

NAVEEN KRISHALI

B-Sc. in Electronics

CISSP, OSCP, ISO 27001 LA, ITIL

EMAIL- CLOCKWISE.07@GMAIL.COM

Phone - 9494519827, 6281784956

DOB- 18 Jul 1982



IT & InfoSec Manager, Information Security Governance and Compliance, Lead Auditor for Eastern Naval Region, Member of Eastern Naval Region Incident Response Team, Embedded systems specialist in Radar Technology

Eastern Naval Command
Indian Navy

Core Competance: VA/PT, Risk assessment, Risk mitigation, Security audits, securing UD assets and network infrastructure

PROFILE

A highly motivated certified Offensive security professional with strong leadership traits having 20 years of experience in Indian navy. I am having 10+ years of experience in IT Security, governance and compliance, Security operations, Risk assessment, firewalls management & auditing, DR & BCP, Design and implementation of security architecture in strict disciplined environment expecting zero fault tolerance, management of SOC. Additionally, I also have conceptual knowledge on Identity and access management, DevOps architecture, Physical security and administration, product evaluation.

- ❖ **Responsible** for overall organisational operations and security.
- ❖ **Audits.** Supervising internal audits and co-ordination of external audits. Preparation of audit summaries and further policies implementation for .
- ❖ **Risk Management.** Vulnerability assessment of IT resources of entire eastern Naval Command with 7000+ device count. Penetration testing of open source applications and in-house developed applications prior production deployment. Skilled in risk analysis, risk mitigation ensuring compliance to standards. Acquiring, processing, analyzing and reporting of security incidents.
- ❖ **Security Policies.** Responsible for domain based policies for securing assets in Eastern Naval region.
- ❖ **SOC manager.** SOC implementation and UAT in Eastern and Southern Naval regions.
- ❖ **Asset Security.** Automation of asset discovery and compliance by creating multiple scripts for Naval Headquarters (python & batch scripts).
- ❖ **Policies & Plans.** Implementation of policies, procedures, guidelines and organisational tactical plans. Providing recommendations to higher management regarding administrative policies creation and implementation.
- ❖ **Training.** Carrying out training on Information security procedures and guidelines as well as technical lectures to all stakeholders in IT operations.
- ❖ **BCP & DR.** Setting up of Business Continuity Plan, Disaster Recovery & Backup Strategy. Running full-interruption tests to check effectiveness of DR & BCP.
- ❖ **UAT and rollout** of IDM solution in Eastern Naval Command.

- ❖ **Firewall.** Management of Next generation GAIA appliance firewall in a complex NAT environment covering nearly 70 locations. Audits of individual firewalls held by other units.
- ❖ **Team Management.** Efficient guidance and management of teams of Security administrators, Server administrators and networking professional with key focus on security and compliance to policies.
- ❖ **Resource planning** for efficient virtualization of servers and upgradation. Financial resource planning and distribution of devices to other remote locations for upcoming projects.
- ❖ Overseeing the creation of rules/alerts, reports/dashboards, escalation/management of incidents.
- ❖ **Relationship Management.** Managed service provider relationships. Prepared RFIs, RFPs, reviewed bid proposals, contracts and scope of work, PNC, TNC and other documentation for projects and associated efforts.

PROFESSIONAL EXPERIENCE AND ACHIEVEMENTS

Senior Infosec Engineer (Mar 2020 - till date)

- ❖ **Individual Contributor** role in Flipkart Internet Pvt Ltd. Current profile includes:
 - Carrying out vulnerability assessment of all assets of Flipkart.
 - Security assessment of upcoming projects, providing detailed guidance on security aspects and providing approval.
 - Advising the management about formulation of security policies.
 - Reviewing the perimeter security of the organisation.

Information Security (Apr 2009 – Feb 2020)

- ❖ **Served in Southern Naval Command Headquarters** of Indian Navy for 4 years. Professional experience:
 - Team leader Information Security
 - Firewall administrator
 - Supervision of VA-PT of Southern region.
 - Planning and implementation of SIEM and SOC, incidents handling as SOC manager.
 - Carried out internal audits, supervision and co-ordination of external audits.
 - Dissemination of system and administrative policies for placing required controls in areas of concern.
 - Implemented online examination solution.
 - Liquidation of security vulnerabilities during implementation of Secure Wireless facility. This setup included two factor authentication of devices connecting to internet.
 - Carrying out security testing of applications before being placed into production.
 - Advising management and stakeholders regarding securing networks.
 - Member of Technical Steering Committee. Providing technical suggestions to management regarding purchase of hardware and software solutions.
 - Awarded commendation award from *Flag Officer Commanding Southern Naval Command* for contribution in Information security and IT field.
- ❖ **Served in Eastern Naval Command Headquarters** of Indian Navy for 6 years. Professional experience:
 - Carried out roles of supervising Information Security teams, IT operations, Firewall admins, Network admins and Server admins.

