NeuraLegion

Creating & Implementing a Modern-day DAST Solution

INTRODUCTION

Over the past decade, Software Development has transformed, with more and more organizations adopting DevOps practices due to the significant advantages they offer, including:

- **Ability to deliver faster**
- **Reduce the time it takes to fix issues**
- **Deploy with fewer bugs**
- **Reduce development cost**

Advantages of DevOps Practices

While DevOps provides considerable value, as more organizations adopt these practices, they are encountering a significant challenge with security vulnerabilities. We all read, and hear about these challenges daily in the publications about organizations being hacked and impacted.
Organizations are experiencing these problems are due to the fact that Application Security solutions and processes have not kept up with DevOps practices. Many providers speak about DevSecOps, but in reality the solutions in the space were developed for Application Security professionals and are not purpose-built for modern-development practices. These shortcomings are especially apparent in legacy DAST solutions which at a high-level fall short in the following areas:

- **They have not kept up with modern dev practices so fall short in coverage**
- **Not effective in identifying API vulnerabilities**
- **Designed for AppSec professional and not easy for developers to adopt**
- **Inability to scan authenticated APIs & Web Apps**
- **Take too long to run in a DevOps SDLC**
- **Are wrat with false-positives**
- **Are not native SaaS solutions**

Legacy DAST solutions fall short in a modern dev environment

NeuraLegion's solutions are built from the ground up for the modern development environment and intended to be a core building block of DevSecOps. This white paper discusses the various factors that are critical to building a modern DAST solution.

