TALK

SO LONG, SECURE CODING,

HELLO, SECURE DEVELOPMENT

Laura Bell Main
CEO and Founder, SafeStack

Laura Bell - CEO and Founder of SafeStack

Apprentice Software Developer

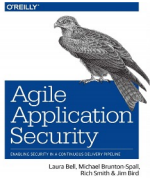
AI and Robotics

CERN

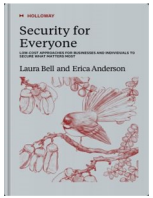
Counter Terrorism

Penetration Tester

Security Consultant



Founder



CEO

Help me understand the real picture of #AppSec

All results are anonymous

Data will be open-sourced when the survey ends

The world is not as mature as we like to think

Cutting Edge

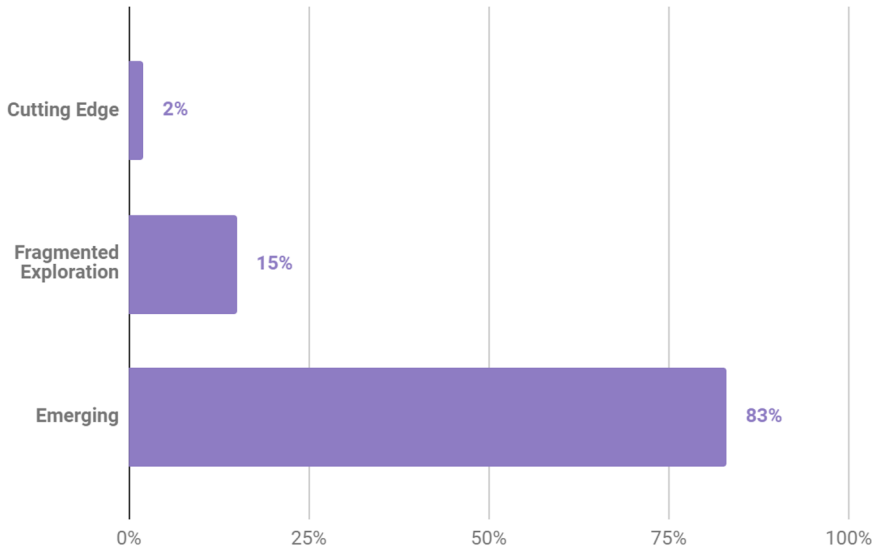
Bleeding edge of application security, DevOps, actively building application security teams

