LevelBlue

CASE STUDY

How a leading UK financial firm strengthened cybersecurity with LevelBlue's Co-Managed SOC and Penetration Testing

The financial services firm's responsibilities require it to house a great deal of incredibly sensitive client financial data, all of which is highly sought after by cybercriminals.

The challenge

The financial services firm has been a LevelBlue Co-Managed SOC with Splunk as the SIEM client since 2017. While the financial services firm had and retains a well-trained and equipped security team, it needed help managing its SIEM and ensuring it received actionable intelligence based on the data the SIEM was analyzing.

Some issues included its in-house security team lacking the manpower and bandwidth to monitor the SIEM 24×7 and the ability to fine-tune the SIEM on an ongoing basis. Partnering with LevelBlue would boost its security capability and effectiveness and allow it to receive a full return on its SIEM investment.

The solution

The client opted to partner with LevelBlue, which has deep expertise in managing Splunk's SIEM with other clients, as its MSS provider to deliver Co-Managed SOC (SIEM) services.

The firm was also impressed with LevelBlue's technical abilities surrounding SIEM management, such as fine-tuning the tool to operate at peak efficiency.

Additionally, the partnership encouraged the client to bring on LevelBlue to help with the development of a new mobile app, ensuring it would be secure.

LevelBlue suggested running penetration tests on the app. The financial services firm adopted the idea and LevelBlue was able to create and implement a penetration testing program within two months. Three rounds of testing were completed to ensure the app's security was solid, and LevelBlue came back after each test recommendation for the firm.

The penetration testing program proved so successful that the financial services firm expanded the number of hours dedicated to these exercises and offered LevelBlue a small Red Team engagement opportunity.

The client also became interested in conducting a Purple Team event.

Previously, the financial services firm had used a different firm for this activity, but the financial services firm's excellent experience with LevelBlue over the years helped spur it to give LevelBlue a try.

The initial Red Team operation was a success, with no problems found within its system, as expected.

The result

The financial services firm's proactive nature toward cybersecurity, which entailed moving from a long-term Co-Managed SOC to penetration testing as the need arose and then on to Red and Purple Team testing, shows that it understood that each change it made added to its threat surface and that additional measures had to be taken to safeguard the company and its client's data.