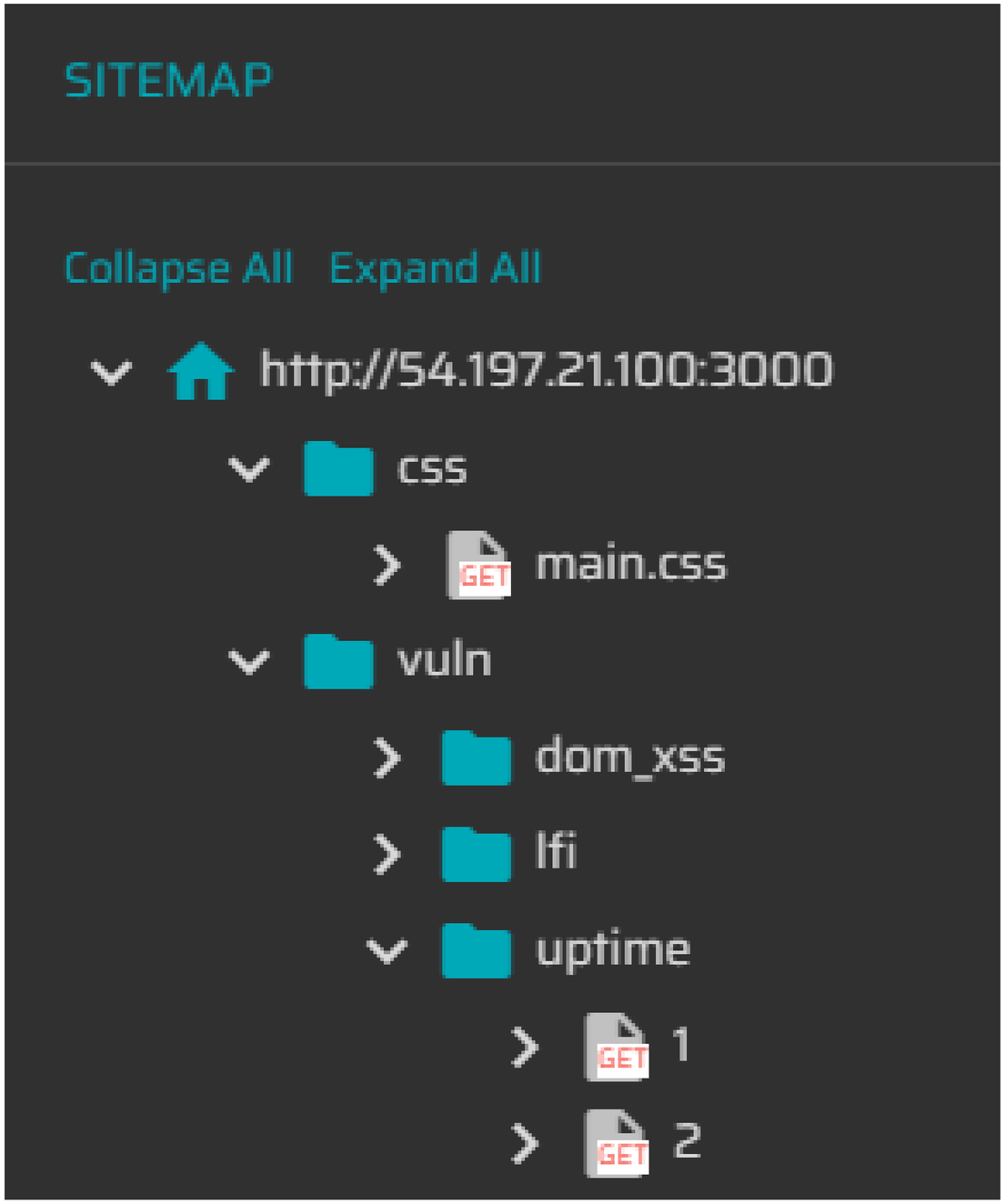
DEPTH OF COVERAGE / ANALYSIS

Coverage is the first critical element for creating the best DAST solution. As the old saying goes “You can’t find what you can’t see”. In order to be able to identify vulnerabilities you have to be able to very effectively analyze and identify the attack surface. This includes the attack surface for Websites, WebApps & various API formats.
In order to create a comprehensive map of the targets, it is not enough to crawl the target. A modern DAST solution has to interact with the target and discover all the entry points and parameters. This includes:

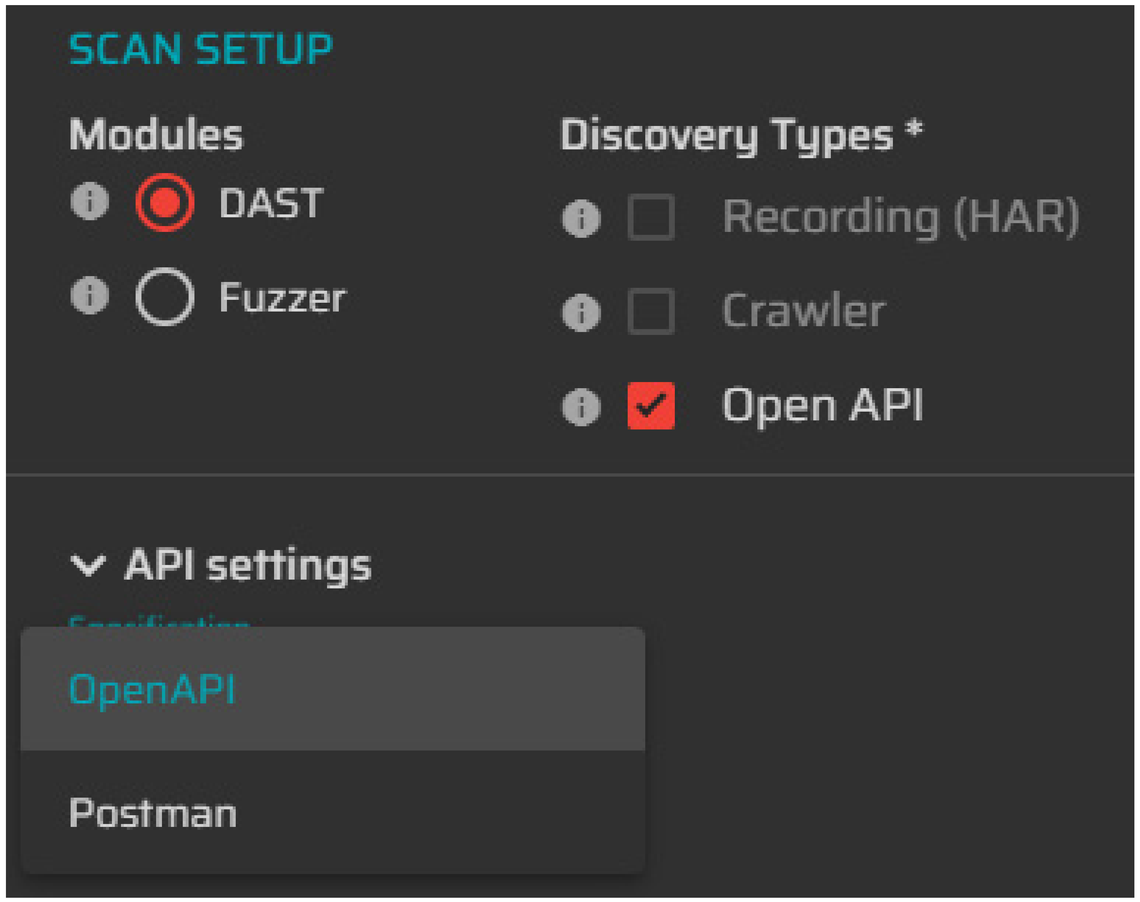
- **Effectively scanning authenticated sites and APIs**
- **Interacting with Single Page Applications (SPAs) by using browser automation to capture client-side events, secondary requests, etc.**
- **Effectively discovering APIs including REST, GraphQL & SOAP APIs by capturing API requests while crawling or directly via API schemas**
- **Easily deploy and scan in a Micro-services environment**
- **Fully parsing complex types such as JSON, XML, etc. regardless of depth, encoding or location in the request data**
- **Analyzing parameter data-types to provide context and improve attack efficiency**

