CxO Trust Newsletter - January 2022

Closing the Cloud Security Skills Gap

For several years, the cybersecurity discipline has experienced what's known as negative unemployment. Simply put, the demand for talent is higher than available supply. The increasing number of data breaches and ransomware attacks has companies of all sizes and in all industries looking to hire dedicated information security professionals. They can no longer keep relying on their "IT" teams to also handle information security.

In addition to the insufficient supply of talent, our profession also has a long way to go to ensure diversity and inclusion across all ranks. Fortunately, there is broad recognition of this and varying efforts to hopefully improve it in the coming years.

But the focus of this article isn't about the imbalances in the workforce diversity or supply-demand of available talent, rather a growing skills gap as it relates to cloud security. When you think about the areas of identity and access management, incident response, data security, encryption and many others - the differences in how you manage these topics within the cloud are non-trivial.

Taking incident response for example - within cloud environments, the teams will need to monitor different elements than you would in traditional on-premises environments. Do the incident responders have proper access and visibility into the various cloud services so they can detect, remediate and prevent attacks? Do they understand how to utilize the capabilities available within their cloud providers to effectively respond?

The skills gap is compounded by the double edged sword of rapid innovation within cloud computing. With dozens of entirely new forms of cloud computing services being launched by the major cloud providers each year, not to mention continued evolution of existing services and available configurations - it quickly becomes a daunting task for any individual to keep up with knowledge required to effectively manage cloud security.

Fortunately, while these are real challenges today, the capabilities available to security practitioners when operating in cloud environments usually far exceeds the traditional, on-premise counterparts. This is true both in terms of availability of detailed information (audit trails of every API call), strong access controls, and speed of access to detect/interject. In addition, there is a wealth of education, reference, and support available from the various Cloud Security Alliance working groups and forums.

In closing, keep calm and carry on sharpening your cloud security skills. We all play a part and can individually as well as collectively contribute to decreasing the cloud security skills gap.