SIDDHANT TUPE

Senior Staff Engineer - CISSP, CEH, ISO 27001

+91-9167374427 siddhanttupe712@gmail.com linkedin.com/in/siddhant-tupe
https://defensivelayer.net/ Bangalore, Karnataka, India

SUMMARY

Cybersecurity Leader with 15+ years of expertise in security architecture, network defense, and threat detection across on-premises and multi-cloud environments. Proven track record in engineering advanced solutions such as CrowdStrike Next-Gen SIEM with Cribl, Zscaler Threat Deception, Wiz Secrets & Non-human identity management to strengthen enterprise security posture. Recognized for driving cost-efficient, resilient designs while aligning cybersecurity programs with business goals and compliance needs.

EXPERIENCE

Sr. Staff Engineer - Infosec Engineering

Albertsons Companies India (Retail)

10/2025 - Present Bangalore, India

Roles & Responsibilities

- Reporting to Director of Security Engineering responsible for driving various security engineering & strategic initiatives
- Leading end-to-end Zscaler ZPA/ZIA Zero Trust rollout for 100,000 users replacing legacy VPN as part of ZTNA strategy
- Designing & Deploying Threat Deception technology across Endpoints, Networks, Clouds, Active Directory & Perimeter assets
- Deploying Wiz Secrets management & Non-human identity detection & remediation efforts across multi-cloud estate
- Driving infrastructure architecture optimization project for performance improvement & cost savings
- Mentored security engineers; contributed to hiring, career planning, and team capability building

Senior Cyber Architect - Global Cyber Defense

Maersk (Logistics)

03/2019 - 10/2025 Pune, India

Roles & Responsibilities

- Report to the Director of Cyber Operations with ownership of cross-functional security architecture and consultation responsibilities across on-prem and cloud-hosted infrastructure. Partner with Strategy and Service Owners to evaluate critical risks and implement timely remediation plans.
- Improved security posture by designing & deploying NG SIEM, IDS/IPS, Zero Trust Network Access (ZTNA), Firewall policy analyzer, Prisma Cloud/Microsoft Defender CSPM, Anti-Malware CDR, Threat Deception solutions across global infrastructure.
- Regularly reviewing CSPM & CWPP reports to address Compliance, misconfiguration & policy violations against NIST 800-53, CSF & CIS benchmarks for Azure, AWS & GCP Cloud.
- Supported design & implementation of Azure & AWS Networking related projects which included deployment of Hub & Spoke Architectures, Vnet/VPC peering, Azure Firewalls, load balancer & IPSec VPN deployment.
- Responsible to produce solution document with design diagrams, SOP, Best Practices during design & implementation phase for smoother transition to operations teams.
- Work with risk management team, Product Owners & Cybersecurity strategy team to analyze/evaluate Cybersecurity risks, identify gaps in security controls, prioritize risks & suggest security controls to close gaps to improve security posture.
- Led a team of 12+ network security professionals, overseeing end-to-end Network Security Operations across Next-Generation Firewalls and Zscaler Internet Access (ZIA) Proxy platforms.

CERTIFICATIONS

Cybersecurity for Leaders with AI
Indian School of Business - ISB

Certified Information Systems Security Professional (CISSP)
ISC2

ISO 27001 - Lead Auditor
DNV

Introduction to Generative AI
Coursera

GCP & Oracle Cloud Infra foundation
Coursera

AZ-104 : Azure Administrator Associate
Microsoft

Akamai Zero Trust & Web Perf. Foundation
Akamai

Zscaler Certified Cloud Administrator (ZTNA)
ZScaler

ITIL® Foundation v4
Peoplecert

CEH - Certified Ethical Hacker
EC-Council

CCSA - Check Point Certified Security Admin.
Checkpoint

KEY ACHIEVEMENTS

Top Performer Award
Outstanding performance & contribution towards Cybersecurity practice across Maersk

Critical Incident Response & Business Continuity
Recognized for exceptional contributions during the Russia-Ukraine war and COVID-19 crisis by implementing a kill switch and expanding remote work capabilities with zero disruption.

EXPERIENCE

Tech Lead – Security Management

T-Systems ICT India (MSSP)

07/2018 - 02/2019 Pune, India

Roles & Responsibilities

- Reported to the Head of IT, with end-to-end responsibility for the design, deployment, and daily operations of Next-Generation Firewall (NGFW) solutions integrated with Advanced Threat Protection capabilities. This included the implementation of Intrusion Prevention Systems (IPS), Web Proxy, HTTPS Inspection, and Application Control, ensuring robust perimeter security and policy enforcement across the enterprise network.
- Participated & supported vendor RFI/RFP evaluations, Developed SOPs, LLD's, and HLD's, ensuring alignment with security best practices, improving documentation efficiency by 70% and accelerating project deployment timelines.

Technical Lead – Network Security

Wipro Technologies (MSSP)

08/2011 - 07/2018 Bangalore, Mumbai & Pune

Roles & Responsibilities

- Reported to the Delivery Head for Europe and the US region, responsible for leading a 15-member team and overseeing the successful delivery of multiple customer engagement focused on Network Security Operations.
- Accountable for end-to-end project execution, resource planning, and service delivery across diverse client environments, ensuring alignment with regional business objectives, SLAs, and security compliance standards.
- Configured firewalls, proxies, IDS/IPS. Identified vulnerabilities. Optimized settings. Ensured monitoring.
- Utilized AlgoSec Policy Analyzer to review and optimize over 10,000 firewall rules across multivendor environments, including Cisco, Check Point, and Fortinet. Identified and eliminated unused, redundant, and non-compliant rules, significantly improving firewall efficiency, security posture, and audit readiness.
- Configured and managed SSL and IPsec VPN connectivity for 1,800+ branch locations, ensuring secure, reliable access to enterprise resources. Implemented network monitoring solutions to proactively track uptime, performance, and capacity, enabling high availability and optimized network health across distributed environments.
- Executed device upgrades, patch management, and hardware replacements following an N-1 strategy to ensure stability, vendor support, and minimal risk exposure. Maintained system integrity and compliance by applying tested versions and proactively managing lifecycle operations across critical security infrastructure.
- Handled incident and change management tickets, performing end-to-end troubleshooting across network devices using tools like Wireshark for packet-level analysis. Provided cross-functional support for troubleshooting issues at both the server and application levels, ensuring timely resolution and minimal business disruption.

EDUCATION

M.Tech. Systems Engineering (WILP)

BITS Pilani

01/2012 - 12/2015 Mumbai, India

B.Sc. I.T.

Dr.B.A.M.University

07/2008 - 03/2011 Aurangabad, India

SKILLS

Cybersecurity · Network Security · Cloud Security · Risk Management · CISSP · Solution Design · Zero Trust · Wiz CSPM · Defense in Depth · Secrets & Non-Human Identity · Threat Deception · Cloud Security · CWPP · CSPM · Defender for Cloud · Microsoft Sentinel · Microsoft Azure · GCP Cloud · AWS Cloud · ITIL · Web Proxy · Vulnerability Scanning · Qualys · Wireshark · NIST Standards · CIS Benchmarks · Python · Policy Compliance · Prisma Cloud · EDR

CLIENTS

BFSI Domain - HDFC Bank

Onsite - Mumbai

BFSI Domain - Central Bank of India

Onsite - Mumbai

BFSI - Munich RE

Onsite - US

Energy & Utilities - RWE NPower

Onsite - UK & Germany