Renato Campos

Cybersecurity Prework

Monday August 31, 2020

Security Analyst

Facebook

Menlo Park, CA

Facebook's mission is to give people the power to build community and bring the world closer together. Through our family of apps and services, we're building a different kind of company that connects billions of people around the world, gives them ways to share what matters most to them, and helps bring people closer together. Whether we're creating new products or helping a small business expand its reach, people at Facebook are builders at heart. Our global teams are constantly iterating, solving problems, and working together to empower people around the world to build community and connect in meaningful ways. Together, we can help people build stronger communities - we're just getting started.

Facebook is seeking an experienced Security Analyst to join our team. This position will be responsible for understanding and supporting the design of Facebook's organizational, procedural and technological security controls within the context of the global regulatory frameworks applicable to our business. The position will also help codify these controls in supporting documentation and explain them to internal and external stakeholders.The Security Analyst will be someone with a passion for implementing innovative security controls that mitigate risk to the company, empower Facebook's culture of rapid innovation, and help demonstrate Facebook’s dedication to security to the world. This role requires a mix of broad, business and technical acumen, the ability to inspire and influence decisions pertaining to regulatory standards, and a polished ability to communicate with key internal stakeholders. This role is a full-time position.

- Help demonstrate Facebook’s commitment to security to external stakeholders
- Understand technical implementation details necessary to identify and assess security risks and recommend mitigating controls
- Participate in the development and oversight of required corrective action plans relating to security compliance issues
- Support business relationships with the internal and external security auditors and regulators
- Identify, research and evaluate new compliance requirements and ensure they are incorporated into Facebook’s security policy framework
- Support the communication of policies, procedures, and plans to internal stakeholders regarding security and compliance best practices around applicable laws, regulations and controls
- Support the identification, validation and remediation of information technology controls

required by Irish Data Protection Act, GDPR, Federal Trade Commission, Sarbanes-Oxley, Payment Cardholder Information Data Security Standards (PCI DSS), regulations governing personally identifiable information (PII), and other applicable regulatory compliance frameworks

- Data Security Standards (PCI DSS), regulations governing personally identifiable information (PII), SOC2 and SOC3 trust principles, and other applicable regulatory compliance frameworks
- Partner with internal teams to ensure successful security programs that align with compliance requirements
- Understand the security needs of internal and external stakeholders around external business partners and maintain a process that meets stakeholder needs
- Manage daily activities and functions of the external business partner management program
- Coordinate and drive business partner security assessment activities for both inbound and outbound relationships
- Lead assessments of business partner security risk, develop mitigation plans, and work with internal stakeholders to assign monitoring responsibility. Prepare and complete annual risk assessments and assist with regulatory and accreditation audit preparation as needed
- Support business partner selection on significant sourcing decisions and reassess security risk for business partners prior to contract renewals

- 5+ years experience in information security compliance
- 2+ years experience supporting compliance programs within the technology space
- 5+ years experience in security controls across all security domains such as access management, encryption methods, vulnerability management, network security, etc.
- Project management skills

Facebook is proud to be an Equal Opportunity and Affirmative Action employer. We do not discriminate based upon race, religion, color, national origin, sex (including pregnancy, childbirth, or related medical conditions), sexual orientation, gender, gender identity, gender expression, transgender status, sexual stereotypes, age, status as a protected veteran, status as an individual with a disability, or other applicable legally protected characteristics. We also consider qualified applicants with criminal histories, consistent with applicable federal, state and local law. Facebook is committed to providing reasonable accommodations for candidates with disabilities in our recruiting process. If you need any assistance or accommodations due to a disability, please let us know at accommodations-ext@fb.com.

Renato Campos

Cybersecurity Prework

Monday August 31, 2020

Terms

1. **vulnerability:** Given a potenetial threat to perform unauthorized actions within a general computer system (hardware or software), a vulnerability is the mode or vessel through which an exploitation of access is carried out.
2. **experience:** Given a concept, action, role, subject, or profession; experience is the familiarity of practices and methods gained over time through practical exposure to the given subject.
3. **encryption:** In relation to software cryptography, encryption is the method or process through which data is broken up and encoded through a series of computations. Typically, an encrption key is also generated through the process of encryption which is capable of applying a series of inverse computations to recover the original data.
4. **access management:** In relation to cybersecurity, access management (often reffered to as Identity and Access Management or IAM) is the assignment and management of security groups or roles. Groups and roles may have unique levels of privileges or access to particular data within an operating sytem. Such privileges can also be coordinated to exist within networked systems.
5. **compliance:** In relation to cybersecurity, compliance is a set of rules and definitions (often known as a framework) that regulate how data is transfered in a secure manner. There are several standardized compliance frameworks that are used today.
6. **information security certification:** In relation to cybersecurity, an information security certificate is a document authenticating that an individual has the required core knowedge and skills (usually with respect to an industry standard or compliance) to fufill the requirements of a security role.
7. **SQL:** Structured Query Language, or SQL, is a specialized programming language of commands for a particular application or program intended for dynamic management of a relational database.
8. **data visualization:** Data visualization is a graphical (or image-based) representation of a set of data (finite or infinite) under certian constraints. Such representations are therefore subject to a more intuitive (or geometrical) mathematical analysis with the expectation to gain a deeper understanding of the data in question.
9. **data analysis:** Data analysis is the process through which data is transformed or modeled in static or dynamic instances in order to gain a deeper understanding of the data being acted upon.
10. **OSINT:** Open-source Intelligence, or OSINT, is a framework formed by a collection of freely

available information found in online security communities.