www.gridsec.com | +1 (916) 800-4545 | Folsom, CA

About GridSecurity

GridSecurity is enabling the world's energy future by delivering scalable and effective managed network operations, managed security services, and managed compliance services for inverter-based generators and control centers.

We are a fast-growing company in an industry undergoing a historic transformation. At our core, we aim to operate at the intersection of what our people are passionate about, what they are good at, and what adds value to our clients. In doing so, we help our clients build the grid of tomorrow.

At GridSecurity, our people come first. We foster a flexible, candid, and collaborative environment where employees are empowered to grow, do meaningful work, and achieve their professional goals. We strive for the perfect blend of autonomy and teamwork, seeking to maximize an individual's potential. We firmly believe that if you treat your employees well and put them first, then the clients and business are inherently taken care of. One way we seek to achieve this objective is rewarding each employee as an owner of the business through our Incentive Compensation Program.

Onboarding Engineer

We measure GridSecurity's success by the caliber of people on our team, the quality of our work, and the trust we build with clients over time. As an Onboarding Engineer reporting to the Site Integration Manager, you will play a critical role in onboarding client environments into GridSecurity's managed services by deploying, configuring, integrating, and validating both network and systems infrastructure.

This is a hands-on technical role requiring experience across both networking and systems administration. You'll work across firewalls, switches, routing, virtualization, Windows and Linux servers, identity, endpoint security, backups, and other technologies to build secure, reliable, and supportable client environments.

In this role, you'll collaborate across the entire GridSecurity team, contributing not only to your core responsibilities but also to projects that drive our company forward. We foster an owner's mindset, teamwork, open and candid communication, and continuous learning – all necessary traits for you to be wildly successful on our team.

JOB RESPONSIBILITIES

- Network and Systems Onboarding and Integration
    - Execute the technical onboarding of client environments into GridSecurity's managed services, working across network and systems infrastructure to resolve dependencies and integration issues and ensure environments are secure, reliable, and operationally ready.
    - Deploy, configure, administer, and troubleshoot network infrastructure, including:
        - Firewalls, including policies/ACLs, NAT, IPsec VPNs, high availability, segmentation, path monitoring, and failover
        - Routers, switches, modems, VLANs, trunking, and routing
        - IDS/IPS and virtual networking across platforms such as VMware ESXi and Microsoft Azure
    - Deploy, configure, administer, and troubleshoot systems infrastructure, including:
        - Windows Server, Active Directory, GPO, and supporting identity infrastructure
        - Linux servers, including Ubuntu and Red Hat
        - VMware/Hyper-V virtual infrastructure
        - Microsoft Entra ID, Okta, and other identity and access technologies
        - Server and workstation security baselines, endpoint protection, and security monitoring technologies
        - Backup and recovery solutions
    - Implement and validate security controls GridSecurity is contractually responsible for managing on behalf of customers.
    - Support patch management, secure configuration, and vulnerability remediation across network and systems infrastructure.
    - Perform technical validation and QA/QC to confirm configurations, integrations, documentation, and security requirements have been successfully completed.
    - Generate and maintain technical evidence supporting contractual and applicable compliance requirements.
    - Coordinate directly with customers and internal teams to gather technical requirements, resolve implementation issues, remediate risks, and successfully deliver onboarding milestones.
    - Partner with Project Management to communicate technical progress, dependencies, risks, blockers, and resource needs throughout onboarding.
    - Ensure completed environments are appropriately documented and operationally ready for transition to GridSecurity's Operations teams.

- Process Development and Documentation
    - Develop, maintain, and improve SOPs, technical procedures, configuration standards, network diagrams, and onboarding documentation.
    - Identify and address documentation gaps to improve the consistency, scalability, and supportability of GridSecurity’s onboarding practices.
    - Maintain accurate technical records and documentation needed to support ongoing operations.
- Business Development
    - Represent GridSecurity professionally in every interaction, building trust with clients, partners, vendors, candidates, and industry peers while strengthening the company's reputation and brand.
    - Contribute to business growth by identifying opportunities to better serve existing and prospective clients and sharing those opportunities with the appropriate teams.
    - Build and maintain positive professional relationships that support collaboration, client success, and long-term business growth.
    - Continuously develop an understanding of GridSecurity's services and capabilities to effectively communicate our value and connect clients with the right resources when opportunities arise.
- Challenge the Status Quo
    - Continuously look for opportunities to improve our people, processes, technology, services, and client experience by identifying inefficiencies, reducing complexity, and recommending practical, scalable solutions.
    - Contribute ideas and feedback that support operational excellence, continuous improvement, and GridSecurity's long-term strategic objectives.
    - Demonstrate curiosity, initiative, and an ownership mindset by constructively challenging existing practices and helping drive positive change.
- Continuous Learning and Development
    - Take advantage of opportunities to attend training, conferences, industry events, webinars, and professional development activities that expand your knowledge, strengthen your skills, and support your current role and future career growth.
    - Pursue relevant certifications, continuing education, and learning opportunities that enhance your effectiveness and contribute to the growth of the organization.
    - Share knowledge, best practices, and lessons learned with teammates to foster a culture of continuous learning and collective success.

