https://www.applebank.com/security-center/how-to-protect-yourself/online,-mobile-and-social-media-security

Decline Accept Cookies

Apple Bank Careers

Sign In

Home Search for Jobs Join Talent Network

Security Operations Center (SOC) Analyst, AT

Apply

New York, NY

Full time

Posted 10 Days Ago

2024-0380

Hybrid/New York, NY
Pay Range: $80,000 - $100,000

The Security Operations Center (SOC) Analyst, AT will work closely with Apple Bank's Managed Security Service Provider (MSSP). The success criteria of this role is contingent upon the Analyst's expertise in SIEM event correlation and alert handling. This position will also assist in additional tasks, including risk monitoring, incident management, forensic investigation, threat hunting, and management reporting.

ESSENTIAL DUTIES & RESPONSIBILITIES

- Monitor and escalate security alerts through SIEM and other security tools
- Monitor and analyze tactics, techniques, and procedures (TTPs) in the threat landscape applicable to the Bank's corporate infrastructure.
- Evaluate and escalate threat capability gaps within the SOC and make recommendations to management.
- Seek out malware threats, phishing scams, compromised assets, and other anomalous events on a proactive basis and escalate to management as applicable
- Collaborate with other teams within the organization, outside of information security, to address security events.
- Facilitate information security department requests by assigning tickets to appropriate team members, acting as a liaison between stakeholders.
- Collaborate with Help Desk and end-users to resolve web traffic blocks efficiently utilizing our CASB solution.
- Analyze and proactively block potential and verified threats and exploitation.
- Monitor news, security sites, and other threat actor activity channels for new/current threats.
- Remain current on the latest threat scape, attack vectors, and countermeasures.
- Develop and maintain documentation on threat SOC use cases and procedures.
- Provide reporting to management on the status of open and closed SOC tickets.
- Perform other duties as requested.

SKILLS, EDUCATION, & EXPERIENCE

- Bachelor's degree in Computer Science, Information Systems Management, or other related field is preferred ; demonstrated equivalent skills and experience is acceptable in lieu of educational requirements.
- 0-2 years of relevant work experience required, preferably in financial services and or banking industry preferred.
- Excellent communication (verbal + written) with the ability to communicate clearly and concisely with internal and external parties.
- Understanding of a broad range of security technical concepts.
- Must have excellent analytical, multitasking, and organizational skills.
- Familiar with most common exploited CVEs and remediation methods.
- Must be available after business hours.
- Threat hunting experience optional.

Visa sponsorship not available.

About Us

Since 1863, Apple Bank has been a stable banking presence in New York City and its surrounding communities. We seek to put the best interests of our customers first and to manage our company prudently and

Read More

Our Employment Policy

Apple Bank's employment policy is to provide equal opportunity to all persons. We have made a commitment to equal employment opportunity through a positive and continuing affirmative action program. No employee or

Read More

We are an equal opportunity employer and do not discriminate on the basis of race, color, religion, sex, sexual orientation, gender identity, national origin, disability, military and/or veteran status, or any other Federal or State legally-protected classes.