/2015 12:07:07 PM | REJECT |
| 69.85.183.27    | 123   | 123   |     |     | 1 | 76 | 10/01/2015 12:08:07 PM | ACCEPT |
| DB1             | 123   | 123   |     |     | 1 | 76 | 10/01/2015 12:08:07 PM | ACCEPT |
| DB2             | 123   | 123   |     |     | 1 | 76 | 10/01/2015 12:09:10 PM | ACCEPT |
| 131.107.13.100  | 123   | 123   | DB2 | UDP | 1 | 76 | 10/01/2015 12:09:10 PM | ACCEPT |
| DB2             | 123   | 123   |     |     | 1 | 76 | 10/01/2015 12:09:59 PM | ACCEPT |
| 209.244.0.4     | 123   | 123   | DB2 | UDP | 1 | 76 | 10/01/2015 12:09:59 PM | ACCEPT |

Providing a search console to drill down into specific instance / security group level investigation.

# Visualise Connectivity on Per Instance Basis

D9 Dome9 Clarity / Production / eu\_west\_1 / ec2 / DataBase\_001

Zoom: fit 1:1 + - | Layout: detailed compact | Group IP: auto | Hide Empty SG | print ec2 vpc-4f334a24

**DataBase\_001**

- sg-24d5b653 [internal]
- no description
- [Open in Central](#)
- No Instances**
- Rules (6)**
  - All ICMP
  - All TCP
  - SSH
  - MySQL
  - TCP 5666
  - All UDP
- Upstream (4)**
  - default
  - app-test-00
  - DataBase\_001
  - DataBase\_PROD
- Downstream (2)**
  - DataBase\_001
  - DataBase\_PROD

The diagram illustrates the network path for the 'DataBase\_001' instance. It starts from the 'Internet' and passes through several security groups: 'regression\_test\_00', 'DNS\_SERVER01', 'Dynamic-dns', 'IDS-PROD', 'SG-WEB-PROD', 'Lb\_PROD', 'SG-APP-PROD', 'Quick\_Start\_001', 'quick-launch-00', and 'app-test-00'. The path then goes through 'BLOGS\_001', 'VPN\_GW', and 'default' gateways. Finally, it reaches the 'DataBase\_PROD' and 'DataBase\_001' instances. The 'DataBase\_001' instance is highlighted in yellow in the diagram.



## Verify that all user accounts are active

13 NON COMPLYING 17 RELEVANT 17 TESTED

HIGH

Show more

## Password Policy must require at least one uppercase character

1 NON COMPLYING 1 RELEVANT 1 TESTED

HIGH

Show more

Security Policies Assessment History **PCI-DSS**

### Filters

Showing 40/40 [CLEAR](#)

Search

### Results

- Passed (21)
- Failed (19)

### Severity

- High (31)
- Low (8)
- Medium (1)

### Validation Types

### Results

#### FAILED Unused Security Groups

a security group with no attached protected assets. PCI-DSS Section 1.1.6, 1.1.7 Removing Unused Security Groups is the expected outcome of a 6 months firewall review and proper justification for used rules.