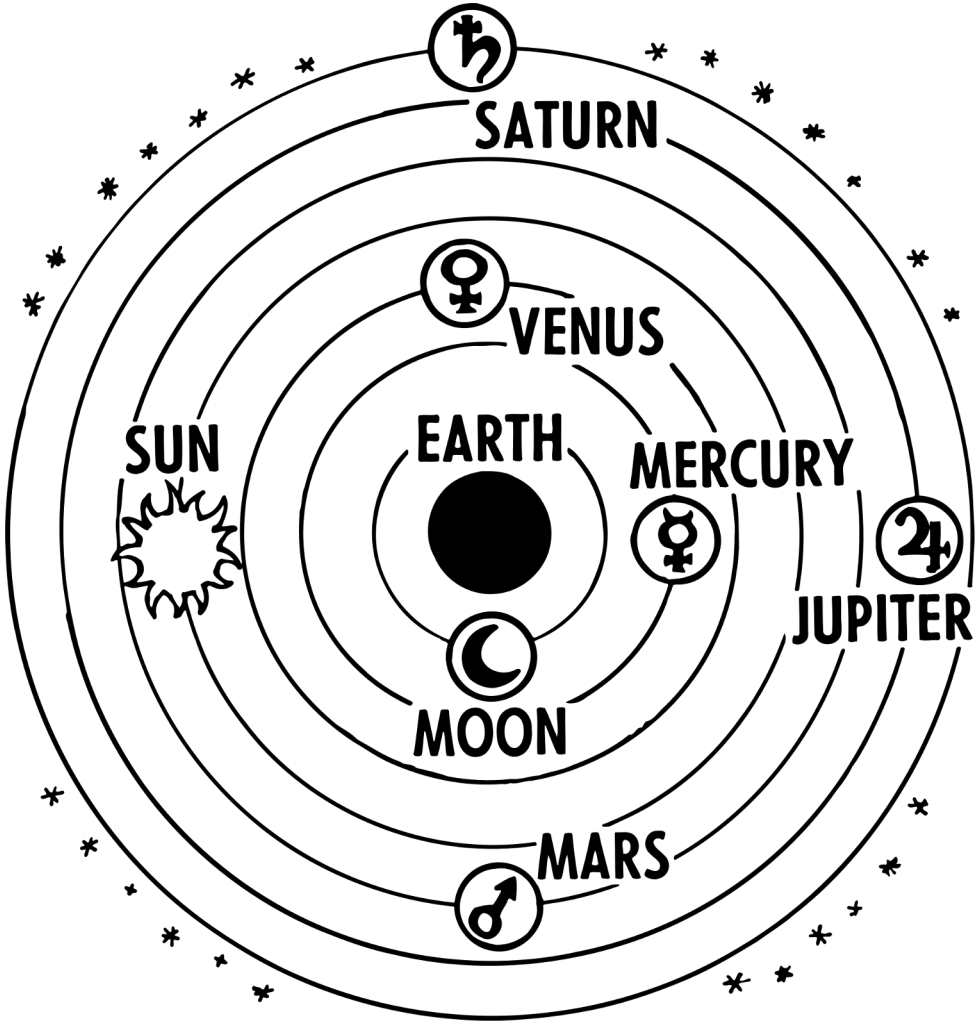
Fragmented Exploration

Fragmented approach to all security domains, looking for guidance and coherence

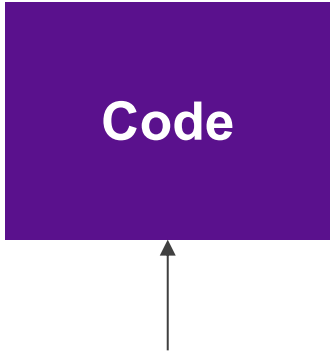
Emerging

Immature or traditional security practices only.




SATURN
VENUS
SUN
EARTH
MERCURY
JUPITER
MOON
MARS


Design
Code
Test
Deploy
Support



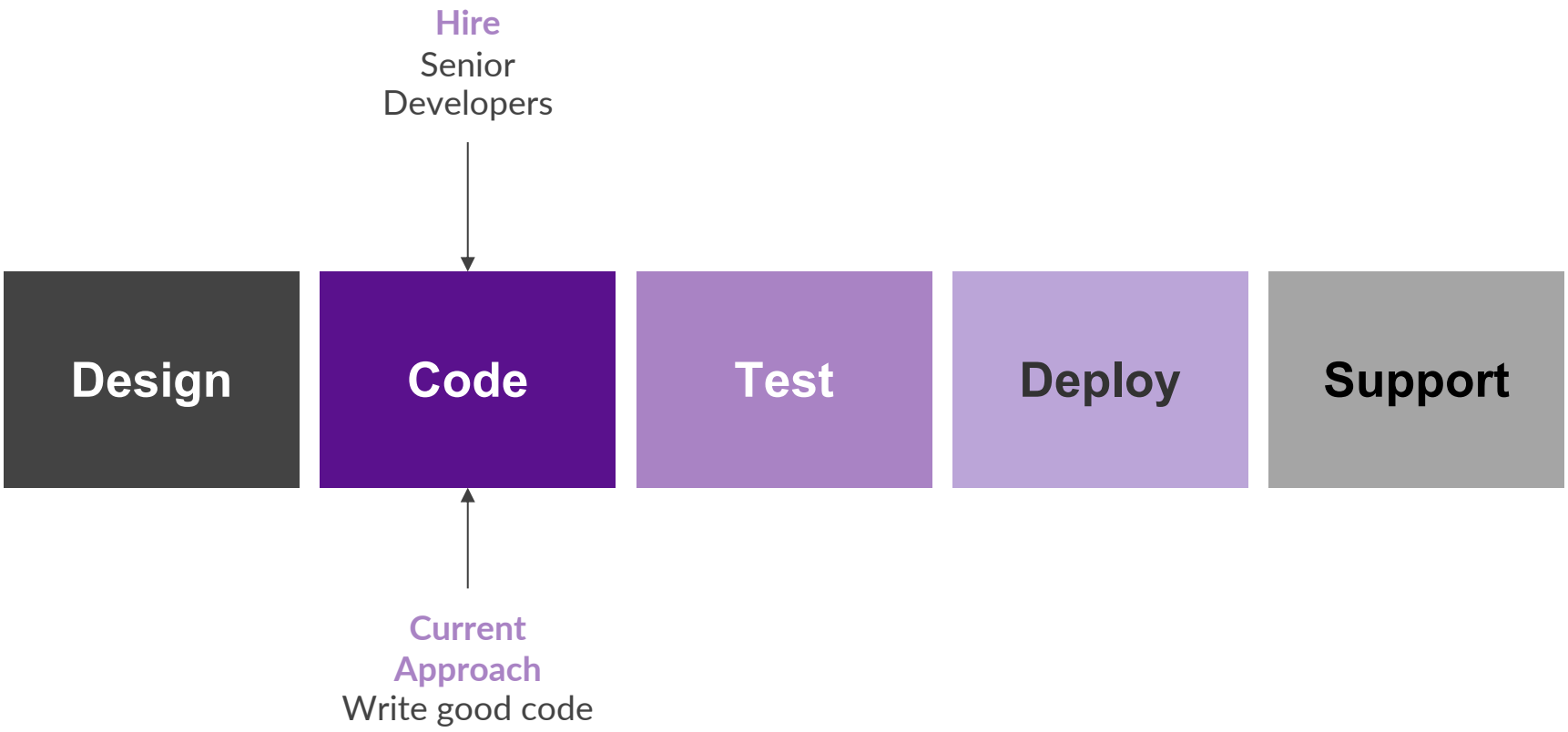
Current Approach

Write good code

And it’s not just the SDLC that’s causing this **blindspot**

developers!
developers!
developers!

