

BISWAJIT PRADHAN

Kolkata, West Bengal 743502 | +91 836 777 7110 | erbiswajitpradhan@gmail.com

Professional Summary

Persistent senior professional with eleven years of comprehensive experience in Cyber Security, AI-driven solutions, and Vulnerability Management. Skilled in leveraging artificial intelligence and machine learning to enhance vulnerability detection and remediation processes. Provide strong technical direction across multiple projects, driving innovation through AI-powered tools and analytics.

Skills

- Artificial Intelligence
- Large Language Models like OpenAI, Meta Llama and Anthropic
- Vulnerability Management
- Tenable Vulnerability Management
- Vulnerability Prioritization
- Windows and Linux Server OS.
- Qualys Certified
- Inside Sales
- Web Application Scanning using Qualys, Tenable.

Work History

Senior Project Associate

12/2021 to 05/2024

Cognizant Technology Solutions – Kolkata, WB

Qualys Certified Professional (Vulnerability Management)

- Used and deployed artificial intelligence and machine learning for intelligent cybersecurity and Infrastructure reporting.
- Worked on OpenAI, Anthropic, Mistral and Meta Llama like Large language models to analyze threats and fix them using automation.
- Evaluated servers to determine **vulnerabilities** and give **remediation plans**.
- Created Asset Groups, Tags and Asset view reports in Tenable and Qualys for Executive reporting.
- **Managed a team of seven members for vulnerability scanning and prioritization.**
- Worked across departments in Change Management, built various service catalogues on Service Now for SSL, Vulnerability remediation request creation.
- Worked in DigiCert SSL creation, tracking and management.
- Install, Configure and Manage Nessus Agents, Scanners.

- Risk Assessment of Vulnerabilities based on the company's security postures.
- Built technical documentation and standard operating procedure for Vulnerability management teams in the organization.
- Configuration, Management and Troubleshooting of Nessus agents, built scripts around easy deployment, troubleshooting and management for Nessus agents using Bash and Batch.

Project 1: Qualys Certified Professional (Vulnerability Management – Security Engineer)

Client: USA Based Retail Food Corporation.

- Conduct regular vulnerability assessments and penetration testing to identify and prioritize potential security weaknesses.
- Created Asset Groups, Tags and Asset view reports in Tenable and Qualys for Executive reporting.
- **Managed Auth Scan credentials like credential rotation, testing and configuration.**
- **Managed a team of seven members for vulnerability scanning and prioritization.**
- Collaborate with cross-functional teams to evaluate software and system designs, providing security guidance and recommendations.
- Develop and implement effective security protocols, policies, and procedures to mitigate risks and strengthen overall security posture.
- Monitor security logs and alerts to detect and investigate potential security incidents or breaches.
- Stay up to date with the latest security threats, vulnerabilities, and industry best practices, and make appropriate recommendations for improvement.
- Maintain and oversee the installation, configuration, and maintenance of security-related software and tools.
- Conduct security audits and reviews of existing systems to ensure compliance with regulatory requirements and industry standards.
- Provide security awareness training and guidance to employees, promoting a culture of security awareness and responsible behaviour.
- Collaborate with vendors and external partners to ensure the security of integrated systems and third-party software.
- Participate in incident response activities, including investigations, remediation, and post-incident analysis.
- Maintain detailed documentation of vulnerabilities, assessments, and remediation efforts.
- Built SOP and Technical documentation on How To's of Qualys tool.

Project 2: Tenable.io Vulnerability Management Specialist

Client: USA Based Energy and Rubber Manufacturing Corporation.