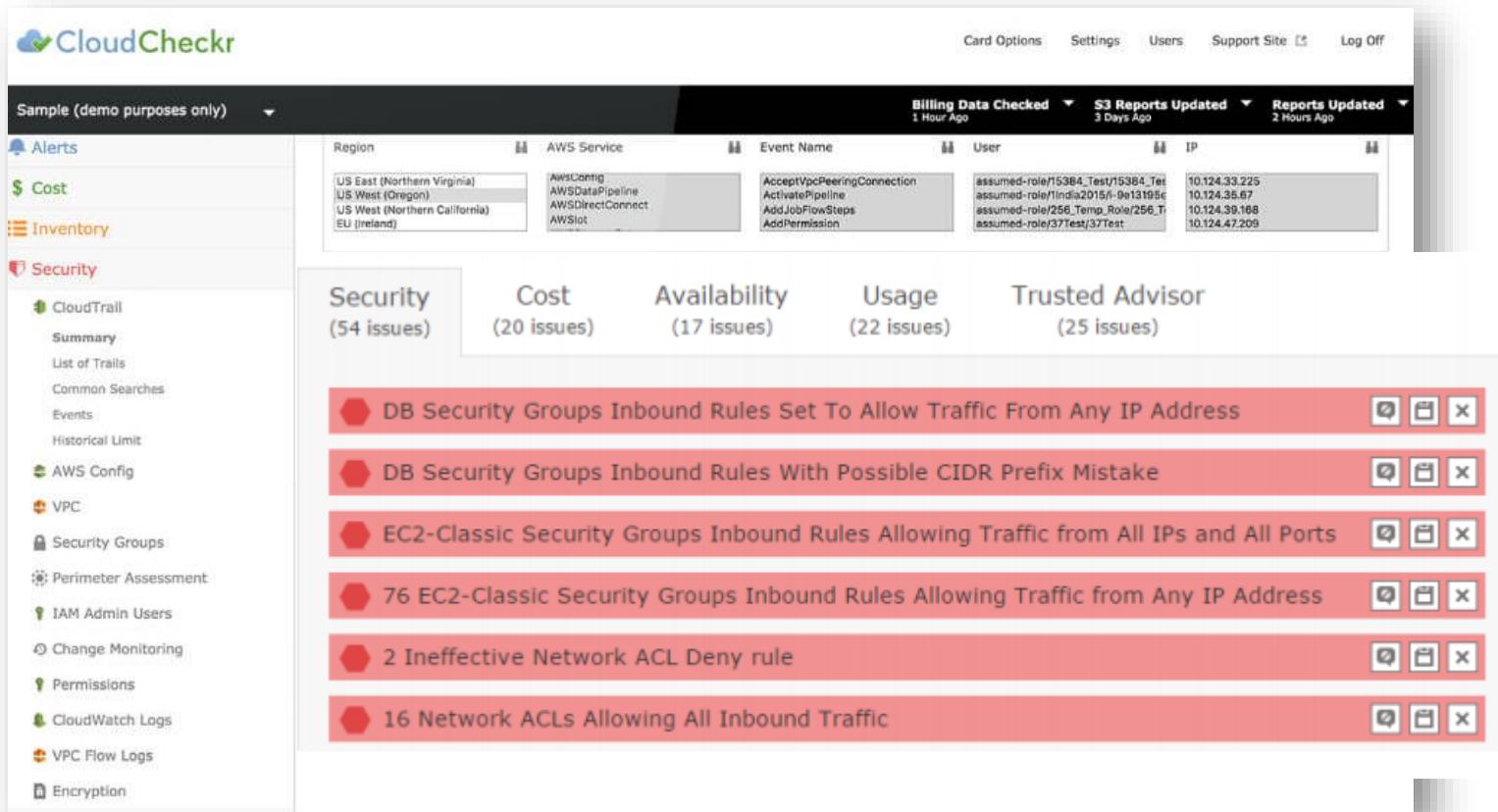
HIGH

Show less

5 NON COMPLYING 14 RELEVANT 15 TESTED

| Id          | Name                    | Region | VPC          | Preview |
|-------------|-------------------------|--------|--------------|---------|
| sg-233c9645 | App2_ApplicationServers | Oregon | vpc-89e113ec | entity  |
| sg-4f3c9629 | App2_DB                 | Oregon | vpc-89e113ec | entity  |
| sg-b50aa0d3 | App2_LoadBalancers      | Oregon | vpc-89e113ec | entity  |
| sg-07359f61 | App2_Web                | Oregon | vpc-89e113ec | entity  |
| sg-78d3a71e | test                    | Oregon | vpc-89e113ec | entity  |





