Rezilion Certify Datasheet

Building a product your users can trust requires trusted inputs from the initial code commit through your entire CI/CD pipeline. The key is to establish policies up front so it doesn't slow down development, giving you a powerful combination of speed and security. Rezilion Certify allows you to pre-define the trusted path to production from repository to release to reduce your risk.

By smart-gating the pipelines to production and continuously monitoring your runtime environment for changes, enforce a desired state of your applications and infrastructure before, during and after release. Smart Gates work by establishing custom security thresholds based on your organization's risk tolerance and can be customized based on the destination environment. Certify builds on the vulnerability validation process established by Rezilion Validate to ensure that Smart Gates only flag or stop builds that have loaded vulnerabilities above your established security thresholds.

Once your application is running in production, it's important to combat drift from established golden images. Certify runs continuously in production to detect and alert on any changes to the application that happened outside of your trusted pipelines. Certify provides details when unsanctioned changes are introduced in production to quickly evaluate and triage for remediation, if necessary.

Key Benefits:

- **Prevent Risk**
  Certify that all your code is in a desired state and meets security standards and compliance requirements
- **Prevent Drift**
  Prevent unsanctioned changes from entering into your runtime environment without being scanned or tested in your CI/CD pipeline.
- **Prevent Delays**
  Give maximum autonomy to developers while providing unprecedented control for security teams,reducing friction across your org.
- **Take the right action at the right time**
  In the event of a compromise, have detailed knowledge into the origin, nature and location of the threat to interrupt attacker persistence.
- **Shift Security Left**
  Sanction specific release pipelines and implement smart gates to define secure paths to production.
- **Identify Rogue Actors**
  Immediately identify users making changes to production outside of approved channels

Key Features:

- **Automated Security Review**
  Define simple and transparent risk-posture thresholds across all your pipelines and scanners based on Rezilion's ability to validate actual risk.

- **Trusted Pipelines**
  Ensure only code from trusted sources is running in production by certifying the repositories and processes responsible for promoting releases into runtime

- **Smart Gates**
  Only block releases that have loaded vulnerabilities, don't waste DevOps time forcing them to patch vulnerabilities that don't pose a risk.

- **Enable DevOps Autonomy**
  Help DevOps to release code with acceptable risk posture by showing them exactly what they need to fix in order to meet your defined standards.

- **Continuous Assurance**
  Scan once pre-deployment, assure continuously in runtime. Guarantee that 100% of the code being executed in production meets your standards 100% of the time.

- **Instant Drift Detection**
  Get notified, immediately, when unsanctioned changes are introduced in production to quickly evaluate their context and triage for remediation, if necessary.