REQUIRED TECHNICAL SKILLS

- Demonstrated hands-on experience working across both network and systems infrastructure, with the ability to troubleshoot issues and dependencies spanning multiple technologies.
- Strong knowledge of network fundamentals, including:
  - Layer 2: Switching, Ethernet, VLANs, STP, CDP/LLDP, and LACP
  - Layer 3: TCP/IP, static/dynamic routing, ARP, NAT, and IPsec
- Experience configuring and troubleshooting firewalls, including policies/ACLs, VPN tunnels, high availability, segmentation, NAT, and redundancy.
- Experience configuring and supporting network infrastructure, including routers, switches, VLANs, and related network security technologies.
- Proficiency in Windows Server administration, including Active Directory, GPO, DNS, and DHCP.
- Experience administering Linux systems, including service management, package management, permissions, and basic command-line administration.
- Experience with virtualization technologies such as VMware ESXi and/or Hyper-V, including associated virtual networking.
- Working knowledge of identity and access management, endpoint security, system hardening, backup/recovery, and vulnerability and patch management concepts.
- Ability to apply security and configuration standards across network and systems infrastructure.

REQUIRED PROFESSIONAL SKILLS

- Strong interpersonal and customer service skills with the ability to translate technical concepts for non-technical audiences.
- Excellent written and verbal communication, including technical documentation.
- A continuous improvement mindset with a focus on process efficiency and reliability.
- Critical thinking and prioritization to maximize value for both GridSecurity and clients.
- Adaptability in dynamic environments with the ability to make timely, informed decisions.
- Collaborative team player who contributes to shared goals and supports colleagues.

PREFERRED QUALIFICATIONS

- Experience with technologies commonly used within GridSecurity environments, including Palo Alto, Fortinet/FortiGate, Cisco, Microsoft Entra ID, Okta, and Microsoft Azure.
- Experience with cloud platforms such as Azure and/or AWS, including IAM, virtual machines, and networking.

- Familiarity with endpoint security and management technologies, including EDR, encryption, and patch management solutions.
- Scripting or automation experience using PowerShell, Bash, Python, or similar technologies.
- Experience integrating infrastructure with SIEM or security monitoring platforms such as Splunk.
- Familiarity with configuration and endpoint management technologies such as Ansible, SCCM/Intune, or similar tools.
- Experience working in an MSP, MSSP, systems integrator, or other environment supporting multiple customer infrastructures.
- Experience working with enterprise security frameworks, regulated environments, or compliance requirements.
- Relevant network, systems, cloud, or infrastructure certifications, such as:
    - CompTIA Network+, CCNA/CCNP, or PCNSA/PCNSE
    - Microsoft Azure Administrator Associate (AZ-104)
    - RHCSA or Linux+
    - VMware Certified Professional (VCP) or equivalent

Benefits & Compensation

COMPENSATION

The base salary range for this position is $80,000 - $120,000 per year, depending on qualifications and experience.

PAYROLL SCHEDULE

Pay is the 7th (for the 16th to end of month) and 22nd (for the 1st to the 15th) of each month.

GRIDSECURITY INCENTIVE COMPENSATION PLAN

GridSecurity Inc. offers an Incentive Compensation Plan to reward employees, based on performance, in the form of Incentive Stock Options and/or cash bonuses on a monthly basis. As a full-time employee, you are eligible to participate in GridSecurity's Incentive Compensation Plan after a 90-day waiting period for new hires. Additionally, as part of our offer, GridSecurity will include an initial award of 5,000 ISOs.

401K PLAN AND COMPANY MATCH

GridSecurity offers a 401k retirement savings program. GridSecurity will match all employee 401k contributions up to 6% of your gross cash compensation (salary and bonuses). Employee and employer contributions begin on the first calendar day of the employee's second calendar month of service. Employer 401k match contributions vest immediately. For example, if the employee begins on June 15th, the employee will be eligible to participate in the 401k program and receive a company match effective the payroll period beginning August 1st.

