PARITOSH KUMAR TRIPATHI

Contact Details

E-Mail: imparitoshkt@gmail.com

Mobile: +91-8884229919

Mobile: +971-586540073

Core Competencies

- Cybersecurity transformation
- Cybersecurity Strategy
- Cybersecurity Risk Management
- Cyber Security Architecture
- Business Continuity Planning
- Audit & Compliance

Certifications

- CISSP by ISC2
- IEC 62443
- Digital Transformation INSEAD
- Google AI Essentials
- Google Cloud

Education

- BPGP IIM Ahmedabad (Class'26)
- Diploma in Embedded System Design – 2005
- B.Tech (ECE) UPTU – 2004

Affiliations

- ISA 99 Senior Member
- Past:
  Department of Homeland Security International Joint Working Group on ICS Security
- Past:
  IEC 62443 Working Group 3

Profile Summary

A versatile & outcome-oriented leader with 18+ years of cybersecurity experience across cybersecurity product development, research, and consulting. My focus & expertise are in defining & driving cybersecurity transformations from cyber strategy, policy design, and operating models to implementation and sustenance at designing and implementing robust security frameworks to safeguard company assets and data while ensuring compliance with regulatory standards.

Strong background in building high-performance teams, managing incident response, and executing strategic initiatives to enhance security posture. Proven ability to collaborate with senior leadership to align security objectives with business goals, ensuring long-term organizational resilience. Expertise in risk assessments, security architecture, GRC, vulnerability, and crisis management, focusing on proactive security measures and continuous improvement.

- Ideated and led the OT Cybersecurity Experience Centre at PwC Dubai, providing kind amalgamations of cyber-physical in the form of digital twins, 3D models, and security stack integrated with ML models for first-hand fully immersive attack defense emulation for both internal and external users.
- Forging alliance partnerships with Nozomi, Dragos, MS DIoT, Fortinet, ArcSight and Splunk.
- Led the talent pool ramp-up specifically for OT security.
- Liaised with the internal organization channel and the vendor partners to add five external hires.
- Instrumental in driving several internal initiatives on OT security, such as delivering lectures at Khalifa University, hiring process, and conducting training for fresh hires on OT security.
- Published international papers on security with o v e r 5 0 citations. My research work has been cited by research scholars from Princeton, Texas A&M, and Virginia Tech, among others.
- Represented PwC at corporate sports events by participating in cricket and badminton tournaments.

Work Experience

Since Jan'25: Seclance Middle East Consulting LLC, Dubai as Partner

- Developing service offerings and strategic alliance in the Middle East market driving revenues and growth while maintaining the bottom line.
- Advising CISOs and CXO group on cybersecurity initiatives and strategies particularly relating to AI, digitalized supply chains and Cloud.

Oct'22-Feb'24 PricewaterhouseCoopers, Dubai as Senior Manager

Led and delivered the complete OT security service offerings of PWC ME in the ME market, particularly ones focusing on OT cybersecurity strategy, OT security managed security services under the build-operate-transfer (BOT) model and managed GRC.

- OT SOC strategy: Developing OT SOC strategy covering SOC Managed Security Services setup, Operating model, Log Source identification and integration, service catalog, and onboarding plan.
- OT SOC Architecture: Studied the client environment and developed an architecture taking into consideration the local regulation for each geography, integration at plant, regional, national, and cross-geography levels, including requirements for data retention, data diode message transfer, Nozomi Guardian integration, EPS count, connectivity and use cases.
- OT SOC Use case development: developed specific use cases related to Windows event logs and Nozomi data feeds for an OT environment. The logs were then configured in Splunk and ArcSight and fired successfully.
- Enterprise Security Architecture: Led an engagement on enterprise security architecture for an Oil major wherein I helped in assessing the current as-is, defining the business drivers and attributes, identifying gaps in the current ESA, and putting together a roadmap for achieving a target state.

Nov'18-Sep'22 PricewaterhouseCoopers, Dubai as Manager

Led multiple engagements focusing on cybersecurity, including OT, particularly relating to assessments, architecture design, target operating model, and audits for several regional clients across industry verticals.

- Conducted assessments (architecture, systems, network, and backup recovery) on multiple OT systems from different vendors as part of an assessment exercise conducted for 40 ports globally. I was first required to deal with different Executives (e.g., COOs, CIOs, and Security Directors) at each site to get approval to perform the assessments and then coordinate the execution teams to work effectively during the Pandemic. I also added significant technical expertise to the findings reports and future state architecture designs - on a site-by-site basis
- Defined target architecture for several sites to ensure use cases around IT-OT integration, remote access, and wireless technologies are securely used.
- Developed assessment frameworks based on IEC 62443, NCA OTCC, and other international security standards.
- Led complex cyber projects at a petrochem for global cyber GRC assessment, a global analysis and design of a first-in-region IT/OT "cyber hub" concept for SOC operations and Incident Response,
- Conducted security audits based on national regulations and international security best practices for an ME regional oil company for its offshore plants. Present audit reports to technical teams and executive management.

Aug'17-Jul'18 Al-Hosn Cybersecurity Consulting, Abu Dhabi as Senior OT Security Specialist

Delivered projects relating to cybersecurity FAT and SAT from design to implementation.

- Developed FAT and SAT cybersecurity guidelines for the client and validated these with OEM before implementations
- Supported third party for penetration testing of equipment and security solutions per the guidelines
- Drive the project based on the project plan to completion

Jan'15-Jul'17 PwC, Bengaluru as Manager

Led and delivered multiple risk assessments and architecture design projects for many clients for their IT and OT landscape.

- European O&G major, where I managed the risk management lifecycle for their upstream business for close to 2 years under secondment.
- Oil major in India, security assessment for their well-heads and crude oil processing terminal
- Refinery in India, conducted security assessment, secure architecture design, and implementation in coordination with their DCS vendor for midstream business.
- IT/OT assessment and recommendations for a European agro-chem major headquartered in Switzerland with plants across the globe.
- Assessment of crown jewels of an FMGC major across their IT and OT landscape

Jun'06-Jan'15 CDAC, Mumbai as Technical Officer

Led multiple cybersecurity research and development initiatives, particularly related to intrusion detection systems for OT environments. This entailed developing proposals for the government of India and the Ministry of Electronics and Information Technology, forging relations with other national and international research centers, and providing solutions to key ministries and entities of the government.

- Design and Development of an Intrusion Detection System for an electric utility wherein we modelled a 9-bus electric network mimicking one of their distribution substations using the PSAT tool and wrapping it up with an IEC 104 protocol stack embedded in a PC-built RTU. A master-slave topology was followed during the normal course of operations. We then injected false data using multiple attack scenarios that induce an actual OT attack by manipulating process value, triggering an abnormal process state, thus resulting in either power failures, blackouts, or cascading impacts on automatic generation control. The detection engine was modelled over time and would then correlate process parameters/variables to ascertain if it was an attack.
- Design and Development of Protocol Anomaly Detection Engine focusing on the DNP3 protocol stack. The idea was to investigate PDU and see what function objects and values could create an unstable state for the master or slave. The anomaly engine is a stateful detection engine that ensures that the context of the communication and sessions are mapped well to attack conditions. The detection engine followed a tree data structure, and the packets were parsed using signatures for flagging attack conditions.
- Rule engine development for a network intrusion detection system. This entails algorithm design to match packet tuples as they arrive on the ethernet interface. Ported the code on multiple embedded system platforms to improve speed and accuracy and manage throughput better.