Salt Security and Wiz Integration Brief

Introduction

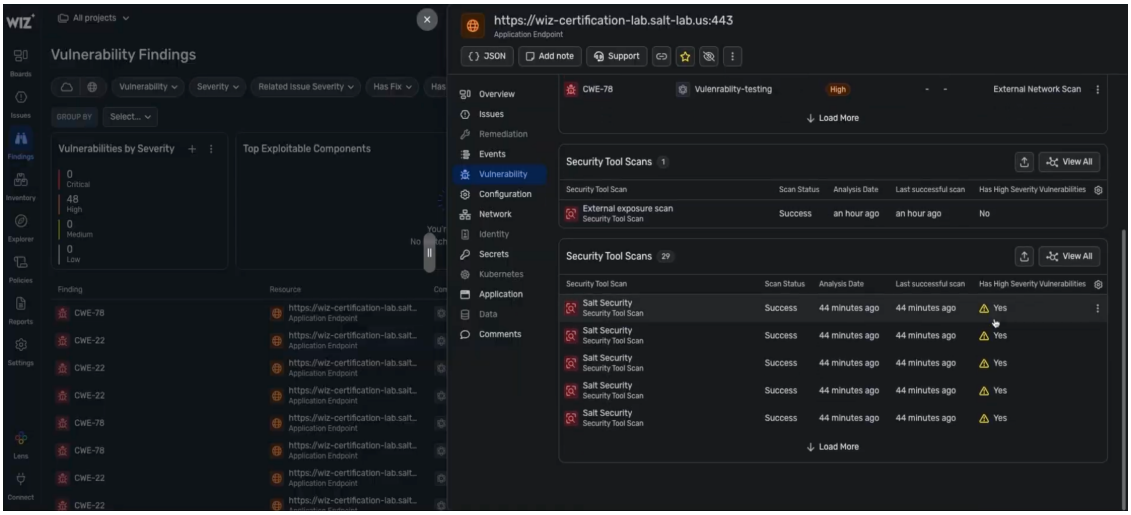
APIs represent a significant cloud security vulnerability, susceptible to both inadequate security measures and malicious attacks. To mitigate these risks, organizations require solutions that provide comprehensive API protection, secure deployment practices, and adherence to relevant compliance standards.

The integration between Salt Security and Wiz provides a strong solution for API threat protection and governance. Surfacing vulnerabilities and threat activity directly within the Wiz dashboard it enables effective attack chain analysis. This integration is designed for Cloud Security teams, AppSec professionals, and SecOps analysts looking to bridge the gap between API security and overall cloud posture management.

Key Benefits

Unified API Security and Posture Management with Attack Chain Context:

- **Enhanced Visibility:** Salt Security provides API posture assessments to identify vulnerabilities and detect active attacks, relaying detailed information to Wiz. This provides a unified view of API security threats and posture gaps across cloud security findings.
- **Contextual Risk Analysis:** The integration enables security teams to understand API vulnerabilities and active attacks within the cloud. By correlating posture gaps and threat activities in Wiz, organizations can prioritize risks and see how API attacks connect to broader security incidents.



Proactive API Posture Governance and Threat Response:

- **Compliance Enforcement:** Salt Security helps organizations enforce API security best practices and meet compliance requirements by identifying posture gaps that violate regulations or internal policies, ensuring adherence to best practices.
- **Vulnerability Remediation and Incident Response:** Surface API posture vulnerabilities and active API attacks directly in Wiz to streamline remediation workflows, enabling faster incident response.

Streamlined Incident Response Workflows:

- **Automated Workflows:** The integration enables the automatic creation of incidents in Wiz when critical API threat thresholds are met, thereby enhancing investigation and remediation.
- **Contextual Intelligence:** Analysts receive actionable insights specific to APIs within the Wiz framework from Salt Security.

Key Use Cases

- **Identifying and Addressing High-Risk Gaps:** Proactively find APIs with weak authentication and issues that could lead to security incidents, while detecting and responding to attackers exploiting vulnerabilities.
- **Enforcing API Security Standards:** Ensure all APIs comply with corporate policies and best practices by monitoring their security posture, detecting, and blocking malicious traffic.
- **Streamlining Compliance Reporting:** Generate reports in Wiz that display API security posture and compliance, providing detailed information on attacks for incident investigation.

Technical Highlights

- **Seamless Integration:** A 2-click integration allows for quick and easy connection between Salt Security and Wiz.
- **Posture and Threat Data in Wiz:** Salt Security sends detailed posture gap information, automatically updated every 24 hours, and critical API attack data, instantly relayed upon detection, to Wiz, where it is correlated with cloud resources to provide an up-to-date view.
- **AI-Powered Threat Intelligence:** Salt Security's AI-driven analysis offers Wiz threat intelligence, including malicious intent recognition, which aids in risk prioritization and reduces alert fatigue.
- **Intent-based Correlation:** Wiz improves detection by correlating Salt Security's API data and AI-driven insights with broader cloud security information.
- **Unified Dashboard with Attack Chain Visualization:** Security teams can view and manage API posture vulnerabilities and active API attacks, along with their potential impact and role in attack chains, all within the Wiz dashboard.

Conclusion

The Salt Security and Wiz integration provides a powerful solution for modern cloud security. By combining API threat protection with robust posture governance and attack chain visibility, organizations can gain comprehensive visibility into their API risk, enforce security standards, and improve their overall cloud security posture, enabling more effective threat detection and response.