HELECLOUD

Building a Security Information and Event Management System (SIEM) for SentryBay

SentryBay®

The Challenge

In a world where remote working is the new normal, SentryBay have developed and patented a technology which protects the end-user device from data breach. The SentryBay products provide protection from advanced threats at the key points where data is most vulnerable: at point of data entry, during transmission and when exposed to new phishing and malware attacks. Endpoint data protection is essential for overcoming security gaps in both technology and user behaviour.

The ever-increasing demand for such protection has made SentryBay a trusted partner to some of the world's largest enterprises – from Mitsubishi Bank to the Federal Reserve. Having customers in the financial sector means SentryBay's AWS infrastructure had to be PCI compliant and secure 24/7/365 which is where HeleCloud's Managed Security & Compliance Services came in.

The Solution

To ensure SentryBay's estate is fully compliant to the PCI standard, HeleCloud started by building a SIEM using ElasticSearch and Kibana where all logs and security data can be ingested and then correlated. The ELK-based SIEM is integrated with AWS Security Hub and is fed data from CloudTrail, Amazon Inspector, EC2 Systems Manager Logs, RDS logs and CloudWatch. Using AWS Security Hub's native PCI and CIS rules packages, we get a real-time picture on the security posture of the account. On top of that, HeleCloud's Managed Security & Compliance Service adds custom rules for all compliance controls that are not currently covered by AWS Security Hub, some of which have automated remediation rules installed such as vulnerable ports being opened or CloudTrail being disabled.

With all security data ingested and parsed into the SIEM, the next step was to create alerts on any warning and critical events which when triggered go directly to the HeleCloud Security Service Desk. Combining manual and automated security incident response, we can ensure the environment will remain secure and compliant at all times, regardless of when the next audit is.

An important part of every compliance audit is being able to provide reports that illustrate that the estate's security is constantly monitored against the compliance standard's controls. The HeleCloud SIEM contains a package of PCI dashboards which can be readily used for audits as well as a custom in-house built add-on which exports the dashboards from Kibana into an S3 bucket on a schedule. This way, SentryBay can see a snapshot of the environment's security posture without having to keep a year's worth of data into the SIEM or re-import it from cold storage. This reduces greatly the cost of the SIEM and adds an extra convenience for the audit process.

The Results

Using the SIEM's benefits of combining the entire infrastructure's security data in one place for visualisation and analysis, plus the added automation for compliance audit and remediation, and last but not least the expertise of the HeleCloud Managed Services Team, SentryBay was able to successfully pass their PCI compliance audit. With the right tools, automation, processes and people, the infrastructure remains continuously compliant and secure, allowing SentryBay to focus on their business goals and pass each year's audit stress-free.

"As a security company we recognise the importance of security for our AWS infrastructure. HeleCloud aligned well with both our vision and challenges, being responsive to our needs and ensuring we are able to easily meet our compliance commitments."

Andrew Aitken-Fincham

SentryBay Senior Web Developer