In order to provide the best coverage you need to interact with the targets, expand menus etc.

NeuraLegion's unique sitemap visualization enables you to see all the paths that were detected to insure the broadest coverage possible and to make sure nothing is missed:



Specifically for API coverage, you should not only be able to point the scanner at the API. You should also have the ability to upload Swagger files where these exist, or point us at Postman collections to automate the scan and make sure it is much faster and more comprehensive.



IDENTIFYING VULNERABILITIES (PAYLOADS)

After you effectively map the targets and unearth all the paths where vulnerabilities could exist you need to scan for all the types of vulnerabilities that could exist. NeuraLegion uniquely offers a combination of DAST & Fuzzer to provide the broadest and fastest expanding set of payloads. There are a number of underlying capabilities that enable this:

» As a SaaS solution we can quickly add vulnerabilities to the list of vulnerabilities we scan for
» 0-day vulnerabilities identified by the Fuzzer are uniquely added to the DAST solution
» Vulnerabilities identified by Pen-testing partners are added to the DAST solution
» The DevSec team is constantly looking for vulnerabilities and adding them

In addition to all the capabilities above, NeuraLegion is the only solution that provides the ability to detect not only technical vulnerabilities, but also Business Logic vulnerabilities. Among other vulnerabilities, the following vulnerabilities are included:

