LogRhythm Incident Response and platform expertise saved retailer thousands

The Challenge

Investigating a possible data breach involving credit card data

A large retail company suspected a data breach had occurred that resulted in credit card numbers being exfiltrated by unknown attackers. Due to Payment Card Industry (PCI) compliance, the company's security team and external Payment Card Industry Forensic Investigator (PFI) firm snapped into action.

Because PFI firms are always external to the organisation's security team, they rarely have deep expertise in any specific platform like LogRhythm. In this case, the PFI firm's solution to a lack of strong LogRhythm expertise was to export all data from the SIEM and then import the SIEM data into tools more familiar to them. The PFI firm's proposed solution would have been time-consuming and delayed the investigation by days. The retailer suggested a workaround to fill in the knowledge gap for the PFI firm in order to conduct a faster overall investigation.

The Solution

Empowering effective incident response with IIR Services

The retail organisation brought in LogRhythm's Incident Investigation and Response (IIR) Services team to assist the PFI firm. LogRhythm's IIR Services team trained the PFI team on using LogRhythm to search in active log data as well as retrieve event data from backup storage; thus eliminating unnecessary export and import processes the PFI firm previously proposed.

The IIR Services team guided the investigators on the most efficient way to design their investigative queries, by writing SecondLook searches and optimising the platform to perform those searches. Additionally, the LogRhythm team designed file integrity monitoring (FIM) rules to monitor critical files, including monitoring for files containing exported credit card data.

Finding value

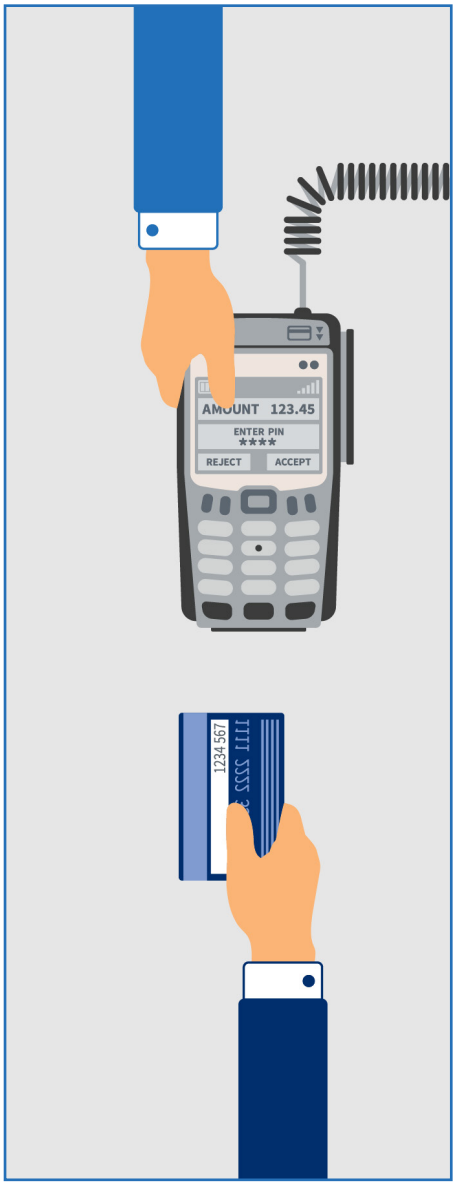
LogRhythm IIR Services saved the retailer thousands in PFI firm fees

The retailer avoided several days of PFI fees using LogRhythm's IIR Services that increases visibility into the possible data breach and reduces the overall investigation timeframe. Since PFI firms utilise hundreds of different security tools to perform their investigations, they are not well versed in incident response on all security tools or SIEM platforms. LogRhythm's IIR Services more than paid for itself in this engagement in costing thousands of pounds less than the added billable hours the PFI firm wanted to take because they lacked LogRhythm platform expertise for incident response. Ultimately, the retailer was able to meet their PCI compliance requirements, as well as remediate the threat from their network.

IIR services' augments your staff or a mandated firm's staff with incident response-specific platform expertise to provide faster response to concerning security incidents.

IIR services case study at a glance

- ✓ Retail company had a possible data breach
- ✓ PFI firm investigated but was not familiar with LogRhythm
- ✓ LogRhythm IIR Services helped the PFI firm use LogRhythm for incident response
- ✓ Retail company saved thousands due to the time saved by using LogRhythm IIR Services



About PCI compliance

Payment Card Industry (PCI) compliance applies to any entity worldwide that stores, processes or transmits credit cardholder's data. If there is a breach or a suspected breach of cardholder data, the credit card company most likely will require an independent forensic investigation to be completed by an external PCI-listed payment card industry forensic investigator (PFI).

What should an organisation with a possible breach do?

It is critical that the victimised organisation contact their PFI and start collecting/preserving forensic evidence immediately once the possible breach is detected. The organisation's internal security team is not allowed to start the investigation. Instead, they must work to preserve and make all data available for the PFI firm. The organisation with the possible breach must engage effectively with the external PFI firm and pay for the investigation.

How much does the victimised organisation pay for the PFI firm?

Depending on the scope of the breach, the timeline for remediation and cost varies on a case-by-case basis. PFI's rate per day ranges from $13,000–$30,000.

What is the PFI firm's role in the data breach investigation?

To complete a thorough and effective investigation, the PFI will require access to data, facilities, and people. They will also need to complete a checklist similar to the one found in the Best Practices for Victim Response and Reporting Cyber Incidents publishing by the Department of Justice, Criminal Division, Cyber Security Unit. The PFI's task is to make a high-level assessment as to whether the organisation was compliant with each of the 12 PCI DSS requirements at the time of the breach. The PFI doesn't attempt to validate compliance (a positive), but rather looks for non-compliance.

Data breach with PCI compliance at a glance

- ✓ Organisations are required to bring on a PFI if there is a possible data breach of credit card data
- ✓ The company with the possible breach is responsible for the cost of a PFI
- ✓ Daily rates for a PFI range from $13,000–$30,000 a day