Job Description of Cyber Security Engineer

_____(Name of the Company) is looking for cybersecurity engineers to maintain a vigilant approach to protect our systems and data in the face of ever-increasing cyber threats. In this position, you will be responsible for a number of functions associated with IT Security-from ensuring the security of software, to selecting and/or constructing and deploying broader network security systems. If you have an analytical mind, outstanding problem-solving skills, and work comfortably under pressure this could you be your opportunity to join us.

Work Profile

As a cybersecurity engineer, you will on a regular basis conduct a thorough risk assessment, identify vulnerabilities within a network, create firewalls and configure systems to enhance the existing security features. You are expected to respond to and document any security threats, resolve technical faults and allocate resources to deliver solutions in a cost-effective way.

Continued education and light research will be a standard part of the job since maintaining industry standards and keeping abreast of new developments since this is an ever-changing and ever-challenging environment.

Responsibilities

- Identify and define system security requirements.
- Maintain all hardware and software in relation to security.
- Monitor types and techniques of hacking attacks.
- Engineer, implement, and monitor security measures for the protection of computer systems, networks, and information.
- Prepare and document standard operating procedures and protocols.
- Configure and troubleshoot security infrastructure devices.
- Test and identify network and system vulnerabilities.
- Conduct proactive research to analyze security weaknesses and recommend appropriate strategies.
- Write comprehensive reports including assessment-based findings, outcomes, and propositions for further security enhancements.
- Liaise with vendors to implement security solutions.

Requirements

- Proven work experience of _____(years) as a system security engineer.
- Experience in building and maintaining security systems.
- Detailed technical knowledge of database and operating system security.
- Hands-on experience in security systems including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, and content filtering.
- Thorough understanding of the latest security principles, techniques, and protocols.
- Familiarity with web-related technologies and network/web related protocols.
- Problem-solving skills and ability to work under pressure.
- Strong attention to detail.
- Strong time management skills.
- Bachelor's Degree in Computer Science or a related field.

About Us

(A brief history and working of the company)

Sample Job Descriptions From Other Companies

#1 VISA

Cybersecurity Engineer

- Bengaluru, Karnataka, India
- Full-time

Visa operates the world's largest retail electronic payments network and is one of the most recognized global financial services brands. Visa facilitates global commerce through the transfer of value and information among financial institutions, merchants, consumers, businesses, and government entities.

We offer a range of branded payment product platforms, which our financial institution clients use to develop and offer credit, charge, deferred debit, prepaid, and cash access programs to cardholders. Visa's card platforms provide consumers, businesses, merchants, and government entities with a secure, convenient, and reliable way to pay and be paid in 170 countries and territories.

In this senior role, you will be responsible to manage various DevSecOps systems for the design, development, operations, and execution of large-scale cybersecurity initiatives. You will be an infrastructure specialist engineer who will be responsible for the design, development, and execution of large-scale Cyber Security initiatives. As a Security DevOps Engineer, you will be part of our cybersecurity team to help design, enhance and build various security solutions in an agile development environment. You will work with colleagues, who will support and challenge you daily. We believe in self-managing agile teams that build products focusing on unit testing, code reviews, and continuous integration for excellent code quality. You must be dedicated to delivering production-ready code in short periods and willing to go beyond the routine.

Key Responsibilities

- Develop innovative solutions to protect the Visa brand, networks, assets, and products by implementing state-the-art detection, prevention, and response capabilities.
- Design, engineer, operationalize and maintain the security systems which support continuous deployment/integration solutions.
- Development and maintenance of DevSecOps infrastructure, automation, support day-to-day operations by monitoring and resolving problems, automated deployments, and participate in Agile SCRUM activities.
- Have strong problem-solving and debugging skills.
- Have experience in enrolling devices for health monitoring frameworks. This includes gathering critical health and resource utilization metrics of appliances, services, and telemetry data.
- Efficiently managed and maintained cluster of devices in large-scale enterprise datacenters with minimum to zero downtime.
- Contributing to open-source projects and supporting open source excites you.
- Have excellent communication and interpersonal skills and above all, you are a team player!
- Mentor and lead the team on various aspects of business and security technologies.

Key Skills Needed:

- Excellent understanding of cybersecurity concepts.
- Agile development – incorporating Continuous Integration and Continuous Delivery utilizing technologies such as GIT, Maven, Jenkins, Chef, Crucible, Sonar, Junit.
- Linux – Strong Linux and systems engineering knowledge.
- Python – Experience with python web frameworks.
- AngularJS – You've built Angular directives beyond just wrapping a jQuery plugin around an element.
- Node.js – You've created multiple API-centric web applications.
- Elastic Stack – You have used Kibana and Elastic search for logging and developed plugins, codecs for specific use cases.
- Network experience: Socket, TCP/IP, UDP, and Multicast.
- Independent – no micromanaging here, but you must be able to communicate.
- Monitoring Stack – You have used Monitoring tools such as Grafana, Time series databases like Influx dB/graphite, and Alerting tools like Prometheus/Kapacitor.
- Configuration Management – Experience with Configuration management tools Such as Ansible/Salt stack/Chef/Puppet.

