WIZ + D3

Executive summary of the integration

This integration ingests Cloud Security data from Wiz into D3, helping automate incident response. The integration pulls Wiz Issues related to cloud misconfigurations, vulnerabilities, and other cloud security risks, helping security teams identify and remediate threats in cloud environments.

The integration supports commands like fetching events, updating issues, adding comments, and listing project details. Using correlated data from Wiz and other security tools in the security stack, D3 automates threat remediation workflows with AI-generated playbooks– enabling faster, more accurate responses to security incidents across cloud platforms like AWS, Azure, and Google Cloud.

Market challenge

SOC teams face an overwhelming volume of alerts every day, often struggling with alert fatigue from false positives. Manual prioritization is time-consuming and can lead to slow response times and missed alerts. The Wiz & D3 integration enriches alerts with deep cloud context, correlates cloud risks across attack timelines, and triggers automated playbooks to take remediation actions, such as isolating compromised workloads.

Benefits of the integration

- **Automated Alert Triage:** Combine Wiz data with context from all your security tools to automatically understand if it's a high or low severity threat.
- **Faster Incident Response:** Accelerates detection, analysis, and remediation of cloud security issues. D3 correlates Wiz context-rich cloud alerts with other IOCs across the tech stack to trigger automated remediation workflows.
- **Enhanced Cloud Security Posture:** Improves visibility and management of security risks across multi-cloud environments (AWS, Azure, Google Cloud) to correlate risks, prioritize security incidents, and automate remediation actions in cloud environments.
- **Improved Efficiency:** Streamlines operations, minimizing the need for manual intervention and enabling quicker, more effective responses to threats.

The better together story

Wiz identifies cloud risks such as misconfigurations, vulnerabilities, and toxic combinations. These findings are ingested into D3, where they are correlated with other relevant threat data from across the tech stack, to provide an enriched view of the threat. D3's AI-generated playbooks remediation actions such as patching vulnerabilities, isolating devices, and resetting passwords.

In other words, the integration allows customers to automate workflows to remediate threats in cloud environments. These automated workflows trigger remediation steps that address vulnerabilities, enable faster response times, and more.

The integration allows for scheduled, automated pulls from Wiz into D3, ensuring security teams have the most current data. This saves time, reduces human error, and improves response accuracy.

Wiz users can add comments and update Issues from within the D3 platform. Users can also push notifications to team members on Slack, Teams, Jira, and more to streamline communication.

Use case overview, challenge and solution

Use case

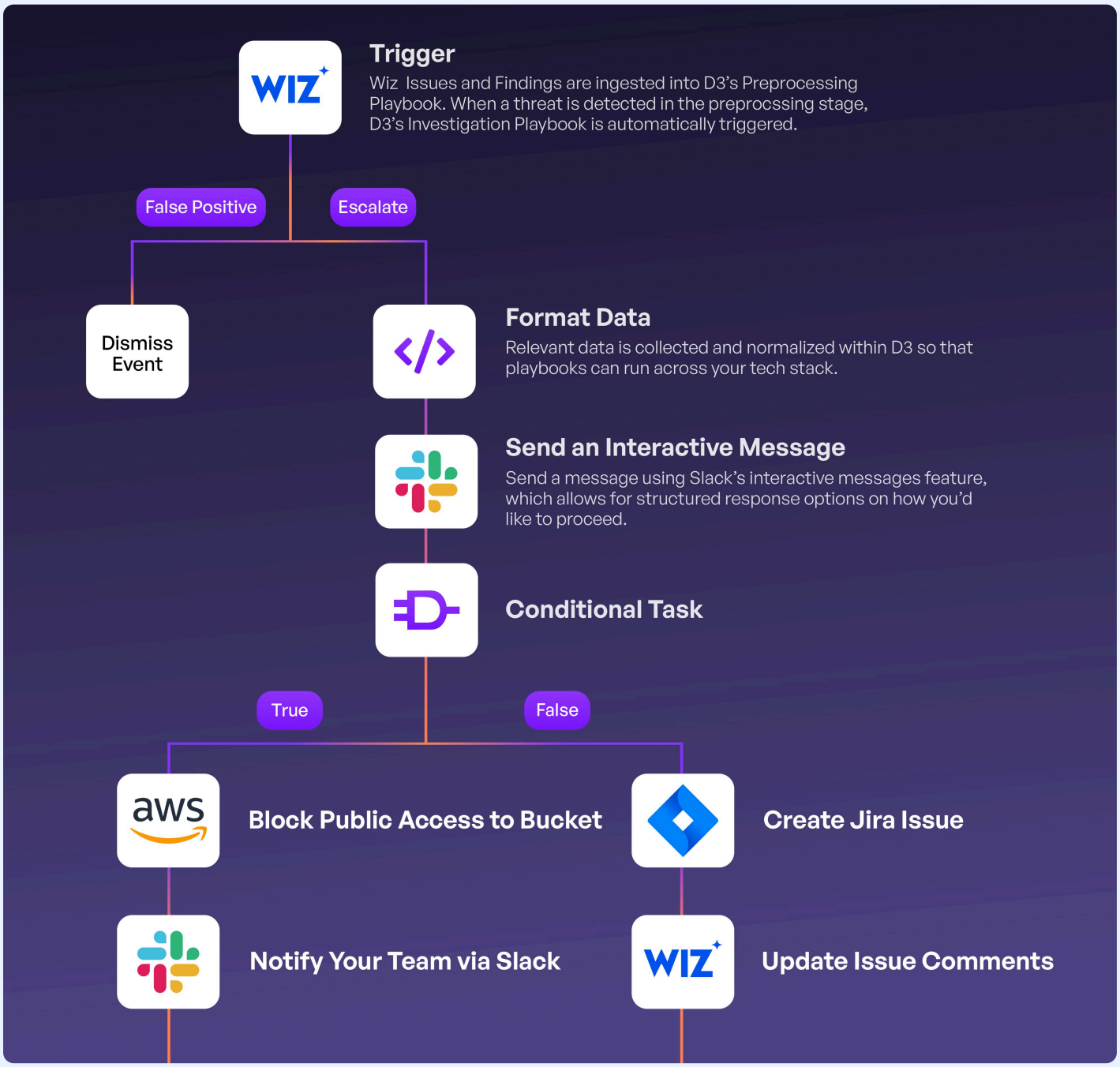
Large enterprises with a multi-cloud environment face the constant risk of cloud misconfigurations and vulnerabilities that could expose them to data breaches and compliance violations. A large enterprise could receive over a million alerts a day– and with many of these being false positives, your SOC Analysts can be tied up with manual triage.

Challenge

For example, an enterprise accidentally misconfigures one of their AWS S3 buckets with “public read access”. Wiz alerts the security team of the misconfiguration. Because of the integration with D3, the Wiz alert is automatically ingested into D3, and the S3 bucket is checked against their list of critical assets. With this information the security team can easily assess the alert and risk level.

Solution: Enhanced Vulnerability Data with Contrast Security

From there, D3’s AI-generated playbooks help security teams run remediation actions to isolate, secure, and remediate the threat. These actions may include immediately restricting access to the S3 bucket, collecting logs of any activity that occurred, updating the Wiz Issue, assigning follow-up tasks to team members, or generating reports.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 45% 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.

About D3 Security

D3 Security offers the only platform that combines AI, automation, and orchestration across unlimited integrated tools with an automated preprocessing pipeline that reduces event volume by 90% or more. D3's AI-generated playbooks automate enrichment and remediation tasks, while making it easy for enterprises and MSSPs to build, modify, and scale workflows for SecOps, incident response, and threat hunting.