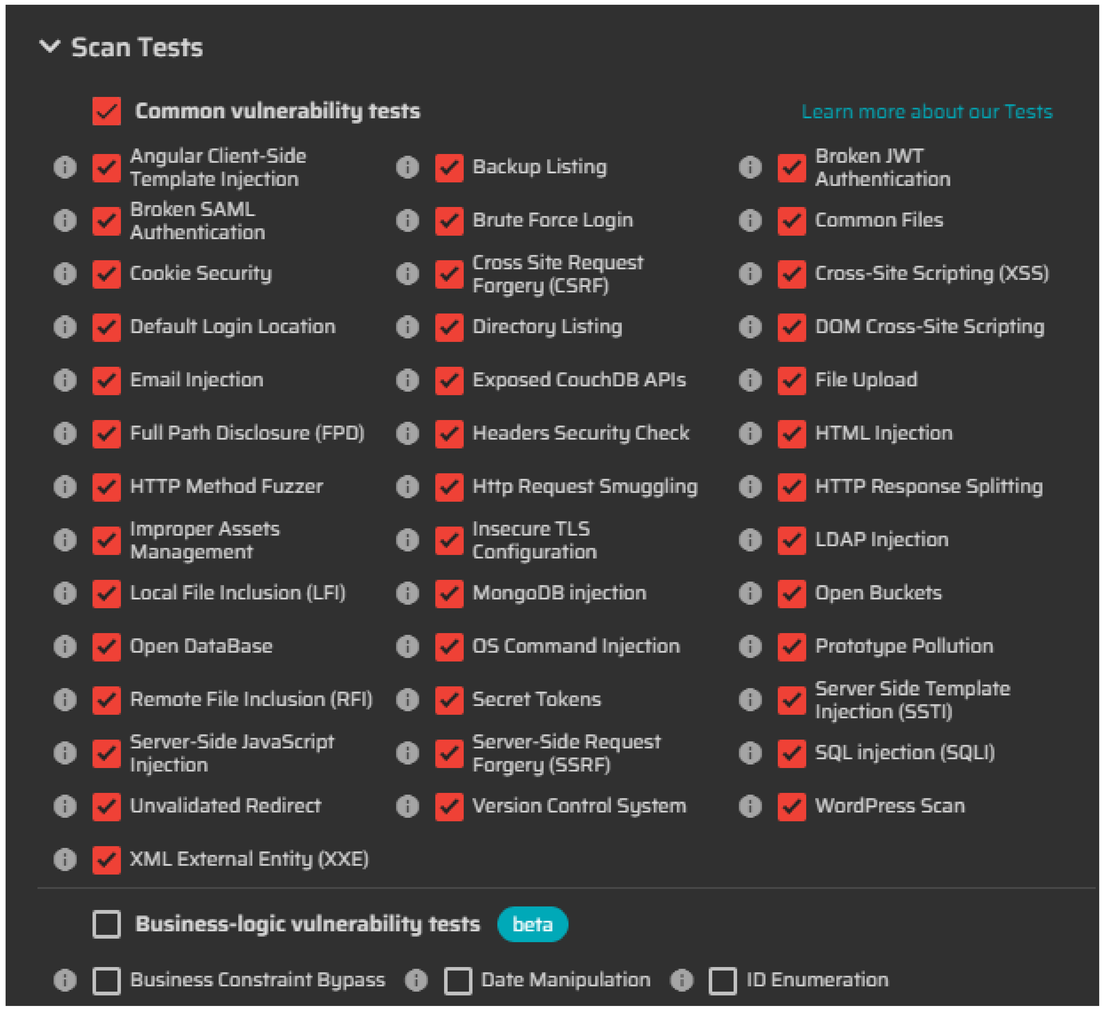
» Business Constraint Bypass
» Date manipulation
» ID Enumeration
» Mass Assignment

To identify a complete list of vulnerabilities you have to extend beyond technical vulnerabilities and identify Business Logic Vulnerabilities.

"The NexDAST technology was simple to deploy and integrate into our customer engagements and began showing immediate value. NexDAST has reduced the amount of wall clock hours AND man hours we used to spend doing preliminary scans on applications by about 70%. If you're doing appsec, and doing a lot of it, you need to look at NexDAST."

