Using Brinqa Technology to Improve Application Security and Reduce Risk

This study describes the implementation of the Software Development Lifecycle (SDLC), tied with a risk analysis view, using Brinqa technology. As a result, the Depository Trust and Clearing Corporation (DTCC) achieved improved application security and risk reduction.

About DTCC

The Depository Trust & Clearing Corporation (DTCC) is a United States financial services company that provides clearing and settlement services to financial markets. DTCC provides ways for securities buyers and sellers to make exchanges safely and efficiently, as well as providing central custody of securities.

Since DTCC’s inception over 40 years ago, Risk Management has been its primary function. This role involves efficient identification, measurement, monitoring, and control of risks. These risks, all associated with securities exchanges, focus on credit, liquidity, and systemic and operational risks impacting DTCC and the marketplace.

DTCC relies on internal custom application development for extremely specific business-critical applications for the organization. There are over 300 developers currently responsible for writing code, and thousands of internally developed applications, combined with commercial applications and free, open source applications, DTCC makes large investments in internal development. Given the organization’s concern with Risk Management, many risks must be considered with internal application development. Prior to implementing Brinqa, there was no way of quantifying and measuring the risk of progressing applications forward to production during the Software Development Lifecycle (SDLC).

Business Challenges

The challenges that DTCC faces can be summarized as follows:

- DTCC uses a variety of tools and assessment technology for application software security. These include tools for static code analysis, application penetration testing (pentest), open source software issues, and insider threat analysis. However, DTCC does not have a common taxonomy for representing the risk related to these issues. A common repository to provide a holistic view of security information for the applications is likewise missing.
- The business product line owners and executives need a standard framework to represent risk and exposure. They lack visibility in identifying the most critical issues that impact their application portfolio.
- As part of the overall Building Security in Maturity Model (BSMM) process, DTCC needs quantified toll gates to measure application lifecycle progress and to monitor product and application risk during the development lifecycle. These toll gates are needed to assess the criticality of issues impacting the application / business and verify whether the application can safely move to user acceptance testing (UAT) and production. These toll gates need to consider the multiple tools used for evaluation.

The Brinqa Solution

DTCC established a team to develop DTCC Application Vulnerability Scoring (DAVS). The DAVS goal was to provide a consistent scoring and reporting methodology for application security risk. This included input from pentest, vulnerability management, static code analysis, and Free / Open Source Software (FOSS) inclusion in the application development.

As a part of this initiative, Brinqa worked with the IT Risk and Application Security team to provide a framework for collecting, analyzing, and scoring data in such a way that risk factors could be reported to executive management and business product line owners.
In addition to risk analysis and reporting, DAVS used Brinqa Risk Analytics software to collect and provide workflow for analysis. Brinqa was also used for graphical management reporting of vulnerability data. SDLC practices were implemented in this process.

Brinqa’s Risk Analytics was implemented using the following methodology:

(1) The first step in this framework is to model the data from various sources. Data sources include business information, ownership information and governance and compliance data. The data collected from the list of applications included additional information, such as the inherent risk, business criticality and classification. In addition to the application data source, information was also integrated from the governance, risk and compliance (GRC) system in order to capture the controls and exception information which would be modeled in the analysis.

(2) Next, the applications captured in Step 1 were integrated with the various assessments including Open Source Software, static code, and application pentests. The business context of the applications, such as the criticality of the application, was applied to the issues.

(3) Next, the issues were prioritized based on an analysis using the following steps:

(a) The first step was to analyze the individual issues using the Common Weakness Scoring System (CWSS) model and the severity of the issue and the business criticality. The inherent risk and data classification of the application were also used for the analysis. The result was a quantified score which was assigned to each issue.

(b) Second, the combination of each issue score was used to derive the overall assessment score (taking into account the scores from the tools used for evaluation). This value was compared to the toll gate check to determine if an assessment had passed / failed.

(c) Finally, the combination of various assessment scores was used to rate the application.

(4) Data was sliced and reported to the various audiences including executives, application owners and each application developer.

Brinqa Risk Analytics provided robust risk modeling and prioritization using a correlation engine. For the DTCC implementation, the Brinqa Risk Analytics platform was used to configure the algorithms for Risk Analysis. The Brinqa risk prioritization model supports correlation and analysis of the aggregated data. The risk model provides advanced quantitative risk scoring, statistical risk models and scenario testing. The quantitative risk score calculations factor in all relevant parameters such as weights, tolerances, thresholds, and aggregation and data normalizations to establish an accurate representation of risk for an application. The Brinqa risk model is available for “What If” analysis for risk forecasting, reduction in risk exposure, and risk mitigation planning. A comprehensive issue library provides automatic issue discovery—including issues created as a result of an assessment, loss event, near-miss, or control test failure.

Customer Benefits

DTCC used Brinqa Risk Analytics to improve the SDLC process, normalize information gathering efforts, reduce incident remediation efforts, and provide normalized application risk scores. As a result, DTCC experienced:

- Automated SDLC process with criteria defined by quantitative modeling to determine application lifecycle state.
- Capability to measure the trends of application risk scores with a data warehouse.
- Customized visibility for business owners and senior management of application risk, tailored to their specific needs.
- Prioritization of the issues by risk to the organization.
- Consistent and clear information on risk posture.
- Effective and efficient resource utilization.
- Ability to predict and respond to threats.
- Automated, relevant and efficient risk assessments.

In addition, DTCC was able to have a holistic view of application risk – seeing information from many sources on a single console, and getting management reports on the incorporating data. DTCC was able to use both top-down and bottom-up approaches to identify, measure, and track risks.

Brinqa Risk Analytics provides enterprises a competitive advantage by taking a proactive and financially-driven approach, using forward-looking risk concepts and tools to enable better decisions to mitigate threats and capitalize on opportunities. Contact us at info@brinqa.com.