brinqa

CASE STUDY

Improve Application Security and Reduce Risk

The Depository Trust & Clearing Corporation

SOLUTION HIGHLIGHTS

- Holistic view of application risk
- Consistent application security risk scoring and reporting
- Real-time decisions on business application risk

ABOUT DTCC

The Depository Trust & Clearing Corporation (DTCC) is a United States Fortune 500 financial services company that provides clearing and settlement services to financial markets. DTCC enables securities buyers and sellers to make exchanges safely and efficiently. It also provides central custody of securities.

Since DTCC's inception more than 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 makes large investments in internal custom application development, employing more than 300 developers for its highly specialized business-critical applications. overall the company has thousands of internally developed, commercial, and free, open source applications. Given the organization's focus on risk management, the internal development team must consider many risks. Prior to implementing Brinqa, DTCC had no way to quantify and measure the risk associated with progressing applications into production throughout the software development lifecycle (SDLC).

THE BRINQA SOLUTION

DTCC created a team to develop DTCC application vulnerability scoring (DAVS). The goal was to provide a consistent scoring and reporting methodology for application security risk. Input included pen test results, vulnerability management, static code analysis, and free and open-source software (FOSS) used in application development.

As a part of this initiative, Brinqa worked with the DTCC's IT risk and application security team to provide a framework for collecting, analyzing and scoring data so risk factors could be reported to executive management and business product line owners.

BUSINESS CHALLENGES

- Producing vulnerability-free code with 500-1000 software builds a day
- Broad set of AST tools — Fortify (SAST), Burp Suite (pen test), Nexis (FOSS), and insider threat analysis
- Tool-based security view was slowing down development process
  - Developers log in to 10 AST tools to understand app risk
  - No view of risk across all apps
  - No organizational view of app risk ownership or method of comparing to other organizations

USE CASE

The primary goal was to evaluate and demonstrably improve the security of its crown jewels — the applications and technology assets supporting the most critical business functions. To do this, DTCC needed to build a solid understanding of their technology infrastructure and its impact on the business.

DTCC had been using a legacy, homegrown asset management system and ServiceNow CMDB. Both systems were still active and often presented complementary, redundant or conflicting information. To build true business context, DTCC needed to incorporate additional systems for information that was not retained in either of its existing IT asset management systems.

HOW DTCC IMPLEMENTED BRINQA'S RISK ANALYTICS

The team began by modeling data from various sources including business and ownership information, and the governance, risk and compliance (GRC) system to capture the controls and exception information. The collected data also included information such as the inherent risk, business criticality and classification.

The captured application data was integrated with various assessments including open-source software, static code, and application pen tests. Business context, such as an application's criticality, was applied to the issues which were then prioritized based on analysis using the Common Weakness Scoring System (CWSS) model, the severity of each issue, and its business criticality. The inherent risk and data classification of the application also were used for the analysis. The resulting quantified score was assigned to each issue.

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 or failed. The combination of various assessment scores was used to rate the application. Data was sliced and reported to key audiences, e.g., executives, application owners and developers. Brinqa Risk Analytics provided robust risk modeling and prioritization using a correlation engine. Brinqa Risk Analytics platform configured 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 an application's risk. 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.

DTCC achieved a holistic view of application risk — seeing information from many sources on a single console and getting management reports on the incorporating data, using both top-down and bottom-up approaches to identify, measure and track risks.

CUSTOMER RESULTS & BENEFITS

Risk evaluation gates incorporated into the entire CI/CD pipeline to ship vulnerability-free code enabled:

- 10x reduction in developer time spent in security tools
- 85% reduction in security team time spent monthly to prepare risk reports
- Real-time decisions on business application risk vs. monthly evaluation
- Confidence that the right AST findings are fixed based on prioritization that is specific to their environment and business processes