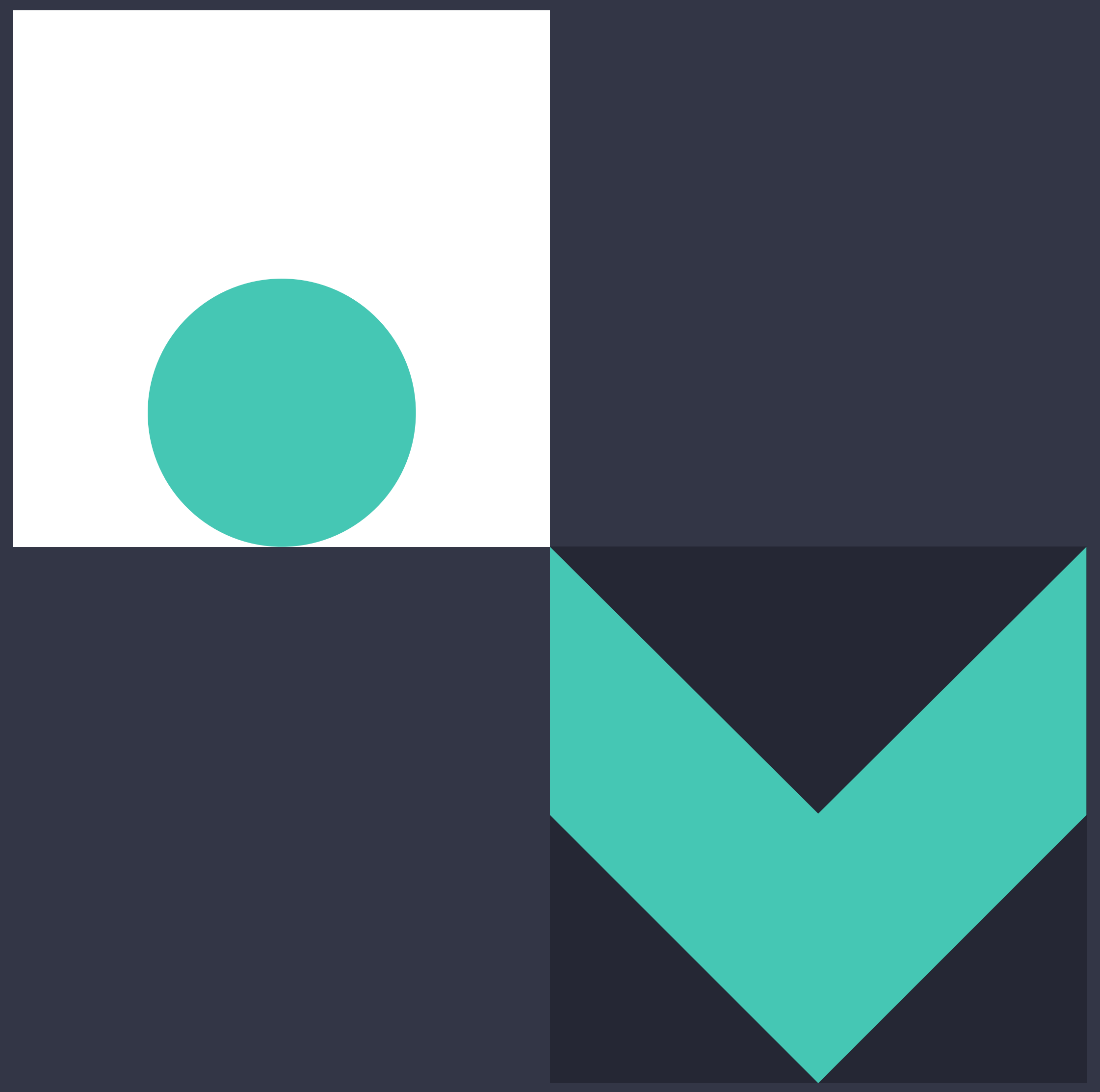
A guide to modern web application security



