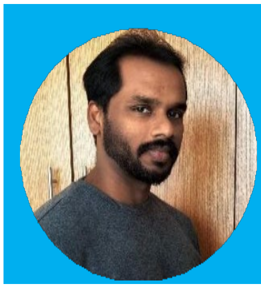


SANTHOSH KUMAR

Principal Security Architect

☎ 00971-556707167
✉ Santgutz2000@live.com
LinkedIn
Dubai, UAE
Projects

CSSLP | CEH Certified Ethical Hacker | CIPT Certified Information Privacy Technologist iapp | aws CERTIFIED | ANTHROP\C

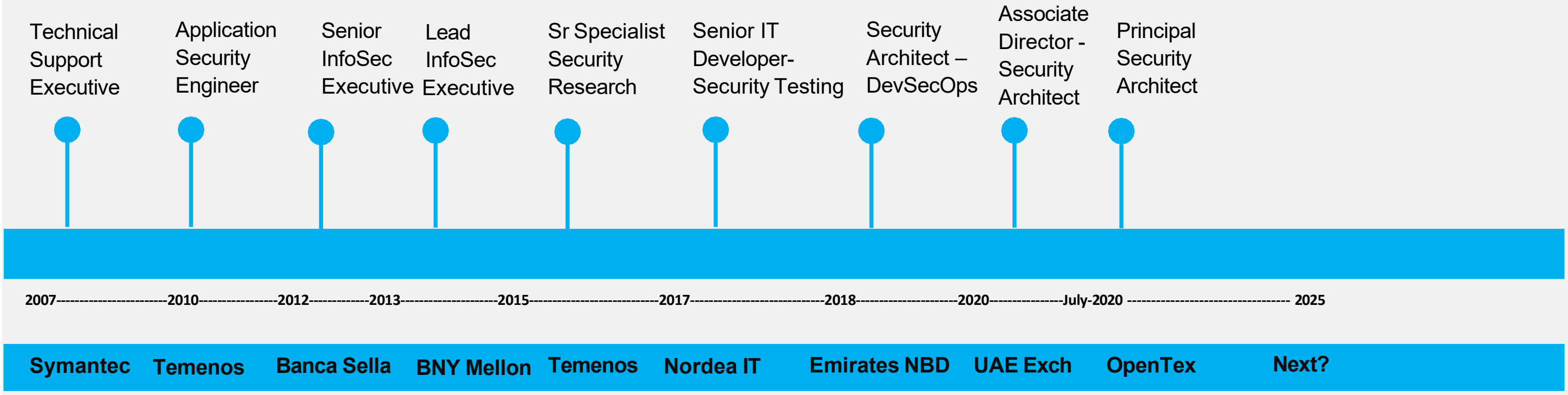
Profile

I am Santhosh Kumar, an information security expert with over 18 years of experience in designing and implementing robust security architectures across diverse industries. My expertise spans cloud security, application security, secure SDLC, and vulnerability management, securing cloud infrastructures, web applications, payment systems, blockchain technologies, data platforms, and core banking solutions. As an AI enthusiast and expert, I explore innovative ways to integrate AI into day to day productivity, cybersecurity, and building apps simplify work. My proficiency extends to static code analysis SAST, DAST, interactive application security testing (IAST), privacy, penetration testing, and cloud security measures, ensuring organizations stay ahead of evolving threats. Passionate about sharing knowledge, I actively engage with the security and AI communities to foster innovation and security excellence. Through collaborations with industry leaders, I have helped drive impactful security transformations, leveraging emerging technologies to strengthen organizational resilience.

Key Skills

- Risk & Compliance
- CI / CD Integration
- Threat Modeling
- Secure SDLC
- Web application Firewall (WAF)
- Vulnerability analysis & Management
- Amazon Web Services Security
- Identity and Access Management
- Web & Mobile Application Security Testing
- Interactive application security testing
- SAST & DAST
- Database Security
- Azure Security
- Open-source security
- DevSecOps Toolchain
- Encryption and PKI
- Secure design principles
- API & Microservice Security
- Cloud Security architecture
- IAM, SAML, Federation, ADFS
- Runtime Application Self-Protection (RASP)
- Defensive Coding Practices

Professional Journey



Technical Support Executive | Application Security Engineer | Senior InfoSec Executive | Lead InfoSec Executive | Sr Specialist Security Research | Senior IT Developer-Security Testing | Security Architect – DevSecOps | Associate Director - Security Architect | Principal Security Architect

2007------------------------2010-----------------2012-------------2013--------------------2015---------------------------2017----------------------------2018----------------------2020----------------July-2020 ------------------------------------ 2025

Symantec | Temenos | Banca Sella | BNY Mellon | Temenos | Nordea IT | Emirates NBD | UAE Exch | OpenTex | Next?

