CASE STUDY

mimecast

certinia

Certinia Protects Data from Departing Employees and Third Parties

An Insider Risk Management solution built on the right combination of strategy and technologies.

Company Name: Certinia
Industry: Technology
Company Size: 1000
Use Case: Data Protection

Certinia is a provider of customer-centric business applications built on the Salesforce platform. With employees spread across eight locations, it's critical for Certinia to design a well-integrated Insider Risk Management program to protect their critical intellectual property (IP).

The Problem

Protecting Data from Departing Employees and Third Parties

On an annual basis, the Certinia security team conducts an executive information security risk assessment to align team priorities with business objectives and identify the most pressing risks in the organization. Reputational, operational, and financial risks are high priorities because they have significant business impact. Based on this assessment, Aaron Momin, CSO at Certinia, determined that Certinia data leaking by departing employees, to competitors or to third parties was a significant security risk with the potential to cause major business impact.

These findings became the backbone of how Certinia defines its business data risk tolerance. In other words, any data leak that involves departing or former employees, competitors, or third parties is considered high risk. From a data security perspective, this means that the security team needed to deploy and integrate the right technology, and establish repeatable workflows, to mitigate Insider Risk in these high-risk situations.

As a consequence of doing this annual assessment, we've continually found that Insider Risk is our top concern. And that's why we're investing heavily into Mimecast Incydr," says Momin.

The Challenge

The Need for Speed & Reducing Alert Fatigue

Any security leader today is familiar with the challenges related to the industry's skills shortage. To effectively protect data from Insider Risk, and meet executive expectations, Certinia needed the ability to quickly detect and respond when critical Insider Risk events occur.

Their security team simply didn't have time to manually sift through a mountain of alerts to

determine which are high risk and which aren't. To save them time, and decrease alert fatigue, Momin knew they needed a solution that could prioritize the risk that matters most and provide flexible ways to automate response. "For our security team, speed to response is critical. It's not about boiling the ocean, but mitigating the top risks against the company — and prioritizing our efforts," says Momin.

Customer Requirements

- **Solve top use cases:** The annual risk assessment helped Momin and his team identify protecting data from departing employees, competitors and third-parties as the key use cases they needed a solution for.
- **Protect the data that matters most:** Certinia determined that their organization's "crown jewels" primarily consisted of source code, IP, and customer data (source code, IP, customer data, etc.), and they needed a solution to secure it.
- **Focus on speed:** Certinia needed a solution that could help them quickly prioritize the alerts that matter most without contributing to alert fatigue.

The Solution

Why Incydr was the right solution for Certinia

Through his tenure in data security, Momin knows that data is always - changing, meanwhile threat actors, business transactions and workflows are always evolving. This dynamic means that it is essential to have a solution that can provide continuous visibility into risk exposure. As Momin and his team looked further into solving these complexities they discovered **Incydr**™ provided the best solution for Certinia to manage Insider Risk. "We recognized that Incydr could help us discern and prioritize what we should be looking at, which would help our team focus on what matters most, rather than having to look at everything under the sun — or having to rely fully on an MSSP."

Key Features & Integrations

Incydr makes this possible because it detects file exposure and exfiltration across computers, cloud and email systems, using its agent and API-based integrations. This comprehensive approach to monitoring everything becomes Incydr's baseline of what's normal and what's abnormal. Incydr is then able to filter out trusted activity so that Certinia can easily identify when files are going to untrusted destinations or devices. With intelligence from Incydr and guidance from their advisory services, Certinia gained a baseline of what user behavior and data movement is normal and what is abnormal in their environment. This foundation makes it easy for Certinia to leverage key Incydr features and integrations to customize an IRM solution for their specific needs and priorities.

Prioritize alerts with Insider Risk Indicators (IRIs)

Certinia relies heavily on Incydr for its ability to prioritize risk. Incydr's risk prioritization is powered by Insider Risk Indicators (IRIs), which are the activities or characteristics that suggest corporate data is at higher risk of exposure or exfiltration. In addition to being a user of IRI's, Certinia was a beta customer for the creation of **Incydr's prioritization model**.

