advanced network systems
Technology. Security. Delivered.

JOB DESCRIPTION

Cybersecurity Engineer

Full-Time | Exempt | Remote

Our Cybersecurity Engineer plans, maintains, and monitors security measures for the protection of our clients' information technology networks and data, as well as internally supports the cybersecurity of our own organization. This remotely-based position has regular interaction with clients of varying technical knowledge, vendors and other business partners, as well as internal management. The predominant goals for the position are to continually maintain a high level of subject matter expertise, provide conscientious communication, deliver quality technical service and a positive customer experience.

Areas of Responsibility

- Monitor security threat feeds, forums, vendor notices, and other critical resources to stay informed of new and existing cybersecurity threats that may impact our organization, operations and those of our clients.
- Continually share accurate and timely security threat information to our organization.
- Conduct external/internal security audits and vulnerability scans for clients.
- Oversee our managed firewall program including, but not limited to, reviewing firewalls for best practice configurations, performing periodic OS upgrades, verifying the run schedule for monthly reports.
- Maintain primary responsibility for our managed SIEM service. This includes, but is not limited to, onboarding new clients, monitoring and maintaining the SIEM environment, responding to alert notifications, generating reports as required, and coordinating remediation services with Managed Services Engineering team.
- Implement, monitor, and maintain our second-generation managed security service which includes an advanced EDR agent, firewall and server/network logging and monitoring, change management, and best practices/vulnerability auditing.
- Periodically review Managed Services and Managed Security accounts for best practice security policies and configurations as well as report on findings to be addressed.
- Assist with the research, identification and evaluation of new cybersecurity products and services that can be added to our portfolio of client offerings.

Required Knowledge and Experience

Associates degree or above in information technology, cybersecurity or related field, or any combination of education, training and/or experience that fulfills the requirements of the position.

- One or more industry standard security certifications are desirable. CompTIA Security +, CySA+, CASP+, EC Council Certified Ethical Hacker, ISC CISSP.
- Experience with the security platforms, software tools and products utilized by our organization to support clients (ConnectWise, RapidFire Tools, SAINT Security Suite, WatchGuard, Fortinet, etc.).
- Minimum of 2 years of IT Administration or IT Security experience.
- Must have documented knowledge of local/wide area data networking (hardware/software/ protocols/best practices) and network security.

- Proficient in typical network security appliances and applications such as firewalls, SIEM's, Email Security, Endpoint Security
- Working knowledge of cloud hosted applications such as Google Workspace, Microsoft O365, Microsoft Azure, Amazon AWS is desirable.

Requirements and Work Environment

Must be able to work and move in a variety of physical positions to accomplish tasks including sitting and/or standing for extended periods, must capable of extensive and continual use of computer and mobile devices, must be able to speak clearly and verbally communicate. Must be capable of assessing the accuracy and completeness of work assigned.

The regular work environment is primarily indoors in environmentally controlled conditions, but may occasionally involve other environments. Normal hours of work are Monday through Friday, 8:00 a.m. to 5:00 p.m. or other equivalent hours established by the department manager. Participation in an after-hours on-call rotation is required. Due to the nature of the work being performed, some overtime and after-hours work is required.

No significant travel is expected for this position. Must be able to operate a motor vehicle, have a valid driver's license, clean MVR, and reliable transportation to commute to a client location or our company office, when and if needed.

Must be able to pass criminal background verification as well as obtain/maintain Virginia DCJS certification credentials.

About Advanced Network Systems, Inc.

Founded in 1996, Advanced Network Systems delivers industry-leading cybersecurity and network management solutions for small and mid-sized organizations throughout Virginia and West Virginia. Our signature managed security and managed IT programs are designed to reduce the risk, cost and complexity of managing network operations. Whether your organization is a growing small business, government entity or school, we offer a complete service experience that leverages innovative technology and expert advice to achieve our clients' goals. For more information visit us at www.getadvanced.net.

As a member of our cyber services group, you'll find a work environment that's professional, team-oriented and supportive. We offer competitive compensation, an excellent benefits package, and opportunities for advancement. We have a structured path of career development and place a high value on learning, which we support through company-paid certifications and tuition reimbursement for job-related education

How to Apply

To be considered for this position, qualified candidates should submit an up-to-date resume, along with a short message describing why they believe they would make a great addition to our team. Send information to: humanresources@getadvanced.net.

Last updated: 11/1/2021 SJL/LMH