Adding Intelligence to a Data Security Analysis System: Recommendation and Planning Support

Tianyi Li
Computer Science Department,
Virginia Tech
(previously: UX Team, Informatica)
Blacksburg, VA
tianyili@vt.edu

Gregorio Convertino
UX Research, Google
(previously: UX Team, Informatica)
San Francisco, CA
gconvertino@gmail.com

Ranjeet Kumar Tayi
UX Team, Informatica
Redwood City, CA
rtayi@informatica.com

Shima Kazerooni
UX Team, Informatica
Redwood City, CA
skazerooni@informatica.com

Gary Patterson
Product Management, Informatica
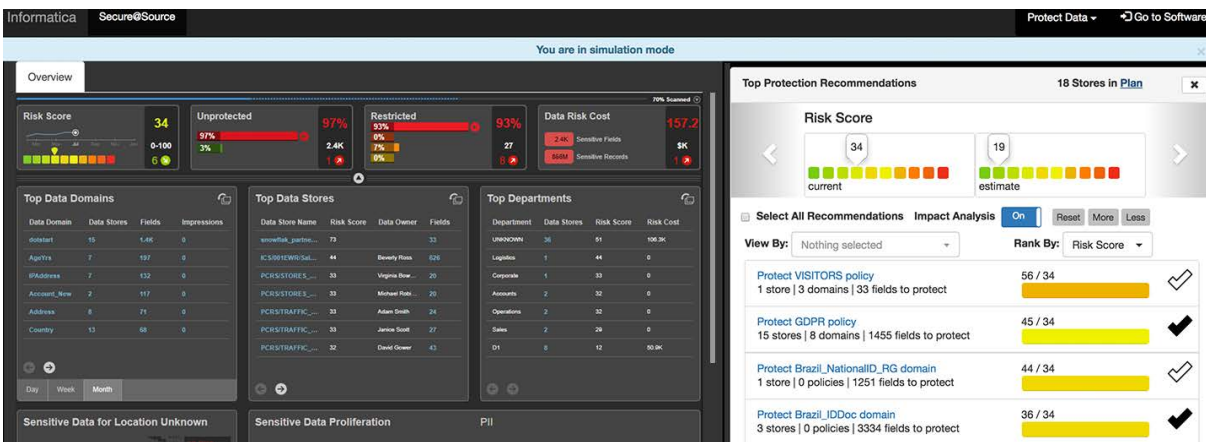Redwood City, CA
gpatterson@informatica.com

Figure 1: Recommender Sidebar Extending an Existing Data Security System [3] (See Video[4])

ABSTRACT

This demo shows a recommender bar and a planning workspace that augment an existing system. The design addresses two challenges for analysts doing proactive data protection: 1) the information overload from the many data repositories and protection techniques to consider; 2) the optimization of protection plans given multiple competing factors.

CCS CONCEPTS

• **Human-centered computing → Interactive systems and tools**.

KEYWORDS

Data security; recommendation; data protection plans

1 INTRODUCTION

A growing number of breaches of company sensitive data have occurred in the last few years, as for Facebook's 50 million user accounts in 2018 or Equifax's 143 million user accounts in 2017. Companies and government organizations are now taking up proactive technologies to secure sensitive data at source. In this new context, data security analysts are challenged by information overload due to the many stores and protection techniques available, and hard-to-optimize protection plans given multiple competing factors.
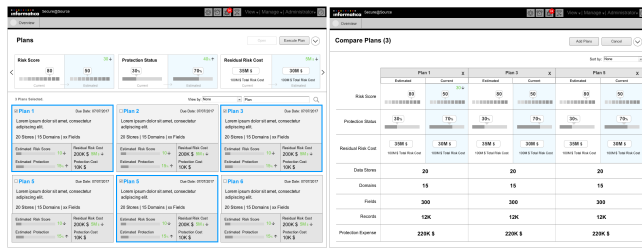
Figure 2: Plan Building Workspace - All Saved Plans (Left), and Compare Plans views (Right)

