

Nguyễn Tuấn Quang Sang (Stephen Sang)

Ha Noi, Vietnam

📞 0889354995 📩 nguyentuanquangsang1999@gmail.com 💻 <https://github.com/dev1line>

OBJECTIVE

Senior Cloud Security & Infrastructure Engineer with 4+ years of experience architecting secure, high-availability systems on AWS. Specialized in Zero-Trust implementation, DevSecOps automation, and Blockchain infrastructure hardening. Proven track record in orchestrating multi-account governance (SCPs, Config) and securing digital assets using ZKP and KMS.

EDUCATION

The University of DaNang - University of Science and Technology

Sep 2017 - Jun 2022

Major: Information Technology

Classification: Very good

GPA: 3.29

CERTIFICATIONS

AWS Certified Solutions Architect – Associate

2026-2029

AWS Certified Security - Specialty

2026-2029

WORK EXPERIENCE

SKYBULL GAMING STUDIO

Jul 2025 - Present

Position: Senior Cloud Security & Infrastructure Engineer

Main responsibilities:

- Cloud Infrastructure Orchestration: Architected and managed high-availability AWS EKS clusters using Helm charts, focusing on infrastructure-as-code (IaC) to enforce security baselines across containerized environments.
- Network Hardening & Isolation: Engineered secure network topologies using VPC Endpoints and Private Subnets to isolate sensitive workloads, ensuring zero-trust communication for Hyperledger Fabric nodes and EVM-based validators.
- Secrets Management & Data Protection: Orchestrated a centralized security framework using AWS KMS and Secrets Manager to automate the lifecycle of encryption keys and sensitive credentials; enforced Zero-Trust principles by implementing strict IAM Policies and Permission Boundaries to eliminate privilege escalation risks.
- Monitoring & Auditing: Leveraged AWS CloudWatch and GuardDuty for real-time threat detection; conducted automated vulnerability assessments of infrastructure and smart contracts using Slither and CloudWatch Logs.
- Cross-Chain Infrastructure Support: Provided deep technical support for multi-platform infrastructure including Substrate (The Root Network), Avalanche (Subnets), and Kaia Network, focusing on node stability and peering security.
- DevSecOps Implementation: Developed automated CI/CD pipelines (GitLab CI/Jenkins) integrating static and dynamic security analysis (SAST/DAST) for Backend services (Go, NestJS, Lambda) and containerized applications.

CMC GLOBAL

Jun 2023 - Jun 2025

Position: Blockchain & Cloud Security Engineer

Main responsibilities:

- ZKP & Cloud Privacy Engineering: Researched and integrated Zero-Knowledge Proof (ZKP) protocols to enhance data privacy and transaction anonymity; orchestrated privacy-preserving computations within AWS Enclaves to maintain strict regulatory compliance.
- Cloud-Native Security Research & Deployment: Evaluated and deployed cloud-based security tools, including AWS GuardDuty and WAF, to protect TON-based decentralized applications, specifically securing private key storage and transaction relayers against external threats.
- Secure SDLC & Infrastructure-as-Code (IaC): Designed secure codebases for high-stakes financial services and developed Terraform scripts to provision hardened cloud environments; implemented rigorous testing frameworks (Unit, Integration, and Security audits) using TONCLI.

- Technical Mentorship: Led knowledge-sharing sessions on Cloud Security best practices (focused on IAM and Secret management) and ZKP concepts to bridge the gap between traditional DevOps and Blockchain security.
- Virtual Machine Security & Debugging: Diagnosed complex logic and security flaws at the VM level using Blueprint, FunC, and FIFT, ensuring the integrity of smart contracts deployed on cloud-based nodes.

NAPA GLOBAL

Oct 2021 - Dec 2022

Position: Software Engineer (Smart Contract Security Focus)

Main responsibilities:

- Security Auditing & Formal Verification: Conducted deep security analysis of Smart Contracts using Slither (static analysis), Echidna (fuzzing), and Foundry (property-based testing) to identify and remediate vulnerabilities like reentrancy and arithmetic overflows.
- Secure Contract Architecture: Designed and audited dApp architectures on Ethereum-compatible chains, ensuring robust logic flow and gas-optimized execution.
- EVM Ecosystem Security: Developed and maintained production-grade smart contracts using Solidity, ensuring 100% test coverage for critical financial logic through advanced testing frameworks.
- Blockchain Integration: Built secure interfaces between cloud backend services and on-chain data using Web3.py and EthersJS, emphasizing secure data serialization and transport.

