Senior Security Onion Support and Professional Services Engineer

Company Overview

We are the builders of Security Onion, a free and open Linux distribution for threat hunting, network security monitoring, and log management. It includes best-of-breed free and open tools such as Suricata, Zeek, Wazuh, osquery, Elastic Stack, and many other security tools. Security Onion Solutions offers appliances, professional services, cloud resources, and official training centered around the Security Onion platform. Founded in 2014 by Security Onion creator Doug Burks, Security Onion Solutions has a small team with a global reach and ethos rooted in the community. We offer a competitive benefits package, excellent work/life balance, and a culture built on communication and trust.

Position Overview

Security Onion Solutions is looking for a Senior Security Onion Support and Professional Services Engineer! The successful candidate will be responsible for working with Security Onion Solutions clients to remotely plan, deploy, configure, tune, triage, and provide break/fix support for Security Onion. This position is customer-facing, remote, full time, Monday - Friday. Light travel up to 10% may be required. This is a unique opportunity to work with a high functioning team in a position where your impact is felt every day.

Required Skills/Experience/Education

- At least 5 years system and/or security administration experience
- At least 1 year of experience with at least one component technology of Security Onion - Elasticsearch, Logstash, Kibana, Beats, Suricata, Zeek, Stenographer, Wazuh, osquery, Strelka
- Strong Linux command line experience
- Understanding of TCP/IP and other networking fundamentals
- Understanding of server hardware fundamentals
- Bash or Python scripting experience

Preferred Skills/Experience/Education

- Engineering or analysis experience with Security Onion or component tools is strongly preferred
- Bachelor's degree or higher in Computer Science, Information Technology, Cybersecurity, or closely related discipline
- Demonstrated ability to troubleshoot problems quickly

- Strong organizational skills
- Experience with data pipelines
- Experience working with containers
- Experience with a signature framework - IDS, SIEM, Sigma
- One or more related professional certifications - GCIA, GMON, GCED, GSEC, Security+, Linux+, Network+, A+, CISSP

Requirements for all Security Onion Solutions Employees

- Must be a US citizen and reside in the US
- Ability to pass a background check and drug screen
- Previous success working with remote teams
- Ability to self-manage time and objectives

How To Apply

If interested, please email your resume to:

hireme-profserv@securityonionsolutions.com