Famous quote from some guy at a conference once


Hire
Senior
Developers
Design
Code
Test
Deploy
Support
Current
Approach
Write good code

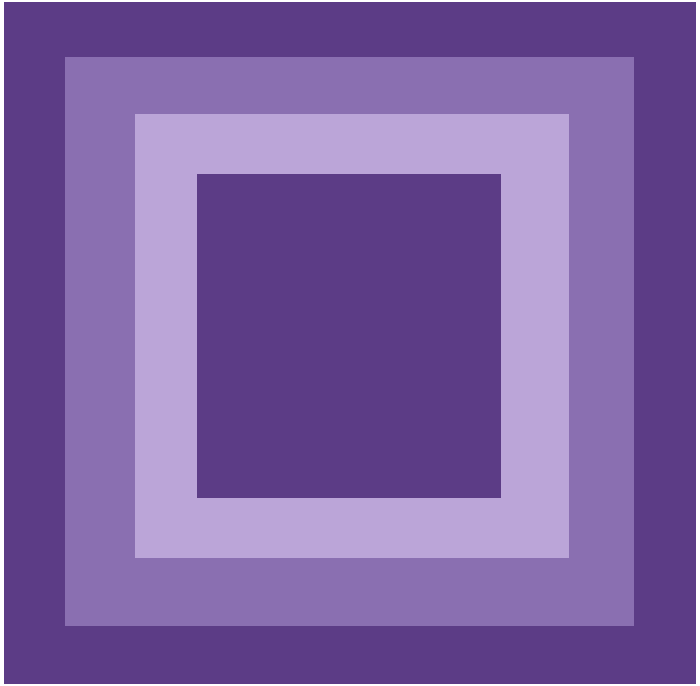
developers
testers
ux designers
analysts
architects
product owners

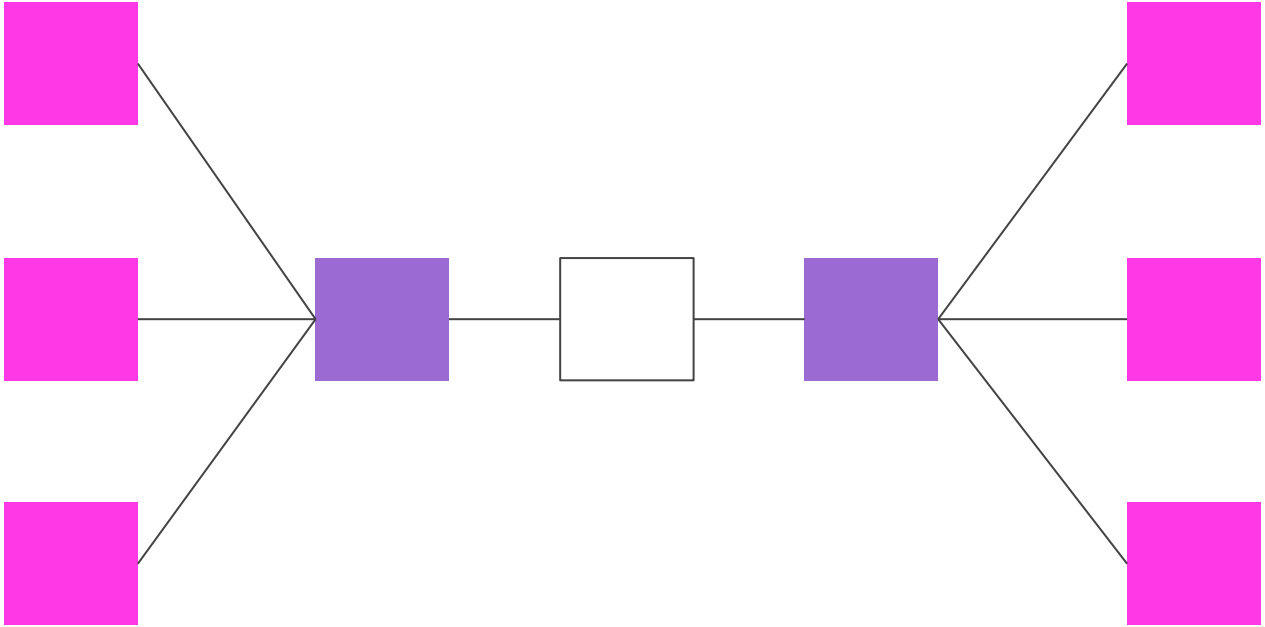

Design
Code
Test
Deploy
Support

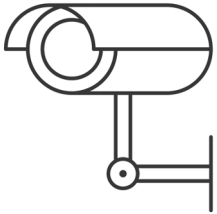
Design | Code | Test | Deploy | Support

Architect

A person who designs a system and supervises its implementation







Zero Trust

Assume that risks can come from any element of your environment and take steps to protect against them.