DETECTIFY E-BOOK SERIES
A guide and checklist

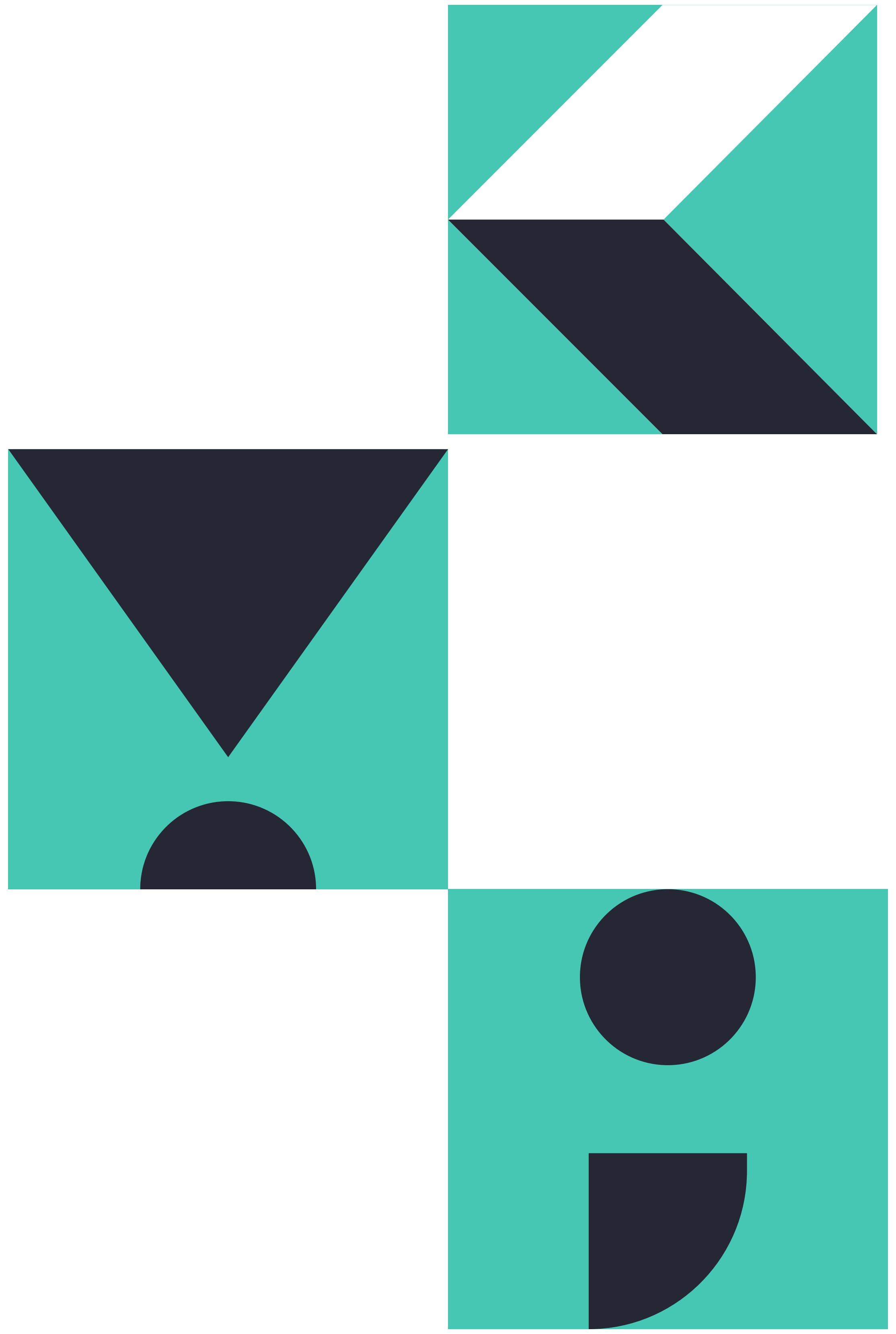
detectify

Modern application security requires speed, scale, and collaboration.

Organizations are shipping code daily, making it challenging for security teams to keep track of changes in the web application and keep up with new security threats. Attack surface reduction is rising steadily on the priority list for security defenders, as opportunistic cybercriminals are finding new vulnerabilities by the second using scripts and automated hacking tools.