- Utilize **Tenable.io** to conduct **regular vulnerability assessments and scans** to identify and **prioritize potential security weaknesses**.
- Manage Tenable Agents across estate to ensure seamless vulnerability reporting.
- Manage Tenable dashboards and build new ones based on executive requests.
- Monitor and Automate **Tenable** activity with **Power Automate** and **API**.
- Collaborate with cross-functional teams to evaluate software and system designs, providing vulnerability management guidance and recommendations using Tenable.io features and capabilities.
- Monitor security logs and alerts provided by Tenable to detect and investigate potential security incidents or breaches.
- Develop and implement effective vulnerability management protocols, policies, and procedures leveraging Tenable.io capabilities to mitigate risks and strengthen overall security posture.
- Stay up to date with the latest security threats, vulnerabilities, and industry best practices related to vulnerability management and Remediation.
- Build, Maintain and oversee the configuration and maintenance of Tenable Scanners ensuring optimal performance and accurate scanning results.
- Conduct regular security audits and reviews of existing systems using Tenable to ensure compliance with regulatory requirements and industry standards.
- Provide training and guidance to employees on vulnerability management best practices utilizing Tenable' s features and functionalities.
- Collaborate with vendors and external partners to ensure the security of integrated systems and third-party software, leveraging Tenable' s capabilities for vulnerability management.
- Participate in incident response activities, including utilizing Tenable.io to investigate vulnerabilities exploited during security incidents, remediate them, and perform post-incident analysis.
- Maintain detailed documentation of vulnerabilities, assessments, and remediation efforts using Tenable' s reporting and tracking features.
- **SSL** management like issue, notify, renew, re-issue on **DigiCert portal** and issued to the relevant teams as per request. Maintain the SSL and Digital Certificate Vault.
- Managed **FortiOS** and **Tenable** Integrations using **FortiSOAR**.
- Run Ad-Hoc scans, Remediation Scans, Web application Scans and Regular Scheduled scans on the entire asset inventory and share with the remediation team to stay compliant.

Worldpay From FIS Global – Indore, MP

- **Qualys Certified Professional (Vulnerability Management)**
- Evaluated servers to determine **vulnerabilities** and **remediate** them.
- Created **Server Automation Remediation Plans** in **IBM Bigfix** (Now HCL) for ensuring security/compliance level at the top.
- Ran **Vulnerability Scans on 100000 servers+ in a Finance Company.**
- Created **Remediation Plans for moderate and high critical issues.**
- Managed **Changes for more than 12 domains across the organisation.**
- **Received the best colleague award 2019.**
- Maintained safe working environments for the large customer base we had.
- **Managed a team of 20 + for assigning tasks and performing patching and remediation on a regular basis.**
- **Leveraged Patches with tool: IBM BIGFIX** (Now HCL).
- Worked across departments in Change Management.
- **Administered and Leveraged Sailpoint and Bigfix** for End user Access and Permissions.
- Managed Endpoints and their Security through tools like **Qualys, Bugtrack, SCCM and IBM BIGFIX** (Now HCL)
- **Worked with Agility and in accordance of the ITIL V4 process standards.**

Enterprise Support Technician

08/2018 to 08/2019

Black Knight Financial Services – Bhubaneswar, Odisha

- **Managing IT Infrastructure Setup** and Service Requests for **Internal Employees.**
- Logging and tracking **incidents/requests** from identification through resolution using ticketing tools like **CA Service Desk, Service Catalogue**, etc.
- Assisting customers (US End-users and US clients) with technical issues including computer hardware and software issues such as **VPN, SEP, Crash-plan, Office, Servers, Slow Performance, Application Specific Support and Remote connectivity**, etc.
- **Researching, documenting and escalating issues** to appropriate support teams per internal procedures and coordinating with them towards issue **resolution.**
- Supporting **builds, upgrades and repairs** of computer systems and servers.
- Assisting teammates with troubleshooting such as identifying, analyzing and providing steps towards issue resolution.
- Installing **Enterprise Hardware, Software** and conducting Repairs, modifications and upgrades of internal components and peripherals.

- Remotely configuring, installing, and managing workstations using **Bomgar Remote Console** and administering user profiles through **Active Directory** and **Sail Point**.
- Submitting **Documents** and **reproducing issues in a lab environment for Knowledge Base Documentation**.
- Mobile Endpoint Management with **IBM MAAS 360** for end users on **BYOD and Corporate Phones**.
- Maintaining security standards on the Devices running **MAAS 360**.

