Our company is growing rapidly and is looking for a security senior analyst. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for security senior analyst

- First responder to security event escalations via email, phone, ticket and chat
- Detect, escalate, and assist in remediation of critical information security incidents
- Document and communicate findings with customers in a detatiled, professional and timely manner
- Improve and challenge existing standard operating procedures in a very agile and fast-paced information security environment
- Identify and design information security use cases to address new and existing cyber threats
- Evaluate and enhance existing SIEM rules, alerts and use cases
- Develop new SIEM rules, alerts, dashboards and reports
- Maintain knowledge of SIE information security policies and goals
- Keeps current on the cyber security threat landscape and trends
- Continually create new knowledge base articles

Qualifications for security senior analyst

- Must be familiar with both Windows OS and Red Hat Linux for troubleshooting and installation
- Conceptual knowledge on different areas of computer security (network, application, cryptography, forensics, incident response)
- Basic understanding of computer networks (VLAN, IP addressing, security

- Understanding of common security attacks (DNS cache poisoning, ARP spoofing, DDoS, XSS, CSRF, SQL Injection)
- OFirewalls (Cisco PIX, ASA, NetScreen, CheckPoint, Nokia, Palo Alto, Juniper)
- OIntrusion Detection (IDS) and Intrusion Prevention (IPS) systems