

Blue Team Tools: SonarQube



George Smith

DESCRIPTION

@GeorgeS11323298



sonarqube

The SonarQube logo consists of three concentric blue curved lines that resemble a stylized 'S' or a signal wave, positioned to the right of the word 'sonarqube'.



Creator: SonarSource, S.A,
Switzerland

SonarQube is the leading tool for continuously inspecting the Code Quality and Security of your codebases and guiding development teams during Code Reviews.

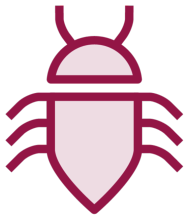
Covering 27 programming languages, while pairing-up with your existing software pipeline, SonarQube provides clear remediation guidance for developers to understand and fix issues and for teams overall to deliver better, safer software.



What Is so Special About SonarQube?



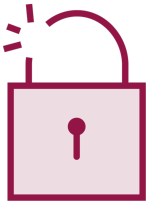
SonarQube Benefits



Bugs



Code Smells



Vulnerabilities

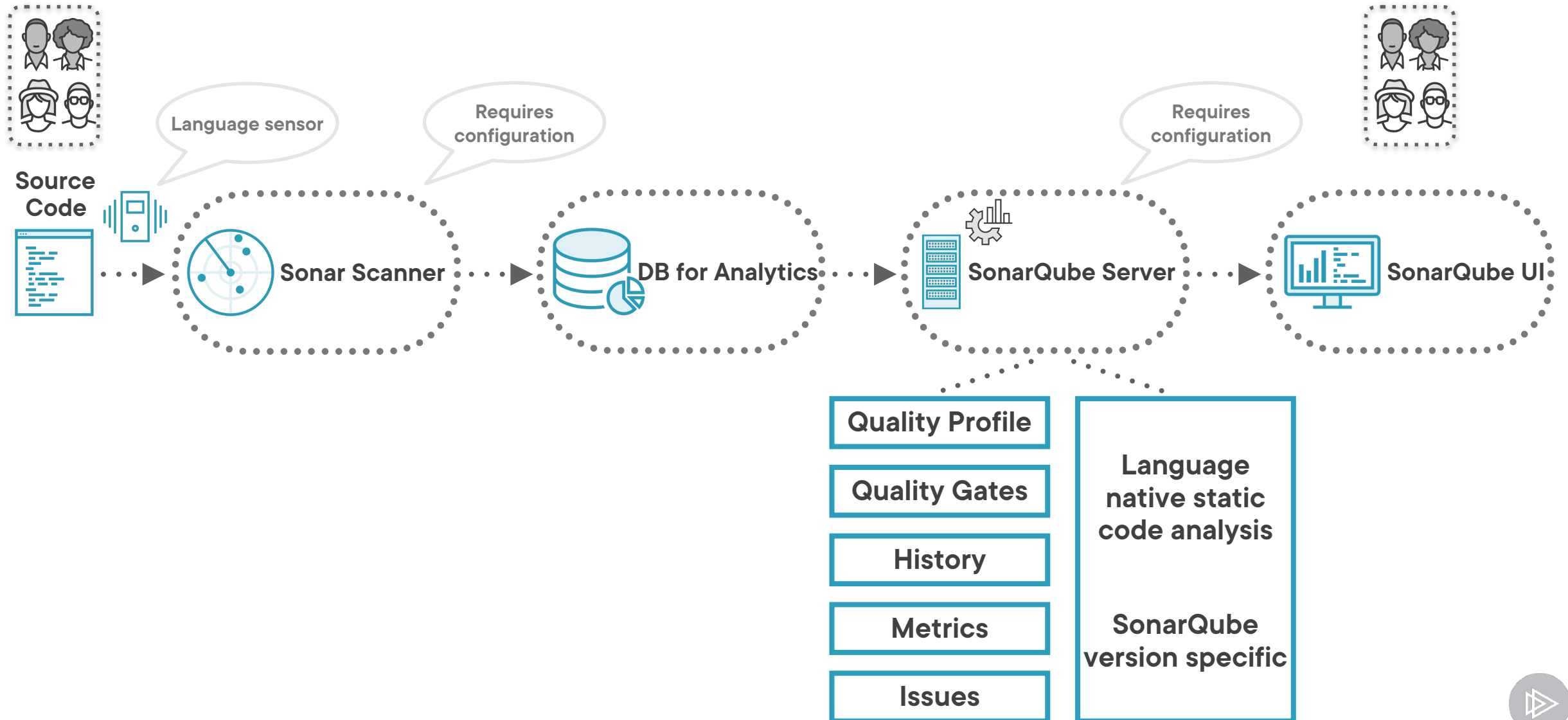


Hot Spots

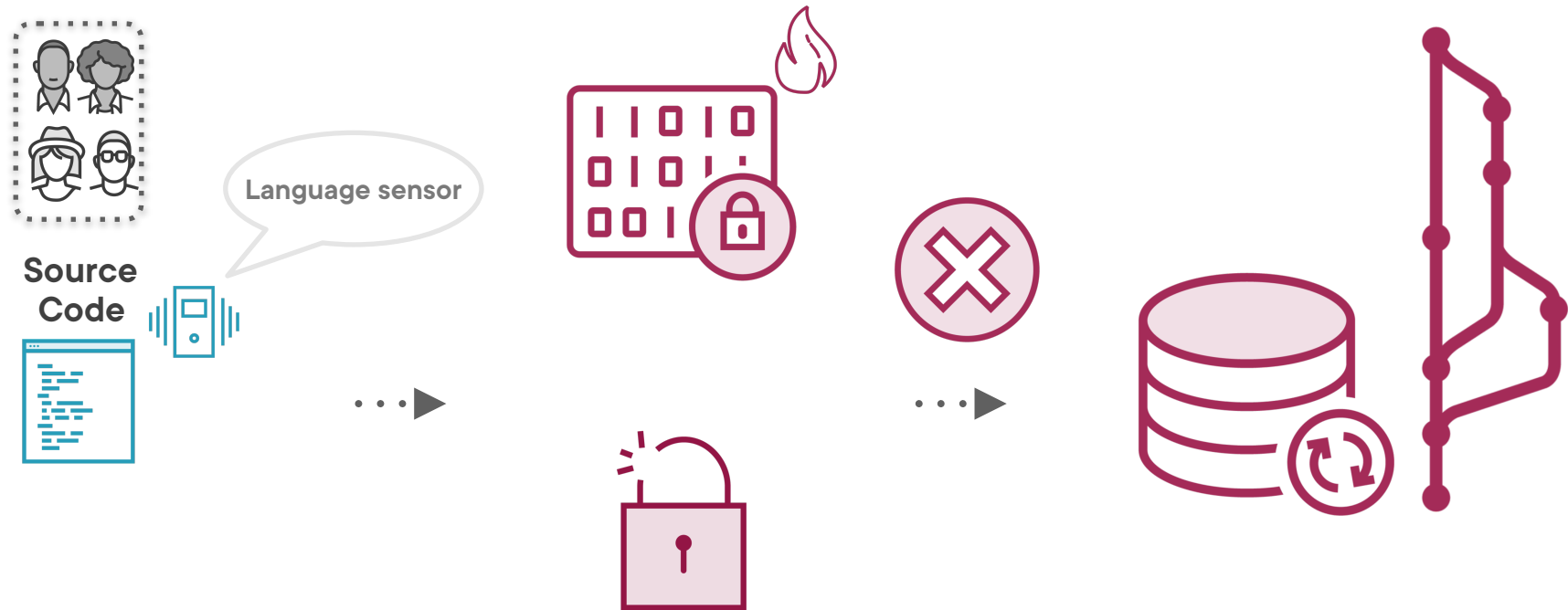
sonarqube



SonarQube Main Component Interactions



Hotspots and Vulnerabilities Prevention



OWASP and MITRE ATT&CK

OWASP

A1 - Injection

