



KOMAINU

Job Description

Job Title:	Security Engineer
Reports To:	Lead Security Architect
Location:	UK - Remote, right to work applicants only

About the Company:

Komainu is the first regulated digital asset custody solution built by institutions for institutions.

Komainu was established as a Joint Venture between Nomura, Ledger and Coinshares to fill a gap in the marketplace and provide regulated entities with a secure and compliant custody service for investment in digital assets. Since then, the trend of financial services firms adopting digital assets has only accelerated, further increasing the need for regulated and institutional-grade infrastructure for digital assets.

To support the rapid growth of the company and to accelerate the institutional adoption of digital assets, Komainu is actively seeking to onboard best-in-class talent globally.

Role Summary:

This exciting role provides the candidate with an opportunity to help design and build the security engineering function in a hyper-agile start-up within the cutting-edge world of decentralised finance.

This role will consist of primarily ensuring that the Microsoft Azure environment is both available and secure, following best-practice and industry frameworks. Initially the role will require supporting Azure from a more general IT perspective until the dedicated IT infrastructure team grows. Experience with setting up, configuring, supporting, and updating Microsoft Sentinel is a key requirement and any experience with the rest of the Azure security suite (DLP, Email controls, group policy, etc) and experience or demonstrable personal interest within finance (TradFi or DeFi) is highly desirable.

The role will also be responsible for vulnerability and patch management activities across the organisation, prioritising critical vulnerabilities and managing them through to closure, supporting leadership with compliance requirements, developing/applying new content/detection rules for other security controls implemented across the estate (EDR, SWG/SIG, IDPS, etc.), and supporting the lead architect with the design and implementation of new security controls.



KOMAINU

Duties & Responsibilities:

- **Azure Platform Engineering** – Ensuring that the Azure infrastructure is maintained, available, and secure.
- **Security Tool Engineering** – Ensure that security tools are available, updated, and appropriately administered.
- **Vulnerability Management** – Prioritise vulnerabilities and orchestrate remediation.
- **Content Development** – Work with Security Operations to identify and design new content then lead the implementation.
- **Capability Development** – Support the lead architect in identifying, implementing, and developing new security controls for continuous improvement.
- **Secure Configuration Review** – Regularly review current configurations for security concerns, raise as risks, provide and conduct remediating/mitigating actions.
- **Process Development** – Review, improve, and create Security Engineering processes.
- **Regulation and Compliance Support** – Support leadership where required for obtaining regulatory and compliance certifications.

Undertaking any other such duties as may be reasonably required by the role.

Qualifications, Skills & Experience:

Required

- Minimum of 2 years working within Security Engineering.
- Able to demonstrate experience in the majority of areas covered in Duties and Responsibilities.
- Strong experience with Microsoft Azure – specifically the security suite.
- Broad experience with Security Operations – understanding how a SOC operates.
- Strong understanding of emerging technologies and security methodologies, including hybrid multi-cloud, containerisation, automation, and SOAR.
- Experience with several security toolsets including SIEM, IDPS, Cloud Security (Zero Trust, CASB, SWG/SIG, etc), SOAR, CVM tools, and EDR.



KOMAINU

Desirable

- Background of working within finance (TradFi or DeFi) or a strong, demonstrable personal interest in the subject.
- Experience with using Zscaler.
- Experience with using CrowdStrike.
- Experience with using Qualys CVM.
- Experience in implementing security content/rules.
- Experienced with process development and an understanding of the ITIL framework.
- Understanding and knowledge of cyber security regulatory frameworks.

Desirable Qualifications

- MS Azure Security: MS-100, MS-500, AZ-500, AZ-700
- Relevant SANS: GFAT, GCLD, GPCS, GCSA, GDSA, GMON, GWEB, GCW
- CrowdStrike: CrowdStrike Certified Falcon Administrator
- Qualys: Qualys Certified Specialist
- Zscaler: ZCTA-IA, ZCCA-IA, ZCTA-PA, ZCCA-PA
- Legacy Qualifications: CCNA Security, MCSA

How to apply:

- Please send an email with your CV and a covering letter to careers@komainu.com