Bellevue University

Cyber Security Engineer

Timothy Jelinek

CYBR250-T301

8/31/2023

The job that was interesting to me is a Cyber Security Engineer at GE HealthCare. They are looking for someone who is knowledgeable and has a bachelor's degree in computer science or STEM. They also want someone with experience in anomaly detection, data analytics, data leakage, policy development, behavior analytics, and log management. Another requirement is hands-on experience with UEBA tools, primarily in policy and content development, log ingestion, case management, and workflow. The ideal candidate would also have strong SIEM experience in data ingestion, modeling, advanced reporting, and administration. They also have listed numerous technical expertise they would prefer. They're looking for someone with two or more years of experience in applications, operating systems, advanced scripting skills, coding skills, working with Agile methodologies, Microsoft 365 suite of data protection tools, host-based detection and prevention suites, data loss prevention tools, and detecting and responding to cyber incidents in an IT environment. There is also a long list of responsibilities for the job. Some of the responsibilities are leading the design and development of solutions, working collaboratively with stakeholders, enabling and maintaining all data sources, providing technical support, managing service parameters, and ensuring compliance with all regional legal requirements globally. This job pays anywhere from $108,000 to $162,000 a year.

For this big of a job, there is a bit of a career pathway. For a feeder role, you could work as a software developer. As a software developer, you would design and build computer programs that power mobile devices, desktop computers, and even cars. The next step would be to get an entry-level position which could be a cybercrime analyst/investigator. A cybercrime analyst/investigator is responsible for protecting

computer networks from cyberattacks and unauthorized access. From the entry-level position, you move on to a mid-level position like a cybersecurity consultant. As a cyber security consultant, you will identify problems, evaluate security issues, assess risks, and implement solutions to defend against threats to companies' networks and computer systems. After all of these positions, you will be qualified to be a cybersecurity engineer.

The entry-level jobs available to get started are software developer, systems engineer, financial and risk analyst, and security intelligence analyst. As a software developer, you analyze users' needs and then develop software to meet those needs. As a systems engineer, you design, create, and implement new systems to help a business flourish. As a financial and risk analyst, you analyze models and data within the scope of business action, predict and determine the likely outcome of a business decision, prepare reports, make recommendations, and use analytics software to calculate huge sums of data. As a security intelligence analyst, you assess the threat different actors pose to an organization, industry, or public safety. All of these jobs are in high demand and are good experience for when you are trying to get the role of cybersecurity engineer. After looking at the requirements and the entry-level positions I now know it is important to investigate these jobs even more in-depth to see which ones I am most skilled to do in order to start on my career path. A cybersecurity engineer is a very important job, and with the importance of the job comes the immense amount of experience and preparation needed to obtain it.

Sources:

"Cyber Security Engineer" LinkedIn, https://www.linkedin.com/jobs/view/3676982616.

Accessed 31 August 2023.