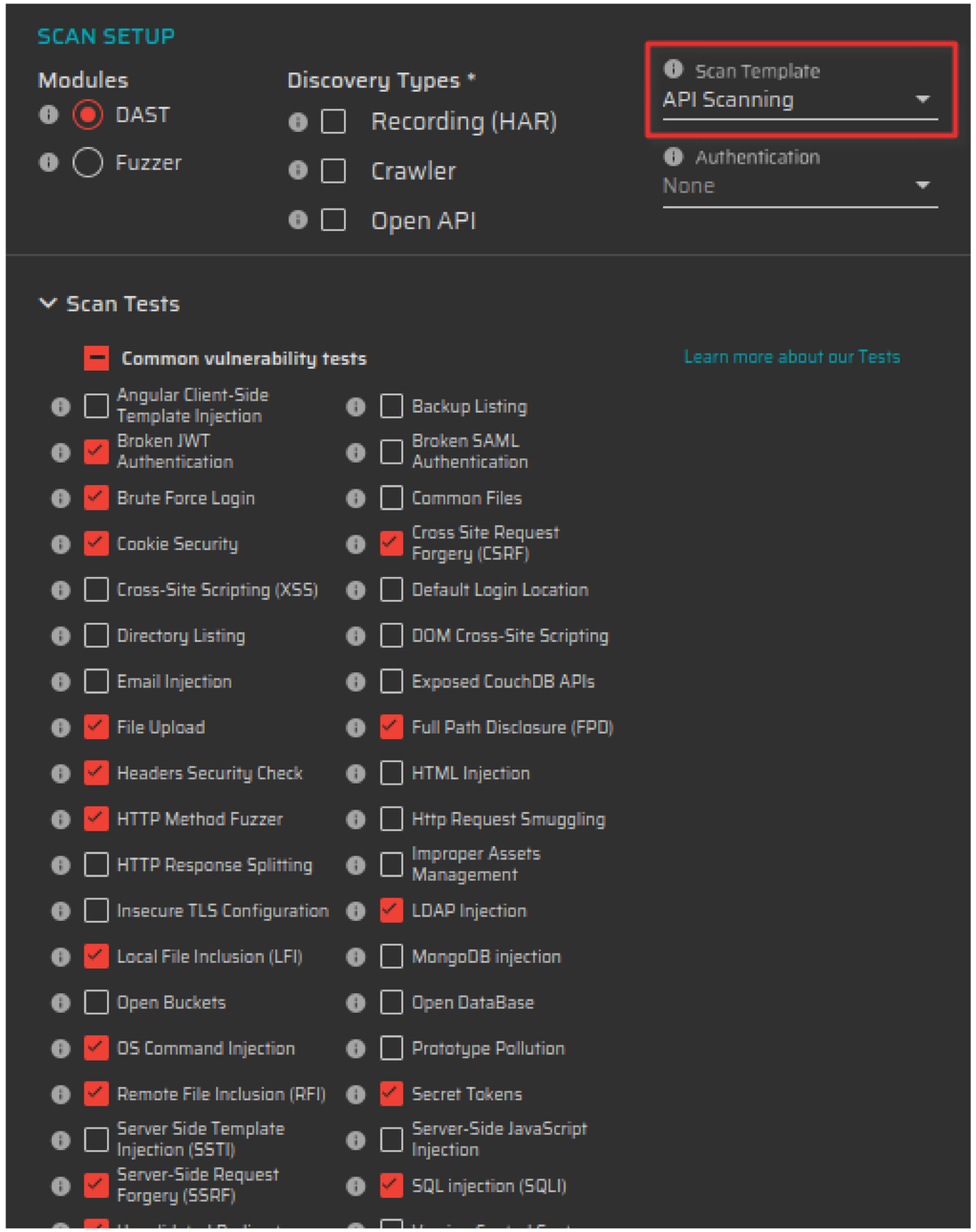
Bobby Kuzma, CISSP Practice Director, Security Assessment & Testing, Herjavec Group

The screenshot below shows a sample of the vulnerability types that we test for with a comprehensive scan:



In addition to having a broad set of payloads, a modern DAST solution needs to be optimized for API scans and enable you to select an API focused scanning template which will automatically only scan for vulnerabilities that are relevant for APIs.

See example of an API focused scan here:

