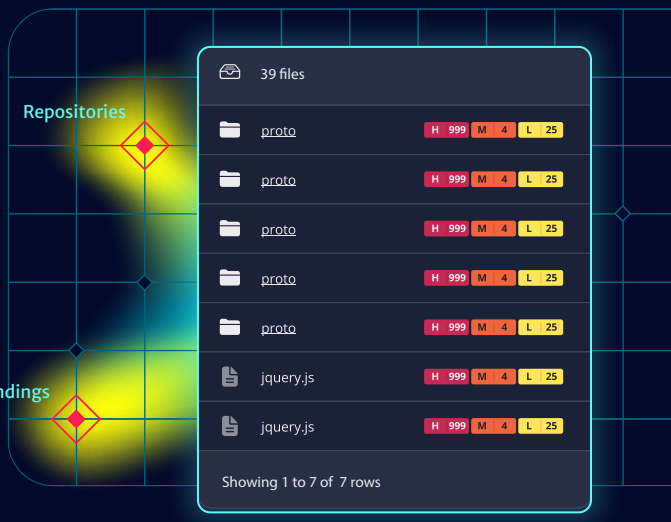
Lightspin

Infrastructure as Code (IaC) Security



Secure your cloud infrastructure prior to deployment

Scan your Infrastructure as Code (IaC) files and identify security risks and infrastructure misconfigurations before deploying them to production.

The State of the Market

IaC technology is growing quickly and provides the opportunity to detect and fix issues before they are deployed to the cloud. While this technology is being leveraged by many companies, there are challenges in the proper implementation of the "shift left" security approach and scanning IaC files to ensure security along the development cycle.

33%

of those within the highest level of security integration, still feel that security is a major constraint on the ability to deliver software quickly[1]

Over 3/4

of the security team continue to think devs find too few bugs too late in the process[2]

37%

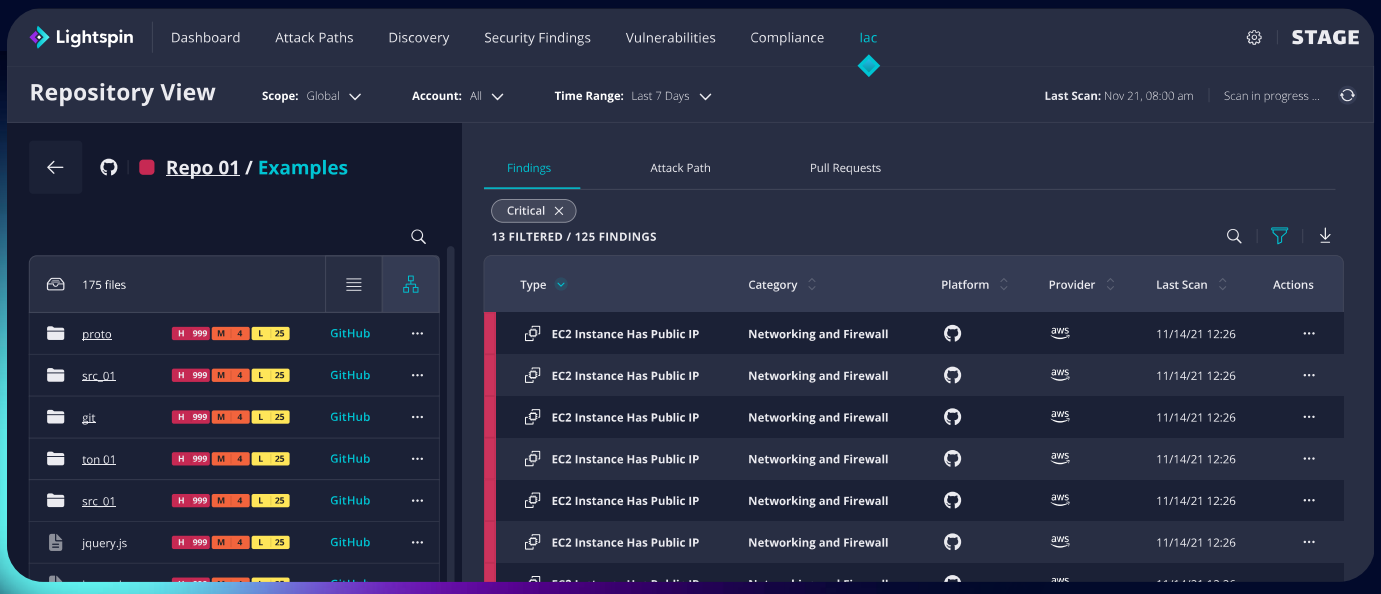
of users don't implement any sort of security testing during CI[3]

Challenges

- **Cloud-based breaches are costly and result in millions of dollars of loss to an organization.** Most organizations leverage legacy cloud security posture management (CSPM) which are limited by their ability to detect security issues only post-deployment.
- **Difficulties in bridging the gap between SecOps and DevOps teams.** A lack of visibility and understanding between development and security functions creates gaps between the efficiency of building and securing code prior to deployment. Teams should be working in tandem, but security can often be an afterthought instead of being built-in during early stages of development.
- **Alert fatigue.** Everything that can be created, modified, and deleted in the cloud, can be created, modified, and deleted in an IaC file. Every misconfiguration, security risk, and exposed credential that is detected on the cloud can (and should) be detected in an IaC file. IaC security poses the same threat of alert fatigue as classic CSPM tools, if not done correctly.
- **Lack of context.** General IaC scans are static – looking at each resource declaration separately from others – even if in the same file – does not provide the full picture or the potential impact these files may have in conjunction with one another.

Lightspin Platform

Born on the graph, Lightspin's cloud security platform helps Security and Dev Teams eliminate critical vulnerabilities and maximize their productivity by proactively detecting all security risks and intelligently prioritizing the most critical issues.



Lightspin IaC Security Solution

Core Capabilities

Enable shifting cloud security infrastructure left. Security shouldn't be an afterthought. As cloud environments dynamically shift, and new features and assets are added, your cloud environment needs to be secure, from build to runtime.

Bridge the gap between DevOps and SecOps Teams. Provide security teams with ultimate visibility into the IaC security status in their code repository, allowing them to review any security issues, misconfigurations, and exposed credentials in their IaC files and folders – in the exact file structure as in the repository itself.

Focus on what is critical and continuously monitor changes. Lightspin aggregates the results of each file in every repository and scores each repository so you can easily understand where to begin. In addition, we analyze all pull requests to identify any new security issues that appear, so you can easily see which PRs had the biggest security impact on the repository.

Visualize your build's impact on your cloud environment. Our graph-based algorithm applies to your build and maps its potential impacts on the connected cloud environment, revealing the potential attack paths or critical vulnerabilities that may have emerged. Lightspin implements the same graph-based approach to your IaC repositories, surfacing complex attack paths prior to deployment.

"Lightspin has allowed us to simultaneously see our actual risk exposure alongside remediation guidance to resolve the most critical issues quickly and effectively."

– Yossi Yeshua, CISO

riskified

[1] https://snyk.io/wp-content/uploads/dso_2020.pdf

[2] https://about.gitlab.com/developer-survey/

[3] https://snyk.io/wp-content/uploads/dso_2020.pdf

For more information about how Lightspin can help you secure your environment from code to cloud, please visit www.lightspin.io/iac-scanning.

Lightspin