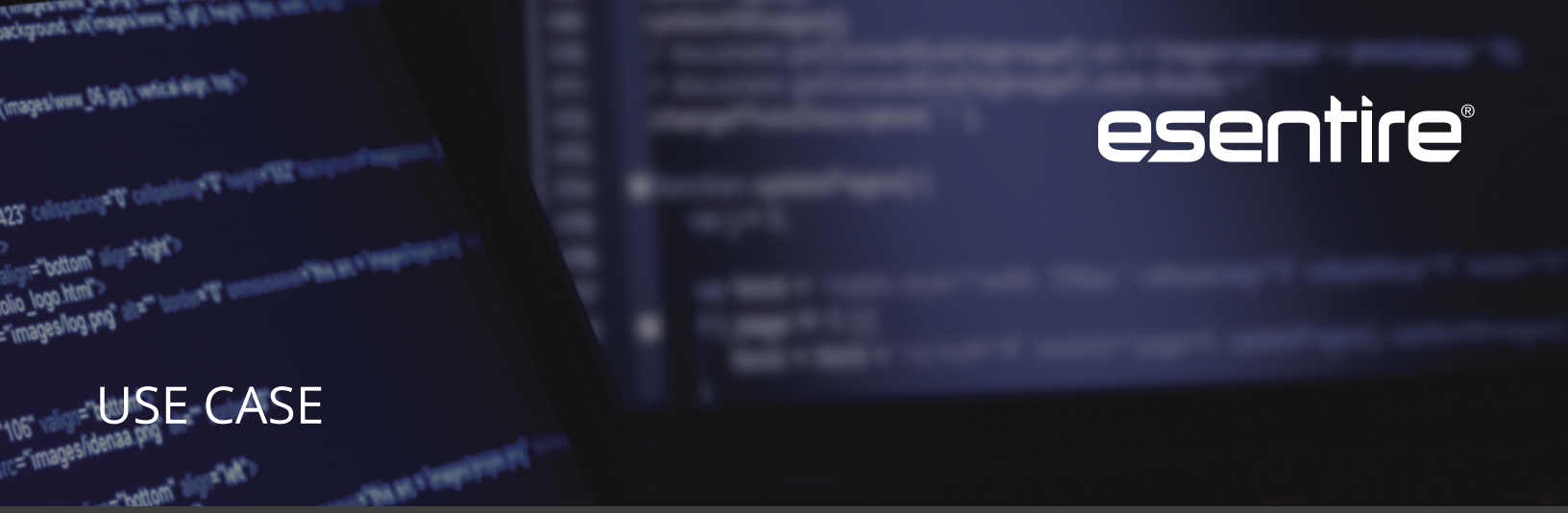

USE CASE

Incident Report: Monitoring Suspicious Employees

Financial services firms host sensitive and confidential information that is critical to the success of their business. The last thing a firm wants to deal with is its own people leaking that information. eSentire Managed Detection and Response™ can help to prevent confidential data leaks resulting from insider threats.

6:00 PM - Sound the Alarm

An eSentire client overheard a conversation amongst employees working together to exfiltrate data, with the intent of leaking it to competitors. The group in question was the firm's IT department, who had a strong relationship with the company's IT provider. Because of the sensitive nature of the situation, the client raised their suspicions to eSentire's Security Operations Center (SOC) analysts, whom they trusted to either confirm or dispel their concern.

6:30 PM - Investigate Employees

The client conferenced in eSentire SOC analysts to establish a plan. Analysts walked the client (who had limited technical knowledge) through the process of gathering the suspect's IP addresses. With a general idea of the kind of information they needed to look for, by 12am the SOC analysts had all of the information required to assemble a report and start a formal investigation. Work continued around the clock until the investigation was completed the following day.

AM Next Day - Prevent and Protect

The next morning the analyst team arranged a call with the client to walk through the findings. The client was impressed but asked analysts to uncover additional detail to determine the involvement of every suspect employee. In addition to continued real-time monitoring, analysts retroactively investigated historic traffic (spanning two weeks) to uncover additional evidence that would support the case. The investigation continued for two more weeks, and provided the client with definitive evidence of a planned data leak. The client was able to confidently dismiss the involved employees. SOC analysts were able to provide additional assurance that no confidential information had been leaked. The SOC's quick response and attention to detail helped the client evade a potentially damaging breach scenario.

Cyber threats can come from inside and outside of your firm. Being able to react quickly is crucial, especially when confidential information in involved. Our 24X7 team of elite security analysts live inside our technology – monitoring, hunting, and responding to threats. Is your firm at risk? Contact us to learn more about how Managed Detection and Response can help protect you.