Preventative

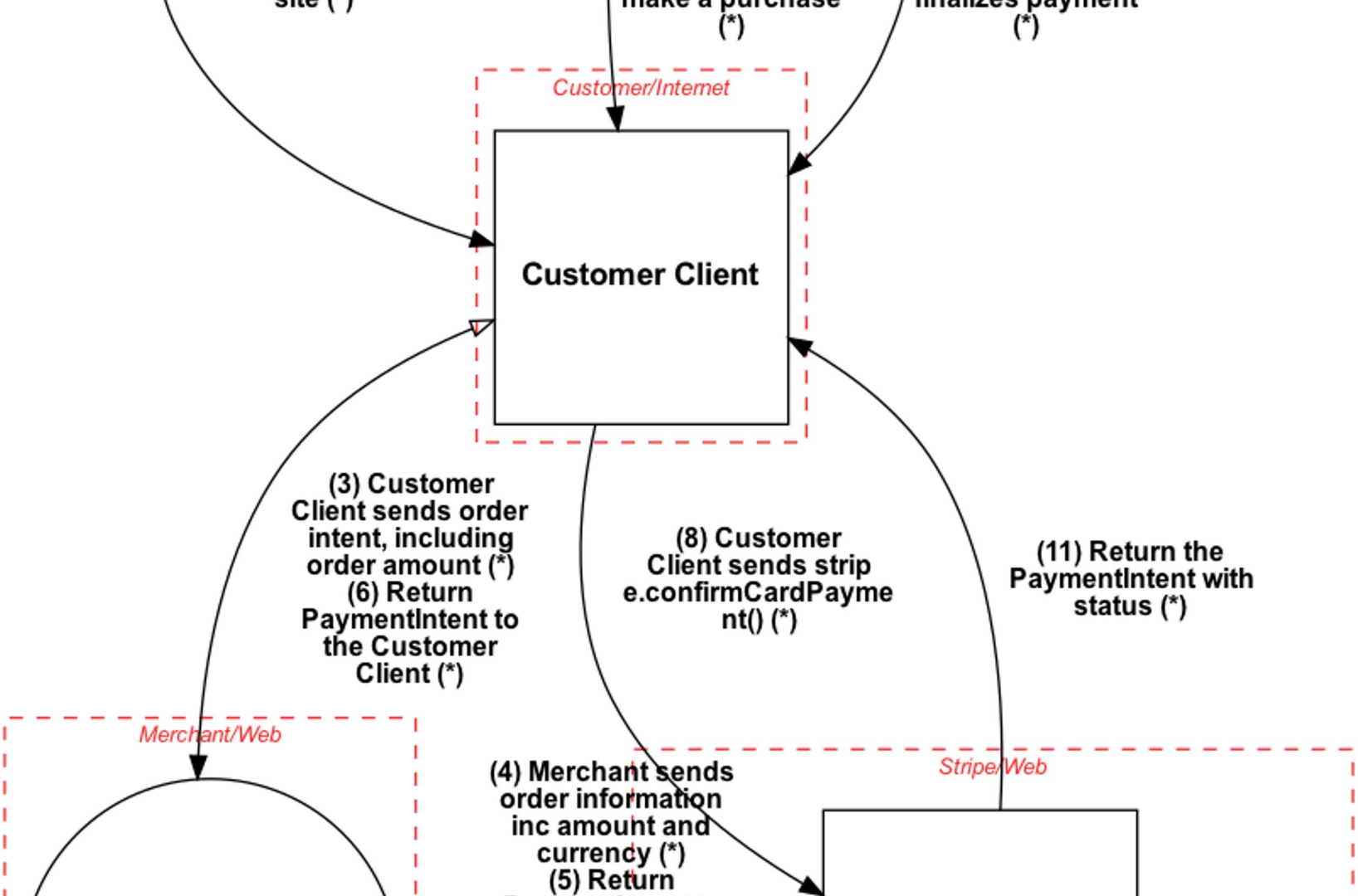
Encapsulation
Encoding
Sanitisation
Automation
Trust zones
Least Privilege
Jump hosts
HTTPS
Encryption
Key stores
PKI
Firewall

Detective

Validation
Verification
Testing
Code review
Logging
Bug Bounties
Pen Testing
WAF
SIEM
Alerting
On-call
Support line

Responsive

IR planning
Redundancy
Replication
Failover
Post mortems


site (*)
make a purchase (*)
finalizes payment (*)
Customer/Internet
Customer Client
(3) Customer Client sends order intent, including order amount (*)
(6) Return PaymentIntent to the Customer Client (*)
(8) Customer Client sends stripe.confirmCardPayment() (*)
(11) Return the PaymentIntent with status (*)
Merchant/Web
(4) Merchant sends order information inc amount and currency (*)
(5) Return
Stripe/Web

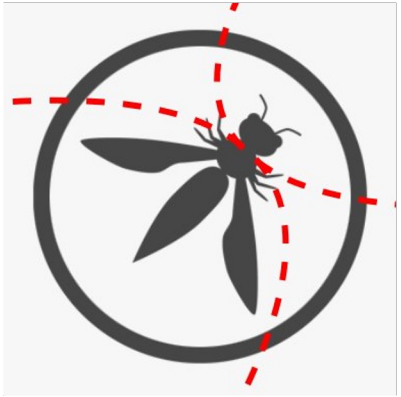
Train everyone to be a security architect

