LevelBlue

CASE STUDY

Why Gossamer Bio relies on LevelBlue Red Teams and Penetration Testing

Gossamer Bio is a San Diego-based clinical-stage biopharmaceutical company focused on the development of therapeutics for pulmonary arterial hypertension and pulmonary hypertension associated with interstitial lung disease.

Gossamer Bio has been a LevelBlue Red Team and Penetration Testing client for several years and has recently extended its contract with LevelBlue for these solutions. A Red Team exercise is a simulated cyberattack designed to test an organization's security defenses and identify vulnerabilities. A penetration test (or pen test) is a simulated cyberattack on a computer system to check for exploitable vulnerabilities.

The challenge

The Gossamer Bio team is a strong proponent of proactive cybersecurity practices, including offensive security testing, to ensure the security program and controls are operating as intended. Per Lisel Newton, Gossamer Bio's Executive Director, Information Security, Risk and Compliance, the company prioritizes partnerships with security providers who align well with the company's core security values and outlook.

Newton noted that Gossamer Bio had experienced challenges identifying vendors whose expertise in testing environments with an element of cloud presence, as well as vendors who aligned well with the company's tools and technology.

"It's very important to us to partner with a provider who is capable of testing our environment in a meaningful way. We've worked with vendors in the past who had very rigid, prescriptive, and inflexible testing approaches, primarily focused on traditional on-premises controls and facility security. While of course these are important focus points, it's critical to test threat scenarios considering a largely remote workforce," Newton said.

While Gossamer Bio was not compelled by regulatory requirements to conduct offensive security testing and related exercises, it understood the need to put its programs and controls to the test to ensure they were functioning as expected to sufficiently protect the company.

The solution

Gossamer Bio concluded its search for a new Red Team and penetration testing partner three years ago when it determined LevelBlue had ticked off its boxes for these activities. Primarily, LevelBlue's Red Team operators and penetration testers had strong expertise, as well as not only willingness, but a keen interest in taking proactive steps to advise Gossamer Bio on how to secure its systems.

Once on the job, the results were immediate. LevelBlue teams went to work conducting cyberattack simulations tailored to Gossamer Bio's specific environment and threat scenario. The feedback and findings were highly valuable, providing actionable insight and program improvement measures Gossamer could take, Newton said.

Newton applauded the LevelBlue process.

"A project, either Red Team or penetration test, would begin with a collaborative scoping process and then last about six weeks. During the Red Team or penetration test, the two sides would interact to the extent we as the customer requested, and Gossamer Bio would, in real-time, address findings as they were reported to us," she said.

Once Gossamer Bio's team fixed identified issues, a retest was conducted to ensure the problem was resolved.

"The LevelBlue team has been fantastic in developing very customized testing approaches, tailored to our environment and our platforms. This included building malware and attacks specific to the tools we use."

A formal wrap-up meeting was held at the conclusion, during which the teams reviewed the final report and ensured it aligned with our expectations, Newton said.

"As we've grown together, LevelBlue has become intimately familiar with our environment. The process is very collaborative and transparent: we openly share information about our systems and their usage, our concerns, and our known threat vectors. This allows LevelBlue to tailor their approach to our specific environment and tools."

The result

Gossamer Bio's primary takeaway from its ongoing engagements with LevelBlue is the valuable insight into the 'unknown'.

"Having external, reputable advice and expertise, as well as having a provider validate what we've put in place, really gives our program confidence and strength. Independent external validation and vetting is mandatory," Newton said.

Newton said LevelBlue's technical expertise and skill set are invaluable.

"Working with LevelBlue has been a night and day experience. First, from a technical proficiency perspective, with their in-depth understanding of both cloud and on-prem environments, but what really sets LevelBlue apart is they are a partner in the true sense of the word – willing to collaborate and develop a customized approach to meet the needs of our environment," Newton said.