BE AN INDUSTRY-LEADING SME WITH GRIDSECURITY

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.

Infrastructure Architect

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 Infrastructure Architect, you will design, deploy, and integrate secure network and system infrastructures that enable our clients’ CIP Low and Medium environments. You’ll collaborate closely with customers and internal teams to implement and support resilient, compliant infrastructure and drive continuous improvements in reliability, efficiency, and security.

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
    - Support project initiatives, such as evaluating, deploying, configuring, and managing security operations technology that allows GridSecurity to operate client’s CIP low and medium impact environments in an effective and efficient manner, including but not limited to:
        - CMDB
        - SIEM

    - IAM/IDP
    - IDS/IPS
    - Network monitoring and visualization
    - Infrastructure monitoring
    - Back-up & recovery
  - Design, implement, and monitor CIP compliance controls GridSecurity is contractually responsible to manage on behalf of our customers
  - Generate and maintain technical CIP evidence to support compliance and contractual requirements
  - Communicate, coordinate, and work directly with customers to resolve escalated compliance issues, remediate security risks, and develop new solutions and capabilities
  - Support day-to-day operations by responding to compliance issues, deploy new infrastructure, and continually improve network reliability and security
  - Support the architecture, deployment, administration, and monitoring of system infrastructure, including but not limited to:
    - Virtual infrastructure (ESXi/VMware experience preferred)
    - Windows Active Directory and supporting Identity Provider infrastructure (Okta and AAD experience preferred)
    - Manage configurations and security baselines of servers and workstations
    - Administer Microsoft GPOs
    - Track, evaluate, and implement security patches
  - Support the architecture, deployment, administration, and monitoring of network infrastructure, including but not limited to:
    - Firewall policies and configurations (Palo Alto, Cisco, and Fortigate experience preferred)
    - Routing and switching configurations (IPsec VPN tunnel experience preferred)
  - Assist the team building and documenting processes and procedures related to CIP compliance requirements
  - Participate in an on-call rotation

- Control Center Network Design and Deployment
  - Lead end-to-end design and implementation of new control center network builds, including developing network architecture diagrams and documentation (e.g., IP schema, port map, rack elevation diagram)
  - Perform hardware sizing and selection based on performance, scalability, and

    - redundancy requirements
    - Develop detailed bills of materials (BOMs) and equipment lists to support procurement and deployment planning
    - Design secure, resilient network infrastructures aligned with GridSecurity's standards and customer operational needs
    - Integrate networking, systems, and security technologies into cohesive, supportable architectures
- Process Development and Documentation
    - Establish and document standard operating procedures (SOPs) for managed security services and infrastructure operations
    - Evaluate and identify gaps in documentation and support the development of necessary documentation for the team
    - Maintain accurate operational and security documentation to ensure clarity and accessibility for internal teams

- Business Development
    - Work with our team to connect with potential clients that we can help.
    - Develop services that add value to current and potential clients.
    - Leverage your business relationships to help grow the GridSecurity client list.
    - Develop relationships and industry contacts to assist clients.

- Challenge Our Status Quo
    - Work on areas of the company in need of focus and improvement.
    - Assist the GridSecurity management by identifying areas of improvement that support our strategic direction.

- Growth
    - Attend conferences, forums, training, and industry engagements that help further brand the practice and demonstrate credibility.
    - Pursue training and professional certifications that align with your current job responsibilities and support your growth into future roles and responsibilities.

REQUIRED TECHNICAL SKILLS

- Strong knowledge of network fundamentals:
  - Layer 2: Switching, Ethernet, VLANs, STP, CDP/LLDP, LACP.
  - Layer 3: TCP/IP, static/dynamic routing, ARP, NAT, IPsec.
- Proficiency with firewall operations, including policy/ACL creation, IPSec/SSL tunnel configuration, high availability implementation, redundancy/failover testing, and troubleshooting.
- Experience configuring and supporting core infrastructure: routers, switches (with VLANs and hardened configurations), and IDS/IPS solutions.
- Familiarity with virtual networking platforms, such as VMware ESXi and Microsoft Azure.
- Vendor-specific expertise with Palo Alto, Fortigate, and Cisco devices and operating systems.
- Proficiency in Windows Server administration (Active Directory, GPO, DNS, DHCP, WSUS).
- Experience with Linux system administration (service management, package management, shell scripting).
- Knowledge of cloud platforms (Azure/AWS) including IAM, virtual machines, and networking integration.
- Familiarity with endpoint security technologies (EDR, antivirus, encryption, patch management).
- Experience with system hardening standards (CIS, NIST, DISA STIGs).
- Scripting or automation skills (e.g., PowerShell, Bash, Python) for deployment and process efficiency.
- Experience with backup and disaster recovery solutions.
- Experience designing and deploying multi-site or control center network architectures, including capacity planning, redundancy design, and documentation.

