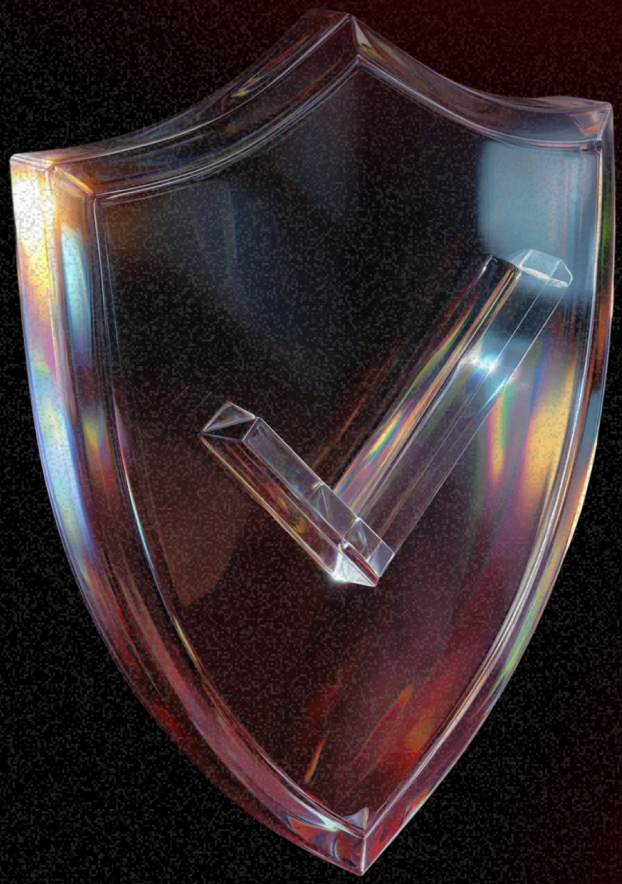
QBurst | A High AI-Q™ Company



Cybersecurity Maturity Assessment Strengthens Risk Visibility and Resilience

Evaluating governance, controls, and monitoring to build a structured roadmap for stronger cybersecurity resilience.

Overview

- Conducted a comprehensive cybersecurity maturity assessment across governance, infrastructure, DevOps, and monitoring domains.
- Identified gaps in governance, identity management, and monitoring, enabling targeted risk mitigation.
- Delivered a strategic remediation roadmap to strengthen security controls and improve incident response readiness.

Client Profile

A South Africa-based financial services group offering retirement, investment, and wealth management solutions across the continent. With an advice-led, multi-manager model, the organization serves institutional and retail clients through consulting, investment, and administration platforms.

Disjointed Security Practices Across Governance and Operations

- Security documentation maturity varied across governance, infrastructure, and development domains.
- Cybersecurity ownership was distributed across multiple teams, limiting centralized visibility.
- Strong interdependencies between infrastructure, DevOps, and security created operational complexity.
- Gaps between policy intent and real-world implementation impacted consistency of controls.

QBurst Solution: Driving a Structured Cybersecurity Maturity Assessment

We conducted a multi-layered cybersecurity evaluation of governance frameworks and operational security capabilities across the organization. The approach combined structured questionnaires, documentation reviews, and stakeholder discussions to establish a comprehensive view of cybersecurity posture across key domains, including governance, risk management, IAM, infrastructure security, application security, vulnerability management, SIEM and monitoring, data protection, backup mechanisms, and incident response.

Core Assessment Areas

- Enterprise-wide cybersecurity maturity baseline across governance and enterprise security functions
- Cross-domain analysis spanning infrastructure, DevOps, and security functions

Remediation Highlights

- Strengthened governance frameworks for consistent policy implementation
- Enhanced identity governance and privileged access visibility
- Integrated security practices within development and DevOps workflows
- Improved vulnerability prioritization and remediation governance
- Expanded centralized monitoring for better threat detection
- Strengthened incident response coordination and preparedness

Implementing a Comprehensive Multi-Layered Security Evaluation

- Questionnaire-driven baseline assessment of cybersecurity capabilities
- Detailed documentation review of policies, procedures, and controls
- Stakeholder interviews to validate real-world security practices

- Cross-functional analysis of governance and operational alignment
- Evaluation across infrastructure, DevOps, and enterprise architecture layers

Impact: Strengthened Cybersecurity Visibility and Strategic Readiness

- Established a clear, enterprise-wide baseline of cybersecurity maturity.
- Improved alignment between governance frameworks and operational controls.
- Enabled leadership to prioritize security investments and remediation initiatives.
- Strengthened coordination across security, infrastructure, and development teams.
- Delivered strategic value by enhancing long-term resilience and readiness against evolving cyber threats.