Health Insurer

Employee Count: 700

Location: Northeast

Challenge: Slim team unable to perform 24/7 monitoring and management of traditional SIEM

Services Provided: Managed Open XDR

Health Insurance Provider Challenged by Traditional SIEM Turn to Managed Open XDR

It is no secret that the healthcare industry requires centralized log management and archiving. As a result, a healthcare insurance provider in New England has been on an extended log management journey.

The journey started with a traditional on-premises SIEM (security incident and event management) solution. The on-premises option provided the necessary control and oversight of its PHI data, satisfying HIPAA requirements. However, dramatic under scoping left them with a poorly performing tool that either did not ingest all its logs or took too long to perform searches. Ultimately, they needed to double the initial licenses and dedicated resources, significantly increasing the already expensive investment.

Additionally, they faced the common challenge of having a relatively small security team with no dedicated staff or a SOC to provide 24/7 monitoring and management of the SIEM.

That is when the healthcare insurance company turned to Brite and the BriteProtect co-managed Open XDR (extended detection and response) security service. The attractive capabilities include the complete co-managed platform, a cost-effective solution, cloud scalability and a 24/7 team to monitor and respond to threats.

Downtime was not an option during the transition for the healthcare insurance provider.

A typical BriteProtect deployment takes approximately 45 days from project kick-off to log collection, normalization, correlation and response. In this time, Brite is collecting logs from all sources through standard syslog, custom parsers or bi-directional APIs. Playbooks are customized for the customer environment, specific escalations and responses.

Jon-Michael Lacek, Director of Security Operations at Brite, comments on this unique deployment, “We had to take a modified approach with the healthcare insurance company since the SIEM was already in place. We started by forwarding all logs and alerts from the incumbent SIEM directly into the BriteProtect platform. One by one, we then pointed the sources directly to the XDR platform, starting with the API integrations with tools like Crowdstrike, Check Point and Tenable. This cut down on the time spent implementing and enabled more time to investigate.”

$4.24m

Global average total cost of a breach

38%

Lost business share of total breach costs

80%

Cost difference where security AI and automation was fully deployed vs. not deployed

The healthcare insurance company experienced a significant reduction in overall spend on alert management and response after the full migration to BriteProtect. Ultimately, the cost of the entire BriteProtect (people, process and technology) equated to about just the total licensing spend on the SIEM - a drastic reduction when you add in the infrastructure and staff needed to operate the previous SIEM. In addition, the advanced AI engine provides more proactive alerting and less false positives. Lastly, the scalability of the cloud eliminated the short-term bursts and long-term growth concerns.

About BriteProtect

BriteProtect is an advanced managed security service that solves the problem of tedious alert management leading to missed critical alerts and employee fatigue. We leverage decades of cybersecurity experience to provide our customers with unprecedented visibility, swift response and expert insights delivered via people, process and technology. Now, organizations can leverage existing security tools by partnering with Brite's team utilizing new, next-generation technology to elevate its security posture and better utilize internal resources.

About Brite

At Brite, people and technology are at the core of everything we do. We're committed to proactively protecting communities and organizations through innovative technology solutions delivered by our talented team.

Brite delivers industry-leading cybersecurity solutions to businesses in various industries across the country. We deliver the most comprehensive IT and security services by providing the right people and proven processes when technology alone is not enough.

Our proven methodology of partnering with thoroughly vetted industry-leading technology vendors, delivered by the Brite team, which is evident by our numerous awards, including a seven-time Inc. 5000 honoree.

Most importantly, we envision partnerships with clients where our team enables others with the technology and processes to better achieve *their goals and objectives*. And we're here to help with Brite People. Brite Solutions.

Brite