OPEN POSITION ANNOUNCEMENT!

Senior Cyber Security Analyst

Open until filled. Posted 08/16/2024

San Diego County – hybrid work schedule set by SDCP

About the role: San Diego Community Power (SDCP) is seeking a Senior Cybersecurity Analyst to join our growing team of IT experts who will be responsible for leading and overseeing the continuous monitoring of the organization enterprise assets, analyzing cyber threats, detecting potential cyber compromises, mitigating cyber vulnerabilities and conducting incident responses. A key priority of this role will be to design, configure, implement and ongoing support of enterprise cyber security tools for the organization including, but not limited to threat analysis, tools enhancement, event correlation, threat hunting/mitigation, and incident response.
The Senior Cybersecurity Analyst will work closely with internal and external stakeholders to support and implement cyber threat hunting activities including analysis of threat intelligence, detection and evaluation of IoCs, and escalation of incidents.

This role will report to the Data Analytics and IT Director.

WHO IS SAN DIEGO COMMUNITY POWER?

San Diego Community Power is a community-driven, not-for-profit public agency providing cleaner energy to the San Diego region. Formed in 2019, Community Power is the second largest Community Choice Aggregator (CCA) in California, serving nearly 1 million customer accounts across its member agencies: the Cities of San Diego, Chula Vista, Encinitas, Imperial Beach, La Mesa and National City, as well as the unincorporated areas of San Diego County.

OUR HISTORY

San Diego Community Power was formed in 2019 as a public, not-for-profit community choice aggregator (CCA) in the San Diego region. We began electric service in 2021 and serve five member agencies: San Diego, Chula Vista, Encinitas, La Mesa and Imperial Beach, County of San Diego, and National City. SDCP was formed to bring local control and customer choice to San Diego while also providing clean and renewable energy at competitive rates. By the end of 2023, SDCP will provide electricity for nearly half the electric load in San Diego Gas and Electric's service territory and will be the second largest CCA in California. For more information, please visit SDCommunityPower.org.

COMMITMENT TO DIVERSITY

At SDCP, we value diversity and are committed to creating an inclusive environment for all employees. We represent a diverse customer base and hope to hire employees that reflect our communities. We provide equal employment opportunities to all applicants for employment and prohibit discrimination and harassment of any type without regard to race, color, religion, age, sex, national origin, disability status genetics, protected veteran status, sexual orientation, gender identity or expression, or any other characteristic protected by federal, state, or local laws.

ESSENTIAL DUTIES AND PRIMARY RESPONSIBILITES

- Responsible for the design, configuration, implementation and ongoing support of Enterprise cyber security tools.
- Serving as the subject matter expert on security systems and concepts, including but not limited to SIEM, SOAR, EDR, IAM, PAM, IPS/IDS, Web Proxy, Firewall, DLP, Email Security, and WAF.
- Ensuring the service ability and integrity of the organization's cybersecurity software, tools and equipment.
- Performing day-to-day operations of the organization's 24/7 cybersecurity control protocols, including, but not limited to threat analysis, tools enhancement, event correlation, threat hunting, and incident response,
- Overseeing threat hunting activities including analysis of threat intelligence, detection and evaluation of IoCs, and escalation of incidents.
- Evaluating vendor solutions, make recommendations, and lead projects for deployment and/or enhancement of security systems.
- Leading the incident response team and execute the organization's Response Plan and cyber incident playbooks.
- Reviewing cybersecurity requests against normal operational security processes and provide approval or escalation.
- Overseeing organization's efforts in digital forensics and eDiscovery.
- Liaise with other departments on operational security matters, requests, and problems.
- Creating/maintaining superior documentation on tools, processes, procedures, and cyber playbooks.
- Understanding network protocols, routing and switching, LAN/WAN, remote access, and encryption protocols.
- Training and mentoring staff in the latest cybersecurity tools and concepts.
- Supporting email routing and messaging systems, email security gateways, and email encryption
- Proactively detecting problem areas and recommending/implementing solutions
- Performs other related duties and responsibilities as required.