A2 - Broken Authentication

A6 - Security Misconfiguration

A7 - Cross Site Scripting

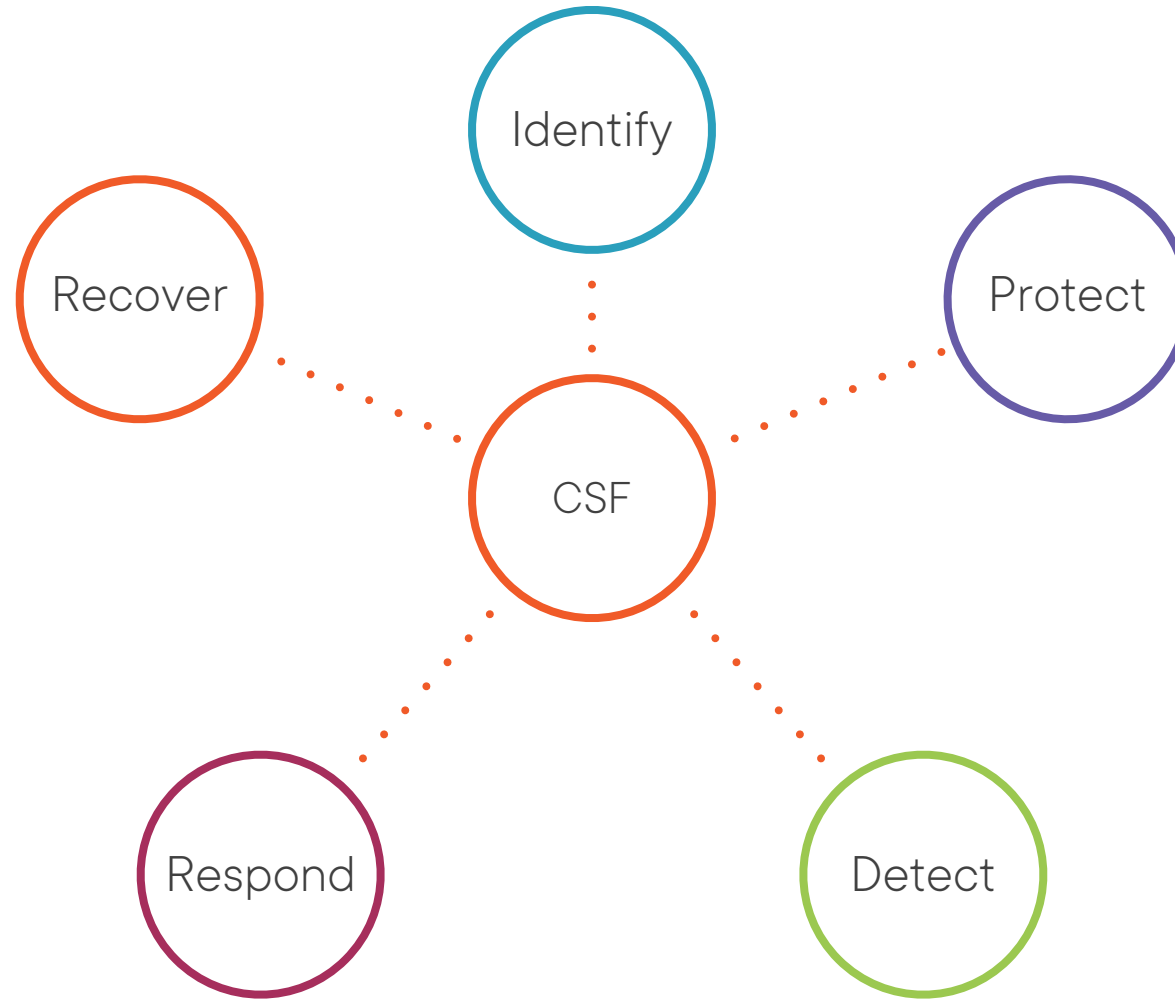
MITRE ATT&CK

T1190 - Exploit Public-Facing Application

T1189 - Drive-by Compromise

T1078 - Valid Accounts

NIST Cybersecurity Framework



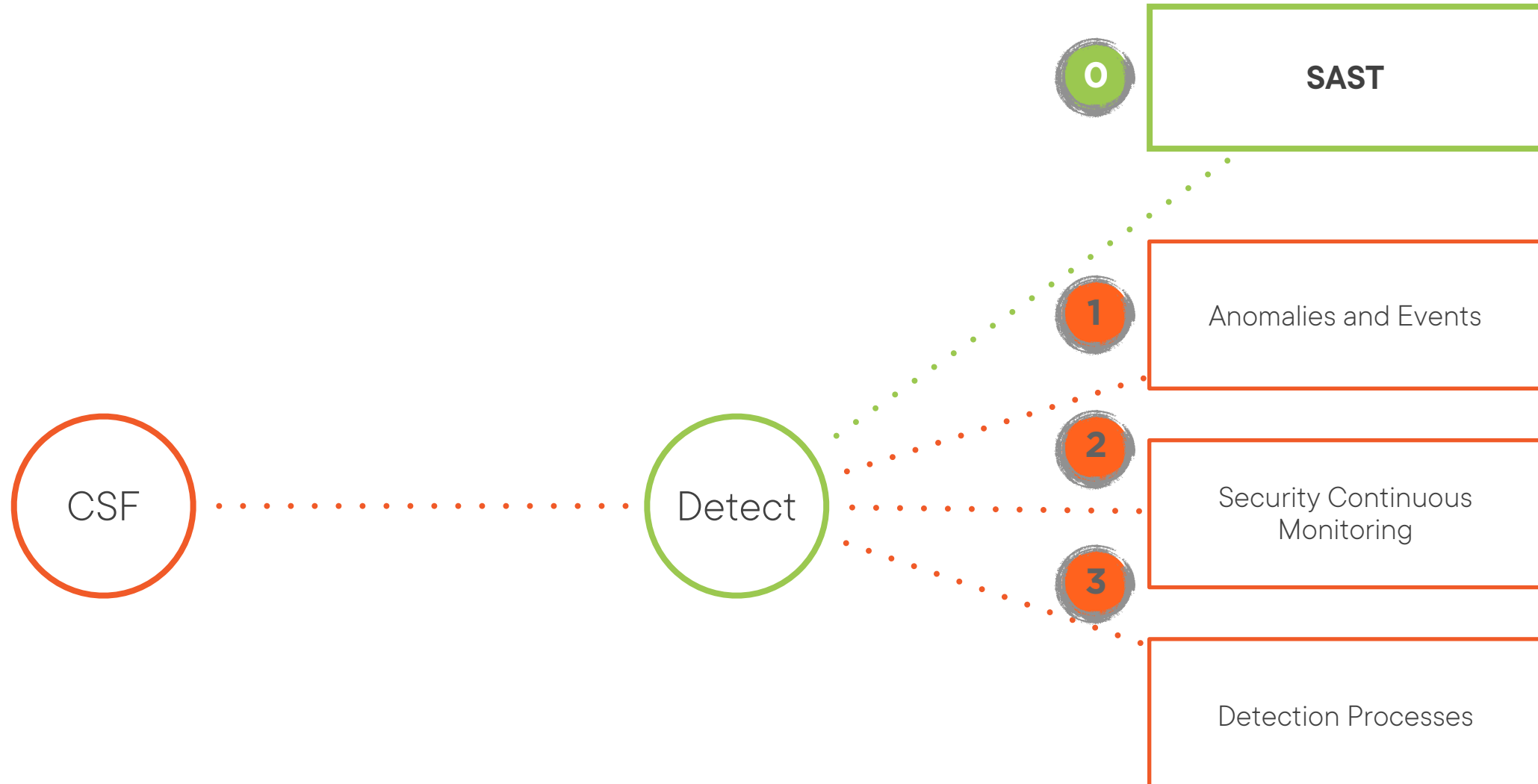
Other NIST measures take place
after a security event whereas