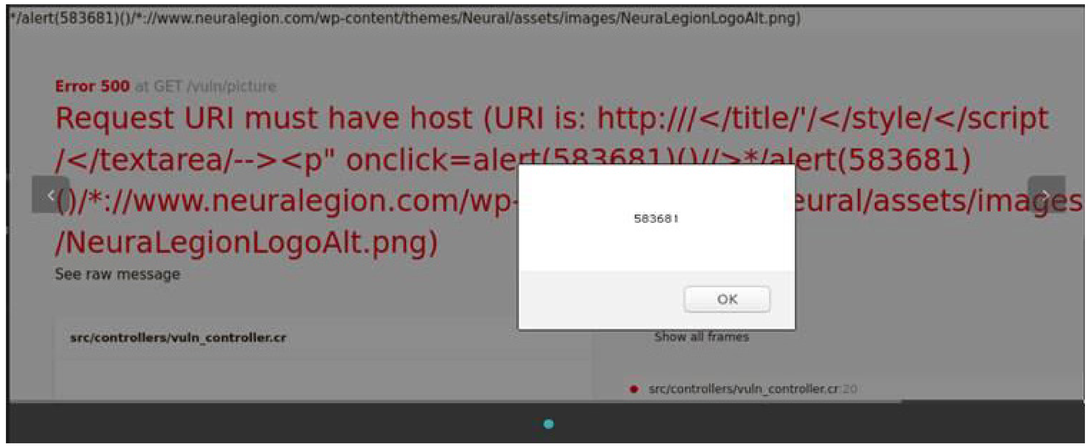


USABILITY / ADOPTION

As the speed of development and deployment accelerates it is crucial that multiple personas in the organization use the DAST solution and benefit from it. It is no longer viable to have the AppSec, or internal and external Pen-testing teams to be solely in charge of identifying vulnerabilities. Developers and QA professionals have to be able to adopt the solutions as well as part of their SDLC.
Each type of user should have the interface they are most comfortable with. NeuraLegion enables AppSec and Pen Testing professionals utilize the intuitive web application while developers can also use the solution via a CLI interface, API, and as part of their CI configuration files (such as .yaml). These capabilities enable security testing as a seamless part of their CI/CD process. NeuraLegion also enables developers by supporting SCM webhooks, such as GitHub Actions, to tie NexDAST scans into the developer's daily actions by triggering scans on specific, defined actions such as Merge to Master, Pull Request, etc.

Solution Built for developers:

Our solutions were built from the ground up to enable both developers & AppSec teams to use them seamlessly. NeuraLegion uses browser automation to validate every vulnerability & eliminate the need for security professionals to review a long list of false positives means that developers are willing to adopt our solutions as they know that vulnerabilities are real. In addition, wherever possible, we provide proof of exploitation (without actually exploiting the vulnerability so we are safe to run in a production environment). As an example in the case of XSS we provide a screenshot showing the vulnerability:



Or in the case of SQLi we provide the names of the tables as proof of potential exploitation. Obviously none of the actual data is accessed as we maintain strict confidentiality measures.
In addition to providing proof of vulnerability, it is also important to provide remediation guidelines for every issue so developers know how the issue can be fixed and they can solve it quickly.
After a problem was fixed by the developer, it is easy to quickly validate the fix by using our "Issue tester" from a specific finding.

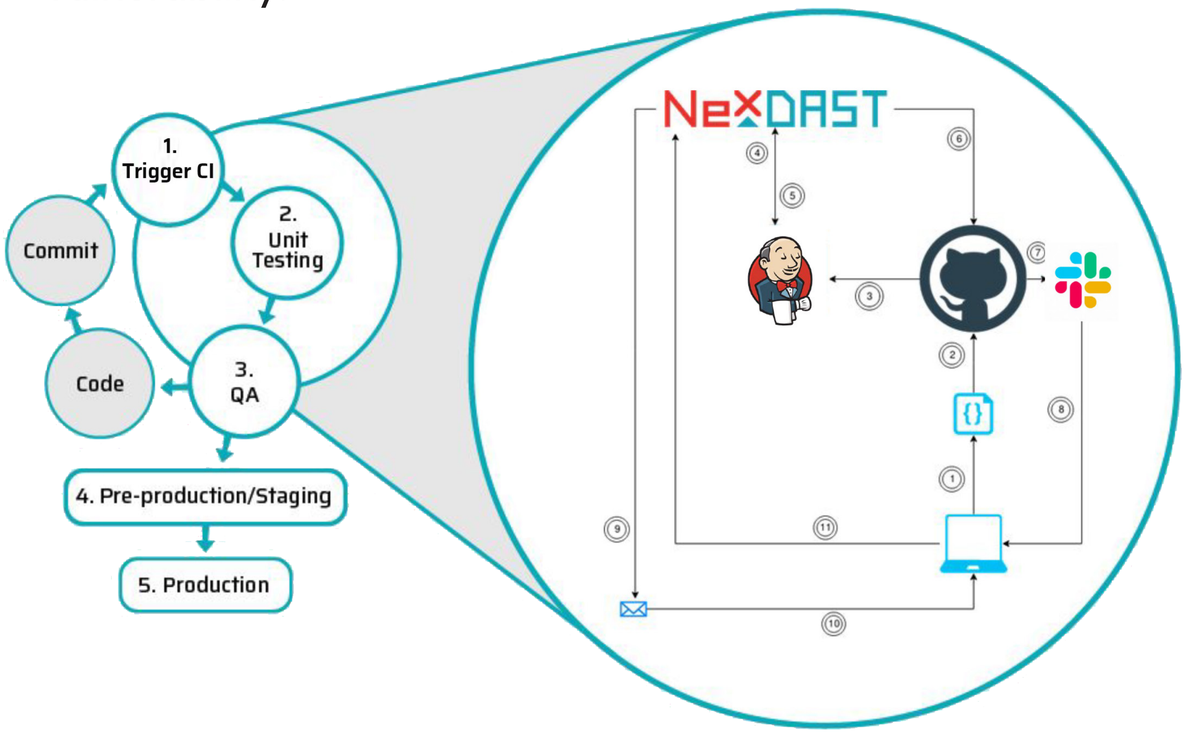
Automation:

