Municipality

Employee Count: 3,500

Location: Northeast

Challenge: Strained internal resources unable to provide 24/7 monitoring and management

Services Provided: Managed Open XDR

Streamlining Security: How a City Overcame Alert Overload

The Challenge

A Northeast city faced a similar challenge to many municipalities – too many tools, too much data, and not enough people to effectively manage the alerts. The city had a comprehensive security stack but was unable to dedicate the proper resources to actively monitor and research the numerous alerts generated by these tools.

Developing Needs

The search for 24/7 security operations center services started in January of 2022. The goal was to contract with a service provider and leverage an outside team of cyber experts to monitor and investigate alerts 24/7/365. The city knew it needed to augment its current internal team, policies, and procedures to effectively handle alerts and incidents. It was well known that the time to detection and response of an incident can have a significant effect on the overall impact and severity.

To accomplish this, the city sought a log management system like a SIEM (Security Incident Event Management) or 'XDR-like' (Extended Detection and Response) solution. It was critical for the platform to integrate with the city's existing security solutions and not a rip and replace solution. Additionally, due to limited bandwidth, a short and streamlined implementation process was necessary.

Chief Technology Officer of the city commented, "We don't have the people to dedicate to alert monitoring throughout the day or in the middle of the night. However, our city has services that run around the clock so we cannot just wait until the morning and hope everything is okay."

Longstanding Relationship

Brite has been a key technology partner for the city for 25 years, beginning with installing the first computers in police patrol cars in 1999. Brite continues to support the city's public safety technology needs, as well as providing cybersecurity technology products. When the need for security services emerged, the existing collaboration expanded into Brite's security operations services division.

"We knew we could provide the necessary world-class security operations services to our home city, just like we have been supporting corporate clients through managed security services for years," shared Trevor Smith, Executive Vice President at Brite.

Brite

$4.45m

Global average total cost of a breach

68.2%

Of government agencies were compromised by a cyberattack

52%

Of government agencies had service outages due to a ransomware attack

Standing out from the Pack

Though Brite was well known to the city IT Department for its involvement with fleet and video technology, the managed security services were lesser known to the team. The CTO attended one of Brite's educational events and learned about the vast scope of its managed security offering.

"I had initial concerns about the capabilities of Brite's security services since I had not interacted with that team previously," stated the CTO. "Attending Brite's managed security services event demonstrated just how capable they are in this space."

A New Partnership Arises

Through a traditional request for proposal process, Brite was selected to be the city's managed security provider in July of 2023. Onboarding was completed within 30 days of the contract signing, which included log collection, normalization, and correlation from all designated sources.

From there, Brite customized playbooks to specifically meet the city's requirements. Leveraging the ML database, the AI was trained using the city's existing data within about 10 days. The process enables efficiency by cutting out noise and providing the analysts with real alerts to investigate. Automation furthers the efficiency with nearly 60% of alerts being analyzed and closed within 11 seconds. The remaining alerts are addressed by the US-based security analysts within 1:56 minutes on average, 24/7/365.

"Based on our customized and agreed upon playbooks, I have Brite's security analysts notify me whenever appropriate. I like that they will contact and my team me about an alert, confirm its severity and recommend an action plan or remediation," shared the CTO. "I am getting the critical information I need to respond or approve a response".

On average, 1 to 3 alerts are escalated to designated resources within the city's team compared to approximately 450 total investigations each month.

The CTO closed with, "We are really happy with the service Brite is providing us. It gives me peace of mind."

Brite

277 days

Average time to identify and contain a data breach

80%

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

About BriteProtect

BriteProtect is an advanced managed security service that solves the problem of tedious alert management leading to miss critical alerts and employee fatigue. We take our decades of cybersecurity experience to provide our customers with unprecedented visibility, swift responses and expert insights delivered by our 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