Other NIST measures take place
after a security event whereas
SonarQube measures are taken
before an event occurs

SAST

Static Application Security Analysis - security-related issues are continuously detected. The tool scans an application's source code identifying the root cause of vulnerabilities and helps remediate the underlying security flaws. SAST solutions analyze an application from the “inside out” and do **not operate on a running system to perform a scan.**

NIST Cybersecurity Framework



NIST Cybersecurity Framework



MITRE ATT&CK

Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

File Analysis

Threat Intelligence

Incident Management



MITRE ATT&CK

sonarqube



Data Type

Network Analysis

OS Analysis

Application Analysis

File Analysis

Threat Intelligence

Incident Management

Source
Code



T1190:

Exploit Public-facing Application

T1189:

Drive-by Compromise

T1078:

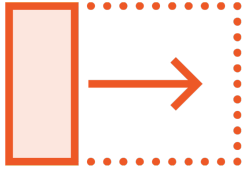
Valid Accounts



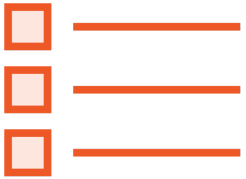
What Are the Advantages of SAST Tools?



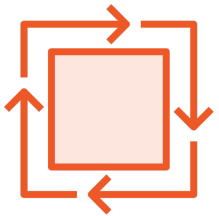
Advantages of SAST



Shifting work to a more abundant resource



Breadth of coverage



Speed

Security resources are scarce.
Developers are more readily
available.

Use SonarQube to scan 100%
of your code base

Use SonarQube to automate
the reviews of security
sensitive code as well

Software Quality Reaches New Heights



Clip 2

Install SonarQube

1. Install package manager
2. Install and configure Java 11
3. Install and configure SonarQube
4. Install and configure Sonar Scanner

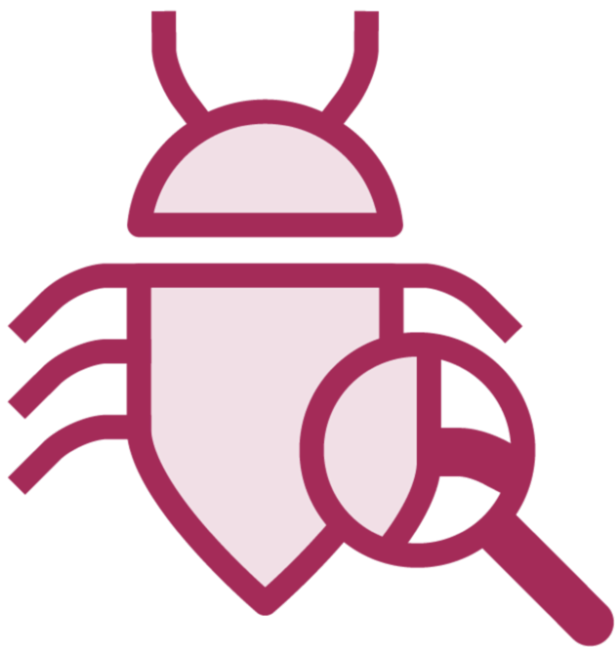


Java 11+ recommended

Set up environment
variables in your default shell

Make sure port 9000 is
available

Bonus Setup Tip



Sonar Configuration

sonar.properties

Path on MacOS: `/usr/local/Cellar/sonarqube/<version>/libexec/conf/sonar.properties`

Path on Ubuntu: `/opt/sonarqube/conf/sonar.properties`

```
sonar.web.javaAdditionalOpts=-Xmx2G
```

```
sonar.ce.javaAdditionalOpts=-Xmx6G -XX:+HeapDumpOnOutOfMemoryError
```

```
sonar.search.javaAdditionalOpts=-Xmx6G -Xms6G -XX:+HeapDumpOnOutOfMemoryError
```

```
-Dnode.store.allow_mmap=false
```

