PlexTrac®

Case Study

Large Enterprise Retailer Unifies Security Operations With PlexTrac

Overview

A large enterprise retailer was managing security findings across multiple teams, multiple tools, and multiple workflows. Offensive security, application security, purple team, red team, and vulnerability management functions were all generating valuable data, but that data lived in separate spreadsheets, reports, emails, and point tools. As a result, the organization lacked a consistent way to consolidate findings, prioritize remediation, automate workflows, and communicate progress to leadership.

To address this, the company adopted PlexTrac as a centralized platform for managing findings, assets, reporting, and remediation workflows across the security organization. By bringing together data from multiple teams and systems, PlexTrac helped the organization move away from fragmented manual processes and toward a more unified, operational approach to exposure management.

The Challenge

As the security program matured, the organization ran into a common enterprise problem: strong security work was happening across the business, but too much of it was disconnected.

Findings were spread across teams and tools

Pentesting, red team, purple team, application security, and vulnerability management teams were each managing findings in different systems. Some data lived in spreadsheets, some in separate tools, and some in manual reporting workflows. This made it difficult to consolidate information, identify patterns, and understand overall risk across the environment.

About the Customer

The customer is a large, distributed enterprise with a mature security organization spanning offensive security, vulnerability management, application security, and security validation functions. Multiple teams were producing important findings and insights, but because each team operated in its own workflows and tools, the broader organization struggled to build a shared view of risk and remediation progress.

The company needed a platform that could support both technical teams and leadership: a place to centralize data, automate operational workflows, improve prioritization, and generate reporting that clearly connected security work to business impact.

Manual workflows slowed action

Reporting and remediation tracking still relied too heavily on spreadsheets, emails, and manual follow-up. Security teams had to spend time piecing together updates, tracking status changes, and coordinating remediation through disconnected systems rather than working from a single operational workflow.

Prioritization lacked consistency

The organization wanted to go beyond simply collecting findings and instead identify broader risk themes, prioritize vulnerabilities based on business impact, and manage longer-term remediation campaigns with greater consistency. That required more structure around ownership, SLAs, and workflow orchestration.

Leadership reporting was too hard to assemble

The security team needed a better way to tell the full story of its work. Leadership wanted to see not only what had been found, but also how issues were being prioritized, assigned, remediated, and validated. Existing reporting processes made it difficult to show the end-to-end lifecycle from discovery to resolution in a clear, repeatable way.

Why the Customer Chose PlexTrac

The organization was looking for more than a reporting tool. It needed a centralized operational platform that could support multiple security teams, multiple data sources, and multiple remediation workflows.

PlexTrac stood out because it could serve as a shared system for findings, assets, procedures, reporting, and remediation management across the organization. The platform aligned well with the company's goal of consolidating security data, automating workflows, improving prioritization, and giving both practitioners and leadership a clearer view of exposure over time.

The team was especially focused on four priorities:

- Centralizing findings and assets across security teams
- Automating reporting and remediation workflows
- Improving prioritization based on business impact
- Generating stronger reporting and metrics for leadership

The Solution

The company implemented PlexTrac as a centralized platform for exposure-related data and workflows across its security program.

Centralizing findings across teams

Rather than keeping each team's work in separate tools and spreadsheets, the organization used PlexTrac to create a more unified environment. Teams including pentest, red team, purple team, application security, and vulnerability management could organize their work within PlexTrac while still contributing to a broader shared view of findings and assets. This allowed the organization to analyze findings by team while also reducing fragmentation at the enterprise level.

Automating remediation workflows

A major goal was to reduce reliance on manual tracking through emails and spreadsheets. PlexTrac gave the team a way to automate parts of the remediation process, including ticket creation and status tracking through existing systems such as Azure DevOps and ServiceNow.

This helped move remediation from a loosely coordinated process to a more structured operational workflow, with clearer ownership and better visibility into progress.

Improving prioritization and campaign management

The team also wanted to better identify recurring risk themes and prioritize remediation based on business impact rather than raw volume alone. PlexTrac supported that effort by providing a more centralized view of findings and allowing the organization to assign remediation work, manage longer-term campaigns, and track progress against SLAs.

