

ROHIT CHAURASIA

ISB | CISSP | CCSP

CONTACT

(+91) 9833279578

ROHIT.CHAURASIA@OUTLOOK.COM

NEW MUMBAI, INDIA

PROFILE

I've transitioned across varied roles in the Information Security domain, beginning my career at the Audits & Assurance end of the spectrum: gradually transitioning into managing the enterprise wide implementation of a SIEM product and building the security capabilities of a startup to make them PCI DSS Certified

My current role the Head of Cybersecurity & IT Infrastructure has me working on defining and building the technological roadmap for the cybersecurity practice, when I'm not at work I volunteer time at the BCI India Next Practice Think Tank which happens to the world's fourth and India's first Think Tank dedicated to Resilience and Business Continuity.

I have received appreciation from the Government of India and Government of Thailand for my help in identifying security vulnerabilities in their cyber infrastructure at multiple occasions and have also been featured in the Continuity & Resilience Magazine as a "Next Generation Practitioner"

As a result of the diverse experience I have in both my professional and voluntary undertakings it has provided the ability to manage multidisciplinary projects and granted me the unique ability to speak both tech and exec

CERTIFICATIONS

Certified Information Systems Security Professional [CISSP]

License: 781238

Certified Cloud Security Professional [CCSP]

License: 781238

eLearn Security Junior Penetration Tester (eJPT)

License: 7344019

Offensive Security Certified Wireless Professional [OSWP]

License: OS-64406

EXPERIENCE

HEAD OF CYBERSECURITY & IT INFRASTRUCTURE

MUTHOOT FINCORP ONE | JUNE 2023 - PRESENT

- Define the strategic vision, tactical execution and technical roadmap to ensure the security of data at MFL ONE
- Lead team of multidisciplinary security experts
- Conduct architectural review for new technology and tools before they are implemented.
- Maintain organizational compliance with international security standards such as ISO 27001

SENIOR SECURITY ENGINEER

FLEXMONEY TECHNOLOGIES | APR 2022 - MAY 2023

- Define the strategic vision, tactical execution and technical roadmap to ensure the security of data at Flexmoney
- Conduct architectural review for new technology and tools before they are implemented.
- Maintain organizational compliance with international security standards such as PCI-DSS, PA-SSF, ISO 27001, CMMC.
- Address client security audits.
- Investigation of Security Incidents and Offenses
- Draft policies and procedures associated with cybersecurity
- Design and conduct Security Awareness Campaigns.

Key Achievements:

- a) Led project for maintenance of organizations security controls in alignment with PCI DSS and RBI Data Localization Requirements

TERRITORY SECURITY ENGINEER- INDIA

CHECKPOINT SOFTWARE TECHNOLOGIES | MAR 2021 - APR 2022

- Imparted technical knowledge and expertise of Check Point suite of cyber security solutions to internal teams, channel partners and customers across the Indian Territory
- Led value-driven conversations with potential and existing customers with ability identify business problems and provide winning solutions
- Assessed customers' cyber security environment, challenges and needs through technical qualifications and propose appropriate solutions
- Conducted virtual demos and meetings to review architecture of clients and recommend solutions.
- Addressed technical queries, offering insight into best practices and managing Proof-of-Concept deployments for CheckPoint clients
- Addressed RFPs & RFIs for various government and private entities.
- Engaged and educated key partners and customers on the latest security technologies
- Worked closely with the business team to engage net new clients in the assigned territory space
- Delivered high impact customer engagements through technical solution design, wrote winning proposals and exceeded expected revenue goals.
- Showcased technical superiority of CheckPoint Solutions at Industry Events.

SECURITY ENGINEER

FLEXMONEY TECHNOLOGIES | OCT 2020 - FEB 2021

- Monitor their organization's networks for security breaches and investigate a violation when one occurs utilizing the various security platforms available.
- Investigation of Security Incidents and Offenses
- Endpoint Monitoring utilizing AWS GuardDuty
- Draft policies and procedures associated cybersecurity
- Define the strategic vision, tactical execution and technical roadmap to ensure the security of data at Flexmoney
- Conduct architectural review for new technology and tools before they're implemented.

Key Achievements:

- a) Led project for organization's PCI Compliance and implemented PCI-DSS Controls across organization. Enabling the organization to acquire PCI-DSS Certification within 4 months.
- b) Implemented an automated software supply chain vulnerability assessment methodology.
- c) Built the Threat Intelligence capabilities for the organization

CERTIFICATIONS

MITRE ATT&CK Intermediate Purple Team

License: Available on Acclaim Portal

Operationalizing MITRE ATT&CK

License: Available on Acclaim Portal

Certified Ethical Hacker version 9 [CEH v9]

License: ECC88697646862

EDUCATION

EXECUTIVE EDUCATION- ELP

INDIAN SCHOOL OF BUSINESS (ISB) | 2022 - 2023

BACHELOR OF SCIENCE, INFORMATION TECHNOLOGY

UNIVERSITY OF MUMBAI | 2014 - 2016

PUBLICATIONS

SPRINGER LINK PUBLICATIONS

GLOBAL PANDEMIC & HUMAN SECURITY

RISK & INSURANCE MANAGEMENT SOCIETY IRIMS, USI

CRYPTOCURRENCY: THE DIGITAL CATALYST TO CLIMATE RISK
HEALTH RECORD DIGITALIZATION - IS INDIA READY?

