wiz + torq

Executive summary of the integration

Integrating Torq and Wiz enables security teams to automate the remediation of cloud security issues, freeing up SOC analysts' time and giving them the ability to tend to the laundry list of low and medium issues that often go untouched. These low and medium issues still pose a threat, so creating automations for them can help avoid a security incident. With Torq and Wiz, SecOps teams can create fully automated or human-in-the-loop remediation workflows for things like expired secrets, or unused privileged access keys.

Market challenge

Torq addresses the limitations of legacy SOAR by providing a faster, more user-friendly, and AI-powered platform for automating security responses for misconfigurations identified by Wiz. This automation can improve a security team's efficiency and effectiveness in dealing with cloud security threats. Legacy SOAR struggles to automate responses to lower severity threat incidents. Torq and Wiz can create automated remediation workflows for these situations, freeing up security analysts for higher-priority threats

Benefits of the integration

- Reduce alert fatigue: Focus on fixing alerts that matter with high fidelity Wiz Issues looking at toxic combinations leading to attack paths.
- Improve security posture: Gain deep visibility into risk across cloud with Wiz and automate remediation and threat response for known risks with Torq.
- Operationalize security: Trigger Torq automation response workflows based on Wiz Issues that are critical to your business operations.

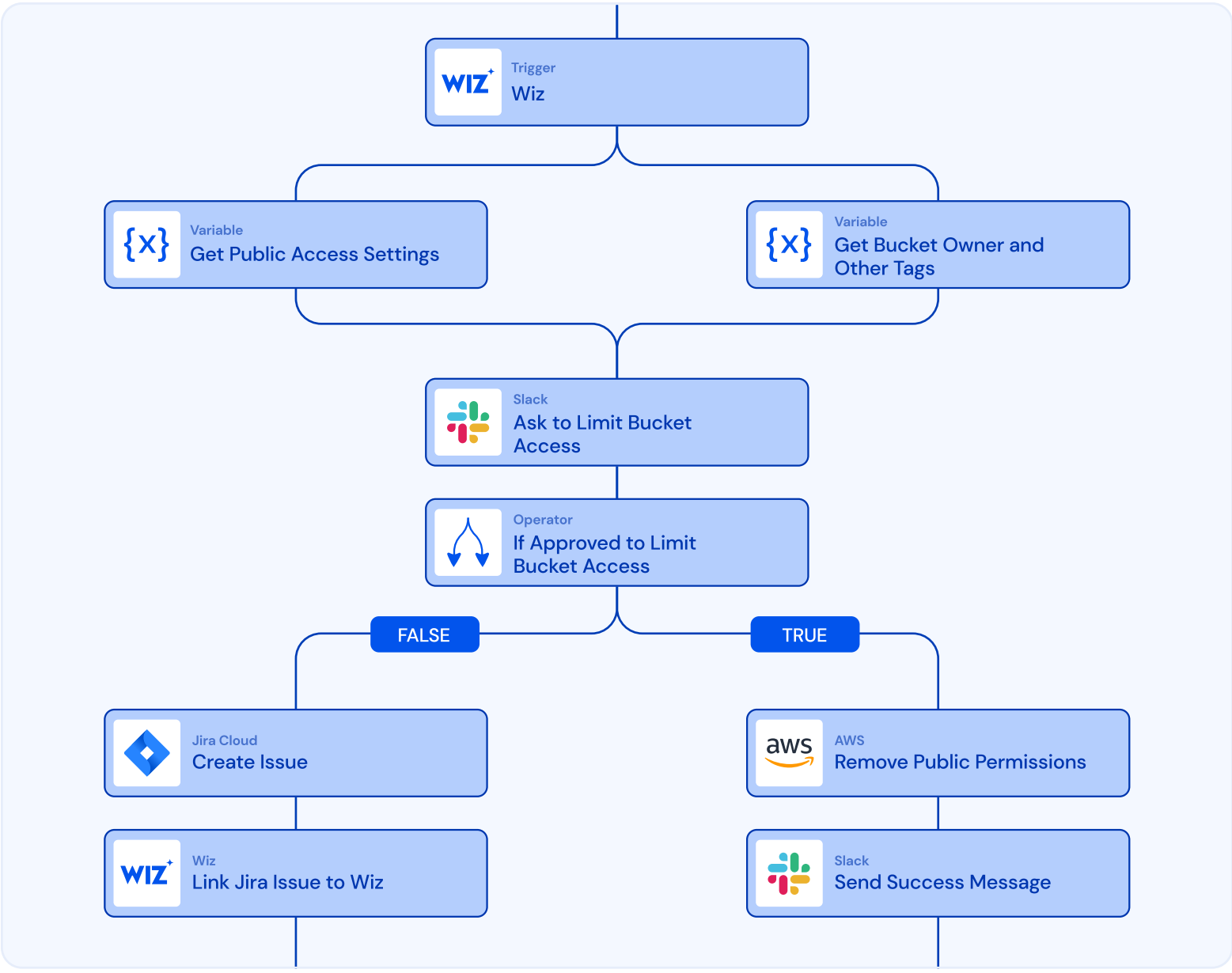
Better Together

Wiz, combined with Torq's no-code security hyperautomation approach, delivers actionable remediation and response to threats with a full audit trail of automated security actions. Torq and Wiz work seamlessly together to provide a real-time advantage in mitigating the ever-evolving cloud-based threat landscape with comprehensive contextual and accurate malicious activity identification. Torq frees up SecOps, CloudOps, DevOps and other teams time empowering them to focus on strategic business initiatives without being overwhelmed by cloud alerts.

Use Case

Automatically Deactivate Inactive IAM Users based on an alert from Wiz on an AWS admin principal, and automatically message in a slack channel with the right owners for approval to deactivate the IAM account.

Limit Public Access to AWS S3 Buckets Containing Sensitive Data On trigger from Wiz data finding for an AWS S3 bucket containing sensitive data, automatically ask a Slack channel or bucket owner to limit public access Enable AWS S3 Bucket Versioning Receive an alert from Wiz on an AWS S3 bucket with versioning disabled, lookup owner tag, ask owner or channel to enable versioning.



About Torq

Torq is a no-code automation platform for security teams. Torq's limitless connectivity, intelligent automation, and curated templates help security professionals accelerate threat response and remediation, identify and mitigate risks, and deliver protection at the speed of modern business. Founded in 2020, the company is backed by Insight Partners, SentinelOne, GGV Capital and Bessemer Venture Partners. Torq has offices in Portland, Oregon, New York City, and Tel Aviv, Israel.

About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.