MINIMUM KNOWLEDGE, SKILL AND ABILITIES

- Possession of at least one active cybersecurity certification such as CISSP, CISA, CEH, Security+ CySa+, is required.
- Experience using IT security systems and tools, including network intrusion detection and prevention (IDS/IPS) systems, and security information event management (SIEM) platforms
- Experience in performing cyber threat hunting including log analysis, digital forensics, and penetration testing
- Demonstrated skill with applying complex security controls and configurations to computer hardware, software and networks
- Proficiency in conducting incident after-action reviews and recommending mitigation strategies to avoid recurrence
- Understanding the NIST 800-53 framework and application of its controls in operational security.
- Proficiency in scripting languages and PowerShell
- Proficiency in network security concepts and troubleshooting enterprise firewalls, IDS/IPS, DNS Security, and WAF
- Proficiency in Microsoft Office365, Azure Cloud, and related security concepts
- Intimate knowledge of security tools such as SIEM, SOAR, EDR, DLP, and Web Filter/Proxy
- Red-teaming/offensive security expertise
- Strong project management, organizational and communication skills.
- Experience supporting and working with cross-functional teams in a dynamic environment.

QUALIFICATIONS, EDUCATION AND EXPERIENCE

The ideal candidate will possess a bachelor's degree in Information Computer Sciences, Information Computer Technology, Information Systems, or in a related field **AND** a minimum of five (5) years of professional experience in a cybersecurity lead role. Possession of at least one active cybersecurity certification such as CISSP, CISA, CEH, Security+ CySa+, is required.

WORK ENVIROMENT & CONDITIONS

Prolonged periods sitting at a desk and working on a computer. The position requires occasional carrying, lifting and/or moving objects up to 25 pounds. Occasional local travel required and reliable transportation to be able to attend SDCP events, meetings, and workshops as needed is expected.

At SDCP we work in the communities we serve and in the office. SDCP works to ensure a safe and healthy workplace for employees and in our communities. SDCP requires employees to be fully vaccinated for COVID-19.

SDCP is an agency required to adopt and promulgate a Conflict-of-Interest Code ("COI"). The COI code requires employees in designated positions, including those identified under the interim disclosure process to file a Statement of Economic Interests (Form 700) on an annual basis. A Successful candidate accepting this position may be required to file Conflict of Interest forms subject to the regulations of the Fair Political Practices Commission.

This job description may not be inclusive of all assigned duties, responsibilities, or aspects of the job described, and may be amended at the discretion of SDCP as needed

Compensation:

Salary Range: The position salary range is: $98,100 to $132,500; with exact compensation to be determined by SDCP, depending upon experience.

Benefits: Standard benefits package including but not limited to:

Insurance: SDCP offers group health benefits, including medical, vision, and dental insurance, for eligible FT employees. SDCP pays 100% of health group benefits, including medical, vision, and dental insurance premiums for employees and dependents. Also provided is a $100,000 Life & AD&D policy, STD and LTD coverage that is 100% paid by SDCP.

Retirement: SDCP offers a 457(b) plan for employee contributions and contributes 10% of eligible compensation to the employee's Money Purchase Plan.

Paid Time Off: 11 holidays per year + paid winter holiday *(between 12/24-12/31)*, 160 hours of accrued paid time off per year *(increases with time in service)*, and 96 hours per year of accrued paid sick leave.

SAN DIEGO COMMUNITY POWER IS AN EQUAL EMPLOYMENT OPPORTUNITY (EEO) AND AMERICAN DISABILITES ACT (ADA) EMPLOYER

How To Apply

Applicants must submit their resume, cover letter, and references using the "Apply today" functionality on our Career Opportunities webpage at:

SDCommunityPower.org/about/career-opportunities