Case Study

BINARY DEFENSE

Insurance company keeps customer data safe from threat actors with help from Binary Defense SIEM management

Business Overview

Private insurance firm serving over 300,000 customers

Challenges

Insurance company concerned with cybercriminals targeting them to steal customer data

SIEM management was time-consuming

Building an internal SOC was not within budget

Results

Binary Defense monitors AT&T Cybersecurity SIEM instance and is an extension of the insurance firm's team

Rapid access to dashboards and information to help respond more quickly to threats

"As an insurance company, we sell trust. It's not a tangible product. And that's what we feel we get from Binary Defense. We trust them." -Security Manager, Insurance Organization

Insurance companies need to keep customers' personal information safe
Insurance companies are tasked with selling services to their customers that offer protection. Whether this is automotive, home, life, or other insurance types, customers entrust these companies to provide them with a feeling of financial safety should they experience misfortune.

So, imagine the consequences if an insurance company was responsible for exposing its customers' personal data due to a cyberattack. Threat actors can extort consumer data from insurance companies by deploying ransomware or other malicious types of attacks. They can steal financial information through means such as credential stuffing, where criminals use compromised password information across multiple websites in the hopes that someone has used the same password on more than one site. A few high-profile insurance organizations have seen their name in national news headlines due to breaches, causing a ripple in customer trust.

As a result, the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (#668)[1] was drafted as a way to regulate how companies are handling consumer data and mitigate the chance of a security breach. This model requires insurers to develop and maintain a security program and continually assess the risks faced by the business. As of 2020, not every state in the US had adopted this policy, but more are moving toward adoption.

Large insurance provider needed SIEM support
Most IT security staffs are overburdened with maintaining their security infrastructure and investigating incidents. They often look to a third-party managed security services provider (MSSP) to work as an extension of their team and notify them when an incident needs to be remediated.

An insurance company in the Midwest, serving over 300,000 customers, selected Binary Defense to offset the task of monitoring their Security Information & Event Management (SIEM) solution. Despite having twelve people on staff, the insurance company realized that they couldn't keep up with the around-the-clock monitoring that needs to happen to make an investment in SIEM effective. "It was hard to do it ourselves," the Security Manager for this organization said. "When you have a small team, maintaining a SIEM, implementing detection use cases, and responding to alerts feels a lot flying an airplane and trying to do engine maintenance at the same time." He noted that their on-premises SIEM was running slower and slower to the point where it wasn't performing. They weren't able to keep up with tuning, and instead, had a mountain of alarms that was bogging everything down.

"We were ready for a partner," he said. "To build our own 24/7 SOC was just not cost-effective and it was going to be slow to build up. We wanted a

Binary Defense SIEM Services

Customized SIEM solutions to meet the needs of your specific environment.

Tuning on a continuous basis to improve accuracy of SIEM instance.

Dedicated security analysts managing your SIEM 24x7x365 through our Security Operations Center.

Security Operations Task Force members are an extension of your team.

We don't have to wait on a query. We get the information right away. We can rapidly view dashboards and get the info we need when we are responding to a threat detection." – Security Manager, Insurance Organization

quicker solution."

The company chose Binary Defense after researching a handful of organizations that were either too large and made them feel like they weren't going to get a personalized level of service, or not sophisticated enough to handle the needs of the insurance company. "Binary Defense was able to provide more customized services," the Security Manager said. "We feel like an important customer to them."

Binary Defense is an extension of the team

Binary Defense helped them install a cloud-based version of AT&T Cybersecurity USM Anywhere™, which immediately solved the performance issue. Now, the Security Manager says, "we don't have to wait on a query. We get the information right away. We can rapidly view dashboards and get the info we need when we are responding to a threat detection." In addition, Binary Defense assisted with tuning the SIEM to help them cut down on all the noise being generated by the alarms.

Binary Defense is an extension of the insurance company's team. During implementation, the two organizations spoke on weekly calls. Now, the Binary Defense Security Operations Task Force notifies the insurance company's security team when an alarm needs to be investigated, rather than the team spending valuable time chasing down irrelevant alarms.

The IT Manager noted a purple team engagement the organization recently conducted where Binary Defense was able to detect a threat within an average of seven minutes, which was well under SLA.

"As an insurance company, we sell trust. It's not a tangible product. And that's what we feel we get from Binary Defense. We trust them," the Security Manager said.

1 https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf