Sign In

Cyber Security Intrusion Analyst

Denver

Addison

Charlotte

Posted 30+ Days Ago

Full time

20048576

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

Apply

Apply with LinkedIn

Job Description:

The Identity Defense organization aims to protect digital identities which allow access to the Bank's internal network, resources and applications An Identity Defense analyst has the accountability for researching, designing, engineering, implementing, and supporting solutions to prevent and detect anomalous use of accounts.

Support design efforts related to build out of new processes, controls and supporting governance related to implementation of human and non-human account monitoring to protect the Bank. You will utilize in-depth technical knowledge and business requirements to help design and implement a scalable solution, inclusive of monitoring, alerting and escalation framework. Partner with senior leaders from line of business organizations to triage security events and report on impacting security incidents.
You will regularly collaborate with experts in and out of our team, both in country and in other regions, so excellent communication skills are very important. Role will also involve discussion with employees as part of alert analysis and disposition. If you are seeking a demanding role within Global Information Security (GIS) and have the required skills, this will be a great opportunity for you. Typically, applicants should have 5 to 7 years of cybersecurity or engineering experience.

Required Skills:
• Advanced cybersecurity monitoring and event analysis skills. The security analyst will leverage Splunk, SIEM, and other cybersecurity monitoring technologies to analyze traffic, activity, and events across the environment. Splunk experience is required.
• Data analysis/Data science skills. The security analyst will analyze logs and other security telemetry using a combination of cybersecurity and data analytics tools. Experience with modern data analytics tooling is required, recent

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.

experience in an ELK stack or similar data framework is preferred.
• Strong Intrusion Analysis background. Resource must be able to identify and interpret weblogs from various webservers.
• Knowledgeable of current exploits. Resource must be able to identify common exploits from the appropriate web and event logs.
• Working knowledge of Linux, Windows, and OS X operating systems.
• Comfortable with scripting languages and regular expressions
• Strong knowledge common network protocols
• Working knowledge of enterprise Client / Server architecture
• MITRE ATT&CK Threat Framework/Threat Modeling
• Experience building operationally sustainable processes
• Experience designing solutions which meet or exceed regulatory guidelines (FFIEC)
• Advanced knowledge of authentication protocols and telemetries
• Analyze data and evaluate relevance to an specific incident under investigation
• Present findings via written reports and orally to key stakeholders in clear and concise language
• Effectively communicates investigative findings to non-technical audiences

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

Similar Jobs

Cyber Security Intrusion Analyst | Denver, More...

Network Detection and Response Developer | Addison, More...

Network Detection and Response Developer | Addison, More...