LevelBlue

CASE STUDY

# How LevelBlue transformed SOC operations for a major government client

*A premier government agency tasked with protecting secrets critical to national security and critical infrastructure recognized that a segment of the department required additional cybersecurity services. These services included 24×7 security operations center (SOC) monitoring for several of its most important installations, which are spread across the country.*

LevelBlue

## The Challenge

The primary issue the agency needed to address was implementing 24×7 SOC monitoring that would help protect almost a dozen geographically dispersed national science research centers. The client had also previously discovered gaps when the agency's in-house and contracted security staff were not working, primarily evenings and weekends.

When the negotiation was taking place, a contractor operated the SOC, but the agreement was ending in less than a year, and the client had to have a replacement in place.

LevelBlue's conversation with the client began by holding detailed meetings with its CISO and team to better understand its needs with an emphasis on how many alerts the SOC handled on a regular basis. The client also wished to retain its current security technology stack, so it needed an agnostic vendor when it came to working with outside MDR and EDR solutions.

## The Solution

LevelBlue recommended a group of solutions that would fully accommodate the client's security and budgetary needs. LevelBlue has long-term partnerships managing products from the client's security vendors and was able to offer the following services.

- **Co-Managed SOC for Splunk** LevelBlue's solution will reduce alert noise for clients by up to 90%, reducing alert fatigue, allowing the client to retain ownership of all data, and identifying active threats with 24×7 real-time global threat monitoring.
- **Managed Detection & Response** for CrowdStrike Microsoft Defender – This service is anchored by LevelBlue's MDR solution, monitors for threats in real-time, detects and responds to incidents within minutes, and augments any in-house security team, allowing it to focus on business-related issues.
- **Threat Intelligence-as-a-Service** LevelBlue's elite SpiderLabs team of threat hunters, incident responders, forensic investigators, penetration testers, and researchers conduct cutting-edge research, deliver the foremost intelligence, and proactively protect the client.
- **Digital Forensics and Incident Response** If needed, LevelBlue's Digital Forensics and Incident Response consulting services help determine the source, cause, and extent of a security breach quickly and better prepare for an incident.

## The Result

The client accepted LevelBlue's proposal, noting that in addition to being confident in the security solutions proffered, it had a solid relationship with and a level of trust in LevelBlue's executives and sales staff. Several of them had years of experience working with the members of the client's team.