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

DESIRED QUALIFICATIONS

- Network certifications, or equivalent, such as:
    - CompTIA Security+
    - Comp TIA Network+
    - PCNSE/PCNSA
    - CCNA/CCNP
- Systems certifications such as:
    - Microsoft Certified: Azure Administrator Associate (AZ-104)
    - Microsoft 365 Certified: Enterprise Administrator Expert
    - Red Hat Certified System Administrator (RHCSA) or Linux+
    - VMware Certified Professional (VCP) or Hyper-V equivalent
- Experience with SIEM integration (Splunk)
- Familiarity with configuration management tools (Ansible, Puppet, SCCM/Intune)
- Experience working with enterprise security frameworks or compliance standards

Benefits & Compensation

COMPENSATION

The base salary range for this position is $100,000 - $150,000 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 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 $75,000 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

This position accrues three (3) weeks (120 hrs) of vacation per calendar year. This increases to four (4) weeks (160 hours) on your third anniversary. Your balance will roll over each year, and you have the ability to bank up to 1.5x your annual accrual. In addition to vacation, this position accrues an additional five (5) days (40hrs) of Sick Pay per year, with the ability to roll and bank up to ten (10) days (80 hrs.) 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

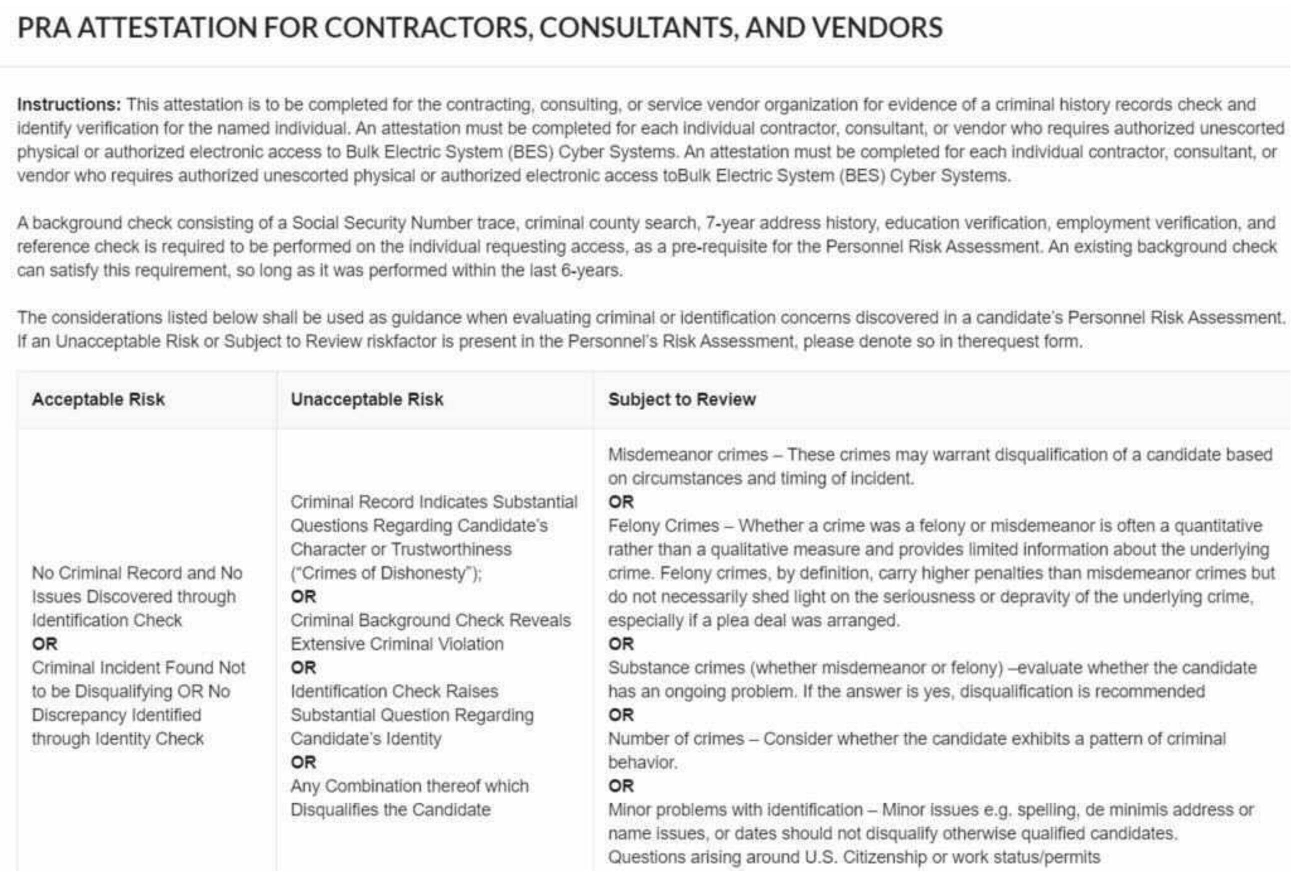
You will work from your home office with occasional trips to GridSecurity’s HQ or client sites, as needed.

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.



PRA ATTESTATION FOR CONTRACTORS, CONSULTANTS, AND VENDORS

Instructions: This attestation is to be completed for the contracting, consulting, or service vendor organization for evidence of a criminal history records check and identify verification for the named individual. An attestation must be completed for each individual contractor, consultant, or vendor who requires authorized unescorted physical or authorized electronic access to Bulk Electric System (BES) Cyber Systems. An attestation must be completed for each individual contractor, consultant, or vendor who requires authorized unescorted physical or authorized electronic access toBulk Electric System (BES) Cyber Systems.

A background check consisting of a Social Security Number trace, criminal county search, 7-year address history, education verification, employment verification, and reference check is required to be performed on the individual requesting access, as a pre-requisite for the Personnel Risk Assessment. An existing background check can satisfy this requirement, so long as it was performed within the last 6-years.

The considerations listed below shall be used as guidance when evaluating criminal or identification concerns discovered in a candidate's Personnel Risk Assessment. If an Unacceptable Risk or Subject to Review riskfactor is present in the Personnel's Risk Assessment, please denote so in therequest form.

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 Question 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