Fannie Mae

Lead Cyber Security Threat Detection Engineer (SOC)

Reston, VA, USA
Employees can work remotely
Full-time
Worker Classification: Remote

Company Description

At Fannie Mae, futures are made. The inspiring work we do makes an affordable home a reality and a difference in the lives of Americans. Every day offers compelling opportunities to modernize the nations housing finance system while being part of an inclusive team using new, emerging technologies. Here, you will help lead our industry forward, enhance your technical expertise, and make your career.

Job Description

As a valued colleague on our team, you will act as team lead while monitoring and evaluating threats to Fannie Mae's cybersecurity. In this role, you will set up checks and warnings to alert management when suspicious activity is detected, as well as coach and mentor less experienced team members.

THE IMPACT YOU WILL MAKE

The Lead Cyber Security Threat Detection Engineer (SOC) role will offer you the flexibility to make each day your own, while working alongside people who care so that you can deliver on the following responsibilities:

- Assist with the onboarding of logs into the SIEM
- Utilize the Cyber Kill Chain to develop detection content for the entire attack life cycle
- Contribute to Standard Operation Procedure development
- Utilize knowledge of latest threats and attack vectors to develop custom Splunk correlation rules for continuous monitoring
- Review logs to determine if relevant data is present to accelerate against data models to work with existing use cases
- Stay up to date with latest threats and familiar with APT and common TTPs
- Coach and mentor less experienced associates to enhance their understanding of Fannie Mae's information security activities and systems.
- Apply advanced skill, knowledge, and/or experience while leading teams to create cyber indicators to maintain awareness of systems and alert when abnormal behavior is detected.
- Consider interrelated technologies and processes to improve existing indicators to detect more advanced threats.
- Lead the monitoring of cyber threats in real-time.
- Identify opportunities to improve collaboration and communication with Incident Response while investigating

- Identify opportunities to improve collaboration and communication with Incident Response while investigating threats and attacks.

Qualifications

THE EXPERIENCE YOU BRING TO THE TEAM

Minimum Required Experiences

- 4 years

Desired Experiences

- Bachelor degree or equivalent

Skills:

- Experience with a SOAR platform (IBM Resilient)
- Experience with (Yara, Snort, Splunk, Python, Powershell, Carbon Black, Web Application Firewalls, etc)
- Extensive knowledge about network protocols and ports (TCP/UDP, HTTP, ICMP, DNS, SMTP, etc)
- Understanding of the MITRE ATT&CK framework
- Knowledge of Cloud Platforms (AWS, Azure, GCP)

REF ID: REF10428C

Additional Information

The future is what you make it to be. Discover compelling opportunities at careers.fanniemae.com.

Fannie Mae is an Equal Opportunity Employer, which means we are committed to fostering a diverse and inclusive workplace. All qualified applicants will receive consideration for employment without regard to race, religion, national origin, gender, gender identity, sexual orientation, personal appearance, protected veteran status, disability, age, or other legally protected status. For individuals with disabilities who would like to request an accommodation in the application process, email us at careers_mailbox@fanniemae.com.