Data Sentinels of Tomorrow: Cloud Security Specialists

Written by Joshua Bucheli, Researcher and Editor, in cooperation with Thomas Maurer, Senior Cloud Advocate at Microsoft and Peter Kosel, Founder of cyberunity

In the fast-growing field of cloud computing, cloud security specialists are in huge demand. Who are the biggest cloud-providers on the market and what kinds of candidates are they looking for? What do industry leaders see as the biggest hurdles to cloud computing? And what kinds of cloud security specialists are needed in order to overcome these hurdles?

Cloud Computing: A Flourishing Market

Between 2010 and 2020, the global cloud computing market grew by over $125 billion[1]. As a result, over 48% of all corporate data is now stored on the cloud[2]. It is indeed no secret that 'the cloud' is one of the fastest growing IT markets in the world.

This growth is in part due to a recent change in corporate mindset: "The shift that is occurring is one in which the cloud is increasingly being recognized as a secure solution. [...] Especially during COVID-19 times, the cloud is becoming more popular. In the past, everything that came from outside, or was stored outside the company, was highly dubious – but in times of home office, companies are opening up. They are increasingly looking at and implementing cloud solutions, especially in the context of 'zero-trust' approaches" says Thomas Maurer, senior cloud advocate at Microsoft.

[1] https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/
[2] https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/

We store our photos and watch our favourite TV shows and movies on the cloud; we work in virtual teams on our spreadsheets, presentations, and text documents on the cloud; even our medical and financial information is increasingly being stored on the cloud.

As with any technology, the more popular it is, the more likely it is that someone will try to exploit it, for example through cyber-attacks. This is especially relevant for the cloud as it is a technology that deals with one of the most valuable assets of our time: Data.

So, as cloud computing becomes more widespread, so does the need for specialists who are able to ensure the reliability and security of these platforms and the data therein.

According to Thomas Maurer, the major hurdles preventing companies from adopting cloud solutions are twofold. On the one hand, there is still a lack of awareness regarding cloud solutions and their security. On the other hand, there is the closely related feeling of uneasiness that comes with migrating one's data off of one's own 'on-premise' infrastructure:

"Ignorance leads to uncertainty, and with it comes the question of trust: can I trust an external service provider with my data? [...] How does it feel when I can no longer 'touch' the servers on which my data is stored? [...] How can companies retain control? [...] Considering the increasing frequency of cyber-attacks, we are moving in the direction of an intensely convoluted and increasingly complex world."

It is therefore important for organizations to realize that, even if it requires a certain degree of trust, outsourcing their most vulnerable data to the cloud not only increases the security of that data, but also the security of the remaining on-premise environment.

Despite these difficulties, there is a definite trend "towards the cloud" says Thomas Maurer. Global cloud security spending is expected to reach $12.6 billion in 2023 - almost double the spending in 2018[3].

However, we will not solve these challenges simply by throwing money at them. If these hurdles are to be overcome, we will also need enthusiastic cloud security specialists who are well versed in matters of cybersecurity and possess strong interpersonal skills.

[3] https://www.cybersecurity-insiders.com/by-2023-cloud-security-spending-to-reach-12-6-billion/

Industry Leaders and Up-and-Comers

An immense demand for cloud security specialists naturally exists among cloud solution providers and industry leaders such as Amazon Web Services, Google Cloud, Microsoft Azure, Alibaba, and IBM. These companies dominate their respective markets and play a significant role in shaping the future of cloud computing.

Nevertheless, cloud security specialists should not overlook mid-market cloud providers and end users across all industries as potential employers.

What are employers looking for in a cloud security specialist?

Until recently, cloud platforms were often designed and built first, and secured second. But this is changing, and cloud security specialists who want to stand out to employers should be able to recognize and help shape this change.

Data security in the context of cloud computing should be a forethought rather than an afterthought - aspiring cloud security specialists must be able to anticipate and proactively identify security requirements at all stages of cloud computing to ensure a secure design, build, and ongoing security management of cloud platforms.