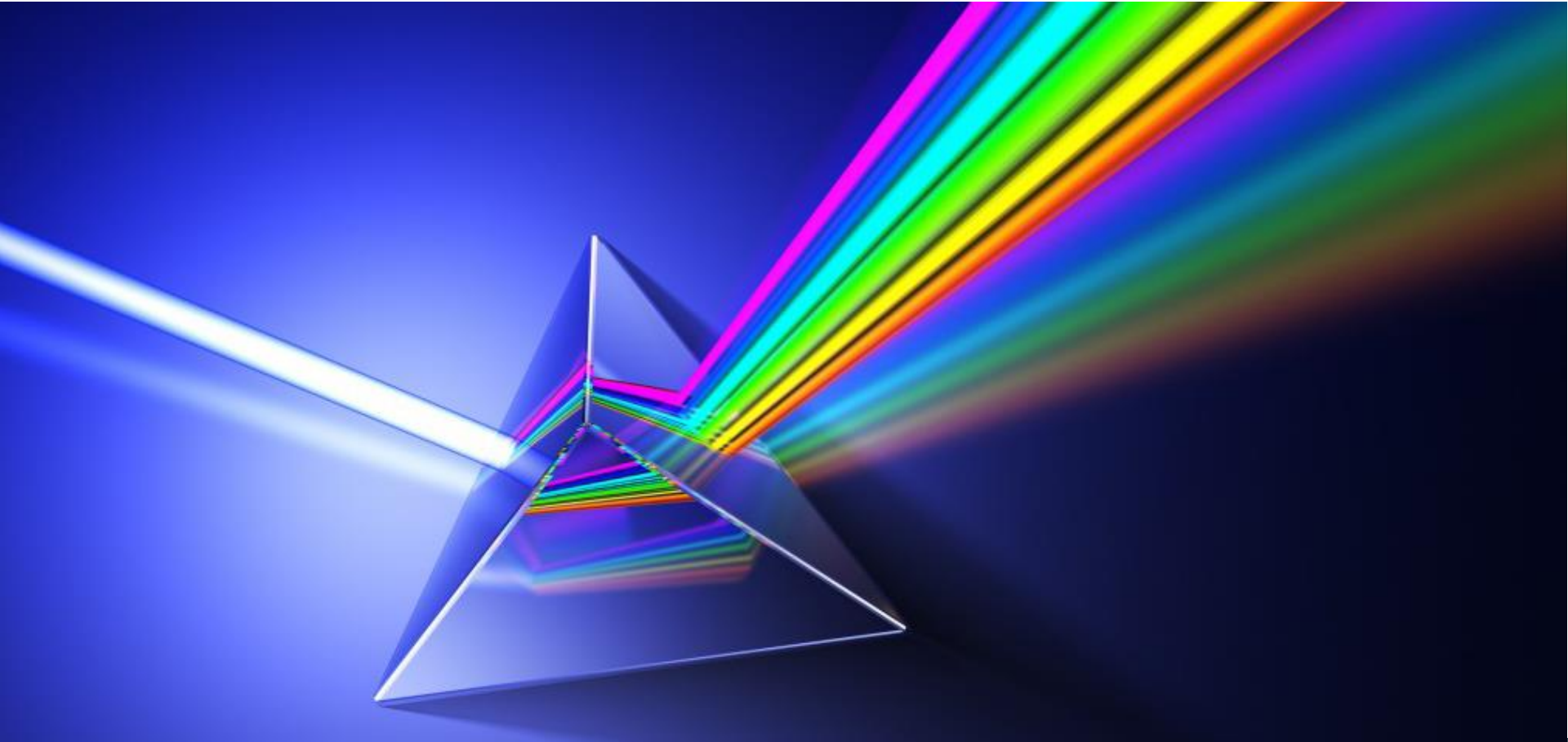
The screenshot shows the CloudCheckr dashboard interface. At the top, there are navigation links for 'Card Options', 'Settings', 'Users', 'Support Site', and 'Log Off'. Below this is a header bar with 'Sample (demo purposes only)' and three status indicators: 'Billing Data Checked 1 Hour Ago', 'S3 Reports Updated 3 Days Ago', and 'Reports Updated 2 Hours Ago'. The main content area is divided into a left sidebar and a main panel. The sidebar contains sections for 'Alerts', 'Cost', 'Inventory', and 'Security'. The 'Security' section is expanded, showing a list of issues. The main panel displays a table of events and a summary of security issues.

| Region                        | AWS Service      | Event Name                 | User                                | IP            |
|-------------------------------|------------------|----------------------------|-------------------------------------|---------------|
| US East (Northern Virginia)   | AwsContig        | AcceptVpcPeeringConnection | assumed-role/15384_Test/15384_Test  | 10.124.33.225 |
| US West (Oregon)              | AWSDataPipeline  | ActivatePipeline           | assumed-role/1India2015/fi-9a13195c | 10.124.35.67  |
| US West (Northern California) | AWSDirectConnect | AddJobFlowSteps            | assumed-role/256_Temp_Role/256_T    | 10.124.39.168 |
| EU (Ireland)                  | AWSIoT           | AddPermission              | assumed-role/37Test/37Test          | 10.124.47.209 |

**Security (54 issues)** | **Cost (20 issues)** | **Availability (17 issues)** | **Usage (22 issues)** | **Trusted Advisor (25 issues)**