Qualifications

- Minimum 8 years of experience in designing and maintaining enterprise infrastructure solutions.
- Out of total years of experience, a minimum of 5 years of experience in Project life cycle activities on development and maintenance projects. Including CI/CD and tools development – preferably open source.
- Minimum Bachelor's degree required from an accredited institution.
- Strong customer-centric mindset.
- Proactive sense of urgency and 'can-do attitude.
- Strategic thinker who can balance big picture strategy with detailed, flawless execution.
- Financial services and card payments experience is a plus.
- Excellent communication skills.
- Excellent team player.
- CISSP, CISA, SANS GPEN, SANS GXPN, SANS GIAC, SANS GREM, OSCP (Offensive Security Certified Professional) is a plus.

Additional Information

Visa will consider for employment qualified applicants with criminal histories in a manner consistent with EEOC guidelines and applicable local law.

Source: visa.co.in

#2 MOODY'S

Engineering & Technology – Information Security

Regular – Experienced Hire

Moody's is an essential component of the global capital markets, providing credit ratings, research, tools, and analysis that contribute to transparent and integrated financial markets. Moody's Corporation (NYSE: MCO) is the parent company of Moody's Investors Service, which provides credit ratings and research covering debt instruments and securities, and Moody's Analytics, which offers leading-edge software, advisory services, and research for credit and economic analysis and financial risk management. The Corporation, which reported revenue of $4.4 billion in 2018, employs approximately 13,100 people worldwide and maintains a presence in 42 countries. Further information is available at www.moodys.com.

Moody's Shared Services is the front line professionals including Finance, Technology, Legal Compliance, and Human Resources, that operationally support our business units. Exceptional Shared Services teams are vital to the international success of our business.

Department

Moody's IT Risk department is looking for a VP Manager Cyber Security Engineer to join its growing organization. This is a challenging position requiring deep knowledge of security products and networking. The candidate will be responsible for building and managing a staff of cybersecurity engineers

The Cybersecurity team is globally responsible for helping the organization balance risk by aligning policies and procedures with Moody's business and regulatory requirements. The team is responsible for the development, enforcement, and monitoring of security controls, policies and procedures, disaster recovery programs, GRC (Governance, Risk, and Compliance) reporting, and the delivery of security services including the company's Cyber Security program.

Job Description

- Responsible for managing a team of cybersecurity engineers.
- Responsible for Moody's cybersecurity project deliverables on time and on budget.
- Partner with technology infrastructure teams and outsourcing providers.
- Develop, collect and mature security metrics for IT Risk programs.
- Documenting cybersecurity exceptions and provide mitigations as needed.
- Provides reviews of cybersecurity engineering design, configuration, and implementations.
- Maintain blueprints and related documentation for all cybersecurity controls.
- Provide Engineering support to operations teams and infrastructure teams for upgrades and enhancements to current security technologies.
- Enhance automation capability across Moody's Cybersecurity portfolio by developing scripts to automate manual activity.

Qualifications

Minimum education and work experience required for this position include:

- Preferred 7-12 years of experience in the IT industry, preferably in financial services or consulting organization.
- BS or BA degree, preferably in technology/business or equivalent.
- Prior experience leading or managing cybersecurity engineering teams.
- CISSP, SANS, or equivalent certifications.
- Have excellent networking knowledge; be able to collect and analyze packet captures, use web debugging tools like Fiddler to analyze SSO connectivity issues.

- Capability to troubleshoot effectively at all OSI layers.
- Experience with firewall technologies, preferably Palo Alto.
- Experience with cloud providers, preferably AWS and Azure.
- Have development experience writing scripts for security controls or cloud services.
- 7+ years IT security product experience.

Key Competencies

- Familiar with one or more following: Python, Ruby, PowerShell, Lambda, AWS, and Azure APIs, ServiceNow APIs, Terraform.
- Familiar with various databases and SQL.
- Ability to quickly assimilate new technologies, tools, internal/external systems, and design frameworks. Strong and broad technology background.
- Ability to think with a security mindset. The successful candidate has a strong IT background with in-depth knowledge of several key security practice area: access control; application security; network security; security architecture; security strategy.
- Strong knowledge of application architecture, development, and secure coding practices.
- Strong written and oral communication skills including the ability to interact directly with customers that do not have an IT background.
- Strong presentation skills involving large and of varying IT background audiences.
- Proven ability to work within a large enterprise that spans multiple continents is governed by change management and has a tiered support model.

