Lightspin

Identifying Orphan Assets to Reduce Exposure

Challenge

According to Gartner, 99 percent of cloud security failures are the fault of the customer. Much of this is due to misconfigurations and improper permissions management. The increasing number of teams and individuals involved in cloud configurations, the high frequency of deployments, and lack of knowledge surrounding cloud security practices have led to an increase in unstructured configurations, permissions, and native services used only for single or several test purposes. But once the test is over, these assets are often forgotten and become orphans.

Asset controls, which are the rules that govern detection without using configurations, permissions, and native services, are broken within most enterprises. Due to these failing manual unstructured asset management processes and activities, enterprises cannot determine which configurations, permissions, and native services they are using. As a result, orphan configurations, permissions, and native services, increase the risk of data breach. For example, let's say the DevOps team creates a Security Group, which allows ANY to ANY traffic. This Security Group is currently not in use, but once another DevOps team mistakenly attaches the Security Group to a private EC2 instance, it will result in an exposure of the internal server to the internet.

How Lightspin Solves it

The Lightspin AWS and Kubernetes contextual security platform enables immediate identification and remediation of orphan assets.

At a glance

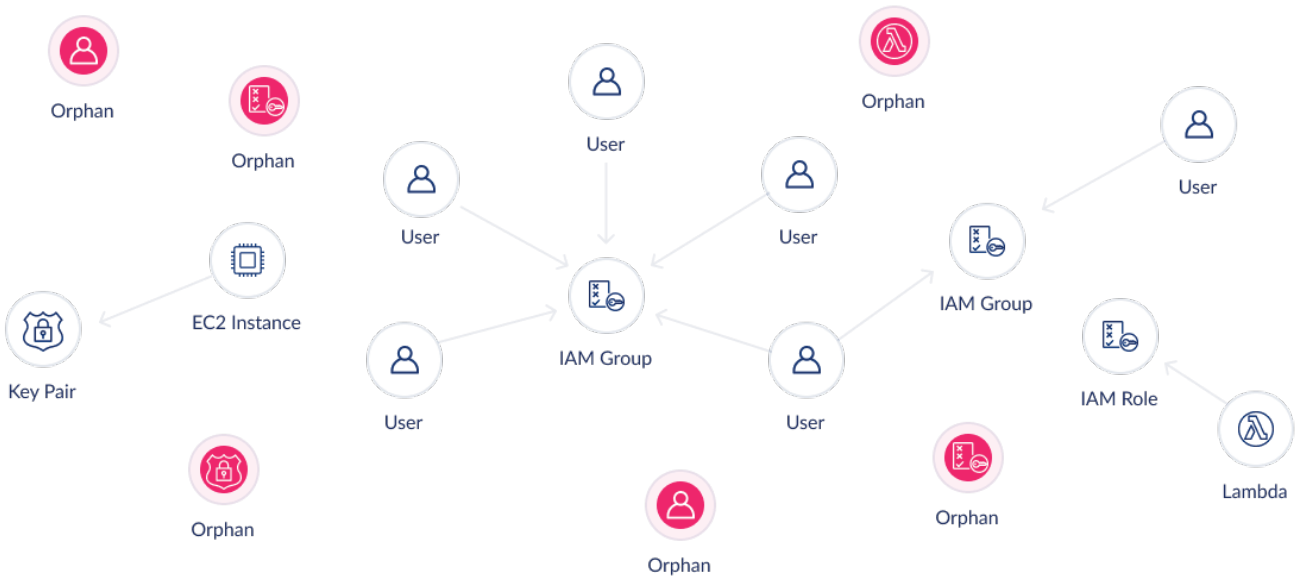
Contextual Cloud Security

Get a rapid visual assessment of your cloud environment using known cloud vendor APIs, from the infrastructure level, down to the single microservice level.

Map and display all Orphan assets in the cloud environment.

Use the recommendation engine to remove them efficiently.

Lightspin



Key Benefits

Intuitive graph-based visualization

Maps all cloud assets and relationships from the attacker's perspective to visualize your current security posture. As a result, the system displays each asset and its connections. The nodes on the graph that don't have any connections are the orphan assets.

Clear remediation plan

Delivers simple instructions for mitigation of all threats, including orphan assets. Integrates seamlessly into your existing workflow.

High accuracy – no false positives

By confirming the asset doesn't have any relationships (attached permissions, configurations, etc.), the graph visualization determines orphan assets accurately.

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