OWASP Threat Dragon

Threat Modelling Cookbook

Threat Modelling Manifesto

Awesome Threat Modelling



ACTION

Draw your system design

Do a simple threat model with your team

Design | **Code** | Test | Deploy | Support

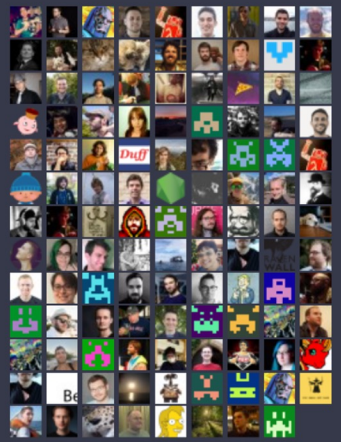
browserify show

package info graph info

# of nodes
172

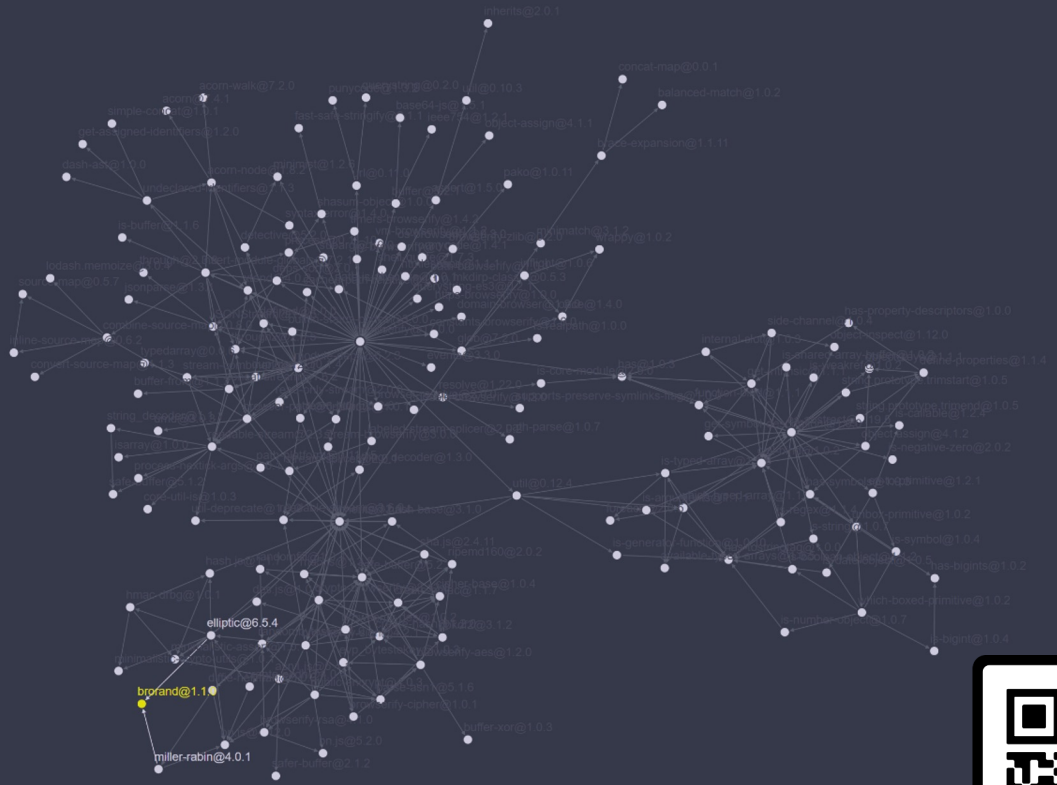
# of links
358

maintainers



licenses

MIT	150
ISC	11
Apache-2.0	5
BSD-3-Clause	3



view source code
share to twitter
become a patron

Show 3D

SCAN ME

Transitive Risk

Risk that is inherited from those you are connected with or to successive members of a sequence

npm
2.37M Packages

Maven
474K Packages

PyPI
446K Packages

NuGet
380K Packages

Go
372K Packages

Packagist
360K Packages

Rubygems
179K Packages

CocoaPods
87.9K Packages

Cargo
83.5K Packages

Bower
69.5K Packages

CPAN
39.2K Packages

Pub
30.9K Packages

Clojars
24.3K Packages

CRAN
22.2K Packages

conda
16.6K Packages

Hackage
16.5K Packages

Meteor
13.4K Packages

Hex
13.1K Packages

Homebrew
7.55K Packages

Puppet
6.92K Packages

Carthage
4.53K Packages

SwiftPM
4.21K Packages

Julia
3.05K Packages

Elm
2.61K Packages

Dub
2.42K Packages

Racket
2.21K Packages

Nimble
1.93K Packages

Haxelib
1.7K Packages

PureScript
586 Packages

Alcatraz
464 Packages

Inqlude
228 Packages

Source: libraries.io

freqtrade / freqtrade Public

Sponsor | Notifications | Fork 3.7k | Star 17.3k

Code | Issues 43 | Pull requests 13 | Actions | Projects | Wiki | Security | Insights

develop | 3 branches | 58 tags | Go to file | Code

xmatthias Merge pull request #6778 from markdregan/patch-1 ... b73f770 19 hours ago 16,275 commits