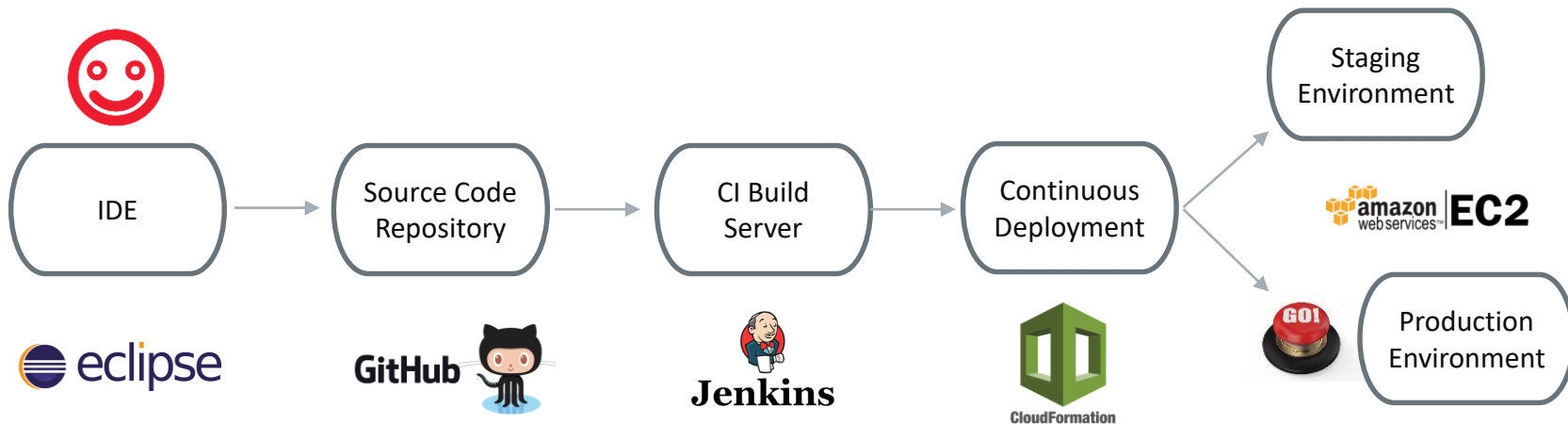
- DB Security Groups Inbound Rules Set To Allow Traffic From Any IP Address
- DB Security Groups Inbound Rules With Possible CIDR Prefix Mistake
- EC2-Classic Security Groups Inbound Rules Allowing Traffic from All IPs and All Ports
- 76 EC2-Classic Security Groups Inbound Rules Allowing Traffic from Any IP Address
- 2 Ineffective Network ACL Deny rule
- 16 Network ACLs Allowing All Inbound Traffic





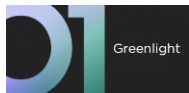
- Automation can dramatically improve security
- Make the application build success rely on the security state of the entire stack environment.
- Don't make it too complicated





