Deloitte.

Rapid identification and remediation of issues smooth an organization's cyber journey

In health care delivery, confidentiality of patient and organizational data is paramount. When a large regional health care organization experienced cybersecurity issues, the time was ripe to accelerate its cloud security modernization efforts.

The organization had been working with an outside incident hunt team, but was less than satisfied with the quality of the relationship and the pace of progress. The contractor seemed more concerned with identifying problems than taking action to remediate them and prevent recurrence.

IT management engaged Deloitte's cybersecurity team to conduct a rapid six-week assessment of its cloud security operations and help it address the issues the assessment uncovered. Based on Deloitte's ability to quickly provide value, the client expanded and extended Deloitte's involvement.

What happened next

When Deloitte began the engagement, the team knew the client would be best served by deploying a Deloitte incident hunt team that could supplement the efforts of the outside team and perform a rapid assessment to reveal gaps. Efforts would be based on industry-leading practices and focus primarily on the Center for Internet Security (CIS) benchmark, while leveraging a Deloitte accelerator that provided a controls matrix template to quickly gather observations, provide recommendations, and identify remediation owners.

Deloitte also created five parallel workstreams—identity access management (IAM), Microsoft/Office 365 (a key area for the company), networking, Azure, and endpoint security—to identify any gaps found in how the client deployed its solutions to the cloud and any of the hunting group's discoveries.

After the work began, progress was rapid. A typical assessment can take 6 to 8 weeks and focuses only on identifying client gaps. However, to help the client address immediate risks, the Deloitte team worked strategically with the client to remediate issues in real time to significantly reduce risk exposure. The client was impressed with Deloitte's understanding of its cyber journey and the quality of our cyber risk framework and asked us to stay. The client was also pleased with the assistance we had provided during challenging situations. A key factor was our ability to integrate with their teams through "over-the-shoulder" guidance and knowledge transfer workshops that helped the client identify and resolve critical gaps that many organizations struggle with due to constraints in bandwidth or expertise. Our ability to help the client accelerate its modernization processes was also instrumental in the extension of the engagement.

Deloitte has become an integral part of the client's cyber journey and security operations going forward, and the organization is confident that it will be able to successfully complete its modernization goals.

The wins

- Rapidly remediated many cybersecurity issues, a result driven by close collaboration with key stakeholders and deep knowledge of the company's infrastructure
- Conducted an executive workshop for the Chief Information Security Officer (CISO) and other security executives focused on understanding and clarifying the organization's cyber journey
- Deployed technical resources and collaborated with/educated the client to enable meaningful repairs
- Leveraged Deloitte's Cyber Risk Framework to jointly implement organizational goals related to cloud landscape security
- Provided additional assistance around scenarios and operation processes that were challenging the client's IT team
- Helped the client accelerate its cyber journey by quickly identifying and explaining the need to address critical issues
- Bolstered confidence in present and future modernization plans through a broad, deep understanding of industry leading practices and a commitment to knowledge transfer

By the numbers

Two weeks

To help the client address immediate risk areas, Deloitte identified five workstreams—IAM, Microsoft/Office 365, Azure (and Azure AD), networking, and endpoint security—with 43 high-risk control findings out of a total of 142 controls. These findings range from processes the client might not have in place to audit access to capabilities not being properly leveraged in mitigating risks. Given the urgency to address high-risk findings, Deloitte pivoted from discovering issues to working closely with the client to help remediate them.

80% decrease in high-risk findings

At the end of just 12 weeks, Deloitte's efforts helped the client successfully reduce the Microsoft/Office 365 high-risk findings, which accounted for the largest number—by 80% to nine open findings. With the success of the rapid remediation effort and our ability to work effectively with operational stakeholders, the client decided to continue engaging Deloitte to help it address 60 medium-risk findings and asked us to lead several program-level efforts around data protection and device management that had previously been driven by other vendors.

Contacts

Jean-Michel (JJ) Heffron
Deloitte & Touche LLP
+1 678 427 6785
Email: jeheffron@deloitte.com

Andrew Rafla
Deloitte & Touche LLP
+1 201 499 0580
Email: arafla@deloitte.com