In fact, between November 2020 to February 2021, over 5232 CVEs have been reported on NIST, which paints the picture that there a lot of vulnerabilities disclosed, and there's an even bigger spotlight on finding security practices that will keep up with this growing mountain of vulnerabilities and exposures in a scalable and sustainable way.

Contents



Today new vulnerability research can be analysed and developed into technologies for testing in as fast as 25-minutes.

Today new vulnerability research can be analyzed and developed into technologies for testing in as fast as 25-minutes* in Detectify's security lab.

With advancements in application security testing, including more intelligent automation, and expanding the expert pools to include once-feared hackers, the industry welcomes the next wave of application security that delivers critical vulnerability information at speed and large scale. It's also thriving on collaboration between security experts and application owners to secure more software and the Internet as a whole.

Finding vulnerabilities in time save you money – and headaches

IBM reports that the average cost of a data breach in 2020 was USD 3.86 million, and the average time from detection to containment was 280 days. Imagine how much money and work-hours organizations could save if they found the vulnerabilities at least 25-minutes sooner.

Acting promptly means:

- Preventing malicious actors from accessing secrets and sensitive data
- Avoiding financial loss to recover from attacks
- Saving developer time and costs lost to roll-back
- Avoiding any reputation damage

3.86 M Average cost of a data breach

280 days Average time from detection to containment

Continuous development, continuous security

It's not enough to rely on a WAF or a single (and costly) manual pentesting to stop criminals from exploiting your digital assets.

Today's leading tech organizations are relying on a combination of hacker-powered security research and security automation to ensure a constant level of application security awareness and defense along the front lines that make up the organizational attack surface.

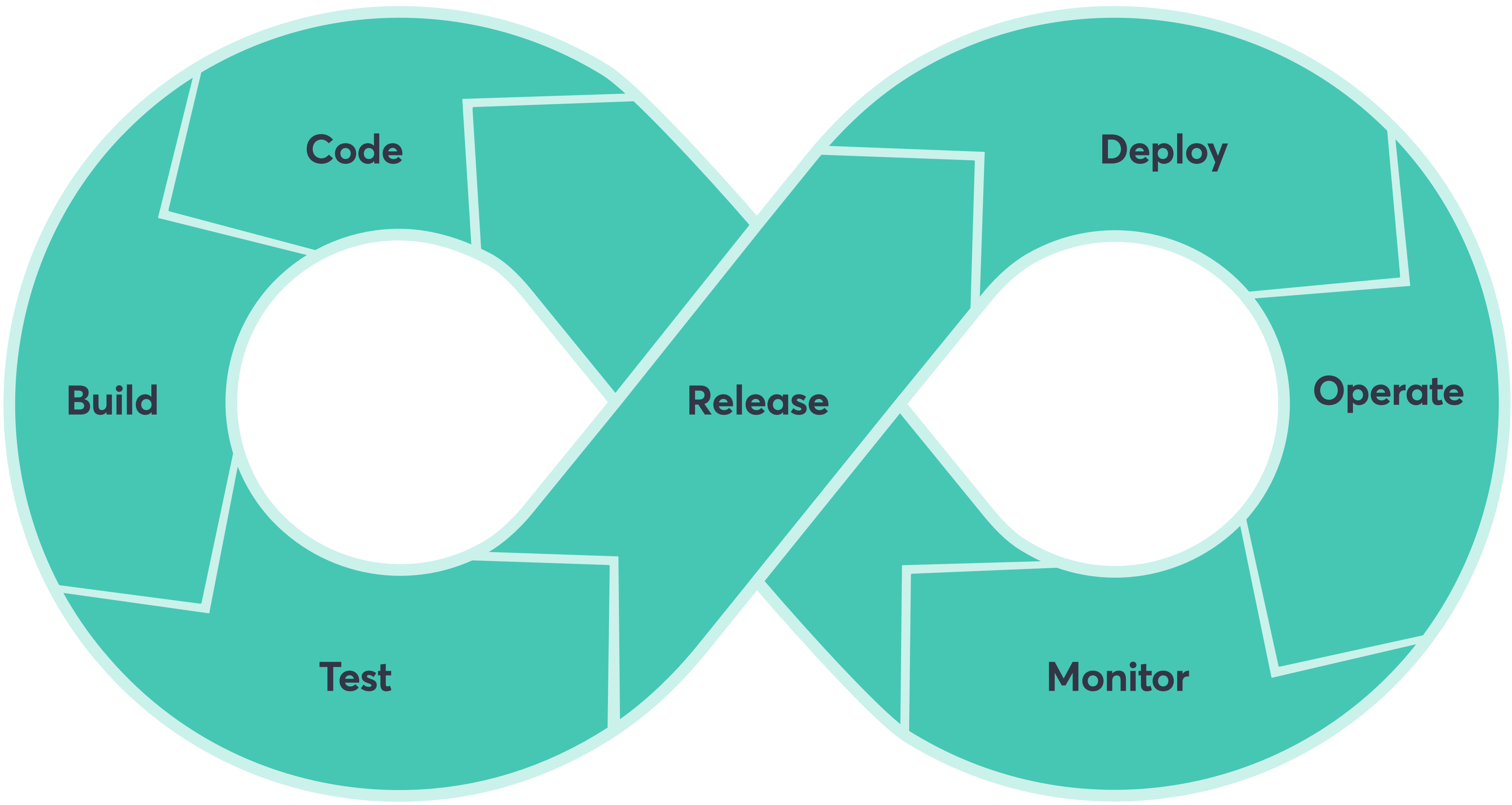
Bringing in expert security knowledge is now affordable for organizations and with the options of both automation and freelancing via crowdsourcing services. Companies recognize that automated checks and more frequent audits of code in production are even more important today to make sure security works with development and not against it.