## Advanced Security Automation

Coding Helpers



Supply Chain Risk



Code Analysis

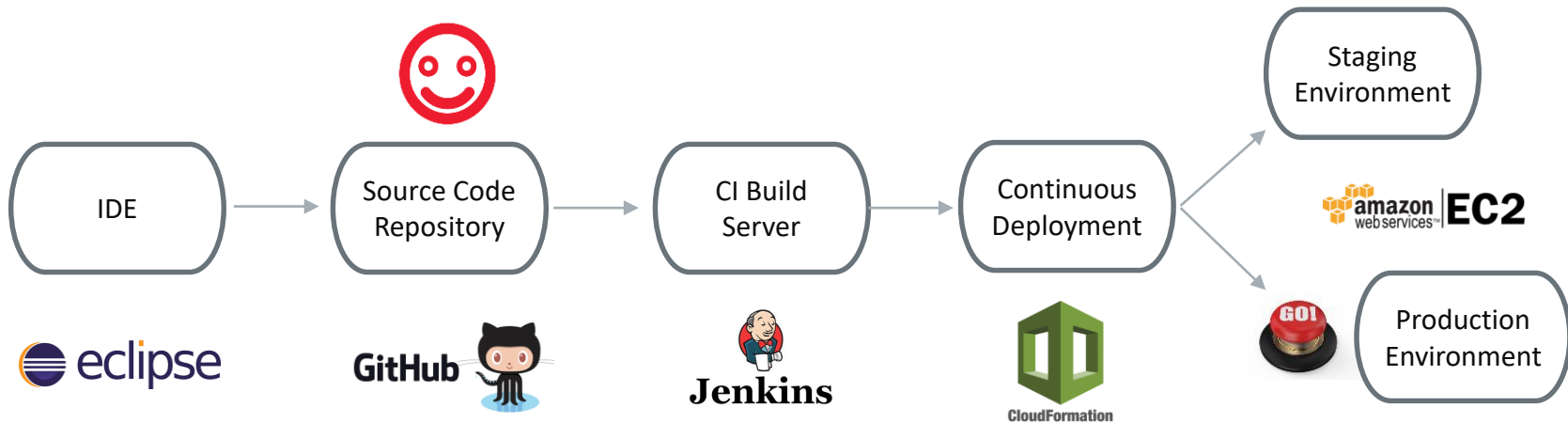


App Scanning



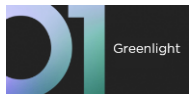
Continuous Monitoring





## Advanced Security Automation

Coding Helpers



Supply Chain Risk



Code Analysis

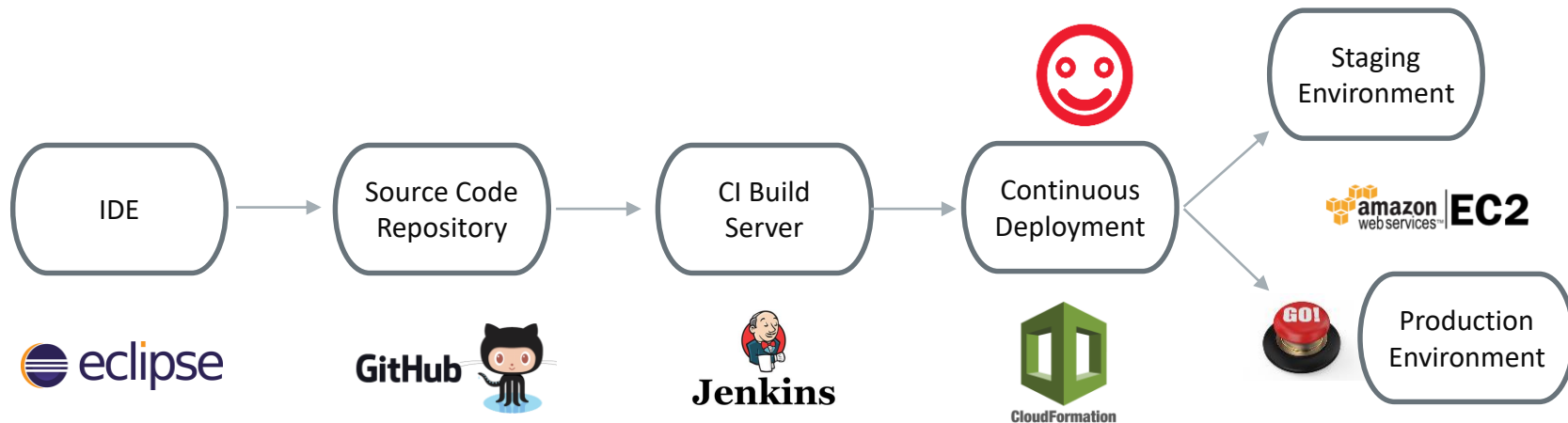


App Scanning



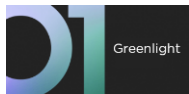
Continuous Monitoring





## Advanced Security Automation

Coding Helpers



Supply Chain Risk



Code Analysis

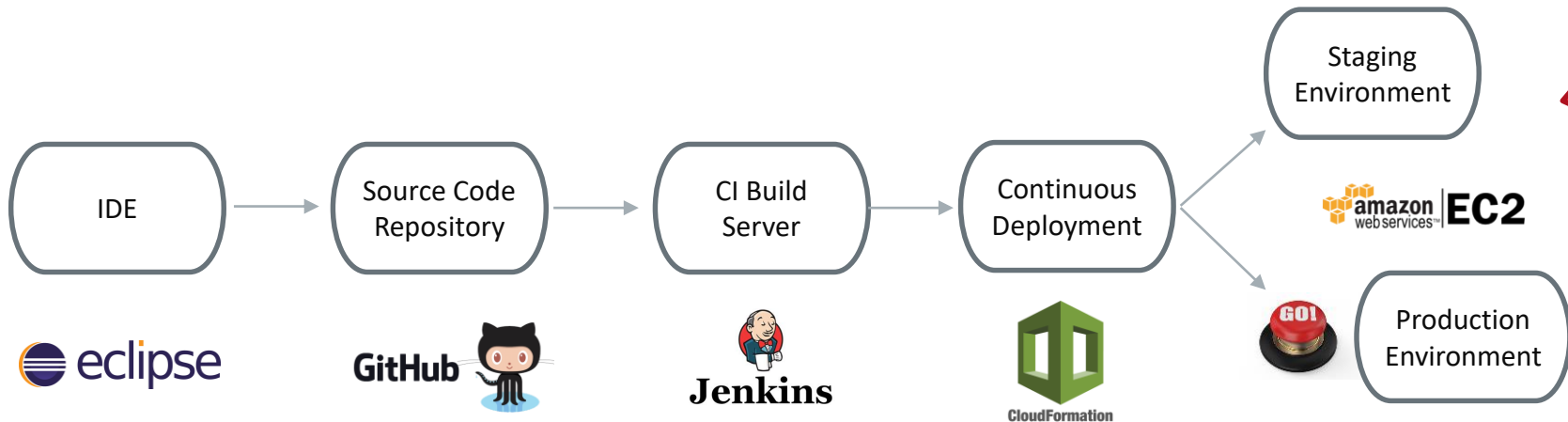


