Lightspin

Detecting Multiple EC2 Instances Using the Same SSH Key Pair to Prevent Hacks

Challenge

Organizations have great difficulty measuring their actual risks when it comes to cloud security, says Gartner. And one area that is frequently miscalculated is the use of default settings.

As organizations scale, the number of EC2 instances in use increases in cloud environments, leading to challenges in managing SSH key pairs. Due to these failing manual access keys, management processes, and activities, organizations use the same keys for multiple EC2 instances. The result is that once attackers compromise one server, they can access all servers that use the same SSH key pair, similar to what took place in the massive hack to SONY Pictures.

How Lightspin Solves it

The Lightspin AWS and Kubernetes contextual security platform continuously visualizes, detects, and blocks any attack path in your cloud and Kubernetes environment and enables you to reduce the risk of multiple uses in a single key pair.

At a glance

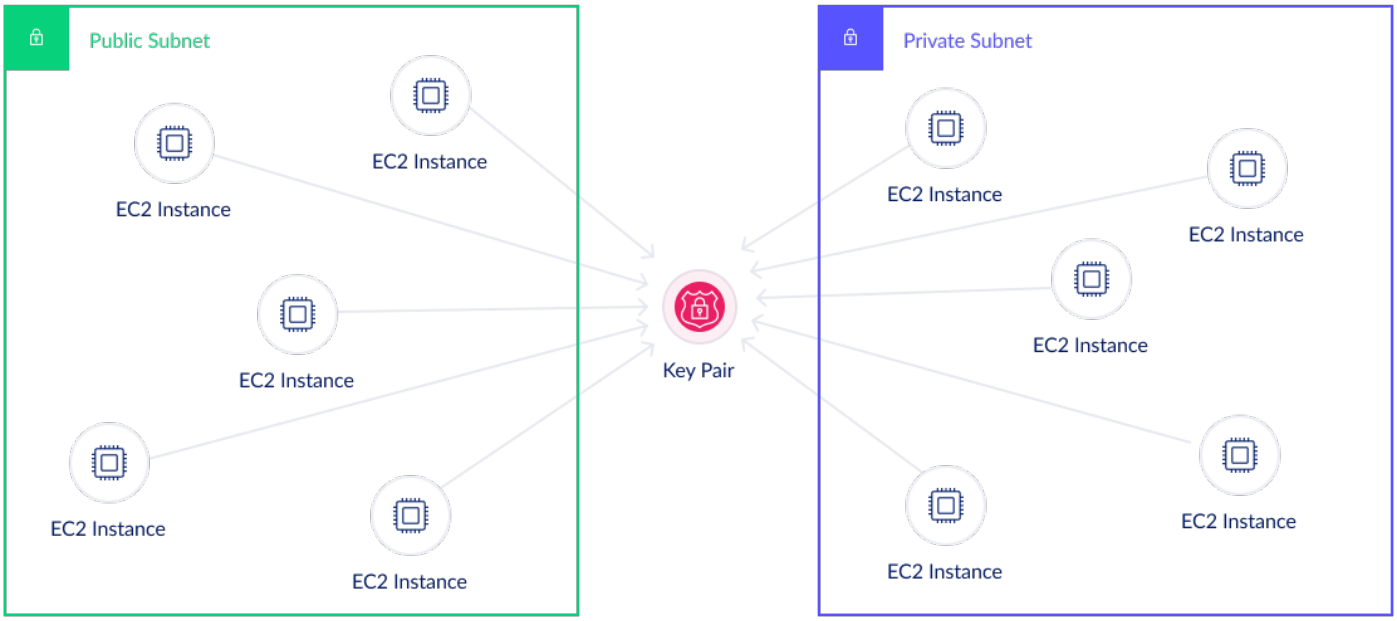
Contextual Cloud Security

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 EC2 Instances using the same SSH key pair.

Use the recommendation engine to quickly address the issue.

Lightspin



Key Benefits

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 SSH Key Pair that has been used by multiple EC2 Instances on the graph.

Clear remediation plan

Delivers simple instructions for mitigation of all threats, including shared SSH key pairs. Integrates seamlessly into your existing workflow.

Real risk and prioritization

By detecting critical attack paths that involve EC2 instances sharing the same SSH Key Pair, Lightspin's platform enables users to address the issue and detect lurking risks quickly.

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