Remove Elasticsearch Folder

Elasticsearch State

Waiting for Elasticsearch to become ready

Remove:

Path on MacOS: `/usr/local/Cellar/sonarqube/<version>/data/es7`

Path on Ubuntu: `/opt/sonarqube/data/es7`

Clip 3

Create a Project in SonarQube

sonarqube 



Rotate tokens regularly

Run an Analysis

sonarqube



Clip 4

Demo

Tasks

- Run a a SonarQube source code analysis
- Analyze the results

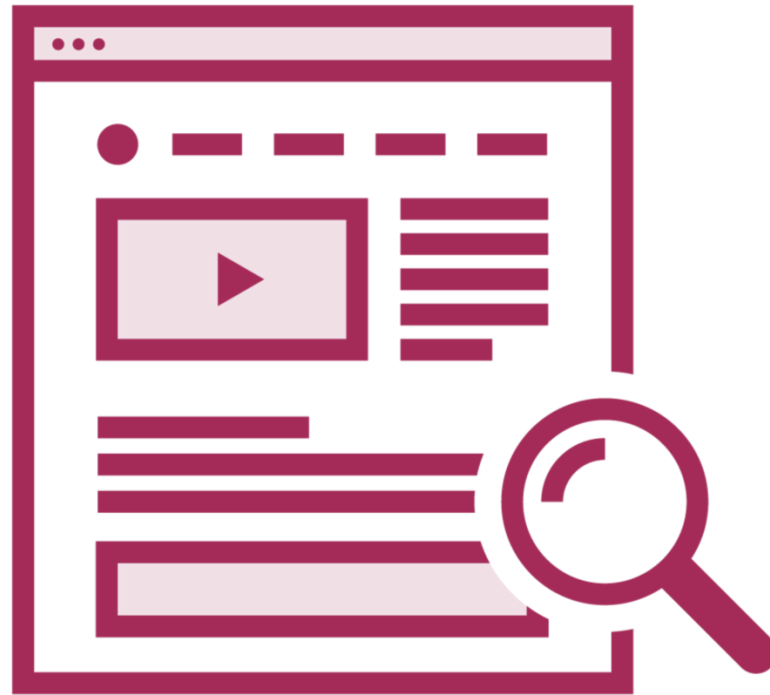
Preparation

1. Create project
2. Obtain security token
3. Generate the command to run an analysis



Additional Resources

sonarqube 



Clip 5

Course Summary

Summary

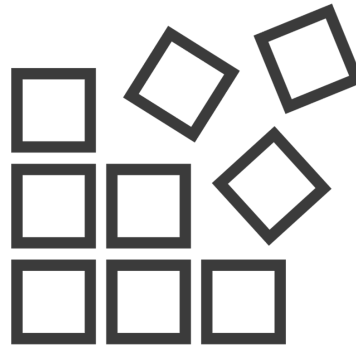
- Install SonarQube
- Create a project
- Configure Sonar for your project
- Run an analysis
- Interpret the results

Custom Plugins

Custom Rules



Assemble



Custom Plugin



More Information

Capabilities

Additional Plugins

<http://localhost:9000/admin/marketplace>

Creating Custom Plugins

<https://docs.sonarqube.org/latest/extend/developing-plugin/>

SonarQube Developer Edition

<https://docs.sonarqube.org/latest/extend/developing-plugin/>

Related Information

Browse Security Rules by Type

<https://rules.sonarsource.com/java/tag/owasp/>

MITRE ATT&CK

<https://attack.mitre.org/tactics/enterprise/>

Key Words

- SQL Injection
- Cross-site Scripting / XSS
- Identity
- Secrets
- Broken Authentication, etc.



Well Done



Thank you for Watching



Please Rate This Course



Thank You