EDWARD ELGAR PUBLICATIONS

SUPPLY CHAIN MANAGEMENT, DISASTER, AND CLIMATE CHANGE

INDUSTRY RECOGNITION

GOVERNMENT OF THAILAND

APPRECIATION RECEIVED FOR REPORTING CRITICAL SECURITY VULNERABILITY ASSOCIATED TO CYBER INFRASTRUCTURE OF GOVERNMENT OF THAILAND
JUN 2020

GOVERNMENT OF INDIA

APPRECIATION RECEIVED FOR REPORTING SECURITY VULNERABILITY IN CYBER INFRA OF A KEY CENTRAL REVENUE DEPARTMENT
FEB 2022

APPRECIATION RECEIVED FOR REPORTING SECURITY VULNERABILITY IN CYBER INFRA OF MAHARASHTRA STATE GOVERNMENT
OCT 2020

APPRECIATION RECEIVED FOR REPORTING SECURITY VULNERABILITY IN CYBER INFRA OF KERALA STATE GOVERNMENT
OCT 2020

APPRECIATION RECEIVED FOR REPORTING SECURITY VULNERABILITY ON WEBSITE OF A KEY CIVIL MINISTRY
JAN 2020

APPRECIATION RECEIVED FOR REPORTING SECURITY VULNERABILITY ON WEBSITE OF A KEY REVENUE DEPARTMENT
JAN 2020

BUSINESS CONTINUITY INSTITUTE

APPRECIATION RECEIVED FOR CONTRIBUTION AT THE BCI INDIA NEXT PRACTICE THINK TANK DURING THE YEAR 2018-2019
NOV 2019

APPRECIATION RECEIVED FOR CONTRIBUTION AT THE BCI INDIA NEXT PRACTICE THINK TANK DURING THE YEAR 2017-2018
MAR 2018

CONTINUITY & RESILIENCE MAGAZINE

INTERVIEWED BY THE INTERNATIONAL MAGAZINE "CONTINUITY & RESILIENCE" FOR THEIR ARTICLE ON "NEXT GENERATION PRACTITIONERS"
MAR 2019

IT SECURITY ANALYST

TMF GROUP | JUL 2019 - JUL 2020

- Monitor their organization's networks for security breaches and investigate a violation when one occurs utilizing the various security platforms available.
- Investigation of Security Incidents and Offenses
- Endpoint Monitoring utilizing CrowdStrike Falcon
- Team liaison for Enterprise Cloud Governance Project

Conduct architectural review for new technology and tools before they're implemented.

Key Achievements:

a) Created a conversational chatbot for the Information Security team which would ensure that end user outreach is seamless and general queries are managed by the bot saving time and effort of team members.

b) Automated manual tasks and helped create key documents for the organization:

- Automated generation of a key monthly report, resulting in reducing turnaround time of the report generation to fraction of the earlier turnaround.
- Defined and documented the Incident Management Process along with key stakeholders
- Created a Service Catalogue for the team
- Created documentation to standardize BAU processes such as:
 - Addition of servers to SIEM
 - Integration of Threat Feeds to SIEM
 - Reference Set Modification on SIEM

OFFICER: CYBER SECURITY IMPROVEMENTS

WILLIS TOWERS WATSON | DEC 2018 - JUL 2019

- Delivering strategic cybersecurity projects within the organization to strengthen the organization's cyber security posture.
- Assist in the definition of project scope, objectives and ensuring technical feasibility.
- Create delivery roadmap with quantifiable milestones.
- Track project performance, specifically to analyze the successful completion of short and long-term goals.
- Manage relationship with stakeholders and establish transparent communication channels.

Key Project:

a) SIEM Integration

- Work in tandem with project manager and MSS provider to engage various interdisciplinary teams and multiple stakeholders in order to ensure full coverage and visibility of the IT estate on the SIEM solution of the organization in order to maintain compliance with various regulatory requirements.
- Participate in global Change Advisory Board meetings as required to represent change in production web servers.

Project Achievements:

- a) Completed integration of ~2500 perimeter web servers (production environment) to the SIEM platform across a span of 60 days.
- b) Planned, documented and implemented an IT estate wide process in order to identify any log collection agent failure and automated restart eliminating manual rework completely and establishing metrics around the failure rate of the agents.

OFFICER: INFORMATION SECURITY

WILLIS TOWERS WATSON | OCT 2017 - NOV 2019

- Advising the Service Manager on emerging threats and the firm's cyber security capabilities in context to the threat.
- Point of contact to complete highly unique, voluminous and detailed Security Questionnaires utilizing expertise in IT Security, Risk Management, related frameworks and by building and maintaining an in-depth knowledge and understanding each business unit's IT environment and security controls.
- Proactively built relationships with both requesting parties and those with domain specific expertise to ensure successful representation of the IT Security Program to external parties.
- Managed a large volume of high-detailed projects while ensuring quality, timely delivery and open communication with the requesting party to ensure they are kept abreast of progress and any potential risks to successful completion.
- Interact with Auditors during security audits and work with multiple teams globally to collate required evidence.
- Managing the Information Security Mailbox that serves as the single point of contact globally for colleagues to resolve Information Security queries
- Plan and deliver improvements to the maturity of the process

JUNIOR OFFICER: INFORMATION SECURITY

WILLIS TOWERS WATSON | OCT 2016 - OCT 2017

- Security Incident Management for phishing incidents
- Respond to and, where appropriate, resolve or escalate reported Security Incidents using the Service Now platform.
- Updating and maintaining Data Incident Register
- Collate security incident and event data to produce monthly exception and management reports.
- Review & Assess Risk associated to Security Exceptions for Legacy Applications, Access to USB, Access to Cloud Storage Systems, Third Party Libraries.
- Point of contact to complete highly unique, voluminous and detailed Security Questionnaires utilizing expertise in IT Security, Risk Management, related frameworks and by building and maintaining an in-depth knowledge and understanding each business unit's IT environment and security controls.