

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.

Control Center Integration Manager

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 the Control Center Integration Manager, you will be responsible for the leadership, execution, and continuous improvement of GridSecurity's control center technical services. Reporting to the Director of Onboarding & Integration, you will oversee the successful design, implementation, integration, and transition of client control centers and CIP-Medium environments into GridSecurity's managed services, including technical architecture and implementation, team development, cross-functional coordination, client communication, compliance readiness, quality assurance, and operational readiness. The Control Center Integration Manager is accountable for ensuring this work is executed effectively, consistently, and in alignment with GridSecurity's technical standards, service commitments, client requirements, and applicable NERC CIP requirements. The team also serves as an advanced technical resource for complex Site Integration needs and supports operational CIP-Medium activities as needed.

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.

KEY RESPONSIBILITIES

- Leadership, Strategy & Team Development
  - Lead, coach, develop, and manage the Control Center Integration team, including conducting recurring 1:1s with direct reports, establishing clear priorities and performance expectations, providing ongoing feedback and development, and driving accountability for results.
  - Own and continuously improve GridSecurity's approach to control center technical services, including technical standards, reference architectures, processes, tools, and documentation to enable consistent, scalable, and high-quality delivery.
  - Translate organizational and project priorities into team execution plans, effectively balancing control center projects, professional services engagements, advanced technical support, interim CIP-Medium operational needs, team capacity, skill requirements, and competing priorities.
  - Establish and monitor key performance metrics to evaluate quality, efficiency, predictability, capacity, and customer experience and drive continuous improvement.
  - Remove roadblocks and maintain the technical depth necessary to effectively guide the team, challenge technical decisions, support complex issues, and directly contribute to execution when needed.
- Control Center Technical Services & Execution
  - Lead and actively participate in technical work across the control center lifecycle, including new control center design and build, CIP-Low onboarding, CIP-Medium transitions, infrastructure changes and integrations, and related professional services engagements.
  - Guide the architecture, design, deployment, configuration, testing, and troubleshooting of networking, systems, infrastructure, and cybersecurity technologies supporting secure, resilient, scalable, and operationally supportable control center environments.
  - Oversee the development of technical designs, specifications, and implementation documentation required to support successful control center deployment and ongoing operations.
  - Serve as a hands-on technical resource and escalation point for complex control center work, determining when to directly contribute or engage the appropriate resources based on expertise, capacity, urgency, and project priorities.
  - Support recurring and event-driven operational CIP-Medium activities, technical evidence generation, and issue resolution as needed in partnership with Operations and Compliance teams.

    - Conduct technical QA/QC and readiness reviews to ensure implementations and documentation meet GridSecurity's technical, security, contractual, operational, and applicable compliance requirements and are effectively transitioned to Operations when appropriate.
    - Participate in applicable on-call or escalation support as needed.
    - Perform other duties and support additional initiatives as assigned.
- Client & Cross-Functional Partnership
    - Build strong, effective working relationships with cross-functional partners, particularly Project Managers and Operations Managers, to maintain alignment on priorities, ownership, timelines, dependencies, risks, resource needs, and successful project outcomes.
    - Partner closely with Project Managers throughout the control center lifecycle to establish clear ownership, milestones, technical requirements, dependencies, and escalation paths.
    - Partner closely with Operations Managers to ensure technical decisions, configurations, documentation, and implementations support long-term operational readiness and effective transition into steady-state support.
    - Work directly with customers and external stakeholders to gather technical requirements, resolve blockers, troubleshoot implementation issues, and support successful project outcomes.
    - Proactively identify and communicate technical risks, issues, dependencies, decisions, and recommended next steps to technical and non-technical stakeholders.
    - Collaborate with Site Integration, Compliance, Security Operations, Network Operations, Systems Operations, Customer Success, and other teams to coordinate project activities, resolve cross-functional dependencies, and ensure effective operational handoffs.
    - Incorporate lessons learned and stakeholder feedback into processes and standards to continuously improve delivery quality and the customer experience.
    - Serve as an escalation point for operational issues related to control center work and recently transitioned environments, providing hands-on technical support when needed.
- 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 EXPERIENCE

- 7+ years of progressive experience in network engineering, systems or infrastructure engineering, cybersecurity, OT/ICS infrastructure, technical implementation, or a related field, including experience leading complex infrastructure designs, deployments, or technical projects.
- Experience supporting NERC CIP-regulated environments, including practical knowledge of technical controls, operational processes, and evidence requirements applicable to CIP-Medium environments.
- Experience leading, mentoring, supervising, or managing technical professionals, with demonstrated ability to coach, develop, establish priorities, manage workload, and drive accountability for results.
- Strong hands-on technical knowledge across networking, systems, infrastructure, and cybersecurity technologies, with the ability to troubleshoot complex issues, evaluate technical designs, provide technical guidance, and directly support implementation when needed.

- Experience designing and implementing secure, resilient network and infrastructure architectures, including firewalls, routing, switching, segmentation, secure remote connectivity, and redundancy/high-availability concepts.
- Experience developing technical architecture and implementation documentation, such as network diagrams, IP schemas, equipment specifications, bills of materials, configuration standards, SOPs, and implementation plans.
- Experience implementing, integrating, or supporting infrastructure and cybersecurity technologies such as SIEM, IAM/IDP, IDS/IPS, network and infrastructure monitoring, CMDB, and backup and recovery solutions.

REQUIRED PROFESSIONAL SKILLS

- Strong written and verbal communication skills, including the ability to communicate technical concepts to non-technical audiences.
- Strong leadership, coaching, and team development skills.
- Critical thinking and sound decision-making under pressure.
- Strong organizational, prioritization, and workload management abilities.
- Continuous improvement mindset with a focus on operational excellence.
- Ability to build collaborative relationships with clients, partners, and internal stakeholders.

PREFERRED QUALIFICATIONS

- Experience working for an MSSP, MSP, systems integrator, engineering firm, or other customer-facing technical services organization.
- Experience supporting electric utilities, renewable energy, power generation, control centers, or other critical infrastructure environments.
- Experience supporting Operational Technology (OT), Industrial Control Systems (ICS), and/or SCADA environments.
- Experience designing, building, integrating, or supporting control center infrastructure across multiple stages of its lifecycle.
- Deep working knowledge of NERC CIP requirements applicable to Medium Impact BES Cyber Systems and associated technical controls and evidence.
- Hands-on experience with Palo Alto, Cisco, Fortinet/Fortigate, or comparable enterprise networking and security technologies.
- Experience with IPsec VPNs, network segmentation, high-availability architectures, secure remote access, and related critical infrastructure technologies.

- Experience supporting NERC CIP audits, evidence requests, control validation, remediation activities, or transitions from CIP-Low to CIP-Medium environments.
- Relevant networking, systems, infrastructure, or cybersecurity certifications, such as CCNA/CCNP, PCNSE, CISSP, Security+, GIAC certifications, or equivalent industry credentials.

Benefits & Compensation

COMPENSATION

The base salary range for this position is $130,000 - $160,000 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 (ISOs) and/or cash bonuses on a monthly basis. Full-time employees are eligible to participate in GridSecurity's Incentive Compensation Plan following the applicable 90-day waiting period for new hires. Additionally, this role is eligible for an award of up to 10,000 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

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.

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.