It is therefore essential that cloud security specialists not only master the DevOps phases of cloud computing, but that they also have the necessary soft skills to integrate security into each of these stages.

In addition to this holistic 'SecDevOps' approach, aspiring cloud security specialists should be aware of key cybersecurity concepts (e.g., NIST framework guidelines), technologies, methodologies, and best practices for various platforms, operating systems, and software.

They should have a sound understanding of the various cloud computing models- **IaaS**, **PaaS**, **SaaS**, **public-**, **private-**, **hybrid-** and **multi-cloud** - as well as the security concerns associated with each. An in-depth knowledge of data analytics and machine learning, as well as the respective security risks associated with **data at rest**, **data in motion**, and **data in use**, will also help aspiring cloud security specialists stand out from their competition.

They should be familiar with the design and implementation of **data-**, **network-**, **application-**, and **container-security** measures like **firewalling**, **identity** and **network access control**, and **DDoS protection**.

Ultimately, cloud providers are looking for people with a good mix of cybersecurity know-how, data privacy experience, and compliance knowledge, explains Thomas Maurer. However, he also stresses the importance of what he calls 'T-Shaped Learners' - specialists who have a broad knowledge base, while at the same time specialising in two to three areas (for example, cloud network security or data privacy).

Finally, it is also important that individuals pursuing a career in cloud security are able to perform risk assessments and demonstrate compliance during regulatory audits. Therefore, depending on the geographic scope of their work, they should also have at least a basic understanding of the **GDPR**, **ISO 27001**, **DPA**, and other relevant international and local data protection regulations.

Certifications worth having:

In addition to traditional university degrees in computer science there are also several certifications available for security specialists who want to set themselves apart. This is particularly important for those entering the field from other backgrounds, for whom promising opportunities are also available so long as they back up their affinity for computer science with relevant qualifications.

"The important thing is to have a solid base knowledge of IT and to focus on one topic and immerse yourself in it. [...] Choose a topic and complete the corresponding certificates such as the AZ-500 exam for Cloud Security Engineers and the Azure Security Engineer Certificate", recommends Thomas Maurer.

IT managers and employers also like to see the following certifications: Certificate of Cloud Security Knowledge (**CCSK**), **CompTIA Cloud+** and **CompTIA Cloud Essentials**, Certified Information Systems Auditor (**CISA**), Certified Cloud Security Professional (**CCSP**), and Certified Information Systems Security Professional (**CISSP**).

Soft skills: What do employers like to see?

Hard skills and qualifications aside, cloud security specialists would also be well served to emphasise certain highly sought-after soft skills.

First and foremost, interpersonal skills are a big plus: communicating, persuading, and negotiating effectively and empathetically with architects, developers, programmers, and other departments and team members in the DevOps pipeline is far from trivial. The ability to translate security diagnoses and solutions into easy-to-understand presentations, documentation, and policy recommendations for management is also a significant asset.

Due to the fast-paced nature and constant evolution of the cloud computing market, cloud security specialists who want to stand out to employers should demonstrate their dynamism, ability to innovate, and propensity to think outside the box.

Overall, a lifelong-learning attitude is highly desirable. Thomas Maurer's advice for aspiring cloud security specialists: Keep on top of the fast-changing world we live in – be smart and recognize where needs exist that are not being met. Engage in honest self-promotion by doing good and talking about it, and have fun passing on your know-how and sharing knowledge with others.

Cloud security specialists who actively pursue personal development training will stand out in a particularly positive light. The goal should be to question one's own impact in order to continually develop one's abilities, both in general and with regards to security-specific qualifications.

In conclusion, Peter Kosel of cyberunity said it best: "The very fact that someone considers and develops their personal impact by pursuing further training is testament to an openness, eagerness to learn, and, above all, a positive attitude. And when all is said and done, it's *attitude* that is the deciding factor."