Deloitte.

Together makes progress

An emerging life sciences company stands up a cybersecurity program within three months

The challenge

The newly hired chief digital and information officer (CDIO) at this fast-growing drugmaker had a dilemma on his hands. He had discovered some foundational gaps in the company's cybersecurity operations and suspected there were others. The board of directors was expecting a report on the cyber situation, but the CDIO's resources for further action were limited. Moreover, the contract with his current managed services provider was expiring, and he was up against the clock transitioning to the new provider's platform.

It was time to call in reinforcements. What would it take, the executive asked Deloitte, to stand up a minimum viable security program?

Finding strengths to build upon

To find out, we launched an accelerated cyber assessment, or ACA. The ACA is an abbreviated version of Deloitte's standard cyber assessment process. It is aimed at identifying security requirements so fledgling cybersecurity operations can get to the next level of maturity.

The assessment took three weeks, in this case. During that time, we uncovered several immediate actions the client could take to significantly improve their cybersecurity environment.

- **Strategy.** We recommended putting a cybersecurity strategy in place under the guidance of a dedicated strategic advisor from Deloitte and making certain improvements to the controls environment, such as configuring multifactor authentication

- **Operations.** Action items here included implementing 24/7 security monitoring of end points, carrying out vulnerability management, adding log sources to provide a broader picture of security threats and system behavior, and developing an incident response plan
- **Continuous improvement.** We found improvement opportunities in asset management, data protection, and data classification, as well as in some of the company's disaster recovery and business continuity protocols

We prioritized our recommendations by impact and overall level of effort. Then we put together a road map of goals to work toward, along with the resources required to address each one, so the company's cyber operations could move up the maturity curve over time.

After reviewing our findings, the CDIO engaged the ACA team to help implement the improvement opportunities. We worked collaboratively with the internal IT team in the United States as well as in India, where both the client and Deloitte had on-the-ground personnel. Together, we documented the cybersecurity environment's architecture and processes. We also kept track of the improvements we put in place—including tool configurations—and the capabilities required to keep their cyber operations running smoothly.

Results

Within three months, the company went from very little cyber capability to foundational security baseline. From there, they transitioned smoothly into a longer-term arrangement in which Deloitte began to handle around-the-clock security monitoring by standing up a Cyber Operate command center. The new arrangement included several flexible hours that Deloitte provided for tackling additional cybersecurity priorities uncovered during the previous three months of post-ACA work.

High quality cybersecurity is achievable even for emerging companies where capacity is at a premium. Our stakeholder needed to know what could be done in the nearest amount of time to move the needle significantly. We took what we found, prioritized what we knew, and worked alongside the client's team to build out some of the additional capabilities to help them start maturing their security within a compressed timeline.

About Deloitte Cyber Operate

Deloitte Cyber Operate managed security services bring cloud-based threat hunting, detection, response, and remediation capabilities to your cybersecurity environment. Specialists pursue threats before they become attacks and respond to reduce the business impact. Example services include:

- Cyber threat intelligence
- Cyber tabletop exercises
- Incident readiness and response
- Zero trust identity prevention, detection, and response
- Enterprise prevention, detection, and response
- Attack surface management and vulnerability management
- Multi-cloud security

Contact us today to see how Deloitte ***Operate*** can deliver for you.

Contact us:

Chris Stanoch
Managing Director
Deloitte & Touche LLP
Email: cstanoch@deloitte.com

Mark W. Adams
Specialist Leader
Deloitte & Touche LLP
Email: markadams@deloitte.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC. All rights reserved.