RICKARD CARLSSON,
CEO DETECTIFY

"If you don't run recurring testing on your production environment and aren't able to feed that information directly to the engineering and developer team – potentially through a quick triaging process, then why do the complexity of testing the staging environment?

Finding vulnerabilities in staging doesn't matter; what matters is what's live."

Read the full interview on Application Security Weekly.



Researchers and hackers continuously discover new vulnerabilities as they exploit new and legacy code. This is why continuous application security is recommended.

This includes running dynamic application security testing (DAST) or black-box testing as part of a web vulnerability management strategy. This means running security checks on code that's live in production and continuously to prevent real-life attacks and actively exploited vulnerabilities.

Automated web security checks for widespread vulnerabilities in the background, allowing engineers to focus on software development.
In a security-mature company, developers and Ops include security with software development by scanning for vulnerabilities after deployment and in the background regularly. This means scans are initiated automatically and only alert if something critical is found, making sure any severe security bugs found in production are remediated as soon as possible.

Ethical hackers

You may never be able to hire them for a full-time position, but they can still play a key role in protecting your web application.
Here’s how companies welcome ethical hackers in to help check security in a safe and legal way.

Responsible Disclosure Policy

First step is to open the door to ethical hackers. Set up a policy that defines what applications are available for security testing and the types of vulnerabilities in scope so hackers understand where the boundaries are before they run the risk of legal action. Hackers report out of good will with expectation for a reward. A public mention like on an online “hall of fame” is appreciated.

Bug Bounty Programs

Bug bounties are essentially responsible disclosure programs that reward ethical hackers for reporting vulnerabilities. The rewards can be anything from t-shirts and stickers to payouts adding up to thousands of dollars.

Automated Security Powered by Hacker Knowledge

With responsible disclosure and bug bounty programs, companies can only remediate one vulnerability at a time. Detectify collaborates with Crowdsource ethical hackers to build up an always up-to-date testbed that helps every user start checking for the latest web vulnerabilities in as fast as 25-minutes from hacker-to-scanner.

