https://jobsfor7.com/job/lead-engineer-threat-detectionremote-or-hybrid/

Lead Engineer – Threat Detection(Remote Or Hybrid)

Job Location
United States
Remote work from: USA

Base Salary
USD 40 - USD 50

Employment Type
Full-time, Part-time

Description
The pay range is $111,200.00 – $200,200.00

Pay is based on several factors which vary based on position. These include labor markets and in some instances may include education, work experience and certifications. In addition to your pay, Target cares about and invests in you as a team member, so that you can take care of yourself and your family. Target offers eligible team members and their dependents comprehensive health benefits and programs, which may include medical, vision, dental, life insurance and more, to help you and your family take care of your whole selves. Other benefits for eligible team members include 401(k), employee discount, short term disability, long term disability, paid sick leave, paid national holidays, and paid vacation. Find competitive benefits from financial and education to well-being and beyond at https://corporate.target.com/careers/benefits.

JOIN TARGET CYBERSECURITY AS A LEAD ENGINEER – THREAT DETECTION

About Us

As a Fortune 50 company with more than 400,000 team members worldwide, Target is one of the world's most recognized brands and one of America's leading retailers. But behind the brand our guests love, is a culture of continual innovation – and right now, we are up to big things. The Cyber Fusion Center is the heart of Target's security team and a place where innovation happens daily. Interested in a culture that combines invention and creative freedom, ongoing learning, engineering excellence, and stellar outcomes? We are, too – that's why we work here. Join our team to take new enterprise security solutions from concept to release, collaborating with both software & security engineers to innovate on helping defend Target's network using cutting-edge technologies.

We are looking for an individual with experience writing detection content for external or internal threat actors derived from threat intelligence, threat hunting, detection research and other sources. This individual should be able to analyze collected threat intelligence, identify detection opportunities and develop, test and tune detection content. The ideal candidate will have experience writing detection for both host and network-based log sources across a myriad of both custom and

Hiring organization
Target

Date posted
October 15, 2024

Valid through
31.05.2025

APPLY NOW
Apply Now

industry tools.

Core responsibilities of this job are described within this job description. Job duties may change at any time due to business needs.

About You
• 7+ years of hands-on detection experience
• Demonstrates a deep subject matter expertise with threat detection, response, and mitigation
• Capable of identifying detection opportunities sourced from threat data
• Exhibits an understanding of concepts such as Pyramid of Pain, MITRE ATT&CK, and other organizing frameworks
• Maintains deep technical knowledge within areas of expertise
• Stays current with new technologies via formal training and self-directed education
• Splunk, ElasticSearch, Python, Zeek, SIGMA, Suricata and YARA technologies
• Cloud based detection within GCP and AWS
• Host based detection experience leveraging Sysmon, CrowdStrike Falcon, etc.
• Experience managing automation tools and CI/CD pipelines for detection and response.