# Lead Security Engineer

*Chicago, IL*

## Summary

The Cyber Defense Team is BCBSA's first line of defense against attackers. We are passionate security professionals responsible for defending the privacy and security of the data entrusted to us by our members. We are responsible for handling all malicious activity on BCBSA's networks. The Security Engineering and Assessment team exists within CyberDefense and is responsible for engineering solutions to protect BCBSA from threats and continually assesses BCBSA's security posture.

This role will report to the Director of the Security Engineering and Assessment team and will lead a team of skilled security engineers responsible for security engineering, vulnerability management, application vulnerability assessments, continuous monitoring, and penetration test coordination.

## Responsibilities:

- Supervise and lead the design and implementation of security solutions and detection logic, ensuring adequate support for threat prevention & detection, vulnerability management, incident response, and forensics activities
- Lead the Security Assessment, Vulnerability Management, and Continuous Monitoring programs tasked with identifying risks in the environment and managing their mitigation
- Automate information security activities related to incident response, data analytics, and reporting
- Provide mentorship and thought leadership

## Qualifications

*Required Basic Qualifications*:

- Bachelor's degree in Computer Science, Information Technology, or related field or equivalent experience
- Minimum 10 years of relevant experience with a focus on solution engineering and automation
- Hands-on experience coordinating vulnerability management and/or application assessment processes related to identifying and triaging vulnerabilities and weaknesses in operating systems and applications
- Skilled at automating tasks such as data processing, analytics, and incident response activities
- Experience acting in a security incident response role

*Preferred Basic Qualifications:*

- Bachelor's degree in Computer Science, Information Technology, or related field or equivalent experience
- Experience leading a vulnerability management, application testing, or red team program and presenting the results to both technical and non-technical audiences at all leadership levels
- Experience developing hardening standards for operating systems and applications, ideally using the CIS Benchmarks
- Experience programming in languages such as Python, PowerShell, BASH, SQL, Go, etc.
- Experience building detection rules in SIEM and/or EDR platforms, especially Splunk
- Experience using SOAR platforms to automate incident response activities
- Experience securing cloud platforms, preferably AWS
- Holds one or more relevant Information Security Certifications such as GPYC, GCWN, GCUX, GMON, GDAT, GDSA, GCSA, GCEH, GEVA, or GSE

**For more Information / To Apply:**

**https://careers-bcbsa.icims.com/jobs/3520/lead-security-engineer/job**