Bright

snyk

SNYK AND BRIGHT INTEGRATION

Shift Left to develop and validate vulnerability-free code earlier in the SDLC

About Bright

Bright enables organizations to ship secure Applications and APIs at the speed of business by enabling quick and iterative scans to identify true and critical security vulnerabilities without compromising on quality or software delivery speeds. Bright's dev-centric DAST scanner empowers AppSec and development teams to shift AppSec testing left and scan for vulnerabilities early on in the SDLC.

> *"Our partnership is closely aligned with our mission to shift AppSec testing left and empower Developers to do more, while easing the resource pressures on AppSec teams"*
>
> **Gadi Bashvitz**
> CEO of Bright Security

> *"Our latest partnership with Bright will help us continue our mission to empower developers all over the world with dev-first security by offering our mutual customers the ability to integrate Snyk into existing workflows, tools and processes while helping Bright Security accelerate their move to DevSecOps."*
>
> **Jill Wilkins,**
> Senior Director Global Alliances, Snyk

WHY SNYK AND BRIGHT

By combining Snyk and Bright, organizations can benefit from the following advantages:

Comprehensive Coverage:

By combining Snyk and Bright, a wider range of security vulnerabilities can be detected earlier, providing more comprehensive coverage.

Early Detection:

Both Snyk and Bright identify security vulnerabilities during the development phase before the application is deployed.

Validation and Reduction of False Positives:

Bright can help validate, confirm and report on the existence of vulnerabilities identified by Snyk by interacting with the running application. This reduces false-positives and enhances the overall accuracy of vulnerability findings.

Real-World Simulation:

Bright provides a real-world simulation of how an application might be attacked, allowing organizations to understand and address vulnerabilities that are only detectable in runtime scenarios. Bright captures issues related to authentication, session management, access controls, or vulnerabilities specific to the application's environment.

Continuous Testing:

Combining Snyk and Bright in a continuous integration and continuous delivery (CI/CD) pipeline enables organizations to perform security testing earlier in the software development lifecycle.

How It Works

Bright provides the Issue Linker function that provides a correlated list of only validated issues that were found by Snyk SAST (Code) and by Bright's DAST solution.

Issue Linker compares the Snyk SAST's issues with Bright's scan issues and presents it to developers/ AppSec teams in a clear and easy to understand format.

Issue name	CWE	Snyk Unique ID	Bright Unique ID
Cross-site Scripting (XSS)	CWE-79	ID#b7dae	ID#cHmgT
Cross-site Scripting (XSS)	CWE-79	ID#063a7	ID#trNW9
Server-Side Request Forgery (SSRF)	CWE-918	ID#3909e	ID#2CiaW
Server-Side Request Forgery (SSRF)	CWE-918	ID#876d0	ID#2JEsN
Command Iniection	CWE-78	ID#70163	ID#gGnbb
SOL Iniection	CWE-89	ID#a06e7	ID#myayD
Cross-site Scripting (XSS)	CWE-79	ID#5dac6	ID#n5n5V
XML External Entity (XXE) Injection	CWE-611	ID#ff85e	ID#qQMxU
Open Redirect	CWE-601	ID#63665	ID#1dD8h

Correlation between Snyk and Bright results in faster MTTR earlier in the SDLC and a higher return on investment (ROI) on software security investments.

Additional Features and Benefits:

- Single CLI command for issue validation and verification
- Consistent and reliable issue tracking
- Elimination of duplicate or irrelevant issues
- Output in JSON format for automation and seamless integration

Need more information: shanni.gelfand@brightsec.com +1 (415) 980-5549