This created a more repeatable approach to prioritization and helped the organization focus on the issues that mattered most across the environment.

Strengthening reporting and metrics

PlexTrac also addressed one of the company's most important needs: the ability to report more effectively to leadership. Instead of stitching together updates from multiple teams and spreadsheets, the security organization could generate more comprehensive reporting that showed the full lifecycle from finding to remediation, along with supporting narratives and evidence.

That made it easier to communicate the value of security work in business terms and demonstrate the impact of remediation efforts over time.

Supporting red team and validation workflows

In addition to findings management, the organization saw PlexTrac as a platform for red team operations. The team planned to use it to document procedures, track success and failure during exercises, build plans mapped to frameworks such as MITRE ATT&CK, and eventually automate parts of runbook creation and procedure management.

This expanded PlexTrac's role beyond reporting into a broader operational tool for security validation and adversary emulation workflows.

Building a stronger asset and data model

The company also wanted stronger asset management capabilities to support tagging, categorization, and analytics. Dynamic asset criteria, asset deduplication, and bulk tag management were all important because they would make it easier to organize data, surface metrics, and analyze trends across teams and environments.

By improving how assets and findings were structured, the organization could make reporting, prioritization, and workflow automation more scalable.

The Results

By adopting PlexTrac, the organization laid the foundation for a more connected security operating model.

A more unified view across the security program

Instead of managing findings in isolated team workflows, the organization could begin consolidating data from multiple functions into a single platform. That improved visibility across the program and reduced the manual effort required to bring information together.

Less manual coordination

Automated workflows and integrations reduced reliance on spreadsheets, email threads, and manual status tracking. Teams could move findings into remediation processes more efficiently and spend less time on administrative coordination.

Better prioritization and accountability

With a more centralized view of findings, the organization was better positioned to identify themes, prioritize based on business context, and manage remediation as an ongoing operational effort rather than a series of disconnected tasks.

Stronger reporting for leadership

The team gained a better path to reporting on the full story of its work: what was found, why it mattered, what was assigned, what was fixed, and what evidence supported progress. This improved the team's ability to communicate outcomes and demonstrate value to leadership.

A platform that supports multiple use cases

Perhaps most importantly, PlexTrac gave the organization a platform that could support multiple security functions at once. What began as a need for findings consolidation and remediation tracking also extended into red team operations, procedure management, asset analytics, and long-term workflow automation.

Why It Matters

For large enterprises, the challenge is often not a lack of security data. It is the lack of a shared operating model across teams.

This customer's experience shows why that matters. Pentest findings, red team insights, vulnerability data, and application security results all have value on their own. But when they stay trapped in separate workflows, it becomes much harder to prioritize consistently, automate remediation, and show measurable progress over time.

By using PlexTrac as a centralized platform across teams, the organization moved closer to a model where security work could be operationalized rather than just documented. Findings became easier to track, remediation became easier to coordinate, and reporting became easier to connect back to business outcomes.

Conclusion

This large enterprise retailer adopted PlexTrac to solve a complex but familiar problem: too many teams, too many tools, and too much manual effort standing between security findings and real remediation progress.

With PlexTrac, the organization created a more centralized and scalable way to manage findings, assets, workflows, and reporting across its security program. The result was a stronger foundation for prioritization, automation, leadership reporting, and long-term exposure reduction.

Learn how PlexTrac helps security teams centralize findings, automate remediation workflows, and drive measurable risk reduction at **plextrac.com**

PlexTrac is the leading AI-powered platform for pentest reporting and threat exposure management, trusted byFortune 500 companies and top security providers including Expedia, Mandiant, Deloitte, and KPMG. Built to help cybersecurity teams continuously manage and reduce threat exposure, PlexTrac centralizes security data, streamlines reporting, prioritizes risk, and automates remediation workflows—empoweringteams to drive measurable risk reduction.

Discover how PlexTrac can revolutionize your security operations at:

www.plextrac.com