It takes more than one security tool to keep web applications secure against vulnerabilities

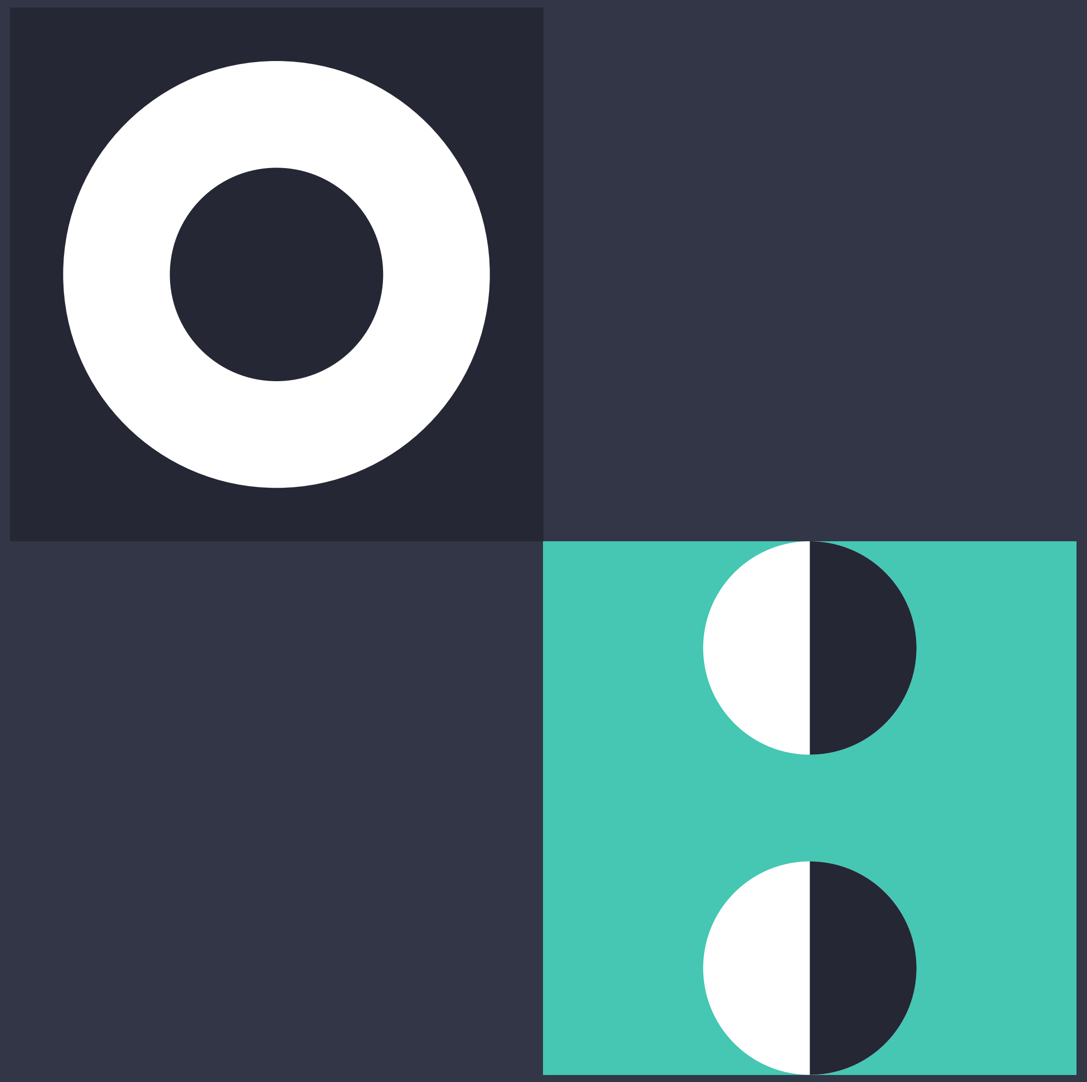
DAST is no silver bullet for the application security of live products. It can complement and even maximize the value you can get out of adjacent appsec options: pentesting and hosting bug bounty programs. The reality of today's security toolbox is having a lot of services that specialize, leveraging their strengths results in a broad and practical approach to security.

Take a look at how these tools work together.

JOHANNA YDERGÅRD
VP PRODUCT DETECTIFY

“Security testing has traditionally been driven by annual compliance audits, but the rapid changes in web security require a new approach.“

Automation and manual pentesting go hand-in-hand



Performed by skilled security experts who try to compromise a web application, in-depth manual pentests help discover vulnerabilities and identify complex attack vectors. However, the amount of code pushed live every day poses a challenge as it is increasingly difficult for security teams to keep track of the latest threats.