A key driver for adoption is automation. NeuraLegion offers a solution that automatically integrates into the CI/CD to make sure scans can be run as part of the process and not delay it. We offer the only solution that can ingest HAR / SWAGGER files and run focused scans instead of using a crawler that will take hours, or days to run. We can run in minutes and not delay the process. This uniquely enables organizations to scan for vulnerabilities much earlier in the development process (Shift Left) and scan on every build, or merge to master instead of waiting for pre-production, or production.

Our focus on integration and automation means that nothing needs to be done manually when using our solutions. For developers (and AppSec) scans can be automated using integration and scan templates. For developers, tickets are automatically opened in your development environment and all the information is provided within your ticketing systems. This means developers never have to leave their dev environment and they are happy.

No-False Positives:

Do you have alert fatigue (too many false positives) resulting in a lot of wasted time & money trying to figure out which vulnerabilities are real and which are false positives? This is a very common problem with AppSec solutions. NeuraLegion has integrated browser automation into our solutions which means that we validate that every vulnerability found can actually be exploited before it is reported. This results in THE ONLY no-false positives solution in the market. We automatically validate each vulnerability.



Azure DevOps · Jenkins · circleci · Travis CI · Jira · slack · GitHub · servicenow · JFrog · OPEN API · AND OTHERS...

SPEED

In order to truly achieve DevSecOps, your DAST solution needs to run at the speed of DevOps.

This means you need to have the ability to run scans in minutes and not hours or days.
To enable this, NeuraLegion enables a number of underlying capabilities including:

- **Automatically ingesting HAR / Swagger files that were created as part of unit testing, or QA Automation to limit the scope of the the scope of scans**
- **Ability to set and run predefined profiles for fast scans**
- **Run parallel scans using multiple scans to break up a large scan**
- **Analysis of parameter types provides our engine with a unique ability to skip irrelevant test for certain scenarios, saving a lot of time.**
- **The ability to automatically eliminate false-positives as part of every scan means that no manual validation is required resulting in an overall faster process from scan to remediation**

TCO

In addition to implementing the best solution, it is important to make sure the Total Cost of Ownership of the solution is low. NeuraLegion's SaaS solution ensures there are no hidden costs for HW, add-on services, or any other hidden costs. The all-in-one pricing means you don't pay separately for support and you are not charged exuberant costs for manual false-positive validation.
The ability to scale our instances as required offers the most cost effective solution on the market.

"NexDAST provided us exactly what we needed. Automated testing on our pre-production environment allows us to find complex issues without human interaction, ensuring our compliance validation is up to the highest standards. NexDAST produces actionable results that immediately flow to developers in their native development environment, saving us a lot of development time and resources."

TEL AVIV STOCK EXCHANGE

Gil Shua, Information Security Specialist and Manager, Tel Aviv Stock Exchange

SUMMARY

NeuraLegion's vision "Application Security From Build to Compliance" is is a vision we work to fulfill every day. We constantly strive to provide the most comprehensive solution that is fully automated and enables our partners to run thousands of scans by developers, QA and AppSec professionals. This vision does not end with technical vulnerabilities. We believe that in-order to provide compliance on every build we need to help identify Business Logic vulnerabilities as well and we are investing significant resources to add Business Logic vulnerabilities as part of our automated payloads. This results in the ability to automate an even larger part of what can today only be tested by manual pen-testing.
Today, >50% of the product capabilities we add come from customer requirements. We are very committed to the highest level of service and providing our partners and customers with the tools they need to perform their job in the best way possible while empowering you to maintain the most secure organization.
NeuraLegion helps significantly improve application security at a lower cost by providing a no-false positive, AI powered DAST & Fuzzer solutions that are purpose built for modern development environments. We integrate into DevOps environments and enable you to run DAST scans as part of your CI/CD flows to identify a broad set of known (7,000+ payloads) and unknown (0-day) security vulnerabilities. We enable you to scan multiple protocols across Web, mobile & API and are built for developers to provide compliance on every build by providing remediation guidelines for every vulnerability identified.