BlueCross BlueShield Association

Security Incident Response Analyst

Chicago, IL

Summary

The Security Incident Response Analyst will focus on security monitoring, threat hunting, and incident response. This role will leverage intuition, general security knowledge, and an array of tools to uncover and respond to malicious activity.

Responsibilities:

- Triage and investigate cybersecurity alerts.
- Monitor and respond to alerts generated by our enterprise security tools.
- Follow established incident response processes to triage security events.
- Triage issues escalated to the Cyber Defense team ensuring quick and appropriate follow-up actions are taken.
- Develop and tune cybersecurity alerts and dashboards.
- Document and manage investigations and incidents in our Incident Management System.
- Improve our detection capabilities by building and enhancing alert rules and actively hunting for evidence of malicious activity.
- Operate and maintain security tooling and platforms.
- Develop and continually improve incident response playbooks to ensure we efficiently and effectively analyze and respond to security alerts.
- Cross-functional shared team work .
- Assist with forensics activities following a security incident.
- Participate in Incident Response on-call rotation.

Qualifications

Required Basic Qualifications:

- Bachelor's degree or equivalent practical experience
- Demonstrated IT experience in the areas of operating systems, networking, and web-based applications
- Passionate about Information Security and technology
- Experience with malware, forensic, SIEM tools and scripting.

Preferred Basic Qualifications:

- *System administration experience (esp. Unix/Linux)*
- *Experience working with Splunk or other SIEM/threat detection platforms*
- *Previous SOC or IR experience is a plus*
- *Software development and/or scripting experience*
- *Comfortable communicating with individuals having varying degrees of technical understanding*
- *Knowledge of common attacks and defense*

For more Information / To Apply:
https://careers-bcbsa.icims.com/jobs/3397/security-incident-response-analyst/job