Threat Detection Automation Engineer

Apply Now

at Reddit (View all jobs)

Remote

"The front page of the internet," Reddit brings over 330 million people together each month through their common interests, inviting them to share, vote, comment, and create across thousands of communities. Come for the cats, stay for the empathy.

The Reddit Security team is rapidly developing and this is an opportunity to get in and have an outsized impact on a highly skilled and motivated team. We look for humble experts with a relentlessly resourceful and entrepreneurial, "can do" view of security. We want to deliver facts and not FUD to the business to enable them to manage risk more effectively. Culture is important to us and a learning and developing mentality is vital regardless of the work assigned.

This role will be responsible for advancing our threat alerting, detection and response workflow capabilities. Remote is an option for the right candidate.

Responsibilities:

- Build and run scalable and sustainable infrastructure to drive the proactive and intelligence-driven identification and management of cyber security incidents
- Automate and integrate workflow between and within the SIEM, big data platforms, threat & vulnerability intelligence ingestion and information security incident response system
- Write signatures and tools to analyze and detect malicious activity
- Create and manage automation within cyber security tools such as cloud-native, network, infrastructure and endpoint tools
- Develop new initiatives where automation or tooling is required to improve workflow
- Regularly triage cyber security incidents post-enrichment and respond to events as part of the cyber security incident management process
- Constantly innovate at the pace of the adversary using latest techniques
- You will mentor and evangelize security practices through cross-functional work with infrastructure and engineering teams.

Qualifications:

- 7+ years of hands-on experience in cyber security automation or operations
- A passion for developing systems and process dedicated to finding and eradicating malicious activity
- Strong background in hunting, forensics, intrusion detection and threat intelligence
- Experience and desire to work with open source software such as Bro, Suricata, Hadoop, ElasticSearch as well as commercial products
- Experience writing tools to automate tasks and integrate systems in Python or equivalent
- Experience with cloud, IaaS, PaaS, 'network-as-a-service' environment is preferable
- Understanding of current security issues and threats and risks that can manifest in larger scale complex systems
- Experience coding Python, Shell or Perl scripts in order to push software and network interaction
- Excellent knowledge of Windows/Linux/Mac internals, ACLs and OS level security protection and common protocols e.g. TCP, HTTPS, IPMI, DHCP etc.
- Understanding and/or experience of AWS security
- Comfortable with automation and configuration management tools such as Jenkins, Ansible, Puppet/chef, Load Balancers, DNS Management, SSO Integration, Authorization Tokens
- Knowledge of SSH, keystores, security certificates, user and password management, authentication and authorization, session management
- Demonstrated track record of managing network security programs
- Proficiency in taking threat models and applying effective network security strategies at scale
- Ability to interact effectively with people at all levels of the organization

Qualities:

- Humble expert with a sense of urgency
- Skilled at taking complex topics and making them simple
- Transparent judgment and stands behind their decisions, right or wrong
- Team focus with an ability to lead in a matrixed organization

Apply for this Job

* Required

(Optional)

First Name *

Last Name *

Email *

Phone

Resume/CV

Attach

Dropbox

Google Drive

Paste

Cover Letter

Attach

Dropbox

Google Drive

Paste

LinkedIn Profile

Website

How did you hear about this job?

Submit Application