Standardize application testing across diverse software environments and automate the process for prioritizing and fixing the most critical issues at every stage of the SDLC.

Complex Attack Surface

With the advent of digital transformation, an ever-increasing number of business functions and processes now depend on software applications. These business applications vary greatly in significance and usage - from mission-critical applications necessary for an organization to deliver its products and services, to trivial ones that support common aspects of day-to-day employee work. The sources of these applications vary greatly as well - from being procured from external vendors to being developed in-house. Information security is tasked with the unenviable task of making sure this diverse software infrastructure continues to enable employees to be as efficient and effective as possible, while making sure that the security and integrity of the enterprise is protected at all times.

Application infrastructure itself is never static. It is constantly evolving with software being upgraded and integrated with an ever-changing collection of systems, some of which may belong to other business entities. For example, consider what happens when you integrate your website with an Enterprise Resource Planning (ERP) system. In doing so, you may inadvertently expose your ERP data to breach by means of a SQL injection attack. There are so many dependencies and moving parts, it can be difficult to determine the seriousness (or indeed, the very existence) of the ERP system’s SQL injection risk exposure.

Knowledge-driven, Automated Solution

To evaluate application risk effectively organizations must analyze information from various application assessment and monitoring tools and programs - SAST, DAST, IAST, SCA, Penetration Testing - effectively and with the knowledge of how these applications support and impact business functions. Brinqa Application Risk Service provides a comprehensive application security data ontology to automate normalization, correlation, and, analysis of data from disparate application testing tools and programs.

The included Brinqa connectors makes it possible to easily collect and collate application asset, vulnerability, context and threat data. Brinqa Application Risk Service integrates the various relevant data sources into a single authoritative source of truth that can now be utilized by all stakeholders and decision makers for effective risk remediation. Data correlation and enrichment functions build the relationships between all the different data points in the ontology that highlight contexts necessary for informed decision-making.
Application Repository
Brinqa Application Risk Service creates an accurate repository that uniquely identifies applications. It consolidates all technical and business information about these assets in one place by integrating asset management, CMDB, code repositories, CICD tools and other relevant data sources. Brinqa Business Rules provide an automated mechanism to identify and address any missing critical information.

Vulnerability Enumeration
Brinqa’s dynamic data ontology and vast collection of AppSec integrations make it easy to uniformly and consistently analyze different types of application testing results - SAST, DAST, IAST, SCA, PenTest. Vulnerabilities from these diverse sources are normalized, correlated, and analyzed against consistent, accurate information represented in the authoritative application repository.

Integrated Threat Intelligence
Brinqa Application Risk Service integrates a host of open source and commercial threat feeds into an organization's application security program - providing comprehensive visibility into known exploits, weaponization, zero-day popularity, pervasiveness and patch availability. This information is crucial to assessing the true impact, likelihood and cost of an application vulnerability.

Risk Prioritization & Insights
Brinqa Application Risk Service combines all criteria behind application sensitivity, criticality, and impact ratings, along with vulnerability classification and threat intelligence, into an open, transparent, and adjustable risk calculation model. Customers can implement their unique risk perspectives in the prioritization process and focus on what matters most to them. Insights about the origins of pervasive risks can be used to tailor employee security education to address the root causes of risks in the application infrastructure.

Risk Remediation
Rule-based automated remediation provides administrators with the ability to create intelligent tickets by grouping vulnerabilities based on inherent classifications, application characteristics, remediation options and ownership. Tickets are created automatically, reducing the remediation gap - the time between vulnerability discovery and remediation. Automated ticket creation improves the effectiveness, efficiency, and consistency of remediation efforts by dynamically enforcing ownership, escalation chains, and SLAs.

Risk Analytics & Communication
Brinqa Application Risk Service tracks key KRI, KPIs and program metrics to monitor risk-reduction, remediation time and window of opportunity. The self-service analytics interface allows stakeholders to leverage a library of metrics and reports, or to define their own. The solution comes with a wide variety of technology and business hierarchy based reports targeted for a diverse audience ranging from C-level executives to developers.

SOLUTION HIGHLIGHTS
- Establish a context-rich application inventory that highlights the most critical applications and associated IT infrastructure on which they depend.
- Connect, model and analyze results from static, dynamic, and penetration code testing with open source dependencies to derive knowledge-driven cyber risk insights.
- Apply cyber risk insights within secure SDLC governance process to determine whether to advance code through the SDLC process.
- Prioritize, remediate, and communicate the most at-risk applications based on a holistic view of application risk, context and threat data.
- Establish best practices and training for developers based on cyber risk insights.
- Holistic view of application security across an organization.

ABOUT BRINQA
Brinqa empowers customers to own their cyber risk with a unique, knowledge-driven approach to cybersecurity challenges. Brinqa Cyber Risk Graph - the knowledge graph for cybersecurity - connects all relevant security and business data, establishes a common risk language, and powers cybersecurity insights and outcomes. Brinqa Cyber Risk Services apply this knowledge to uniquely inform risk management strategies, standardize security data management and analysis, improve communication between teams, deliver actionable insights and automate risk remediation. With Brinqa, cybersecurity programs and processes will evolve with changing risk priorities, threat landscape and technology trends. Learn more at www.brinqa.com and follow us on Twitter and LinkedIn.