Education

- Bachelor of Computer Application

Industry Experience

- Enterprise Sales
- Banking
- Financial Services

Confrences & Hackthons

- Dev Hackthon UAE 2019 - Modreator
- BlackHat EU 2018 – Co-Presenter
- CTF 2016 – Design and Execution
- Speaker – 2022 SoftProm Cybersecurity Azerbaijan
- Speaker – 2023 Bucharest Cybersecurity Conference

Certifications and Trainings

- AWS Security Specialty
- Azure Foundational
- Microsoft Azure Security
- CPH (Python Hacker)
- CIPT
- CSSLP
- CISSP (Pursuing)
- CIPP / E
- TOGAF 9.2
- SANS: SEC545- Cloud Security Architecture and Operations
- SAP HANA 2 Security
- AI Fluency, MCP Development from Anthropic

Infosec Standards, Guidelines

- NIST
- OWASP
- PCI DSS
- ISO 27001, 31000
- CIS
- BSIMM

Countries Served

- United Arab Emirates
- Poland
- United Kingdom
- Saudi Arabia
- India
- Prague
- Sweden

Work Experience

Principal Security Architect July 2020 – Till now

Opentext, Dubai, United Arab Emirates

As a Principal Security Architect at OpenText, I play a critical role in driving the adoption of Fortify, a leading application security solution. From initial engagement with customers to post-sales handover, I ensure seamless solution positioning, technical validation, and strategic alignment with business needs. I lead technical presentations, demos, hands-on workshops, and proof-of-concept (PoC) engagements, demonstrating Fortify's capabilities and making it an essential choice for customers.

I work closely with stakeholders to analyze security requirements, define solution architectures, and create accurate technical Bills of Quantity (BoQ) tailored to customer environments. My role also involves responding to RFIs and RFPs, ensuring compelling and technically sound proposals that strengthen our competitive edge.

Beyond the sales cycle, I facilitate a smooth transition to professional services, ensuring that all gathered requirements, security goals, and implementation roadmaps are effectively handed off for successful deployment. My expertise in application security, secure SDLC, and vulnerability management allows me to act as a trusted advisor, helping organizations enhance their security posture while maximizing the value of OpenText's Fortify solutions.

Responsibilities

- Build trust and strong technical relationships with customers and prospects by understanding their security challenges and positioning OpenText Fortify as the ideal solution.
- Train and mentor non-AppSec presales consultants to effectively position and sell Fortify, equipping them with the knowledge to drive successful engagements.
- Enable and support account managers in articulating the business impact of Fortify, ensuring they can demonstrate why security is a business enabler rather than just a technical necessity.
- Act as an Application Security Champion for strategic customers, guiding them in building mature security programs, adopting DevSecOps practices, and strengthening their secure software development lifecycle (SDLC).
- Advise customers on best practices for cloud security and DevSecOps, helping them implement security automation, shift-left strategies, and compliance-driven security frameworks.
- Represent OpenText and Fortify at sales events, industry conferences, and webinars, advocating for modern security practices and OpenText's leadership in application security.
- Act as the voice of the customer by translating their security needs into actionable insights for product management, ensuring product enhancements align with real-world challenges.
- Develop and maintain competitive analysis matrices, providing detailed comparisons of Fortify versus competitors to strengthen OpenText's positioning in the market.
- Conduct technical deep dives, hands-on workshops, and PoCs, demonstrating Fortify's strengths in static analysis, IAST, and cloud security.
- Collaborate cross-functionally with sales, marketing, and engineering teams to refine messaging, improve product capabilities, and drive customer success.
- Lead strategic initiatives to position Fortify beyond security scanning, focusing on how it integrates into business risk management and compliance strategies.
- Stay ahead of industry trends, continuously researching the evolving threat landscape and ensuring OpenText Fortify remains at the forefront of application security innovation.

Key Internal Projects

- **Scaled Fortify Sales Revenue:** Played a pivotal role in growing Fortify sales quota from $1.5 million in 2020 to over $10 million in 2025, ensuring consistent year-over-year growth and expanding OpenText's footprint in the Middle East region.
- **AI-Powered RFP & RFI Automation:** Designed and implemented an AI-driven automation system for responding to RFPs and RFIs, saving hundreds of hours for presales consultants, improving response accuracy, and accelerating deal cycles.
- **AI-Driven Competitive Intelligence System:** Developed a real-time, AI-powered competitive intelligence platform that instantly compares OpenText Fortify with competitors, providing actionable insights and strengthening deal positioning.
- **Strategic Customer Engagement & Deal Closure:** Over the last five years, engaged with 300+ customers across the Middle East, successfully closing nearly 60% of the opportunities I was involved in, significantly contributing to OpenText's market dominance.
- **Health Check Initiative for Upselling & Portfolio Expansion:** Introduced a Fortify Health Check Program to assess customer security maturity, identify gaps, and position new offerings, leading to additional sales opportunities and increased adoption of Fortify and partner solutions.