ACTIVITIES

PARTICIPATING IN TON GLOBAL BTCFI HACKATHON ON DORAHACKS

Mar 2025 - Apr 2025

Lead Smart Contract Developer – NFT Lending Protocol

- Secure Contract Engineering: Engineered and deployed secure NFT lending logic using FunC and Ton Teleport BTC, focusing on cross-chain asset security.
- Security Research: Conducted extensive research on TON SDK and TONX to implement robust authorization mechanisms for decentralized lending.

PARTICIPATING IN SOLANA CODING CAMP SEASON 2 2022

Oct 2022 - Dec 2022

Team Lead (Soloans Team) – Flash Loan Aggregator

DeFi Infrastructure: Led a 5-member team to build a high-performance flash loan aggregator integrated with Solend and Orca. Optimization & Auditing: Optimized transaction execution speed and audited contract logic to prevent common flash loan attack vectors on the Solana network.

PARTICIPATING IN AURA NETWORK HACKATHON 2022

July 2022 - Aug 2022

Core Member – NFT Staking Ecosystem

- Rust Security: Developed secure NFT staking modules using Rust within the COSMOS ecosystem.
- Infrastructure Learning: Completed advanced training in Rust memory safety and concurrency, applying these principles to ensure the integrity of staking rewards.

LEARNING NEARK5 COURSE IN VBLILAB

Jun 2022 - July 2022

Team Lead (NewEra Team) - Crypto Payment Gateway

- Practical Implementation: Spearheaded the development of a real-world cryptocurrency payment gateway for retail, focusing on secure transaction handling on the NEAR protocol.
- Security Best Practices: Mentored team members on implementing Least Privilege principles in smart contract access control.

SKILLS

Cloud Security

AWS Security Specialist: IAM (Least Privilege, Permission Boundaries), KMS (Envelope Encryption), Secrets Manager, AWS GuardDuty, AWS WAF, Shield, Security Hub, CloudTrail, Config, VPC Security (PrivateLink, Security Groups).

Infrastructure & Orchestration

Kubernetes (K8s) & Containerization: Architecting and managing high-availability AWS EKS clusters; proficient in Docker (Image Hardening, multi-stage builds). Infrastructure as Code (IaC): Terraform, Helm Charts (Secure Templating).

DevSecOps & CI/CD

Automated Security Pipelines: GitLab CI, Jenkins. Security Tooling: Static Analysis (SAST), Software Composition Analysis (SCA), Automated Vulnerability Scanning (Trivy, Inspector).

Blockchain Security

Smart Contract Auditing: Foundry, Slither, Echidna, TONCLI. Architectures: Hyperledger Fabric (MSP, CA, Private Data), EVM, Substrate, Avalanche (Subnets), Zero-Knowledge Proof (ZKP) concepts.

Development	Backend: Golang (Chaincode, Microservices), NestJS, Node.js, Python (FastAPI). Frontend: ReactJS, NextJS. Database: PostgreSQL, MongoDB.
Security Research	Vulnerability Analysis: Specialized in TON (FunC, FIFT, TL-B), Rust-based security for Cosmos/Near, and cross-chain asset protection.

PROJECTS

Decentralized Finance (DeFi) & Privacy-focused Institution

(2025 - Present)

Customer	US
Description	<ul style="list-style-type: none"> - Architected a secure cloud environment for executing Zero-Knowledge Proof (ZKP) computations to ensure transaction anonymity and data privacy. - Combined hardware-level isolation with cryptographic proofs to build a "Trustless" financial settlement layer. - Focused on regulatory compliance (GDPR) while maintaining user anonymity through advanced cryptographic techniques.
Team size	05
My position	Privacy Engineer / Cloud Architect
My responsibilities	<ul style="list-style-type: none"> - Deployed AWS Nitro Enclaves to create isolated compute environments for generating and verifying ZK-Proofs (zk-SNARKs/STARKs). - Integrated ZKP protocols with cloud-native storage to mask sensitive financial data while allowing for public verification of transaction validity. - Hardened the Prover and Verifier node infrastructure on EKS using multi-layer security groups and IAM encryption policies. - Researched and optimized ZKP verification costs on EVM-compatible chains through batching and off-chain computation.
Technologies used	AWS Nitro Enclaves, ZK-SNARKs, AWS EKS, Docker, KMS, Golang, Solidity, Circom.