.devcontainer	Remove compose file for devcontainer	10 months ago
.github	Revert unwanted changes	4 days ago
build_helpers	Check pre-commit verison updates	10 days ago
config_examples	Fix config_examples typo	5 days ago
docker	Update ARMHF image to 3.9	5 months ago
docs	Merge pull request #6715 from nicolaspapp/feat/relative-drawdown	2 days ago
freqtrade	Add bot_loop_start() call in plotting.py	yesterday
scripts	Update more terminology to forceexit	24 days ago
tests	Fix fee handling for futures trades	yesterday
user_data	Default docker to log into log-dir	2 years ago
.coveragerc	Update documentation for create-userdir util	3 years ago

About

Free, open source crypto trading bot

www.freqtrade.io

python | bitcoin | telegram-bot | trading-bot | cryptocurrency | cryptocurrencies | trade | algorithmic-trading | freqtrade

Readme

GPL-3.0 License

17.3k stars

568 watching

3.7k forks

Releases 56

2022.4.2 Latest

yesterday

REVIEW CHECK LIST

Before using a new library, framework or technology, answer the following questions

	Yes
Is it using a suitable license?	☐
Is it regularly released and governed by a well sized community?	☐
Are their active or resolved issues on the project?	☐
Have you looked at the code?	☐
Would you sign off on it?	☐
Is this package and version already known to have security vulnerabilities?	☐

If you cannot answer 'Yes' to all of these questions, find someone to help you or try an alternative option.

ACTION

Use your new security review checklist next time you choose or update a library or framework

Design | Code | **Test** | Deploy | Support

testing
is a
superpower

test coverage is not a
leading indicator of code quality

Scenario - Username enumeration on incorrect login

Given the user navigates to the authentication page
When the user enters a username from valid-usernames
and the user enters a password from invalid-passwords
And the user submits the login form
Then the resulting message should not identify if the username is valid within the system

link your **testing** to your **threat model**

Vulnerability Scanning

Looks for signs that something could be wrong

Example: Temperature check

Automated Testing

Looks for confirmation of a specific issue

Example: A medical test

Manual

Tools that run on demand to check packages

Parallel

Tools that monitor your packages independently of your CI/CD pipeline

Integrated

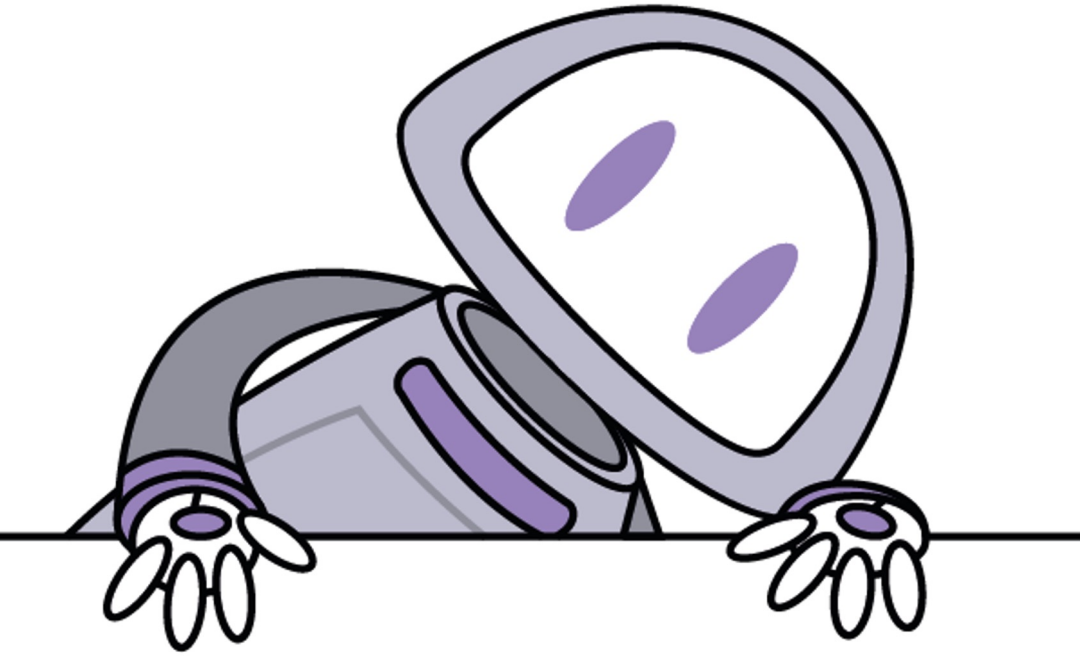
Tools that run in line with your CI/CD pipeline

ACTION

Stop considering test coverage

Allow more time for exploratory testing

Design | Code | Test | **Deploy** | Support



the best security action is one you
don’t have to remember to do

Github dependabot

Github actions

- Semgrep
- TruffleHog
- Check for outdated packages
- Linters
- SAST/DAST
- Owasp Zap?