Figure 3: Functions to evaluate plans implemented in [3]

To help address these two challenges, we present an intelligent user interface that interactively recommends data worth protecting and helps build data protection plans. To enable this interface, we propose a new approach to model data risks by separating the two major concerns: how a data unit is used and regulated (conceptual attributes), and how a data unit is stored in systems (architectural attributes) [6]. Drawing on the risk metrics computed with this new approach, the system provides a sidebar that 1) recommends groups of unprotected data stores that lead to the highest risk reduction, if protected; 2) simulates the aggregated impact of the recommendations selected by the user; 3) captures user interactions and interprets latent user preference to customize the recommendations over time; and a plan building workspace to build and compare alternative protection plans.

2 RELATED WORK AND NOVELTY

We categorize data security systems into two groups. The first group collects and analyzes user events and log data to detect anomalies or identify malicious user activities [5]. The second group flags risks on sensitive data (e.g. Informatica's Secure@Source [3], IBM's QRadar Security Intelligence [1], and Imperva's SecureSphere [2]). This demo focuses on addressing the challenges faced by data security analysts when using this second and more recent group of systems.

3 SYSTEM

3.1 Recommender Sidebar

The system recommends in a sidebar groups of data stores with the highest impact on risk metrics (see Figure 1, bottom right). The algorithm quantifies the impact based on expected risk reduction. Over time, the logged user interaction is fed back to the algorithm to customize the risk quantification and recommendation.

The impact analysis carousel at the top of the sidebar shows the current and estimated future values of risk metrics (see Figure 1, top right). The estimated value is updated as the user selects the recommendations, showing the aggregated impact (see filled checkmarks in Figure 1 and video at [4]).

3.2 Plan Building Workspace

After making decisions in the sidebar, analysts can organize and edit data stores in the plan building workspace.

As shown in the video demo at [4], the plan building workspace visualizes the protection impact per-store ranked by risk reduction.
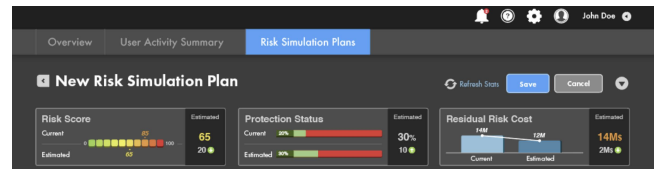
The residual risk values are shown on the side of each store. Analysts can still access the recommender sidebar from this workspace to iteratively refine the plan.

After a user has created multiple plans in the workspace, the details of each plan can be viewed in a full-page view (Figure 2, left). The top of the page shows the aggregate impact of the plans selected, with plan metrics at the bottom.

The plan comparison page displays the plans by column and shows the risk metrics and data details by row (Figure 2, right). The table shows the current and estimated future risk metric values in each plan. Reports on plan comparison can be saved and exported for review before execution.

4 EVALUATION AND NEXT STEPS

The system was evaluated with target users and proxies and received positive feedback [6]. Some functions of the plan building workspace were implemented in [3] (see Figure 3). The recommender sidebar will be implemented in the future.

REFERENCES

[1] 2018. IBM Data Risk Manager. https://www.ibm.com/us-en/marketplace/data-risk-manager. (2018).
[2] 2018. Imperva SecureSphere. https://www.imperva.com/products/securesphere/. (2018).
[3] 2018. Informatica Secure @ Source. https://www.informatica.com/products/data-security/secure-at-source.html. (2018).
[4] 2018. Video demo of the final system. https://youtu.be/QF_IYWcUccI. (2018).
[5] B. Haim, E. Menahem, Y. Wolfsthal, and C. Meenan. 2017. Visualizing Insider Threats: An Effective Interface for Security Analytics. In *Proc. IUI Comp.* ACM, 39–42.
[6] Li T., Convertino G., Tayi K. R., and S. Kazerooni. 2019. What Data Should I Protect? A Recommender and Impact Analysis Design to Assist Decision Making. In *Proceedings of IUI*. ACM.