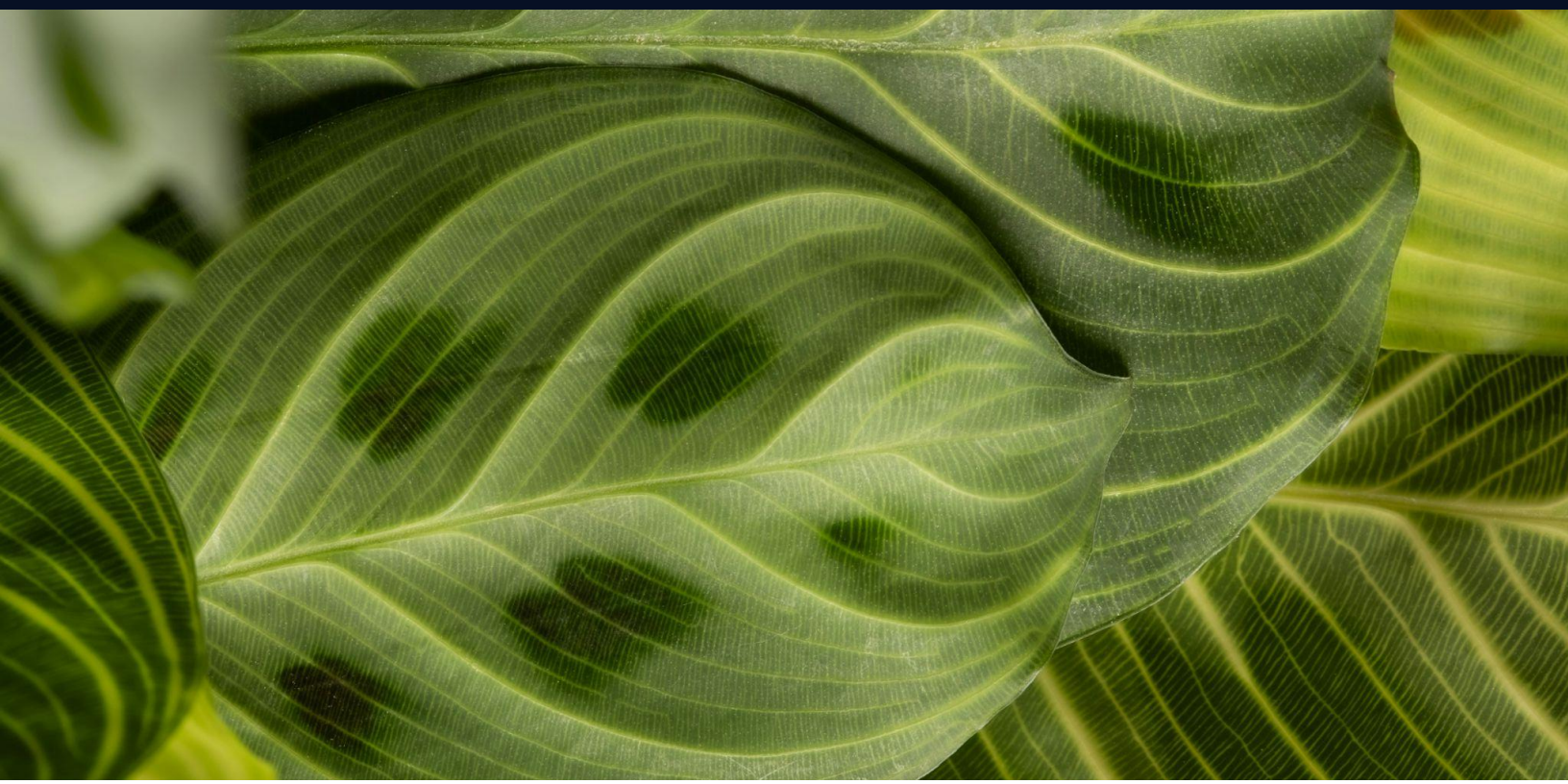
DAYBLINK CONSULTING

Automating Asset Ownership Identification for Vulnerability Management

How we assigned vulnerabilities using data and automation so that security personnel and fix agents could focus on risk remediation



Introduction

A major Communications & Media company faced a large number of long-lived vulnerabilities in their service delivery network for which the asset owner was unknown. Without an asset owner for whom to turn for remediation, each day the situation was going from bad to worse. Their existing manual ownership identification processes were hopelessly overwhelmed by the volume of newly discovered vulnerabilities and newly identified assets. To solve this problem, DayBlink Consulting helped the client wring value out of a fractured data environment by gathering tens of millions of records from various operational systems into a single repository, developing automation to sift through the enormous set of data to find clues to ownership, and building a user-friendly UI to help users fully confirm ownership where ownership identification was not definite enough for auto-assignment. Our solution successfully decreased the number of high severity vulnerabilities without an identified owner by 95% in just 12 months.

Problem

Our client's board of directors sought a significant reduction in the security risk across the company's extensive asset inventory

As a multi-service operator with millions of devices on its network, the company faced challenges in maintaining complete and accurate data within its unified asset inventory tool. Manual data entry by operational teams resulted in incomplete metadata, including crucial asset ownership information. Consequently, the security team struggled to assign vulnerabilities promptly, leading to a surge in high severity vulnerabilities without designated owners, rising to thousands at its peak. We have seen this challenge at numerous clients.