NFT Marketplace & Web3 Gaming Studio

(2025 - 2025)

Customer	US
Description	<ul style="list-style-type: none"> - Integrated a comprehensive security scanning suite into the GitLab CI/CD pipeline to detect vulnerabilities before deployment. - Automated the identification of "hardcoded secrets," vulnerable dependencies, and insecure infrastructure configurations (IaC). - Reduced the production vulnerability count by 85% through "Shift Left" security practices.
Team size	08
My position	DevSecOps Lead
My responsibilities	<ul style="list-style-type: none"> - Implemented Secrets Detection to block commits containing sensitive API keys or AWS Access Keys. - Configured SCA (Software Composition Analysis) to scan Node.js/Python libraries for known CVEs. - Integrated Checkov/Terrascan for IaC Scanning to prevent the deployment of insecure resources (e.g., Public S3 buckets). - Performed security audits on Web3 libraries and smart contract wrappers using Foundry and Slither prior to mainnet deployment.
Technologies used	GitLab CI, Checkov, Trivy (Container Scan), Slither, Foundry, Secrets Detection, AWS Inspector.

Multi-Account Centralized Security Logging & Analytics (SIEM)

(2024 - 2024)

Customer	US
Description	<ul style="list-style-type: none">- Engineered a centralized Security Data Lake to aggregate logs (CloudTrail, VPC Flow Logs, DNS Logs) from 50+ accounts into a dedicated Security Account.- Implemented high-integrity storage for audit trails to meet SOC 2 and PCI-DSS compliance requirements.- Provided deep visibility into infrastructure security posture through advanced analytics and real-time dashboards.
Team size	05
My position	Data Security Engineer
My responsibilities	<ul style="list-style-type: none">- Configured S3 Object Lock in Compliance Mode to ensure log immutability and prevent log tampering by malicious actors.- Optimized log querying performance using Amazon Athena and partitioned data structures in S3.- Developed Amazon QuickSight dashboards to visualize threat patterns and access anomalies.- Conducted behavior analysis on access patterns to Private Key Management services and Indexer APIs to detect early-stage data exfiltration.
Technologies used	Amazon S3 (Object Lock), Amazon Athena, QuickSight, Kinesis Data Firehose, VPC Flow Logs, CloudTrail.

Cryptocurrency Exchange & Validator Service Provider

(2024 - 2024)

Customer	US
Description	<ul style="list-style-type: none">- Developed an automated security response system to minimize MTTR (Mean Time To Respond) for compromised cloud assets.- Integrated Amazon GuardDuty with EventBridge to trigger real-time defensive actions against crypto-jacking and unauthorized access attempts.- Automated the isolation of compromised EC2 instances and validator nodes to protect the integrity of the blockchain network.
Team size	04
My position	Security Automation Engineer
My responsibilities	<ul style="list-style-type: none">- Developed AWS Lambda functions to automate incident response workflows: revoking compromised IAM roles and attaching "Isolate" Security Groups.- Built an automated forensics pipeline to capture EBS Snapshots and memory dumps for post-incident analysis.- Designed a notification system via SNS and Slack to alert the SOC team with detailed threat intelligence data.- Protected Validator Nodes from DDoS and unauthorized intrusion by implementing automated port-blocking and IP-sharding.
Technologies used	AWS GuardDuty, AWS Lambda, EventBridge, EBS Snapshot, SNS, Security Groups, Python (Boto3).

Enterprise-wide Cloud Security Guardrails & Governance

(2023 - 2024)

Customer	US
Description	<ul style="list-style-type: none">- Established a multi-account governance framework using AWS Organizations to manage security policies across 100+ AWS accounts.- Implemented Service Control Policies (SCPs) to enforce mandatory security guardrails, such as disabling unapproved regions and preventing the deactivation of CloudTrail and GuardDuty.- Enforced IMDSv2 globally for all EC2 instances to mitigate SSRF attack vectors.- Standardized infrastructure deployment using Terraform to ensure consistent security postures across production and staging environments.

Team size	06
My position	Cloud Security Engineer
My responsibilities	<ul style="list-style-type: none">- Designed and implemented complex SCPs to restrict high-risk API actions at the organizational level.- Built an automated compliance monitoring system using AWS Config to detect and au
Technologies used	AWS Organizations, SCPs, Terraform, AWS Config, AWS Control Tower, IAM, IMDSv2