HEALTH, DENTAL, VISION, AND LIFE INSURANCE BENEFITS

GridSecurity offers a group medical, dental, vision, and life insurance plan that you and your family are eligible to join. GridSecurity will pay 75% of the cost of the base medical and dental plan premiums and 100% of the base vision plan premium for you and your family. GridSecurity will only pay its share of the premiums for the healthcare plan that GridSecurity provides as the designated base plan for your area. You are eligible for health benefits on the first day of the first calendar month after your start date. GridSecurity has a tenure-based contribution scale that increases by 5% each full year of service, as of January 1st of the benefits calendar year, up to 95% of the base medical and dental plan premiums being paid by GridSecurity. For example, if you start on June 15th, your health benefits will start on July 1st. Also, if you start on June 15th, 2024, your employer contribution will increase to 80% of the base medical and dental plan on January 1, 2026.

GridSecurity also offers a $100,000 Supplemental Life Insurance policy for all full-time employees with premiums covered 100% by GridSecurity.

GridSecurity also offers employees the opportunity to participate in a ***Flexible Spending Account (FSA)*** and a ***Dependent Care Flexible Spending Account*** as part of our employee benefits package. In addition, if you are on a high-deductible medical plan, which our base medical insurance plan is, you will also have the opportunity to participate in a ***Health Savings Account (HSA)***. FSA and HSA plans allow employees to set aside money pre-tax to pay for certain healthcare and dependent daycare expenses.

PAID TIME OFF

Depending on qualifications and experience, this position will either:

A. Accrue two (2) weeks (80 hours) of vacation per calendar year. This increases to three (3) weeks (120 hours) after your first anniversary and to four (4) weeks (160 hours) after your third anniversary. Vacation balances roll over each year, with the ability to bank up to 1.5 times your annual accrual.

   In addition, this position accrues five (5) days (40 hours) of sick pay per year, with the ability to roll and bank up to ten (10) days (80 hours) total.

Or,

B. Accrue three (3) weeks (120 hours) of vacation per calendar year. This increases to four (4) weeks (160 hours) after your third anniversary. Vacation balances roll over each year, with the ability to bank up to 1.5 times your annual accrual.

   In addition, this position accrues five (5) days (40 hours) of sick pay per year, with the ability to roll and bank up to ten (10) days (80 hours) total.

ANNUAL HOLIDAYS

GridSecurity observes the following holidays for a total of 12 paid holidays:

- New Year's Day
- Martin Luther King, Jr. Birthday
- President’s Day
- Memorial Day
- Independence Day
- Juneteenth

- Labor Day
- Indigenous People's Day / Columbus Day
- Veterans Day
- Thanksgiving Day
- Day after Thanksgiving
- Christmas Day
- Plus, your birthday is always a day off - whether on a weekday, holiday, or weekend, you should not have to work on your birthday (*your birthday cannot be rolled or banked*)

WORK LOCATION

You will work from your home office with occasional trips to GridSecurity's HQ or client sites, as needed.

EVALUATION PERIOD

The first ninety (90) days of your employment will be treated as an evaluation period when we will assess your performance and fit with our culture. At the end of this 90-day evaluation period, we will hold a performance review session with you to discuss your performance against the job requirements and expectations. If your performance does not meet those requirements and expectations, we reserve the right to end your employment.

BACKGROUND CHECK

GridSecurity employees must successfully complete a background check prior to beginning employment. We follow the risk assessment table shown below.

Acceptable Risk	Unacceptable Risk	Subject to Review
No criminal record and no issues discovered through identification check **OR** Criminal incident found not to be disqualifying OR no discrepancy identified through identity check	Criminal record indicates substantial questions regarding candidate's character or trustworthiness ("Crimes of Dishonesty") **OR** Criminal background check reveals extensive criminal violation **OR** Identification check raises substantial questions regarding candidate's identity **OR** Any combination thereof which disqualifies the candidate	Misdemeanor crimes – These crimes may warrant disqualification of a candidate based on circumstances and timing of incident. **OR** Felony Crimes – Whether a crime was a felony or misdemeanor is often a quantitative rather than a qualitative measure and provides limited information about the underlying crime. Felony crimes, by definition, carry higher penalties than misdemeanor crimes but do not necessarily shed light on the seriousness or depravity of the underlying crime, especially if a plea deal was arranged. **OR** Substance crimes (whether misdemeanor or felony) – evaluate whether the candidate has an ongoing problem. If the answer is yes, disqualification is recommended. **OR** Number of crimes – Consider whether the candidate exhibits a pattern of criminal behavior. **OR** Minor problems with identification – Minor issues e.g., spelling, de minimis address or name issues, or dates should not disqualify otherwise qualified candidates. Questions arising around U.S. Citizenship or work status/permits.