During discovery, we worked with our client to identify 5 major issues and pain points that exacerbated the problem:

1. **Fractured and Disconnected Data:** asset information scattered across dozens of systems lacked integration and governance
2. **Manual Identification:** security personnel spent hours searching through disparate datasets to find clues that might identify owners, with varying degrees of success
3. **Static and Stale Data:** teams relied on cumbersome email exchanges with static spreadsheets to confirm ownership
4. **No Data Governance:** inconsistent updates to asset ownership across inventory and security tools led to unreliable data
5. **Lack of Data Reconciliation:** teams faced challenges in ensuring updates propagated across systems resulted in persistent data discrepancies.

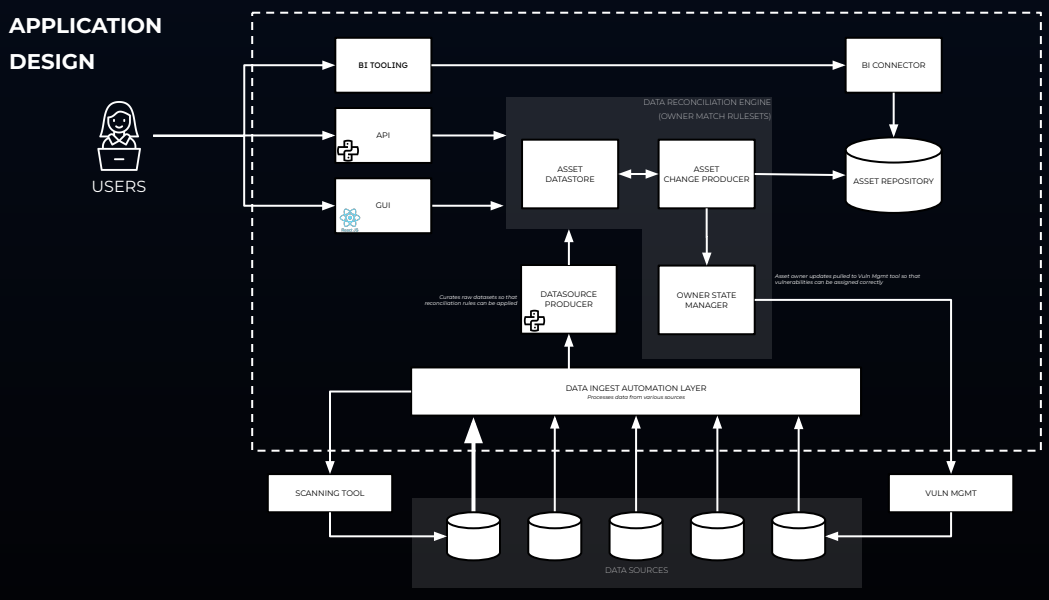
Solution

Our final product is a full stack application used by over 100 teams to more easily manage and collaborate on enterprise security

We designed and built an automated solution for asset owner identification to facilitate timely vulnerability assignment and remediation within target Service Level Agreements (SLAs). While the asset inventory tool had been considered the “source of truth” for asset ownership, the client also used dozens of operational systems to manage assets and operate their network. Many of these systems included asset metadata that could be used to understand ownership. Our team consolidated these data sources into a NoSQL data lake and set up automated ingest to ensure our solution had the latest information. Using these datasets, we developed automation that matches assets to owners based on predefined match rules.

Our sophisticated data reconciliation engine employs various fields and values in the data lake. This not only includes fields with clear ownership information like an email address, but also advanced pattern recognition on attributes such as hostname, operating system, scan tags and many others. To handle a single asset meeting criteria for multiple rules, our solution assigns ownership based on confidence scores determined in collaboration with our client. Lower confidence matches are retained as future ownership candidates.

To empower operational teams in validating or correcting low-confidence matches, we designed and implemented a user interface that enables end-users to confirm or decline that they own an asset. Beyond confirm and decline actions, the application and underlying APIs contain complex logic that enables users to transfer ownership between teams. Additionally, we developed a notification system to alert users of assigned assets requiring immediate review and developed business intelligence dashboards in Tableau for executive leadership insights.



Outcome

Through strategic automation, we helped our client achieve a 97% reduction in missing ownership for assets with high severity vulnerabilities

Our solution continues to proactively identify assets with incomplete owner information, ensuring a consistently low count of unassigned vulnerabilities. Most importantly, since the launch of our product, our client's vulnerability management team has observed a 90% drop in high severity vulnerabilities that remain open beyond their SLA.

Beyond risk reduction, this automation project delivered several other benefits. It substantially reduced or eliminated many manual processes that were time-consuming and frustrating for employees. We estimate that the project will reclaim 50,000 work hours annually for security personnel and operations teams. Assuming a conservative estimate of a six-figure salary for these in-demand employees, those hours translate to over $5M in cost savings each year. Furthermore, the initiative established a robust data platform that now serves as a foundation for addressing other automation and reporting needs beyond ownership identification.

Our ongoing collaboration with the client aims to extend the data platform to support additional asset management and security initiatives. Perhaps most interesting, accurate asset ownership information will become a foundational crown jewel of both the CIO and CISO organizations, enabling new capabilities, metrics and accountability.

90%
drop in high severity vulns open beyond SLA

95%
decrease in open, high severity vulns without a designated owner

50K
hours saved annually across FTEs involved

Making the Case for Automation

We believe that automation 'done right' can unlock incredible ROI and streamline operations for long-term success. Your teams can experience the transformative power of unified and automated security data to more effectively manage vulnerabilities.

WASHINGTON D.C. (Headquarters)

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

CONTACT US

John Morris, Partner
john.morris@dayblinkconsulting.com

Zachary White, Manager
zachary.white@dayblinkconsulting.com

DAYBLINK CONSULTING

www.dayblinkconsulting.com