ACTION

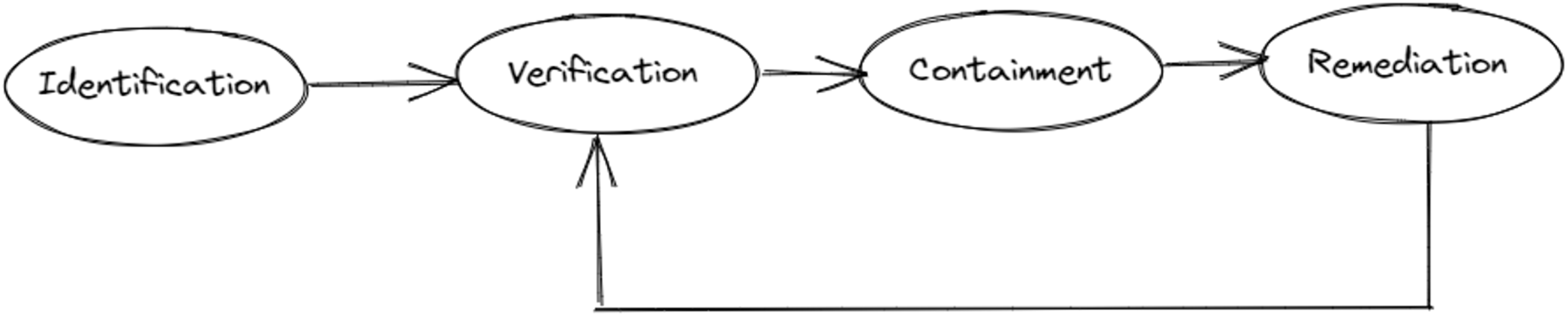
Set up basic security github actions dependabot and trufflehog

Design | Code | Test | Deploy | **Support**

Incident Response Plan

A repeatable process for assessing and responding to unexpected events

A Simple Incident Response Plan



Build playbooks for software security incident scenarios

Examples:

- Account compromise (password breach)
- Unauthorised query or data export
- Data exposure (I can see other people’s stuff)
- Permissions escalation
- Unauthorised data access/view
- Suspicious changes to deploys or builds
- Suspicious activity reported on a customer account

Example playbook questions

- How do you verify the issue?
- How do you contain the incident?
- What logs do you have and how to you find them?
- Who do you need to contact (both to resolve and report)?
- What is the sensitivity of the data that is impacted?
- Where are the backups? (and when were they last tested)
- Where do you keep a record of the incident and what actions you took?
- What additional support will you need?