This is where automated security testing comes in. Running against a web application on a regular basis, automated testing tools are continuously updated with new security tests. With the help of automation, vulnerabilities can be discovered before new code is pushed to production.

The benefits of combining manual pentesting & automated security testing

Maximise the value of manual penetration testing

Security issues are fixed by the development team before new code is deployed to production, allowing pentesters to focus on more complex attack vectors.

Increase the frequency of tests and extend their coverage

With the help of automation, developers can identify and remediate security issues quickly and effectively. Emerging threats are constantly addressed throughout the development cycle, keeping the web application safe in between manual penetration tests with scheduled scans.

Improve security knowledge inside the organisation

Knowledge is spread across the development team instead of being limited to a security team or external security experts. This way, security becomes a core value and a natural part of the development process that is considered from the very first line of code.

Manual pentesting

- In depth pentesting
- Performed by security experts, often working as external consultants
- Not integrated into the developtment process
- Driven by compliance

Continuous application security testing pentesting

- Regular security testing using a fully automated and up-to-date service
- Increased knowledge across the organisation
- Modern, educational and fun UI
- Complementing compliance and supporting teams' security work

Learn how Detectify complements annual penetration audits and helps you get more visibility into your tech stack at detectify.com

Bug bounty programs and automated security scanning are two growing areas in cybersecurity

Get the best of both options

Many have already heard of a bug bounty program or automated web security, and may even be running it as part of their security strategy. A bug bounty program invites ethical hackers to report security vulnerabilities on their websites in exchange for a reward, which is often monetary.

Automated scanners like Detectify are effective at doing a scheduled wide sweep across your web applications to check for common vulnerabilities.

At Detectify, the security tests built into our scanner are sourced from our internal team and Detectify Crowdsource network of 200+ white hat hackers. These two layers of security complement one another and leverage crowdsourced knowledge to provide improved coverage.

We've highlighted a few advantages of combining bug bounty programs and automated security testing.

Learn how Detectify works with ethical hackers in our Crowdsource to help companies with a more resilient security strategy.
View more about Crowdsource.

3 benefits of combining bug bounty programs with automated security testing

1. Maximize the value of your bug bounty program

Automated scanners effectively scan web apps for a wide scope of vulnerabilities such as OWASP Top 10, path traversals and subdomains vulnerable to takeover. Bug bounty programs can then focus on creative and logical bugs.

2. Continuous coverage

Bug bounty programs have become a great asset to security teams to tailor to their needs. Vulnerabilities may come during organized events (eg. Bugcrowd or Hackerone) or throughout the year with ongoing vulnerability disclosure programs.

It's best practice to run automated scans on web applications weekly in between bug bounty events. Constant coverage catches common flaws which may be easily queued into JIRA or another tool.

3. Encourage security awareness within the organization

Knowledge is spread across the development team instead of being limited to a security team or external security experts. Security becomes a core value and a natural part of the development process that is considered from the very first line of code.

Bug bounty program pentesting

- Many ethical hackers testing your system at once
- Bug chaining done by humans that could never be automated by any scanner
- Build connections with the hacking community
- Pay per bug found and severity level

Automated security testing

- Regular security testing using a fully automated and up-to-date service
- Wide scope of vulnerability search including OWASP Top 10, AWS S3 Bucket misconfigurations, CORS and DMARC-records
- Transparency of vulnerabilities found and remediation tips
- Subscription based with unlimited scans for a fixed rate

Learn how Detectify works with ethical hackers in our Crowdsource to help companies with a more resilient security strategy. View more about Crowdsource.

How does Detectify complement pentesting and bug bounty programs?

Stay at the forefront of security

When a vulnerability submitted by a Detectify Crowdsource ethical hacker has been validated by our engineering team, we build it into our tool right away, making it available to all our customers at once.

This ensures that knowledge is shared with our entire customer base. We update our tool bi-weekly, keeping all our customers at the forefront of security.

Scanning with an adjustable scope

With Detectify, you can continuously scan your entire domain or on a specific path or subdomain.

