Job Analysis

Nemanja Milanovic

Old Dominion University

Dr. Sherron Gordon-Phan

10/26/2025

Abstract

This paper presents a critical analysis of a cybersecurity and compliance Analyst role in InMarket, one of the remote working jobs that aim to harmonize innovation and regulatory rules in the field of cloud-based marketing technology. It also discusses what the company anticipates in terms of technical skills and compliance competencies and what implicated soft skills would make the company successful. It also examines the alignment of the requirements to my professional background of privacy engineering, General Data Protection Regulation (GDPR), and cybersecurity education. Through critical evaluation of the job advert, the paper brings forth flexibility, cross-functional co-work, and proactive risk mitigation by InMarket. The discussion finishes with showing how the mission, culture, and role expectations of the company align directly with my professional competencies and career objectives in cybersecurity and provides a significant basis to further develop and make meaningful contribution to the sphere.

Introduction

Due to the growing trend of organizations moving to cloud-native infrastructures, the market for cybersecurity experts who can balance compliance and technical defense approaches has been expanding exceptionally fast. The advertisement by InMarket of a cybersecurity and compliance analyst has been used to illustrate this contemporary expectation of the integration of practical security operations with legal and regulatory knowledge. This paper aims to examine the Cybersecurity and Compliance Analyst job in the company InMarket by considering the objectives of the company, its major duties and implied professional competencies. It will also relate these expectations to my background as a Privateer (Privacy Engineer), who has more than three years of experience regarding General Data Protection Regulation (GDPR) compliance, a self-educated developer, and an upcoming graduate in cybersecurity. Ultimately, this discussion portrays that the proactive cloud security, compliance readiness and cross-functional communication orientation of InMarket is directly linked with my academic preparation, technical abilities as well as my future career path.

Company Overview and Role Purpose

InMarket is a well-established consumer intelligence and real-time marketing activation leader on major brands, which was founded in 2010. Its data-driven platform is advanced analytics and artificial intelligence (AI) to improve the effectiveness of the campaigns, so data security and privacy are inherent to its success. The role of Cybersecurity and Compliance Analyst assists a streamlined AI and Managed Detection and Response (MDR) focused security program to defend a cloud-based advertising infrastructure that operates quickly, remains innovative, and adaptable

to change. The analyst plays the role of a technical operator, the compliance advisor between engineering, legal and security units. This type of partnership emphasizes the philosophy of InMarket that security does not have to limit innovation, it should empower it.

Core Responsibilities and Required Skills

The ad lays emphasize on the applicants with five years or more working experience in cybersecurity and demonstrated experience with cloud security and incident response in addition to experience in handling "SOC 2 Type II and ISO 27001" (Indeed, 2025). It identifies GCP security expertise, MDR/MSSP workflows and penetration testing oversight as some of the important technical skills. These requirements, which are described as technical preceding administrative, are indicative of the fact that InMarket attaches greater importance to operational preparedness and practice than to knowledge in purely policy terms.

The company is also interested in an individual who possess great communication skills, which require a candidate who can equally communicate to engineers, auditors, and legal counsel. This means that interpersonal skills are as important as the technical competence. My education and experience as a Privacy Engineer directly satisfy these requirements; I have created audit documentation, conducted GDPR compliance frameworks, and was a part of legal teams, activities reflective of what InMarket expects in terms of compliance preparedness and cross-correlation.

Connection to Professional Background

My career path is closely connected with the duties described in the ad. Being a Privacy Engineer, I have performed data protection impact assessment, security control to adhere to regulatory requirements, and audit support directly in line with the requirement that InMarket has aimed at someone to own evidence collection and control validation of SOC 2 Type II and ISO 27001. My knowledge of GDPR principles will provide me with enough experience to work with

legal teams and client representatives on issues related to data privacy. Being a self-educated developer, I have a working knowledge of coding practices and cloud deployment models, which explains why the ad is interested in those candidates who have a general idea of what it means to be a developer and even a preference of 2+ years' experience as a developer. My upcoming degree in cybersecurity grows my skills in incident response, vulnerability management, and network defense which is essential in researching and mitigating threats in GCP/AWS settings.

Company Culture and Values

InMarket is an organization with an innovative culture, data-driven culture, and performance-based culture, as indicated by its commitment to an "AI + MDR-first cybersecurity program that is designed to secure but not suffocating innovation" (Indeed, 2025) that points to a fast-paced, flexible, and always-improving culture. InMarket also stresses its inclusiveness, equity, and diversity by indicating that it appreciates the diversity of each opinion (Indeed, 2025). This suggests the presence of teamwork culture that connects teamwork, innovation and moral responsibility. The kind of professionals that best fit in this organization are analytical, proactive and detail oriented whose technical skills on cloud security, compliance, and incident response are strong. Communication and cross-departmental collaboration are also necessary qualities of the position because the analysts should collaborate with and communicate well with the engineering, legal, and compliance teams. Personal traits like curiosity, accountability, problem-solving are also in line with InMarket goals of delivering innovative, secure and measurable real-life results.

Soft Skills

InMarket job advertisement of Cybersecurity and Compliance Analyst job position indicates time management and adaptability as important soft skills. The advertisement suggests the necessity to "juggle investigations, compliance, and client need simultaneously" and "deliver

weekly reports covering incidents, escalations, vulnerabilities, and compliance evidence,", which show the role requires strong organizational and multitasking skills in a break-neck time. Also, terms such as "serve as a bridge between InfoSec and platform teams" suggest the significance of communication and collaboration. The priority and hierarchy of tasks grouping technical, legal, and operational missions demonstrate that success is determined by the effective prioritization of tasks, the ability to respond to new situations rapidly, and the appropriate coordination of activities between departments.

Potential Challenges and Motivations

There are two primary issues that an InMarket Cybersecurity & Compliance Analyst is likely to encounter. First, the position requires the ability to strike a balance between intense enforcement of security regulations and the rapid innovation that the company has to operate within because the analyst should safeguard a fast paced, cloud-native infrastructure, without necessarily slowing down the development processes. Second, the combination of multiple tasks, including incident response, vulnerability management, and readiness to continue audit in frameworks like SOC 2 and ISO 27001 may be exceedingly challenging and demand highly developed organization and prioritization abilities.

Conclusion

The role of Cybersecurity & Compliance Analyst in InMarket represents the combination of technical expertise, knowledge of regulations, and teamwork. The focus on the security of the cloud, artificial intelligence threat detection, and audit compliance indicates the direction the cybersecurity market is taking to comply with automation and data privacy issues. My technical expertise and my current study of Cybersecurity combined with my history as a Privacy Engineer make me well-equipped to handle the expectations of the position. The adoption of the open

culture, personal development prospects, and the mission of the advertisement to safeguard a fast-speed, cloud-existing platform without suffocating innovation makes it a perfect place to develop my career. Ideally, inMarket is looking not only after an analyst but a holistic professional capable of capturing innovation- a field that fits exactly my experience and ambition.

References

Indeed. (2025). *Cybersecurity & Compliance Analyst*. Indeed.com. https://www.indeed.com/jobs?q=security+analyst&l=remote&radius=25&from=searchOnDesktopSerp&vjk=05ee7f2e74832f40