Sign In

Cyber Threat Hunter - Information Security Engineer

Denver

Annandale

Addison

Posted 30+ Days Ago

Full time

20022116

Your full LinkedIn profile will be shared. **Learn More**

Apply

Apply with LinkedIn

Job Description:

This position is responsible for helping to design, build, and deliver major components of Bank of America s threat hunting strategy. You will work on a cross-functional team with deep knowledge of security processes and procedures, best practices, and red teaming to perform in-depth advanced log, system, and process analytics in order to pursue and prove or disprove hypotheses relating to malicious activity. Deep knowledge and experience with information security controls, infrastructure, and implementation techniques as well as familiarity with adversarial techniques, red teaming, and application and infrastructure assessment are key components for this role. You will demonstrate extraordinary organizational and cross-functional communication skills to drive analytics and investigations in to threats throughout the Enterprise.
In this role, you will work with all operational and technical teams within Global Information Security (GIS) in order to gain insight into critical controls and architectural specifics in order to develop analytics that identify malicious behavior accurately while maintaining a low false positive rate. This role advises on and reviews product assessments, policy adjustments, and architectural transformations that impact the global Corporation, and will be a thought leader in the design of cutting-edge detective, preventative, and proactive controls. Direct coordination with Data Scientists to build, improve, and evolve analytical models as part of the evolution of protective strategies is a core component. The use of industry-accepted and reviewed frameworks to enable BAC to stay abreast of and participate in evolving security frameworks and concepts is a must.
Required Skills:
• Deep experience with analytics as a focus area within Information Security
• Extensive knowledge of all domains within Information Security
• Familiarity with offensive strategies and assessment methodology
• Experience explaining analytics in plain English and ability with communicating associated risk
• Ability to see the larger picture when dealing with competing requirements and

About Us

At Bank of America, we're creating real, meaningful relationships with individuals, businesses and communities to help them focus on what matters most. We serve approximately 66 million consumer and small business clients, using our skills and expertise to help make their lives better.

We are committed to attracting and retaining top talent around the world to ensure we continue to deliver together for our customers, clients and communities. Along with taking care of our customers, we want to be a great place for people to work, and we strive to create an environment where all employees have the opportunity to achieve their goals.

Partnering Locally
Learn about some of the ways Bank of America is making a difference in the communities we serve.

Global Impact
Learn about the six areas that guide Bank of America's efforts to help make financial lives better for customers, clients, communities and our teammates.

Diversity and Inclusion
Each employee brings unique skills, background and opinions. We see diversity and inclusion as our platform for innovation and a key component in our success.

• Ability to see the larger picture when dealing with competing requirements and needs from across the teams in the organization in order to build consensus and drive results
• Ability to navigate and work effectively across a complex, geographically dispersed organization
• Experience with more than one EDR, SIEM, and manual log analysis techniques Mission-oriented with an emphasis on making the team successful
• Demonstrated ability to self-direct, with minimal supervision to achieve assigned goals
• Understanding of basic Data Science concepts and processes
• Deep experience working with industry-wide frameworks and standards like MITRE ATT&CK, STIX, TAXII, and SCAP

Enterprise Role Overview

Shift:
1st shift (United States of America)

Hours Per Week:
40

Your full LinkedIn profile will be shared. **Learn More**

Apply

Apply with LinkedIn

Follow Us

Our Values
Learn about our four values that represent what we believe.

Pay Transparency:
http://careers.bankofamerica.com/global/pay-transparency.aspx

Privacy Statement:
https://www.bankofamerica.com/privacy/overview.go