- Vulnerability assessment of all establishments, preparing summary about vulnerable locations, implementing additional system based and administrative policies to place technical controls in areas of concern.
 - Planning and implementation of High availability architecture, converting HA(high availability) zones from distance-vector to Link-state routing.
 - Replacing packet filter firewall with next generation firewall. Writing one to one and one to many IP address mapping rules from scratch.
 - Segregation of Demilitarized zone rules from trusted zone rules.
 - Auditing of firewall rules of nearly 70 establishments.
 - Planning and setting up alternate patch mechanism and bringing up compliance to excellent levels compared to other counterparts.
 - Setting up of BCP and DR. Identifying critical assets, carrying out impact analysis and developing strategy in case of any man made (e.g. terrorist activity, war, power outage) or natural (e.g. floods, storms) disaster. Keeping hot sites ready by ensuring regular backups and replications. Replications included SAN to SAN RCP replication, Hyper-V replications and extended replicas.
 - Member of CIRT for Eastern Naval Command region.
 - Carrying out interviews and induction of new support engineers.
- ❖ Member of CIRT team of both Command Headquarters of Indian Navy.
 - ❖ Core team head for implementation of SIEM across Southern & Eastern Naval Command regions.
 - ❖ SOC manager at Eastern Naval Command Headquarters.
 - ❖ Prior serving in Command Headquarters, served in Naval establishments as sole in-charge of Information Technology and Information Security for a *period of 2 years*, protecting information and assets of Naval ships and establishments.
 - ❖ Holding a total 13+ years experience in Information Security and Information Technology.
- ❖ **Additional Experience**
 - During initial engagement, served onboard Naval ships as Radar systems specialist. Carrying out defect identification and defect rectification in complex radar systems. (Reason for off boarding from ship- underwent ACT reconstruction surgery)
 - Worked as Missile engineer post serving naval ships.
 - Having total 20 years of experience in Indian Navy. Responsible for maintaining co-ordination between subordinates, departmental welfare, grievance handling, and maintaining discipline in the departmental team.

OVERALL GRANULAR SPECIALIZED EXPERIENCE

- ❖ **HAXA-** Restructuring of unplanned network and UD infrastructure to Highly Available Extensive Architecture. It created 6 highly available zones (called HA locations, comprising ADs and core routers), thus providing redundant network connectivity with link state routing protocols and clients getting authenticated from HA domain controllers, which was earlier spreading in a noisy and less efficient fashion.
- ❖ **SIEM implementation** in Eastern Naval Command and units under her. Co-ordination for asset discovery, planning for distribution, financial planning as per hardware requirements for the units lacking hardware resources. Resolving configuration issues falling during the implementation phase e.g. routing issues, setting up of different network for SIEM and isolation using firewall.

- ❖ Resolving complex networking and UD issues in and out of zonal regions.
- ❖ DMZ relocation to dual homed firewall architecture, rewriting the firewall rules. Replacing stateful firewall with next generation firewall and writing rules from scratch. Further troubleshooting for forming a baseline of firewall alerts. Audit of firewall rules maintained by other locations. Conducting training sessions on Firewall and security.
- ❖ IDAM rollout, implementation throughout Eastern region. Migration to new IDAM architecture from old designation based UD architecture. Training of personal on IDAM.
- ❖ Vulnerability assessment of Kochi & Visakhapatnam Naval units. Units of each location counting over 90 in number with 5000 PCs and 300 networking devices. Periodic vulnerability scans using distributed scanning machines placed in HAXA nodes and getting vulnerabilities patched.
- ❖ In view of SCCM non-compliance for a longer period, created an automated patching mechanism with own crafted batch script which brought security compliance to an excellent level. This included separate patch servers for far located units.
- ❖ Establishing the process of BCP, Disaster recovery with SAN level replications and windows failover clusters.
- ❖ Formulation of policies on security compliances all over Eastern region.
- ❖ Utilising knowledge gained during OSCP certification in security of Naval unified domain spreading upto Chennai and west Bengal units.
- ❖ Python scripts for network monitoring and correlating data upto MAC violation level.
- ❖ Managing teams of server administrators, network administrators, antivirus administrators, Linux administrators and Annual Maintenance Contract for Visakhapatnam region and Eastern Naval Headquarter. Day to day jobs assignments to all teams and monitoring performance. Conducting interviews for induction of new support engineers in all teams.
- ❖ **Embedded Systems-**
 - Achieved a good level of understanding of component functions at signal and voltage level, thus reducing RTO by a significant amount.
 - Carrying out cannibalization of obsolete and unsupported spares and improving the quality & amount of radar spares.
 - Penetration testing for buffer overflows in in-house developed applications.

EDUCATIONAL QUALIFICATION

CISSP

Offensive Security Certified Professional(OSCP)

ISO 27001 LA

ITIL

B.Sc. in electronics from CUSAT (affiliated from Cochin University of Science and Technology)

Diploma in Electronics from INS Valsura, Jamnagar (Indian Navy)

Senior Secondary from Shri Bharat Mandir, Rishikesh

- ❖ **Coding and scripting:**

- C, C++, Python, Assembly language, PHP
- Batch scripting, Bash scripting.

- ❖ Highly efficient in brain storming.

- ❖ Certified OSCP on 03/2017. OSCP ID: OS-19188.

- ❖ ISO-27001 LA

- ❖ Pursuing CISM and CISSP certifications before retirement from Indian Navy.

- ❖ **Contributions:**

- **Educational Python scripting learning channel on youtube**
<https://bit.ly/2N7HPYx>

- **Educational Assembly language learning channel on youtube**
<https://bit.ly/302PH31>

CONTACT

Drona – 5N
INS Circars
Naval Base
Visakhapatnam
+919494519827 , +916281784956

Mail- Clockwise.07@gmail.com

LinkedIn- <https://www.linkedin.com/in/naveen-krishali-b5248168/>

I hereby declare that all the information given above is true.

Naveen Krishali