Work Experience

Associate Director – Security Architect — Jan 2020 – June 2020

UAE Exchange, Abu Dhabi, United Arab Emirates

My primary role is to build a secure and hybrid cloud deployment posture for supporting its PAAS (Payment as a Service) business and build a devsecops culture by engaging with devOps.

Responsibilities

- Build and execute security capabilities to protect the organization assets both in on-perm & cloud.
- Secure migration of on-perm application and infrastructure to cloud enforcing cloud-native redesign
- Manage and operate the global threat and vulnerability management (Penetration Testing, Vulnerability Assessment, Web/Mobile Application Penetration Testing)
- Contribute to the “centre of Excellence” for security architecture and cloud security by developing architecture design patterns and controls
- Contribute to “centre of excellence” for cybersecurity by conducting research focused on developing the framework, standards, and guidelines for emerging technologies solutions, and practices such as cloud, DevSecOps.

Key Projects

- Finablr Integration Platform Services (FIPS)
- GooglePay (DirecPay)
- Multi-Cloud Security Reference Architecture
- AWS & Azure Security control design
- Online Money Transfer (OMT)

Work Experience

Security Architect | DevSecOps — May 2018 – Dec 2019

EmiratesNBD, Dubai, UAE

As a security architect and devSecOps engineer who helps developers and solution architects to design and develop secure applications

Key Responsibilities

- Actively participating in architecture reviews/workshops to implement security features to ensure secure by design
- Perform & Drive Penetration testing, Static and Manual code analysis, Security Design Reviews, Threat modeling and Open source analysis
- Enhance the security of environment where applications are deployed by scanning for vulnerabilities and compliance providing necessary recommendations
- My security solutions are always designed considering the user experience and business goals
- Develop strong relationship with key business and technology stakeholders in order to influence and drive the security agenda
- Implemented cryptographic practices throughout the SDLC
- Integrated security solutions such as SAST and DAST in Jenkins pipeline
- Perform manual penetration testing for all the applications to identify business logic issues
- Reverse engineer web applications which helps me to find out of the box issues
- I implement strong security requirements & controls such as
  - ✓ Data / application classification
  - ✓ VA and compliance scan for UAT, SIT, PR and DR with application and dependencies installed and configured
  - ✓ Application security assessment aka penetration testing
  - ✓ Secure code review
  - ✓ Configure application administrative panel, database and operating system access through privileged access management (PAM) (CyberARK)
  - ✓ Ensure data at rest is encrypted (LUKS, Bitlocker and TDE)
  - ✓ Ensure only allowed port / protocol communication is allowed between integrated layers
  - ✓ Configure Web application firewall (F5) for critical and highly sensitive applications
  - ✓ Ensure two factor authentication for public facing systems
  - ✓ Implement CASB for cloud applications
  - ✓ Enhance and integrate DLP for sensitive data containing reports
  - ✓ Configure access controls through IAM and implement SSO
  - ✓ Encryption of data in transit e.g. TLS 1.2 (HTTPS, LDAPS, Secure JDBC and ODBC)
  - ✓ Strong crypto such as SHA3 or AES 256

Key Projects

- Blockchain on cloud (IBM Hyperledger)
- SAP HANA, SAP Router & Solutions Manager
- Finacle 11x (Core Banking)
- Informatica CDC, BDQ & BDM
- Gemalto fraud Monitoring (ThreatMetrix & BehaviourSec)
- Teller cash recyclers
- Enterprise Data Platform - Hadoop
- Cash deposit machines

Key Achievements

- Best Agile Supporter from Emirates NBD Group IT Chief Information officer (2018)
- Best Project Support from Emirates NBD Group IT SVP Data Platforms (2018)
- Stake Holder Management Award from Emirates NBD Group IT (2019)
- Built a baseline security requirement list to standardize the controls defined by security architects
- Implemented security DevSecOps tool chain

Senior IT Developer – Security Testing July 2017 – Apr 2018

Nordea IT, Gydnia, Poland

As a Security Consultant at Nordea IT where I played multiple roles during my tenure which included security Testing, Devsecops and Security Architect.

