DAYBLINK CONSULTING

Optimized Cybersecurity Service Fulfillment

How DayBlink Consulting designed and deployed a best-in-class cybersecurity service management capability

Introduction

The Information Security organization of a large, global financial institution partnered with DayBlink Consulting to overhaul the way cybersecurity services were requested, tracked, and fulfilled across the enterprise. With thousands of service requests submitted annually by hundreds of internal stakeholders—including product owners, application developers, system administrators, and infrastructure engineers—the institution faced an increasingly unmanageable and inefficient process that hindered productivity and weakened stakeholder trust in the InfoSec function.

DayBlink Consulting was designed and implemented a streamlined, scalable, and user-friendly service request model that would reduce complexity, improve turnaround times, and provide greater transparency. By modernizing this core process, the institution aimed to free up valuable internal resources, improve InfoSec's reputation as a partner to the business, and ultimately strengthen the organization's overall security posture.

© DAYBLINK CONSULTING 2025

Problem

The client had a complicated and convoluted approach to ingesting, assigning, and tracking customer requests

Prior to DayBlink's engagement, internal "customers" of InfoSec services were routinely frustrated by an intake process that was burdensome, ambiguous, and time-consuming. Requesting services — whether to initiate a system security plan (SSP), conduct a system architecture review, onboard static and dynamic application security testing tools (SAST/DAST), or submit access control list (ACL) changes—was viewed by many as a cumbersome hurdle. Our analysis revealed several issues within the service model. Despite routine request types, inefficiencies cascaded throughout the process:

(1) Service Ambiguity: InfoSec had nearly 50 different security services available, but no clear guidance existed on which services were applicable to a request. Users often found themselves unsure which combination of services was required, leading to either wasting time & resources or risking non-compliance.

(2) Intake Form Overload: The intake form was overwhelming, containing 100+ questions—many of them duplicative, unnecessary, or not applicable to all service types. Completing it could take several hours, often requiring multiple rounds of clarification with InfoSec staff.

(3) Poor User Interface and Experience: The user interface was clunky and unintuitive, lacking features like progress saving, intelligent form logic (e.g., conditional fields) or error handling. Customers cited this as a key pain point.

(4) Lack of Transparency: After submission, requesters received little to no feedback on what would happen next. There was no communication around timelines, no visibility into the assignee, and no clear point of contact for follow-up questions or escalations.

(5) Reusability Gaps: Even after investing considerable time to complete the request form, users could not save the information in a format that could be reused for subsequent or related requests involving the same system or platform. Every request started from scratch.

Taken together, these pain points created a service environment that felt opaque, manual, and disconnected from broader efforts. The lack of automation and standardization also placed a burden on the InfoSec team itself, spending unnecessary time clarifying requests and navigating a fragmented workflow.

CUSTOMER IDENTIFIED PAIN POINTS

- Documentation
- Metrics
- Communications
- False Positives & Negatives
- Customer Expertise
- Short Term & Auto-Saving
- CX Design & Dynamic Forms
- Single POC
- Tooling
- Question Refinement
- SLAs & Priority
- Instructional Clarity
- Governance
- Process Discipline

© DAYBLINK CONSULTING 2025

Solution

Our team helped the client reimagine and redefine a future solutions

To address these issues holistically, DayBlink Consulting embedded a team within the InfoSec function. The team's mandate was to lead a top-to-bottom reimagining of the request and fulfillment experience. Our approach was executed in four key phases:

(1) Discovery & Voice of the Customer: We launched a series of structured listening sessions with key stakeholder groups across the enterprise. These included product and platform teams, DevOps engineers, enterprise architects, and fulfillment teams within InfoSec. These sessions gathered qualitative insights into user frustrations, pain points, and unmet needs, which were later synthesized into opportunity areas.

(2) Assessment & Roadmap Creation: Based on discovery findings, we developed a comprehensive process map of the existing request lifecycle, identifying redundancies, bottlenecks, and service overlap. We then designed a prioritized roadmap of enhancements, balancing "quick wins" with longer-term architectural changes. Key themes included service rationalization, UI/UX redesign, and process automation.

(3) Requirements Definition and Design: Next, we defined both the functional and technical requirements for a modernized service management system. Drawing from best practices in customer relationship management (CRM) and IT service management (ITSM), we recommended tools and processes that would elevate the InfoSec customer experience. This included improvements in form logic, data reusability, real-time status tracking, and integration with communication tools like email and chat.

(4) Implementation & Program Leadership: As the new design gained approval, We transitioned from a product design role into a program leadership function. We coordinated cross - functional working groups, tracked delivery milestones, managed stakeholders, and facilitated change management efforts to drive adoption.

Throughout this transformation, we emphasized the importance of adopting a customer-centric mindset — an approach welcomed by leadership, who acknowledged that optimizing user experience had historically not been their primary strength.

