

Jaiprasad Mallepat

CISSP

CCSP

CISM

I set the security architecture of one of the world's largest energy companies — and lead its response to frontier AI.

GET IN TOUCH

01

AI & SECURITY

I lead BP's enterprise response to frontier-AI threats — setting the security architecture for one of the world's largest energy companies and authoring the enterprise standard and guardrails for the safe adoption of agentic AI. I drove AI-assisted cyber defense to a 70% reduction in SOC mean-time-to-respond, sit on the Microsoft Copilot for Security Customer Advisory Board, and spoke at Microsoft Ignite. After hours I build autonomous AI systems — a living lab for the guardrails I write by day.

THREAT RESPONSE

Leading enterprise response to frontier-AI threats across BP's global Digital Security portfolio.

GUARDRAILS & STANDARDS

Authoring the enterprise standard and controls framework for safe adoption of agentic AI.

AI FOR DEFENSE

70% SOC MTTR reduction via AI-assisted cyber defense; Microsoft Copilot for Security CAB; Ignite speaker.

BUILDER

After hours I build autonomous AI systems — a self-improving trading platform and a family AI assistant — a living lab for the guardrails I write by day.

[Projects →](#)

02

SKILLS

AI & FRONTIER-MODEL SECURITY

Agentic AI Guardrails & Standards

Frontier-AI Threat Response

Non-Human Identity Controls

AI Governance & Vendor Assurance

AI for Cyber Defense

ENTERPRISE SECURITY ARCHITECTURE

Reference Architectures

Design Assurance

Technology Evaluation

Architecture Review Boards

Leading Architect Teams

CYBER DEFENSE & ENGINEERING

Unified Detection & SOAR

SIEM / UEBA (Sentinel)

SOC & CERT Design

Vulnerability & Exposure Management

Post-Quantum Cryptographic Resilience

CLOUD & DATA

AWS & Azure Architecture

Hybrid Connectivity & ExpressRoute

Data Residency & Transfer Controls

Zero Data Retention

REGULATORY & COMPLIANCE

GDPR

EU AI Act

DORA

NIS2

ISO 27001

SOC 2

PCI-DSS

Cyber Essentials Plus

CERTIFICATIONS & EDUCATION

CISSP

CCSP

CISM

Azure Security Engineer Associate

MSc Security Technologies (First Class), University of Surrey

BTech Computer Engineering (First Class), SRM University

Chief Architect, Digital Security

Jun 2022 – Present

BP / London, UK

Chief enterprise security architect leading BP's security strategy and architecture direction — architecture authority across the full Digital Security portfolio, reporting to the Deputy CISO and working with the SVP and CISO. Lead BP's enterprise response to frontier-AI threats and author the standard and guardrails for safe adoption of agentic AI. Drove £5M+/yr OPEX savings through portfolio simplification; led Microsoft Sentinel adoption (90+ log sources, 5TB+/day migrated in 6 months); achieved 70% reduction in SOC mean-time-to-respond through AI-assisted cyber defense. Selected for the Microsoft Copilot for Security Customer Advisory Board; invited speaker at Microsoft Ignite.

Enterprise Architecture Frontier-AI Security Agentic AI Guardrails Post-Quantum SIEM Team Leadership

Principal, BP Cyber Defence Team

Apr 2021 – May 2022

Infosys Consulting / London, UK

Led architecture and delivery of an automated cloud forensics capability for the BP CERT team — an event-driven platform on AWS and Azure native services collecting evidence across 1,200+ cloud accounts in 18 regions, cutting evidence collection from days or weeks to minutes or hours.

Cloud Forensics AWS Azure Incident Response

Senior Manager, Cyber Security & Infrastructure

Oct 2017 – Apr 2021

Skanska UK / UK

IT Senior Management Team member owning security and infrastructure for a 6,000-seat UK estate within a 52,000-employee global group. Owned the information-security strategy, budget and team; delivered ISO 27001 and Cyber Essentials Plus certification, EDR with managed SOC, a multi-million-pound network refresh and SD-WAN, and a risk-based three-year cyber security strategy.

Security Strategy ISO 27001 SOC Infrastructure Leadership

Virtualization & Cloud Platforms Manager

Sep 2016 – Sep 2017

Johnson Matthey / UK

Owned global strategy and delivery for virtualization and public cloud — 1,700 virtual servers across VMware, Hyper-V, Azure and AWS. Built the public-cloud strategy, led Azure network security and ExpressRoute, and consolidated 40+ datacentres and server rooms into three datacentres and two Azure regions.

Cloud Strategy Azure AWS Datacentre Consolidation

Solution Architect

Apr 2015 – Aug 2016

Johnson Matthey / UK

Solution design and security assurance for corporate programmes including the SAP Global Template and BI/BW. Lead architect for the global Business Analytics and ETL capability.

Solution Design Security Assurance SAP Analytics

Infrastructure Engineer

2008 – 2015

Johnson Matthey • 360 GSP • Independent / UK

Foundation years: private cloud, virtual infrastructure, networks and production-critical manufacturing systems across Europe and North America; systems, networking and security consultancy for SMEs.

Infrastructure Networking Consulting

AlphaForge

LIVE

AUTONOMOUS AI TRADING ORGANIZATION

A self-improving algorithmic trading organization run by AI agents across US equities and crypto — strategy research, statistically-hardened validation (CPCV, deflated Sharpe), risk-laddered execution, and honest benchmark reporting, operating 24/7 under human governance gates. Built as a living lab for the agentic-AI security patterns I write standards about by day.

- Python
- Claude
- Agent Orchestration
- Alpaca
- Quant Validation

Cosmo

LIVE

PERSONAL AI ASSISTANT ON WHATSAPP

A family AI assistant living entirely in WhatsApp: persistent layered memory, proactive heartbeat monitoring, local Whisper voice transcription, vision (receipts, school letters), AI email triage, and a child-safe homework tutor mode — self-hosted, with every action auditable.

- Claude
- Whisper
- Redis
- WhatsApp
- Self-Hosted

More coming

WIP

WORK IN PROGRESS

Additional projects being documented. Check back soon.

Open to interesting problems, collaborations, and conversations. The best way to reach me is by email.

 jaiprasadmallepat@gmail.com

 [LinkedIn](#)

 [DOWNLOAD CV](#)