CASE STUDY

mimecast

Rakuten

How Rakuten transformed insider risk management

Embracing a detection-focused strategy to protect data in a remote workforce

The challenge: A growing need for insider risk management

In late 2019, insider threat management was already on Rakuten's radar as a key priority. However, the urgency to act was driven by a customer requirement to implement a "valid DLP solution" as the company shifted to a more remote work environment.

As a large organization with a diverse range of business units, Rakuten faced challenges in identifying critical assets and understanding where intellectual property (IP) and sensitive data were housed. This made it clear that a modern insider risk management program was essential to protect the company's assets and adapt to the rapidly changing work environment.

A modern approach to insider risk management

Rakuten realized that a traditional, prevention-based approach to cybersecurity wouldn't suffice. Instead, the company needed to embrace a detection-focused strategy that prioritized risk visibility across the organization.

The team integrated Mimecast Incydr with Exabeam Advanced Analytics to monitor file activity and detect anomalous behavior. This approach eliminated the need for traditional data classification and policy-heavy solutions, allowing for more effective mitigation of IP theft and accidental data leaks. By focusing on operationalizing the highest-risk investigations, Rakuten moved away from relying on static DLP controls, which were impractical given the size and complexity of the organization."

Understanding the unknowns

Embarking on an insider risk management initiative required Rakuten to acknowledge the gaps in its existing processes. By partnering with the Incydr team to conduct a comprehensive **Insider Risk Management assessment**, Rakuten uncovered critical insights about its data governance and lifecycle management practices.

The assessment revealed that while some policies were in place, access controls and employee lifecycle management lacked maturity. This process expanded the scope of what the company needed to address, highlighting that insider risk management was about much more than installing software. It required building a comprehensive program and fostering a risk-aware culture. To achieve this, Rakuten started small, focusing on IT and security operations before gradually scaling the program across the enterprise.

Uncovering hidden risks: Pandora's box

When Rakuten integrated Incydr's cloud connector into Exabeam, the team gained visibility into a wealth of file activity and telemetry data. This opened their eyes to risks they hadn't previously anticipated.

For example, they had planned to monitor departing and high-risk employees but discovered other patterns of concern, such as new hires engaging in suspicious activity shortly after joining the company. Incidents like these, including cases where new employees inserted external drives containing potentially stolen data, became a significant learning curve for the team.

"We needed to build a more comprehensive program and risk-aware culture; it was much bigger than installing software to solve the problem."- Rakuten

This expanded understanding of insider risks enabled Rakuten to refine its program and address unexpected vulnerabilities.

Turning down the noise with advanced integration

Rakuten's size, 40,000 employees, meant that managing the volume of data and alerts could easily become overwhelming. To address this, the team relied on Incydr's risk prioritization & filtering capabilities and Exabeam's automation tools to streamline risk analysis.

For example, HR applications were integrated via APIs to automatically track new employees, departing employees, and create watchlists. When an employee on a watchlist triggered specific actions, an incident was automatically flagged for investigation.

One standout feature was the use of file hashes provided by Incydr. By creating a database of critical files, the team could run queries and pinpoint where these files existed within the environment, identifying suspicious anomalies. They also established baselines for normal activity around specific file types, such as source code, enabling faster and more accurate assessments of potential risks.

Building a risk-aware culture

A key factor in Rakuten's success was the involvement of HR and Legal from the start. These teams played a critical role in defining policies, securing end-user buy-in, and shaping case management workflows.

Rather than relying solely on technology, Rakuten built its Insider Risk Management program around people and processes. The security team acted as an objective sensor, feeding high-fidelity signals and context into the Exabeam platform. HR and Legal then determined the appropriate response, whether that involved a corrective conversation with an employee, involving a manager, or taking more serious action.

This collaboration ensured that insider risk management was not just a security initiative but a cross-functional effort impacting the entire organization.

Key takeaways for building an insider risk program

Rakuten's journey offers valuable insights for organizations looking to implement or enhance their own insider risk management programs:

1. **Start by understanding your current state**

Before building a program, it's essential to assess your organization's current maturity level. Identify gaps in policies, governance, and access controls to create a solid foundation.

2. **Foster cross-functional collaboration**

Security teams cannot succeed in isolation. Engaging key stakeholders like HR and Legal from the beginning ensures that the program is aligned with organizational goals and has the support needed for effective implementation.

3. **Recognize that insider risk management is people-powered**

Technology alone cannot solve insider risk issues. A successful program requires a combination of the right tools, a risk-aware culture, and clearly defined processes to address incidents effectively.

A modern, scalable approach

Rakuten's insider risk management program demonstrates the importance of taking a modern, scalable approach to cybersecurity. By integrating advanced tools like Mimecast Incydr and Exabeam, collaborating with cross-functional teams, and embracing a detection-focused strategy, Rakuten was able to protect its critical data and foster a more risk-aware culture across the organization.

For any organization facing similar challenges, Rakuten's experience underscores the need to think beyond traditional DLP solutions and invest in a comprehensive, people-powered approach to insider threat management.

About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscape, you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.