

Zojde Dev Barman

zojdedevbarman@gmail.com | 8486731009 | Motinagar, New Delhi

EDUCATION

NIT SILCHAR

BTECH IN ELECTRONICS AND INSTRUMENTATION

Jun 2016 | Silchar, Assam
Cum. GPA: 7.53 / 10.0

ROKAKHATA HS

HS IN SCIENCE STEAM
May 2011 | Dhubri, Assam
PCM. CGPA: 8.03 / 10.0

LINKS

Facebook:// zdb

LinkedIn:// zojde dev barman

COURSEWORK

CCNA Course
Comptia Security +
Certified Ethical Hacking
AWS cloud computing
SIEM Expert course
Cyber security fundamental
Linux fundamental

CYBER SECURITY TOOLS

SIEM
SOAR
Threat Intelligence/MISP
Fortinet Firewall
Cisco Firewall
IPS/IDS
SLB/SSLA
IDAM
PAM
PKI
Cisco ISE/NAC
Sandbox

SKILLS

Threat Intelligence
Security Incident Response
Risk Assessment and Management
SIEM Integration and co-relation rule
Network Security
Information Security
Basic Knowledge of IDAM and PAM
Compliance and Regulatory Standards (HIPPA, NIST, PCI)
Leadership and Team Management
Communication and Presentation Skills
Vulnerability Assessment

EXPERIENCE

LARSEN AND TOUBRO LTD, SWC | ENGINEER|DATA CENTER

July 2016 - 2017 | Nagpur, Mumbai, IN

- Installed Cisco Routers, Switches, Blade Servers and Dell Vmax done in Command Control Center.
- Installed security components such as Firewall and IPS in Command Control Center.
- Configured preventive rule and policy for Firewall and IPS in the Command Control Center
- Installed Barco video wall for displaying and monitoring Security system from CCC.

LTTS | SR.CYBER SECURITY ENGINEER |SOC LEAD

Oct 2018 - Present | New Delhi, IN

- Hands on experience in Arc sight SIEM tool and integration with various Network elements and Element management system for Indian Army National Data Center and Regional Data Center.
- Implemented and hands on experience in Arcsight SOAR and playbook creation in SOAR for various incident response.
- Implemented and extensive experience in Arc sight SIEM for logs analysis and correlation rule Creation for Indian Army Data Center Project.
- Implemented and hands on experience in Vulnerability assessment (Nessus Scanner), Syementec Antivirus and MISP/GTI.
- Implemented and hands on experience on Firewall, NIPS/IDS, Load Balacer/Security Socket Layer, Sandbox and Cisco ISE/NAC.
- Responsible for providing a Cyber security solution including design and architecture.
- Hands on experience in implementation and managing SOC for Indian Army National and Regional Data Center.
- Worked on designing of SOC frameworks and implementation of SOC/SIEM solution.
- worked on designing solution and implementation of cyber security frameworks such as Security operation strategy ,Vulnerability management, Threat intelligence and analytics.
- Worked with partner vendor(OEMs) and technical team to ensure the technical knowledge is maintained and the project gets delivered as designed in HLD/LLD.
- Acted as a Cyber security lead within the cyber security practice and drive customer communication and engagements, opportunities, OEM Communications.
- Identified potential Gaps and offer solutions to include internal team needs, product improvement and client security posture.
- Configured and reviewed preventive rule and policy on Antivirus, FireWall, NIPS, Vulnerability assement (Nessus Scanner) and HIPS.
- Having good Knowledge of DLP, EDR, XDR, MDR, UEBA, Multiscanning Engin, Web application Firewall and Data right Management.
- Good knowledge on IDAM framework and PAM.