Moody's is an equal-opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, sex, gender, age, religion, national origin, citizen status, marital status, physical or mental disability, military or veteran status, sexual orientation, gender identity, gender expression, genetic information, or any other characteristic protected by law. Moody's also provides reasonable accommodation to qualified individuals with disabilities in accordance with applicable laws. If you need to inquire about a reasonable accommodation, or need assistance with completing the application process, please email accommodations@moodys.com. This contact information is for accommodation requests only, and cannot be used to inquire about the status of applications.

For San Francisco positions, qualified applicants with criminal histories will be considered for employment consistent with the requirements of the San Francisco Fair Chance Ordinance. For New York City positions, qualified applicants with criminal histories will be considered for employment consistent with the requirements of the New York City Fair Chance Act. For all other applicants, qualified applicants with criminal histories will be considered for employment consistent with the requirements of applicable law.

Candidates for Moody's Corporation may be asked to disclose securities holdings pursuant to Moody's Policy for Securities Trading and the requirements of the position. Employment is contingent upon compliance with the Policy, including remediation of positions in those holdings as necessary.

Source: careers.moodys.com

#3 Apex Systems

CYBERSECURITY – SSDLC ENGINEER IN FOSTER CITY, CA AT APEX SYSTEMS

Job Snapshot

Employee Type:
Contractor
Location:
Foster City, CA
Job Type:
VMS Access Entry
Experience:
Not Specified
Date Posted:
9/18/2019

Job Description

Our Client's Cyber Security team is looking for a Cybersecurity engineer with expertise in the Application Security domain, who will be responsible to define consistent Secure Software Development Lifecycle practices for all of their technology projects throughout the planning and delivery cycles that assure that application security vulnerabilities are mitigated.

Very strong application security and web application development experience and team leadership skills are a must.

In this position, you are a passionate and talented application security engineer with a very deep understanding of OWASP, CWE 25, Data Protection, Access management software vulnerabilities, and best practices design and threat modelling skills who can work in a dynamic environment.

You must be dedicated to able to work with developers in producing secure code in short time frames and be willing to go beyond the standard routine.

Qualifications

- 2-4 years of experience with a Bachelor's degree or 2-3 years of experience with a Master's degree in Computer Science, Mathematics, Physics, or equivalent.
- You have a Bachelor degree in Computer Science or a related field and 2 -4 years of Software Development Experience.
- Experience in Web Application Security, SSDLC, and Threat Modelling with MS/BS degree in Information System management / Computer Science / Information Security or a related technical discipline, at least 2 years of Software Development experience.
- Hands-on experience with Software Development Java / C# / C++, JavaScript and HTML.
- Must have a deep understanding of OWASP Top 10 and CWE 25; with a proven track record and experience in implementing and integrating remediation strategies.

- Excellent understanding of web applications, web servers, layer 7 application technologies, frameworks, and protocols with respect to application development and deployment.
- Well-versed in web application design, penetration testing, application risk assessment, and risk categorization.
- Well-versed (experience preferred) with driving and implementing secure development practices into SDLC (SSDLC); ability to successfully integrate security into a developer's world.
- Success in implementing effective Secure SDLC frameworks across a large corporation.
- Ability to effectively present and communicate security threats and risks to any audience and impress upon them the mitigation techniques and strategies.
- Candidates should be familiar with waterfall and agile development processes and have experience integrating secure development practices into both models.
- Knowledge and experience in using SAST, DAST, and fuzz testing tools preferred.
- Highly effective communicator; well-honed influencing and negotiating skills.
- Solid problem solving and analytical skills; able to quickly digest any issue/problem encountered and recommend an appropriate solution.
- Self-motivated; able to work independently; able to negotiate and bring consensus to diverse priorities of product development and solution team.

EEO Employer

Apex Systems is an equal-opportunity employer. We do not discriminate or allow discrimination on the basis of race, color, religion, creed, sex (including pregnancy, childbirth, breastfeeding, or related medical conditions), age, sexual orientation, gender identity, national origin, ancestry, citizenship, genetic information, registered domestic partner status, marital status, disability, status as a crime victim, protected veteran status, political affiliation, union membership, or any other characteristic protected by law. Apex will consider qualified applicants with criminal histories in a manner consistent with the requirements of applicable law. If you have visited our website in search of information on employment opportunities or to apply for a position, and you require accommodation in using our website for a search or application, please contact our Employee Services Department at 844-463-6178-6178.

Source: itcareers.apexsystems.com