Gather

↓

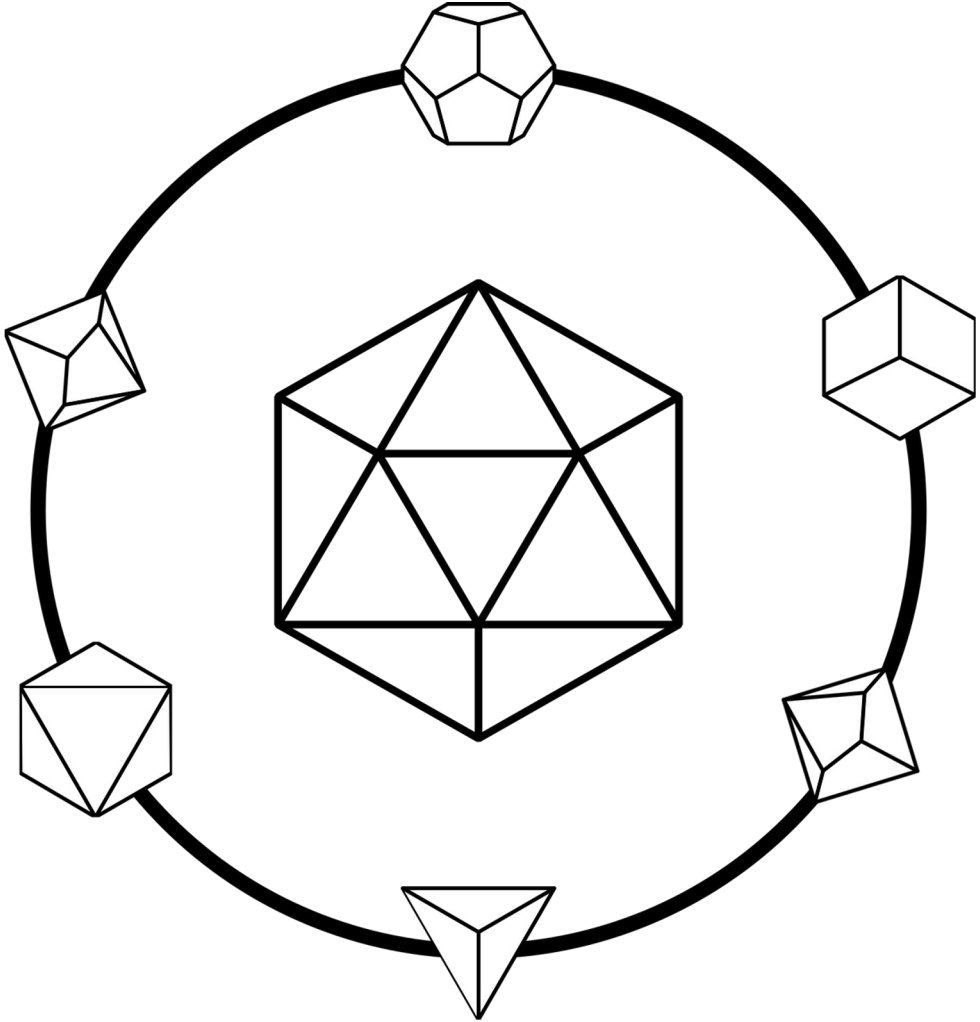
Plan

↓

Test

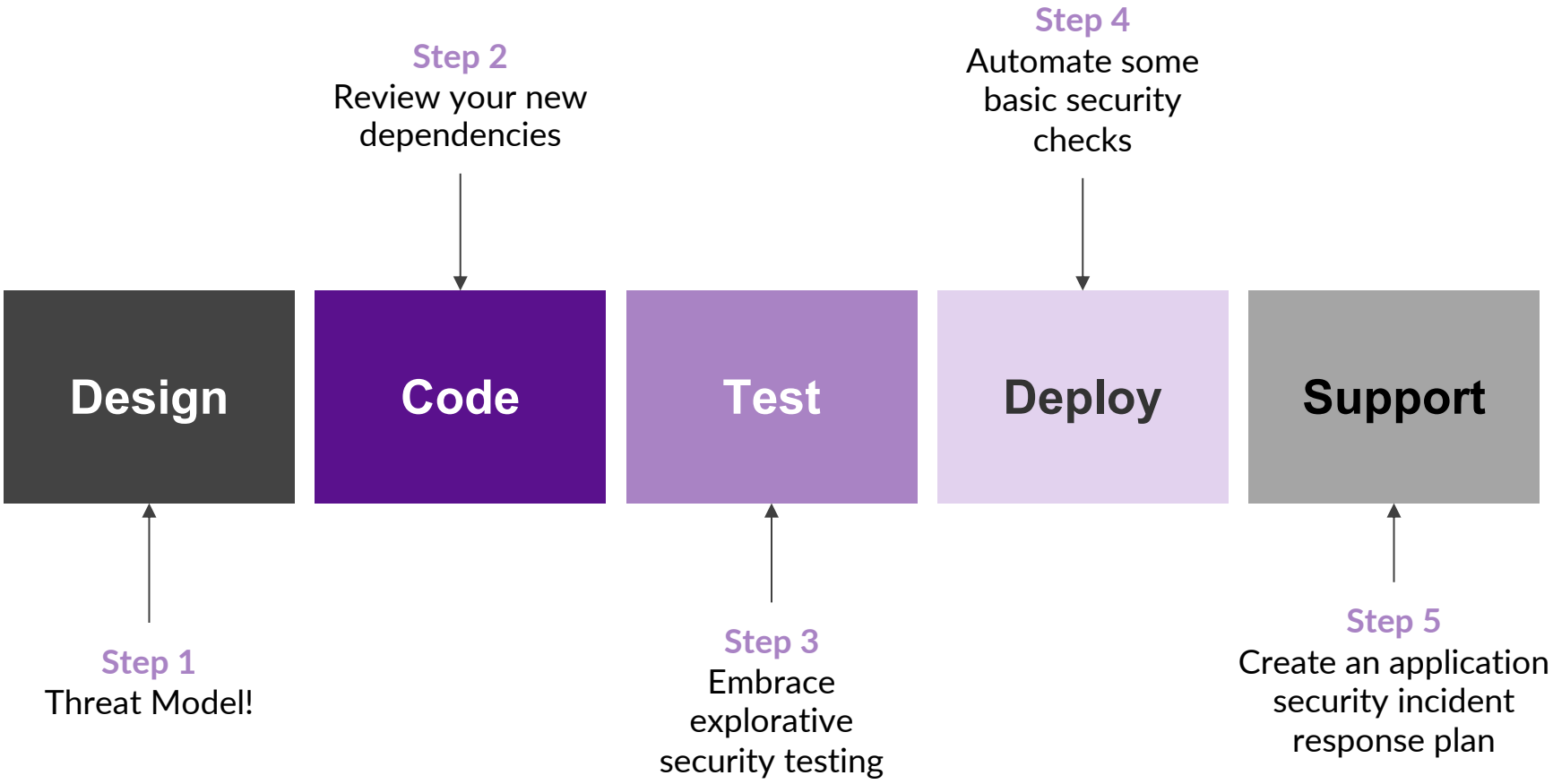
↓

Learn



ACTION

Create an application security incident response plan and playbooks and test them


Step 2
Review your new dependencies
Step 4
Automate some basic security checks
Design
Code
Test
Deploy
Support
Step 1
Threat Model!
Step 3
Embrace explorative security testing
Step 5
Create an application security incident response plan

Free #appsec program
OneHourAppSec

Free All Access Training for
Students

Help with our AppSec Resourcing Survey

50% discount for Startups

Download this slide deck

Laura Bell Main

laura@safestack.io
@lady_nerd
www.safestack.io