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.

Security Analyst

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 Security Analyst reporting to the Security Operations Manager, you will play a key role in protecting our clients by monitoring, investigating, and responding to security threats across their environments. You will work as part of our Security Operations Center (SOC) to analyze security alerts, investigate suspicious activity, respond to cybersecurity incidents, assess vulnerabilities, and provide actionable recommendations to reduce risk. You will also work directly with clients, clearly communicating security findings, response actions, and recommended next steps while helping ensure they receive a responsive and trusted security experience. Your technical curiosity, sound judgment, attention to detail, and ability to remain effective during high-priority situations will be critical to protecting our clients and continuously strengthening GridSecurity's managed security services.

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.

NICE Framework Alignment: This position primarily aligns with PD-WRL-001 (Defensive Cybersecurity) and PD-WRL-003 (Incident Response), with supporting responsibilities aligned to PD-WRL-007 (Vulnerability Analysis). The Security Analyst performs hands-on security monitoring, investigation,

incident response, vulnerability analysis, and security event documentation to identify, assess, and respond to cybersecurity threats across client environments.

KEY RESPONSIBILITIES

- Security Monitoring, Analysis & Response
  - Monitor, investigate, and triage security alerts across endpoints, networks, identities, cloud environments, and other available telemetry using SIEM, EDR/XDR, and other security operations platforms to identify anomalous activity, validate potential threats, and determine scope and impact (T1350, T1084, T1085, T1112).
  - Perform incident triage to determine severity, urgency, potential impact, and appropriate escalation and response actions (T1250, T1251, T1252).
  - Respond to cybersecurity incidents, including investigation and evidence analysis, identification of affected systems or accounts and potential attack vectors, evidence preservation, containment and remediation recommendations, escalation, and documentation through closure (T1315, T1316).
  - Perform vulnerability scanning and analysis, prioritize findings based on risk and exploitability, and provide practical remediation, mitigation, and patching recommendations (T1118, T1119).
  - Apply knowledge of evolving cyber threats, attack techniques, indicators, and vulnerabilities to security monitoring, investigations, and response activities (T1582).
  - Participate in the SOC on-call rotation and provide after-hours response and escalation support as required.
- Client Service & Communication
  - Serve as a trusted point of contact for clients regarding security alerts, incidents, vulnerabilities, and service requests.
  - Clearly communicate security findings, risk, actions taken, and recommended next steps to both technical and non-technical audiences.
  - Facilitate timely escalation of security events and operational issues to appropriate internal and external stakeholders.
  - Support recurring client reporting by analyzing security alerts, incidents, vulnerabilities, trends, and other relevant metrics. (T1290, T1333).
  - Maintain accurate and timely documentation of investigations, incidents, customer interactions, and response activities.
- Process Improvement, Training, and Documentation
  - Continuously evaluate SOC processes, workflows, and operational practices and

recommend practical improvements that increase efficiency, consistency, scalability, and client experience.
    - Collaborate with Security Operations and cross-functional teams to develop, refine, and maintain standardized SOC procedures, playbooks, runbooks, escalation procedures, and response workflows (T1284, T1285, T1286).
    - Participate in post-incident reviews and translate lessons learned into improvements to detections, processes, tools, procedures, and other corrective actions that reduce operational and security risk (T1485, T1109).
    - Maintain organized, accurate, and timely documentation of security alerts, investigations, incidents, vulnerabilities, client interactions, and other applicable Security Operations activities.
    - Participate in internal training, knowledge sharing, and onboarding of new Security Operations team members as needed.
- 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

- 1–3 years of experience in cybersecurity, security operations, information technology, network operations, or a related technical role.
- Foundational knowledge of cybersecurity principles, common threats and vulnerabilities, security controls, and incident response concepts.
- Experience reviewing and analyzing system, network, or security logs and alerts to identify and troubleshoot potential issues.
- Working knowledge of Windows and Linux operating systems and common enterprise technologies, including Active Directory.
- Working knowledge of networking fundamentals, including TCP/IP, DNS, firewalls, VPNs, and common network protocols.
- Familiarity with endpoint, network, identity, and vulnerability management concepts and technologies.
- Experience using ticketing, monitoring, or other operational systems to document, track, and manage technical issues.

REQUIRED KNOWLEDGE

- Cybersecurity principles and practices (K0680).
- Cybersecurity threats, vulnerabilities, and threat characteristics (K0682, K0683, K0684).
- Incident response principles, tools, and handling techniques (K0724, K0725, K0726).
- Cybersecurity policies, procedures, and organizational requirements (K0677, K1183).
- Intrusion detection tools and techniques (K0732).
- Defense-in-depth principles and practices (K0791).
- Vulnerability data sources (K0723).
- System threats and system vulnerabilities (K0751, K0752).
- Network attack characteristics and attack vectors (K0783, K0831).

REQUIRED SKILLS

- Handling and resolving cybersecurity incidents (S0593).
- Detecting host- and network-based intrusions (S0572).
- Identifying anomalous activities and potential security violations (S0838).
- Recognizing and categorizing vulnerabilities (S0544, S0614).
- Performing log file and network data analysis (S0866, S0688).

- Performing incident analysis and event correlation (S0863, S0859).
- Communicating with internal and external stakeholders during security incidents (S0826).

REQUIRED PROFESSIONAL SKILLS

- Exceptional organization and time management.
- Strong written and verbal communication skills.
- Outstanding customer service and relationship-building abilities.
- Ability to manage competing priorities while maintaining attention to detail.
- Strong problem-solving and critical-thinking skills.
- Ability to influence and coordinate cross-functional teams without direct authority.
- Ability to remain composed and decisive in fast-paced environments.
- High degree of ownership, accountability, and follow-through.
- Continuous improvement mindset with a passion for building scalable processes.
- Collaborative team player who demonstrates professionalism, integrity, and adaptability.

PREFERRED EXPERIENCE

- Experience working in a Security Operations Center (SOC), Managed Security Service Provider (MSSP), or Managed Detection and Response (MDR) environment supporting utility-scale energy, renewables, or critical-infrastructure.
- Hands-on experience with SIEM, EDR/XDR, vulnerability management, and other security operations technologies.
- Experience investigating and responding to cybersecurity incidents involving endpoints, networks, identities, phishing, malware, or account compromise.
- Experience performing vulnerability scans, analyzing findings, and recommending remediation or mitigation actions.
- Experience with Microsoft security and identity technologies, including Microsoft 365, Azure, Entra ID, Defender, or similar platforms.
- Familiarity with security frameworks and methodologies such as MITRE ATT&CK, NIST Cybersecurity Framework, CIS Controls, or similar.
- Experience developing or improving security detections, alert logic, playbooks, runbooks, or security automation.
- Familiarity with scripting or automation using PowerShell, Python, APIs, or similar technologies.
- Experience working directly with external clients in a managed services or consulting environment.
- Relevant cybersecurity or technical certifications, such as CompTIA Security+, CySA+, Microsoft security certifications, GIAC certifications, or equivalent.

Benefits & Compensation

COMPENSATION

The base salary range for this position is $70,000 - $110,000 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 $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.