Senior Associate Client Technical Support

09/2016 to 08/2018

Dell International Services – Hyderabad, Telangana

- Providing **telephonic, chat and email support** to customers and vendors for end user applications like **MS outlook, Cisco Jabber, RSA, Bit-locker, VPN, Wireless, Antivirus, Slow Performance** etc.
- **Access administration to different applications to customers from Dell Digital Delivery**.
- Logging and tracking **incidents and requests** from identification through resolution by using ticketing tools like **Service Now, Siebel and Delta**.
- **Providing floor support to L1 engineers in resolving issues and maintaining and updating knowledge base articles in knowledge portal such that it would help other engineers in resolving similar type of issues and understand the workflow**.
- Coordinating with other support **teams to restores normal service operation as quickly as possible and minimizing any adverse impacts**.
- Supporting **installation, operation, configuration, customization, and usage** of assigned **products**.
- Applying **diagnostic techniques** to **identify problems, investigate** causes and recommend and **implement solutions** to correct common failures.

Associate Client Tech Support

09/2016 to 06/2017

Dell International Services India Pvt. Ltd, Hyderabad – Hyderabad, Telangana

System Administrator

07/2012 to 06/2015

Federal Informatics Pvt. Ltd, – Bhubaneswar, Odisha

- For the company and its clients.
- Receiving user queries and requests through Phone, chat and email, for clients facing issues with **SAAS Products** and **Active Directory**.
- Responsible for **Project Management, Client Communication** and **Onsite Issue Fixing**.
- Communicating with clients to understand their needs, requirements and guidelines.
- Planning and scheduling step by step procedures to meet client's requirement.
- Detailed **Analysis of Client's Hosting Instances**.

- Patching the Endpoints and the servers with latest software updates (**LINUX & WINDOWS** Based)
Generating Logs and Reports from the instances for the clients.
- **Verification** of the Reports to be sent to client.
- **Training new joiners.**
- **Active Directory of Federal Informatics and IAM management.**
- Providing Innovation ideas to improve business for the organization.
- **Project Management and Co-Ordination.**
- Used tools like **RDP, Terminals, PUTTY** Etc.

Education

B. Tech: Electronics and Communication Engineering 2015
GIT, Bhubaneswar (BPUT) - Bhubaneswar

ITIL V4 Certified 01/2020
Axelos - Indore

Vulnerability Management: Vulnerability Remediation 12/2019
Qualys - USA

Implementation of Qualys scans using Compliance Suite to run scans on large networks.

Implementation of Qualys using Compliance Suite to create option profiles.

Re-mediate vulnerable servers and ensuring compliance is met.

Secure IT Systems like End User level Endpoints, Servers - AD, Azure, AWS, Exchange, and WEB etc.

Accomplishments

- Supported over 8 projects on ad-hoc basis and helped the Vulnerability Management Team at Cognizant.
- Managed over 155 DigiCert SSL for Client at Cognizant over my tenure.
- Maintained over 95% compliance across all estates in Vulnerability compliance.
- Handled Team of 7 members at Cognizant to run the scope of Vulnerability management across multiple accounts.
- Documented and resolved major issues which led to NPS & CX of 90 % for Dell.
- Promoted as Single point of contact to assist L1 engineers in resolving issues, providing floor support, and performing root cause analysis to the incidents for proper documentation and categorization at Dell.

- Conducting Quality Sessions and providing feedback to the L1.
Conducting RDR, RAR, CSAT Scrubs and providing feedback to the L1.
Received highest number of CSAT surveys in a quarter.
- Have received appreciation and promoted as REX from the top-level management for executing projects within the set time frame and demonstrating outstanding performance.
- Skill fully maintained continued cordial relations with international clients mainly in the US, UK and other Countries.

Personal Dossier

Name : Biswajit Pradhan

Father's Name : Biren Kumar Pradhan

Mother's Name : Jyotsnamayee Satpathy

Date of Birth : 19-09-1991

Languages Known : English, Hindi, Oriya and Telugu

Hobbies : Web Development, Reading and writing about Tech Stuffs & Gadgets.

Permanent Address : **Bhubaneswar, Odisha**

Declaration

I do here by declare that all the above-furnished statement is true to the best of my knowledge and belief.

Date: 20th June, 2023.

Place: Bhubaneswar

Biswajit Pradhan.

(Biswajit Pradhan)