Certinia has customized Incydr IRIs based on what they care about most. Momin explains, "We have a taxonomy that we look at. So any external Google Drive sharing is a top priority. Any public link sharing is a top priority. Shared Slack channels with external organizations — those are a big

> "As a consequence of doing this annual assessment, we've continually found that Insider Risk is our top concern. And that's why we're investing heavily into Incydr."
> **–Aaron Momin, CSO at Certinia**

channel for leakage and risk exposure that we want to look at. And then we let Incydr do its magic."

Simplify alert triaging with Incydr and Slack

Momin and the Certinia security team quickly saw the value of Incydr's comprehensive visibility and risk prioritization. To operationalize this value and streamline workflows for Certinia's security team, they decided to integrate Incydr and Slack. "We built a Slack bot that automatically notifies us to user and file activity, based on rules.

This helps our security team triage alerts more quickly and more effectively," explains Momin. "In the future, we plan to incorporate the ability to take automated actions based on Incydr's risk indicators and alerts," he says. "For example, if a departing employee has just uploaded sensitive documents to a personal Google Drive, we would want to automatically revoke that access in real time."

Incydr Flow for departing employees

Incydr's risk detection lenses help Certinia enhance monitoring for high-risk user groups, like departing employees. Certinia has streamlined this process by integrating Incydr and ADP. Now, when HR adds a new departing employee to ADP, the employee will automatically be added to Incydr's departing employee lens. This generates a departing employee Insider Risk Indicator, which increases the risk score associated with any data exposure or exfiltration caused by the user.

The security team relies on this Incydr Flow, and close partnerships with HR, to ensure that Certinia's data is secured during employee departures. Momin explains,

"So, when we see that this departing employee just uploaded certain kinds of documents to a personal Google Drive account — and Incydr detects a critical IRI — then that becomes a priority in terms of incident response. We also get a lot of important information just through partnering effectively with HR," he explains. "If HR advises that a particular employee is high-risk, we add them to the High Risk Detection Lens and assign a risk factor based on HR's feedback." This allows Momin and his team to speed their time to respond to critical incidents.

Integrated risk scoring engine

Incydr's alert data surfaces substantial intelligence related to employee file-sharing behavior, acceptable data exposure thresholds, and Insider Risk Indicators. Certinia integrates this information into a comprehensive risk scoring engine built in Splunk. This engine brings Incydr's prioritized alerts into focus with other endpoint data risk factors, user internet browsing behaviors, detected phishing activity, and security awareness training scores. This integrated risk score provides Certinia with a comprehensive view into risk.

"It gives us a precise and factual indication of who is most likely to become an insider risk to the company," says Momin. "We can also group risk by function. So, for example, we can decipher that a certain function may tend to be the riskiest based on a high concentration of employees with high risk scores."

> "Shared Slack channels with external organizations — those are a big channel for leakage and risk exposure that we want to look at. And then we let Incydr do its magic."

Educational Controls for Right-Sized Response

Certinia's risk score engine is optimized in accordance with their risk tolerance. It is also what helps inform the response action needed. In many situations, Momin finds that security awareness training is a great way to respond to Insider Risk events. By leveraging this type of educational controls, Certinia can accelerate their time to respond, as well as mitigate future data exposure by building a more risk-aware culture.

Momin explains how this approach will pay dividends to Certinia in the long run, "We can take steps like providing better education and training, maybe heightening some of our security controls with Splunk and Incydr, things like that," he explains. "I think it's really going to mature our overall insider risk program at Certinia."

The Benefits

- Accelerate response by correlating Incydr IRIs and alerts with other security telemetry in their integrated user risk-scoring engine.
- Save time by automating previously manual processes to protect data during employee departures and other high-risk times.
- Secure corporate data by closing Insider Risk Posture gaps with a holistic IRM solution.