With Brinqa Application Risk Service, we connected our disparate application security testing initiatives into a cohesive application risk management strategy. By identifying and focusing on our most critical applications, we drastically improved our overall security posture through targeted remediation of the most dangerous and impactful vulnerabilities.

BACKGROUND

The customer is a global Fortune 500 healthcare firm providing medical services and health insurance throughout the US and in major international markets. As an organization that has seen significant M&A activity, the customer has acquired a great variety of software assets and application security tools over the years. A recent redesign of the application security program aims to reduce the variance in application testing tools and risk remediation processes.

As a healthcare provider, the customer is required to be HIPAA compliant and has worked with external consultants and auditors to develop policies that govern ownership and SLA requirements for HIPAA assets. These policies were designed to help maintain and prove compliance, but in the absence of any automated means of enforcing them, there are significant inconsistencies in how they are being implemented across the organization. The customer has struggled to ensure that all developers and security professionals are properly trained to make the policies an integral part of the software infrastructure.

USE CASE

The primary goal for the customer was to improve the security posture of their most critical applications while implementing a consistent risk analysis and remediation strategy across the software infrastructure. Further complicating the prevalence of different application testing tools in different parts of the organization is the fact that two completely different sets of processes and tools were being employed to manage the applications sourced externally vs. those developed internally.

Internally developed applications were managed by the software development organization — using Jira as the primary repository for asset information as well as for task management. Externally sourced software was managed by IT — using ServiceNow for business application inventory as well as for remediation management.

The customer was required to maintain and demonstrate HIPAA compliance at all times. While they had worked hard to establish policies to help them do so, they were struggling due to inconsistent and ineffective manual processes for tagging HIPAA assets and enforcing ownership and SLAs.

CUSTOMER ENVIRONMENT

- 2000+ Applications
- Checkmarx
- Qualys WAS
- External PenTest
- Data Protection Program
- ServiceNow
- Jira
- FireEye Threat Intel
- LDAP

CHALLENGES

- Disparate inventories for internally developed and externally sourced applications.
- Incompatible SAST, DAST, PenTest results from different vendors.
- HIPAA assets not tracked accurately.
- Remediation ownership and SLAs were not defined or enforced consistently.
SOLUTION

With Brinqa, the customer was able to improve visibility into their software infrastructure and address critical questions of application risk. A single, complete software inventory was created by combining the inventory of externally sourced business applications maintained in ServiceNow, with the repository of internally developed applications being maintained in Jira. Understanding that not all applications are created equal, significant efforts were made early on in the project to ensure that all relevant application metadata was consolidated. Business rules were used to identify any important missing information and create corrective tasks for responsible parties. Inputs from the data protection program were used to validate that all HIPAA relevant applications were tagged accurately.

Issues from Checkmarx and findings from Qualys Web Application Scanning were brought in next using dedicated connectors. Findings were also delivered by an external PenTest agency using a generic XML connector. These were then sanitized of duplicates and false positives, and analyzed in context of application importance and real-time threat intelligence to identify those that posed the biggest threats to the organization. Remediation rules were setup to enforce approved ownership and SLA policies, reflected in the tickets created and assigned automatically. Using bi-directional connectors, tickets were pushed to ServiceNow for IT users and Jira for development. HIPAA compliance reports were configured and delivered automatically.

RESULT

The customer addressed many of their top priorities within the first few month of deployment. During this time, they identified gaps in their application inventory and were able to drive user action to remedy them. They implemented a consistent asset management process by consolidating application data from several different sources and automatically pushing all new information into ServiceNow CMDB - making the CMDB the authoritative source of asset information going forward.

Once all relevant application metadata was collected, the customer was easily able to identify those that had the biggest impact to business. They prioritized improving the security posture of the 'crown jewels' and, over a 3 month period, reduced high-risk vulnerabilities on these critical assets by over 50%. They were also able to reduce the overall vulnerability volume across the entire infrastructure by 20%. The customer accomplished this while creating fewer tickets than before, reducing the overhead associated with managing tickets and improving the efficiency of remediation efforts.

Using a standardized model for representing, analyzing and prioritizing vulnerabilities, the customer implemented a consistent risk prioritization and remediation strategy for data coming from Checkmarx, Qualys WAS, and external penetration testing. Throughout the initiative, customer engaged various business, InfoSec and IT stakeholders with targeted metrics and reports. Previously handled by 3 FTEs, the customer automated all analytics evaluation and delivery with Brinqa, freeing up the resources for more relevant tasks.