© DAYBLINK CONSULTING 2025

Outcome

The transformation yielded measurable improvements across several dimensions of the InfoSec service lifecycle

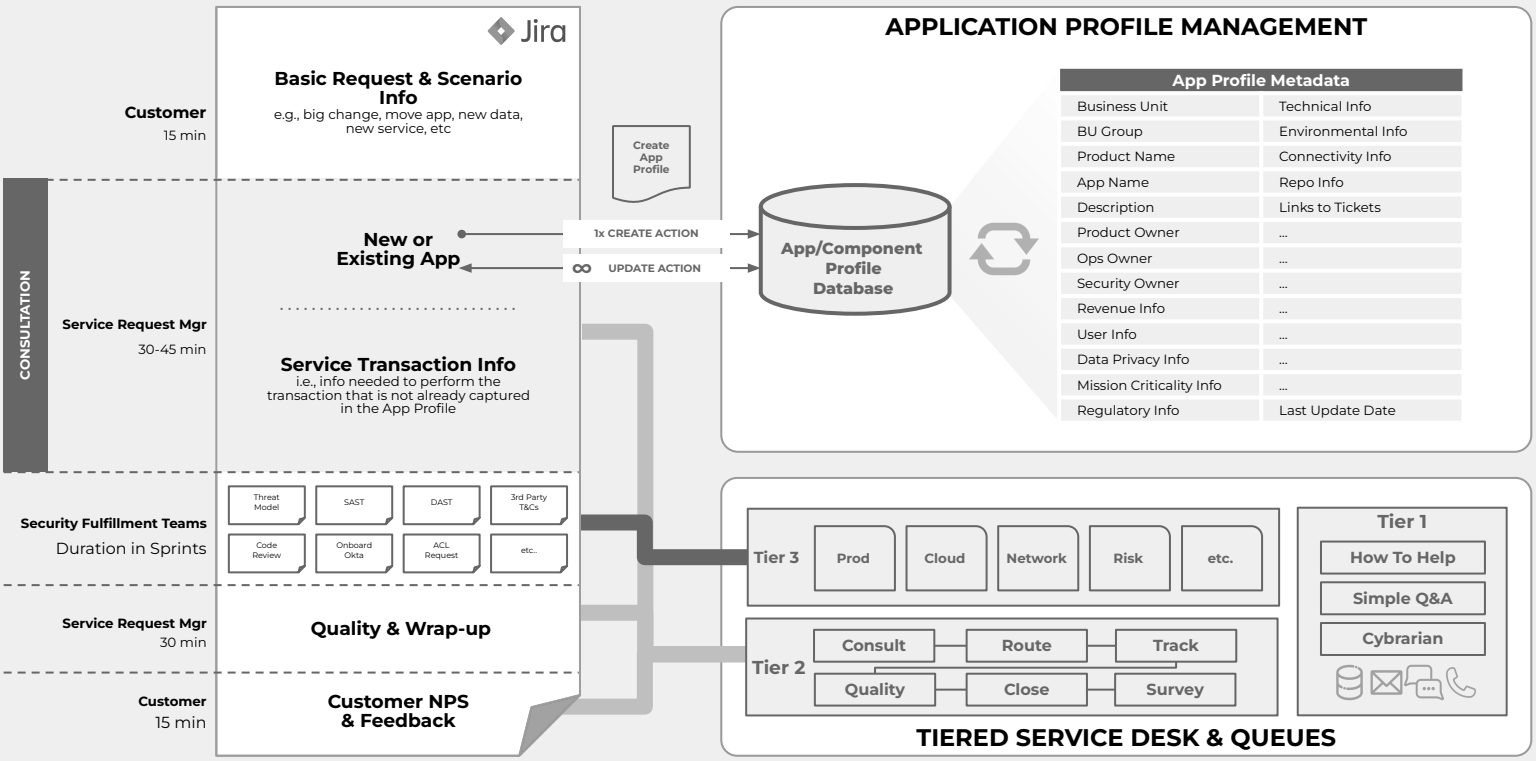
A simplified service catalog reduced the number of available cybersecurity services from nearly 50 to a more manageable and better-defined list. Services were grouped logically, and decision trees were implemented to help users quickly determine which ones applied to their specific need.

Streamlining the intake process eliminated dozens of low-value or redundant questions, cutting the average intake time by over 50%. Smart form logic reduced the cognitive load on requesters, while allowing InfoSec teams to collect the information they actually needed.

A new front-end experience was developed using human-centered design principles. The improved UI allowed for easier navigation, saved progress, and clearly communicated what information was required versus optional.

A new "security request specialist" role was introduced to act as the single point of contact for each submitted request. These specialists provided updates, set clear expectations, and ensured continuity throughout the request fulfillment process.

Target Service Request Automation Process



© DAYBLINK CONSULTING 2025

Backend adjustments were made as well, we partnered with cybersecurity SMEs to document and standardize service delivery steps. This reduced variation in quality and completion times, while enabling better tracking and reporting. Additionally, it reduced the internal knowledge of teams, forcing all fulfillers to utilize a small set of tenured employees to provide context and support.

Finally, we established new self-service and support channels—including office hours, live chat, and virtual consultations—so users could interact with InfoSec in the way that best suited their needs and work style. In many cases, these channels helped to reduce the noise of already automated security functions like password resets.

In total, these improvements led to faster turnaround times, higher stakeholder satisfaction, and reduced manual effort across the board. Just as importantly, the transformation signaled a cultural shift within InfoSec—from a reactive, ticket-based function to a proactive, service-oriented partner to the business.

30%
Reduction in Intake Process

20%
Increase in Ticket Throughput

10+
Service Workflows Automated

© DAYBLINK CONSULTING 2025

WASHINGTON D.C. (Headquarters)

8609 Westwood Center Dr., Suite 110,
Tysons Corner, VA 22182

CONTACT US

Harry Baker, Manager
harry.baker@dayblinkconsulting.com

DAYBLINK CONSULTING

www.dayblinkconsulting.com

© DAYBLINK CONSULTING 2025