Key Responsibilities

- Manage and execution of Penetration testing of core banking application and infrastructure
- Single point of contact for all product security consultation and queries
- Strong application security delivery experience on Agile environment
- Actively participate in key stakeholder discussions to highlight security check points in design and development and provide solution for vulnerability mitigation
- Coordinate with IT Security team to implement additional layers of security protection in WAF
- Work closely with enterprise and product architects to address security threats in design
- Web service API security testing which includes SOAP, REST and XML
- Enhance and Maintain test data (payloads) for quick and active security analysis and fuzzing
- Devsecops implementation planning and support to implement tools like Fortify SCA, Gauntlt, BDD-Security and ZAP ATTACK proxy
- Stack hardening – Enhance the security of environment where Core Banking application are deployed.
- Fuzzing web application with Burp Suite and other mutation fuzzers
- Reverse engineering web applications to identify the core security issues
- Assist Vendor in providing proper remediation solution
- Validate Vendor's security solution to identify potential loopholes
- Implement DevSecOps model of automated security scanning and code scans during releases

Key Achievements

- Quick Starter Award (Nomination) from Noreda IT (2017)
- Implemented agile security assessment process
- Automated security testing including fuzzing using open source tools
- Built an inventory of attack payloads for continuous scan automation
- Built a portfolio of security vulnerabilities for core banking application

Key Projects

- T24 Core Banking
- Nordea collateral management
- Core Banking API Platform
- DevSecOps Practice

Senior Specialist – Security Technology & Research May 2015 – Jun 2017

Temenos, Chennai, India

As a senior specialist - security research headed by chief security officer. I have actively managed ten plus team members including security testers and secure code reviewers during my tenure.

Key Responsibilities

- Write process and procedure for internal penetration testing, static security code reviews, security design reviews, and open source security analysis.
- Perform security architecture analysis for banking mobile apps
- Handle Temenos customer queries regarding product security
- Engagement with pre-sales team to demonstrate security features built in to the product to enable security as a differentiator in sales
- Leading a team of penetration testers and secure code experts
- Perform extensive market research to identify new security products which could aid internal security teams
- Actively participating in architecture reviews / workshops to implement security features to ensure secure by design
- Implement Security controls for new product and enhance security controls for existing products
- Develop relationships with key business and technology stakeholders in order to influence and drive the security agenda
- Drive Penetration testing, Static and Manual code analysis, Security Design Reviews, Threat modelling and Open source analysis
- Stack hardening – Enhance the security of environment where Temenos products are deployed.
- Open source analysis – Security analysis and maintenance of free and open source libraries utilized by products developed in Temenos
- Ensure Temenos products are rigorously penetration tested by external penetration testers by engaging with third party security firms on yearly basis
- Security in Devops - Work with internal development team to setup environments for security assessments and automate security testing both static and dynamic analysis in continuous integration.
- Identify opportunities to develop and improve existing automation processes in security analysis.

Key Achievements

- Devised and executed an organization wide penetration testing for diverse products
- Open SAMM (Software Assurance Maturity Model) Implementation
- Delivered cutting edge security training for product developers and managers
- Ensuring security is always the first agenda in product development
- Evaluated Temenos existing software security practices and built a balanced software security program in well-defined iterations
- Effective Application Penetration Testing model
- Designed a security framework combining security best practices from OWASP, SANS and WASC.
- Automated static analysis tools and process in Unified Temenos Platform (DevOps)

Key Projects

- T24 Core Banking
- Digital Front Office Suite
- Payments Applications
- Wealth Management Suite

Lead Information Security — Nov 2013 – Apr 2015

BNY Mellon (iNautix), Chennai, India

As a lead Information security executive at BNY Mellon and Pershing operations. In this role I played a key contributor to build secure coding program / practices, perform penetration testing and security design reviews.

Key Responsibilities

- Architecting Software with Secure Software Concepts
- Vulnerability Management
- Performing automated code scans and manual analysis of vulnerabilities on monthly basis
- Conduct penetration testing on Web, Mobile (Android & iPhone) applications
- Perform secure architecture analysis for applications
- Assist and recommend solutions to development teams for remediating complex security issues
- Training development teams on secure design & secure coding practices
- Conducting Security Forums to discuss the issues and concerns on application security with development teams
- Provide metrics scorecard which ensures timely delivery, track and monitor issues to closure

Key Achievements

- Implemented global application security code review process and procedure
- Built secure coding maturity model and implemented across organization

Key Projects

- Secure coding Program
- Pershing Application
- BNY Mellon's Application Suite

Technologies / Tools Know How

Following are the tools and technology that I have used in my tenure working with multiple organization

Programming & Scripting	Vulnerability scan and management	IAST & RASP	Manual Application testing	Static analysis	DevOps and Cloud	Container Security tools
C C++Java .NET Python JS NodeJS GO	Twistlock IBM Appscan Webinspect Acunetix Nexpose Nessus IP360 Tripwire CCM OpenVas IBM Guardium Metasploit	Contrast Security Microfocus Fortify RASP Webinspect	Brupsuite Pro Fiddler	Fortify SCA Armorize IBM Appscan Source Edition	Openshift Kubernetes Docker 3Scale Keycloak KONG Hashicorp Amazon Webservices Azure	Anchore Cloud AquaSec Cilium Docker Bench Sysdig Falco Notary Sysdig Secure

References

References are available upon request.