CATALOG is looking for a

Security Engineer

Garden Catalog

About Us

We are a blockchain R&D studio, driven by our commitment to bridging (pun intended) the divide between foundational blockchains like Bitcoin and the thriving DeFi ecosystem. Our core expertise lies in solving intricate blockchain challenges through rigorous research in the realms of cryptography, game theory, and protocol design.

Our mission is to make web3 simple and hassle-free for everyone. No intimidating complexities, just pure potential. We began our journey in 2022, with a previous experience of building two billion-dollar web3 projects, Ren and Rook under our belt.

Our flagship product is the Catalog wallet (catalog.fi), a unique implementation of a multichain wallet that lets you use native bitcoin directly on any app. We also help power web3 projects like garden (garden.finance) to become
cross-chain seamlessly.

We are a lean and fast moving team of like-minded people and are passionate about making our mark in the DeFi space.

Overview

We are seeking a Security Engineer to join our team. The ideal candidate will be responsible for both Web3 and Web2 security paradigms, knowledge of Amazon Web Services (AWS), and proficiency in monitoring and alerting systems. This role involves ensuring the security of our digital assets, infrastructure, and applications.

Eligibility

- Bachelor's degree in Engineering without any backlogs.
- Should have very strong Problem-Solving and Analytical Skills.
- Mandatory to have built projects by self or built a portfolio outside academic curriculum.
- Students should have minimum aggregate marks (including all subjects and in all semesters) of 60% or 6 CGPA.

CATALOG is looking for a

Security Engineer

Garden

Catalog

Responsibilities

- Perform penetration testing of applications/products based on Web, Mobile, Web3 assets like Smart Contract, Bitcoin Script, etc.
- Plan and perform red team exercises in a variety of environments.
- Manage applications/products bug bounty program with validation and response mechanism for vulnerabilities submitted by external researchers.
- Continuous research on new attack vectors/techniques and their mitigations.
- Manage attack surface based on risk assessment for the business.
- Develop scripts, tools and methodologies to enhance security posture of the whole company and its applications/products.
- Manage continuous passive and active monitoring and alert systems such as Prometheus, Grafana, Wazuh, etc.
- Apply knowledge of AWS services to support the maintenance of secure cloud infrastructure.
- Clear communication for vulnerability reports and their remediation required.
- Work with cross-functional teams to align and priorities remediation efforts.
- Comply with company, division and professional ethical standards.

Essential Qualifications

- Foundational understanding of blockchain technologies and associated security considerations.
- Internship experience in a security engineering role or a related position.
- Proficiency in using monitoring and alerting tools.
- Uncompromising personal and professional integrity and ethics.
- Strong exposure to popular application security standards including OWASP top10, SANS top25, NIST, MITRE ATT&CK, etc.
- Any one of these certifications: OSCP, C-PENT, eJPT, PWPP, GPEN.
- Ability to think critically and identify areas of technical and non-technical risk.
- Good at writing technical reports and executive summary to communicate risk to required ones.
- Familiarity with AWS services and basic cloud security concepts.
- Understanding of languages like Go, Rust, TypeScript and Python.