Lightspin

Protect Kubernetes with Contextual Attack Path Analysis

Challenge

Kubernetes has become increasingly popular especially within innovative organizations. But businesses that take this route may suffer from lack of knowledge and experience in Kubernetes, and specifically in its security practices. They also typically experience a significant overload of alerts, resulting from the use of first-generation workload protection and posture management security solutions.

Once the security solution sends an alert regarding a high or Critical-level security issue, the security team has to investigate the incident, estimate the risk, and approve the severity before opening a ticket. The challenge in classifying a single finding as Critical without understanding the impact may lead to an increase in the rate of false positives. Moreover, Kubernetes ecosystems are often constructed from various 3rd party open source components, which are in daily use by the environment. The implementation of these components should be based on best practices, but that's often not the case and organizations may use quick and dirty implementations that include improper configurations, secrets management, and more, which can lead to data breaches.

How Lightspin Solves it

The Lightspin AWS and Kubernetes holistic solution enables organizations to configure Lightspin with least privilege permission access to the Kubernetes Cluster and analyze the RBAC, networking, and configuration layers of the Cluster in an efficient way, which enables a reduction of risk and improves the security level of the Kubernetes environment.

At a glance

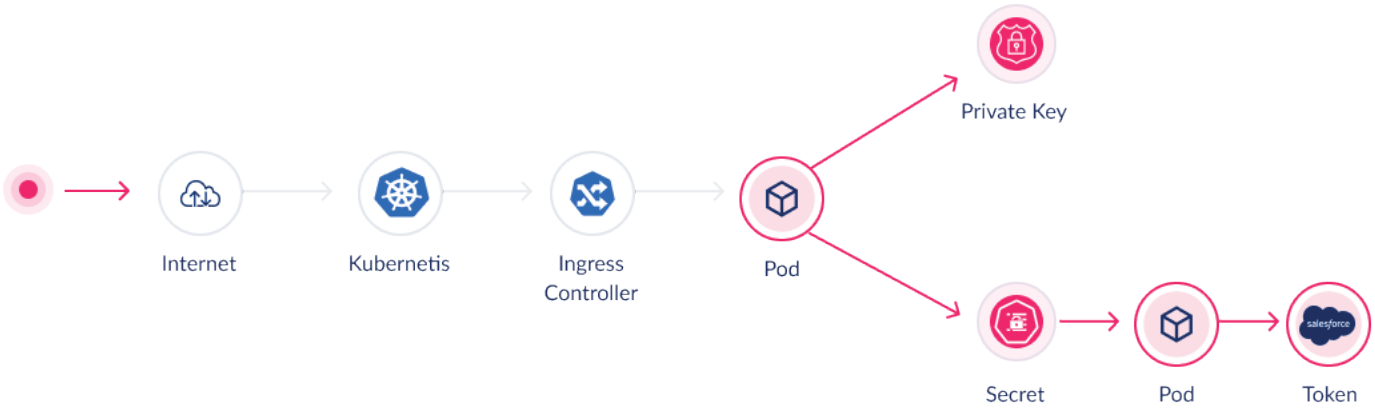
Contextual Cloud Security

Get a rapid visual assessment of your K8S environment, including assets and relationships, down to the single microservice level.

Map and display all K8S Cluster's assets.

Use the recommendation engine to quickly address K8S security issues.

Lightspin



Key Benefits

Eliminate risks to cloud assets

Our advanced predictive graph-based technology enables proactive discovery and remediation of known and unknown threats.
Whether it's a misconfiguration, weak configuration, over-permissive Kubernetes RBAC, or a CVE, we empower your team to address and eliminate all threats to your cloud stack.

Maximize productivity

Prioritization of the most critical issues means your team can focus on what matters most. Our root cause analysis dramatically reduces the number of alerts and general findings, enabling teams to address those that are most crucial.

Effective mitigation, as part as your workflow

Delivers simple instructions for mitigation of all threats. Integrates seamlessly into your existing process and toolset

About Lightspin

Lightspin's contextual cloud security platform protects native, Kubernetes, and microservices from known and unknown risks. Using predictive graph-based technology, Lightspin empowers cloud and security teams to eliminate risks by proactively blocking all attack paths while maximizing productivity by dramatically reducing and prioritizing security alerts, to cut down remediation time. For more information, visit: https://www.lightspin.io/

info@lightspin.io