- Scan begin login or with recorded behaviors
- Reduce redundancies of known bugs reported
- Set your bug bounty scope to go after things not in the scope of the Detectify tool, often more complex bugs found deeper in a system.

Vulnerabilities detected can be shared with developers

Developers are the rockstars when it comes to fixing bugs. When critical vulnerabilities are found, the information is quickly dispatched to the application owner via JIRA or other popular developer tools for frictionless prioritization.

The alert includes guidance on where to find the code error, explanation of each bug and remediation tips.

False Negatives found can be built in

If your bug bounty program finds a False Negative, we can build in a security test to the scanner using the Proof of Concept provided by the bug bounty hunters.

Your scanner will then be set to monitor for the vulnerability going forward.

What our customers say about us

Easy to use

Detectify's simple to use interface, integrations with popular developer tools, team functionality, and informative reports make it easier for you and your team to work with security.

Always up-to-date

To deliver the most up to date and relevant security tests to clients, we have extended our team with external ethical hackers through Detectify Crowdsource, our crowdsourcing platform.

This enables us to challenge the hacker community to identify new vulnerabilities which we build into our service, covering a wide range of technologies.

Frictionless security into your workflows

Whether you work with vendor management, dev ops, development, or security, Detectify helps you integrate security into your workflow.

- Detectify's extensive knowledge base with code examples helps your team learn about security and write safer code.
- Set up your staging environment using Detectify and ngrok.
- Fix security issues before deploying new code to production.
- Detectify integrates with tools like JIRA, Slack, splunk and Zapier, making it easier to track your website's security status
- New tests are added to the scanner on a continuous basis

Security toolbox comparison

Detectify web app scanner	Bug bounty programs	Manual pentesting
Focused application security testing using fully automated and up-to-date testbed	Many ethical hackers testing your system at once. Year-round open program or special events.	In-depth penetration testing of both physical, network and digital assets.
Wide-scope detection including OWASP Top 10, DMARC-records and common misconfigurations (S3 buckets, middleware, CORS, etc)	Bug chaining done by humans that could never be automated by any scanner	Performed by security experts, often working as external consultants
Transparency of vulnerabilities found with proof of concept intended for frictionless remediation by application owners.	Triagers or security team build connections with the hacking community.	Findings are summarized in a comprehensive document to CISO / main point of contact for the pentesters.
Modern, educational and delightful UI, with integrations to popular developer tools or API.	Reports are sent to program's triagers before sent to the vulnerability management workflows	Reports are not integrated into the development process for easy remediation.
Subscription based with unlimited number of scans throughout the web application layer.	Pay per bug found and severity level, depending on the defined scope, often focused on one application.	Pay per audit without guarantee of how far testing will go into your assets.
Recommended to run this continuously throughout the year to help catch known and active automated exploits	Recommended to run this several times a year or in combination with Detectify or other automated scanners to catch more complex and creative bugs.	Run at least once a year. This should catch vulnerabilities (physical or digital) that can't be detected by automated security solutions or bug bounty programs.

Checklist for application security in 2021

Speed

□ Build automated tests to detect newly listed CVEs or known vulnerabilities within 1 hour of detection

□ Act on critical and high-severity vulnerabilities in production as soon as they're verified

□ Security vulnerabilities are remediated with minimal application down-time

Scale

□ Security present throughout the lifecycle, including continuous monitoring in production

□ Application owners can remediate security bugs with information in reports without need for extensive research

□ Continuous security testing in production including legacy code

□ Check applications for vulnerabilities as soon as they're deployed

Collaboration

□ Responsible disclosure policy to access ethical hacker help

□ Access to informative proof-of-concepts with the actual payload or proof of impact for easier prioritization and less false positives

□ Security knowledge that enables development, not block it

□ Detailed vulnerability reports with remediation tips for frictionless remediation by application owners

Harden and scale-up your application security for more visibility in 2021 with Detectify. Explore what it means to have speed, scale and collaboration with a free trial, or book a demo with one of our security experts today. Go to detectify.com to learn more.

A GUIDE TO MODERN WEB APPLICATION SECURITY

go hack yourself.