App Scanning



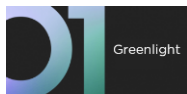
Continuous Monitoring





## Advanced Security Automation

Coding Helpers



Supply Chain Risk



Code Analysis

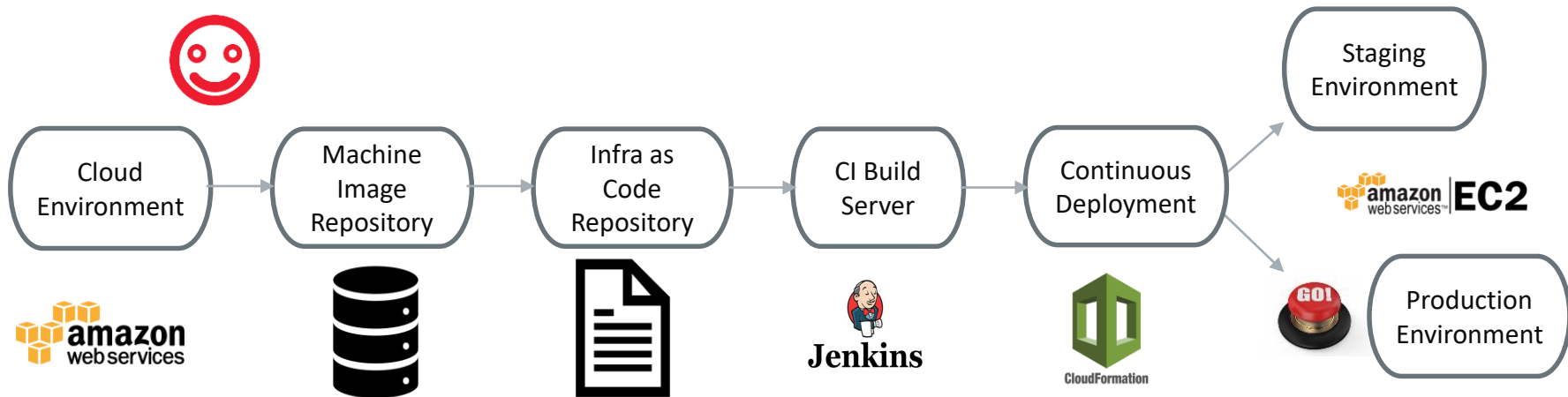


App Scanning



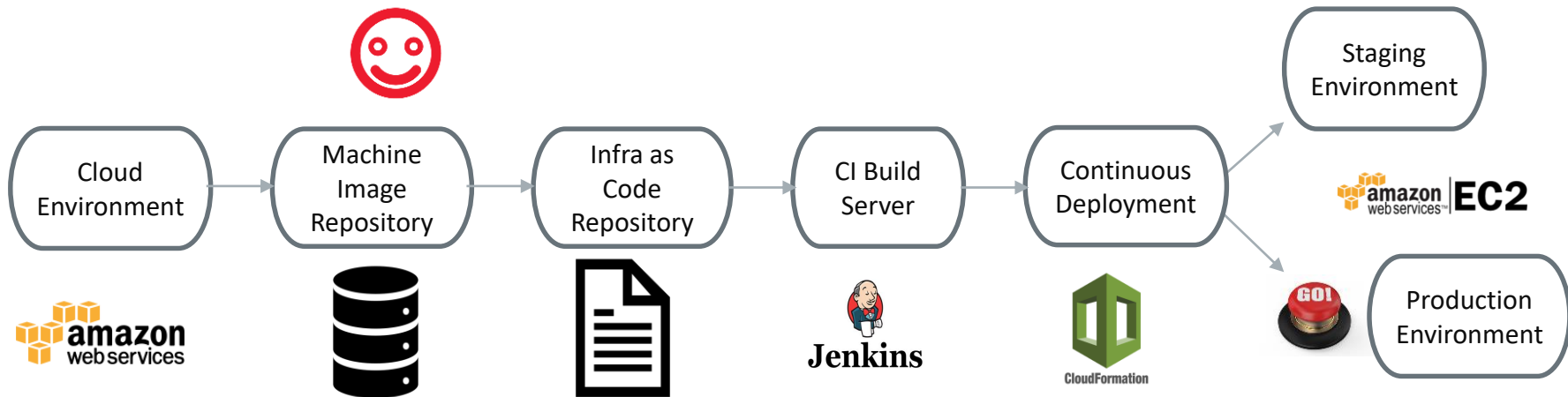
Continuous Monitoring





## Advanced Security Automation

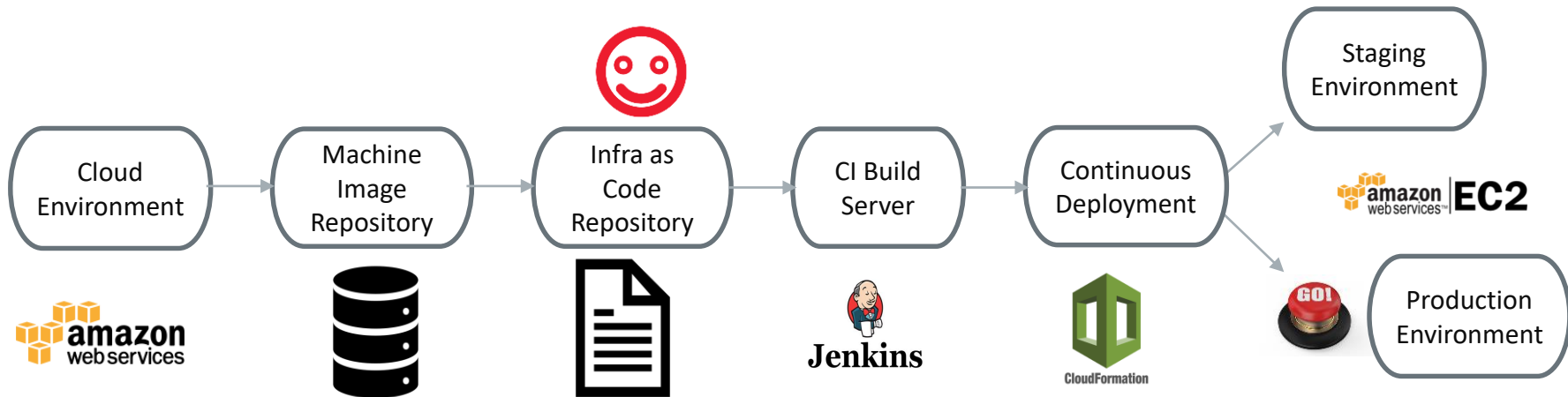




## Advanced Security Automation

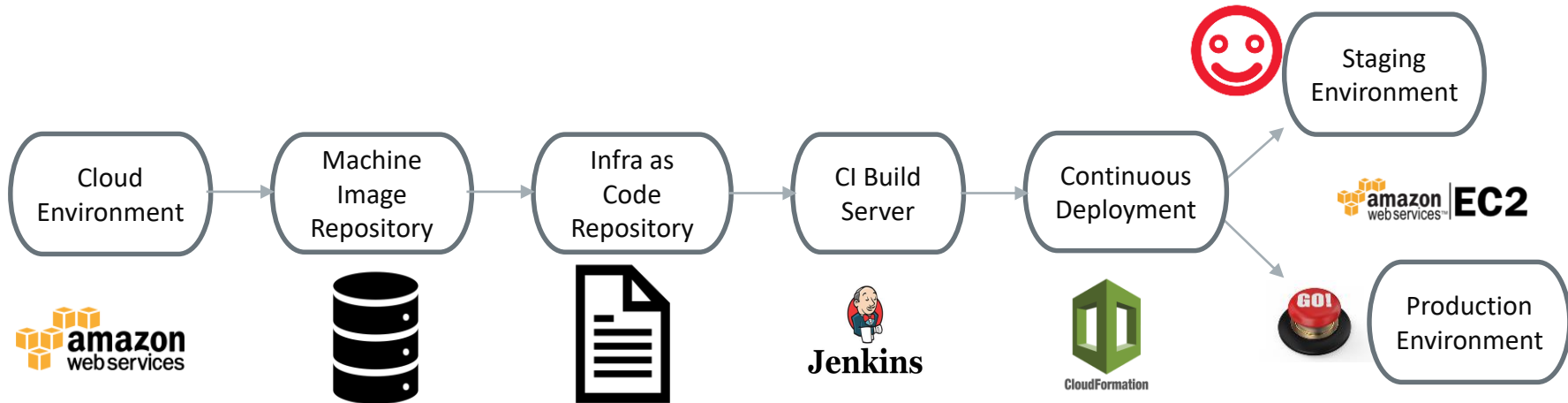






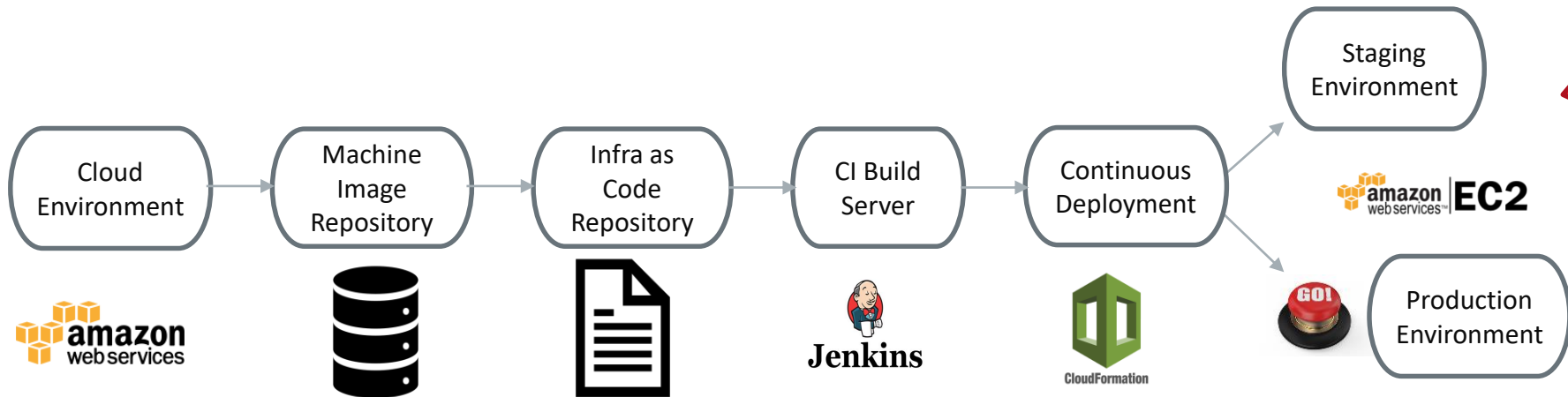
## Advanced Security Automation





## Advanced Security Automation





## Advanced Security Automation





Custom Application (1<sup>ST</sup> party code, 3<sup>rd</sup> party libraries, etc.)



Application Framework (Tomcat, Nginx, Apache, etc.)



Network & OS (Linux, Windows, etc.)



Cloud Platform (Amazon RDS, S3, Lambda, etc.)



Core Infrastructure (Fabric Functions: AWS IAM, EC2, Azure, etc.)



# Thank You!

Murray Goldschmidt | Chief Operation Officer  
[murrayg@senseofsecurity.com.au](mailto:murrayg@senseofsecurity.com.au)

© 2002 – 2017 Sense of Security Pty Limited. All rights reserved.

Some images used under license from Shutterstock.com or with permission from respective trademark owners. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

Security, it's all we do. Knowledge, Experience & Trust.

**Sense of Security Pty Ltd**  
ABN 14 098 237 908

**Sydney**  
Level 8, 66 King Street  
Sydney NSW 2000

**Melbourne**  
Level 15, 401 Docklands Drive  
Docklands VIC 3008

Tel. 1300 922 923  
Intl. +61 2 9290 4444  
[www.senseofsecurity.com.au](http://www.senseofsecurity.com.au)

  
@ITSecurityAU