Executive Profile

Utpal Mondal
Cyber Security – Threat & Vulnerability Manager
utpal.mondal@hotmail.com
Mobile: +1 203 501 8999

Profile

- With over **15+ years** of experience in the Technology industry, as a Cyber Security professional played multiple roles as Threat & Vulnerability Program Manager, Security Incident Response Lead, Application Security (DAST) Lead, SIEM Technology as SOC manager, Security Architect in Infra Vulnerability Management Services.
- Managing end to end Threat & Vulnerability for large enterprise along with Cyber threat management, security incident management and remediation governance across business unit.
- Extensive experience in Vulnerability management process with Qualys/Rapid7, which includes architecture & deployment across org, implementing remediation process, scanning & threat prioritization etc.
- Deployment of multiple Vulnerability management tool (Qualys/Rapid 7) across different organization, business unit within on-premises and cloud environment.
- Implement and roll out best practice for patch management process aligned with Vulnerability remediation across multiple environments with appropriate RACI matrix and governance process.
- Implement of risk-based Vulnerability remediation process, zero touch patching, automation and governance across multiple technologies and domain.
- Implement cross functional process from Vulnerability management leadership point of view, to enable and expedite proactive remediation across multiple business unit.
- Deployment and standardization of CIS compliance across multiple technology, business unit, aligned to audit board.
- Evaluation of new technology, running POC for cloud vulnerability scanning, remediation governance etc.
- Deploying Zero-day threat management process aligned with security incident management & response.
- Expertise in multi-tier end to end security incident life cycle management for any threat from a single or series of security events which violate organisation information security policies, acceptable use policies, or standard security practices.
- In a technical consultant role, managing and delivering application security assessment of various types E.x- Penetration Testing, Application Security Testing, OWASP standard security testing. This includes automated and manual penetration testing for all application, WEBUI, API, Thick client application etc security testing.
- Subject matter expert on Firewall audit, SIEM log review, IPS rule and signature review.
- Expertise in working on EDR technology, Ex – McAfee, Crowdstrike etc.
- Deployment of Proofpoint e-mail security, specialized in deployment of Threat Response Auto-Pull (TRAP) solution.

Specialization Areas	Industry Expertise	Geo Coverage
• Security Architecture – Threat Management Program. • Vulnerability Management Tool Deployment. • Threat & Vulnerability Program Manager. • CIS Control standardization and implementation. • Remediation automation & governance. • Risk based remediation model. • Cyber Security Incident Response Leas (IR). • Zero-Day threat management. • Security Information & Event Monitoring/Management. • Security operation centre – Manager. • Security Incident management. • Application Penetration Testing (OWASP). • Security Programs Development and Management. • Security Event and SOC Expertise, Incident Management. • Firewall audit, Monitoring, Incident Management. • IPS, End point security, DLP Incident management.	• eCommerce • logistic • Retail • Banking • BPO • IT Service • Finance	• USA • EMEA • APAC

Organization	Duration	Roles
Pitney Bowes	May 2021 – Till date	▪ Vulnerability Manager
Wipro Limited	Jan 2014 – May 2021	▪ Lead Administrator ▪ Lead Consultant
Infosys Limited	Dec 2012 – Jan 2014	▪ Technical Lead
Serco Global Services	July 2011 – Dec 2012	▪ Security Administrator
Rolta India Limited	May 2008 – Nov 2010	▪ Executive
eRoads Technology	Feb 2007 – May 2008	▪ Technical Support Engineer

Roles & Responsibilities

Pitney Bowes:

May 2021 - Current

- Program manager for enterprise Vulnerability management lifecycle, including remediation governance, automation of zero-touch patch management & governance, zero-day threat management etc.
- Responsible to handle business relationship and deploying cross functional vulnerability remediation process for various type of Vulnerability identified in different compliance requirement.
- Continuous maturity of VM program across organization align to overall risk mitigation, compliance regulatory and security incident management.
- VM program maturity from re-active to proactive approach and business enablement to prioritize the risk-based Vulnerability assessment and remediation.
- Helping deploying risk-based remediation across multiple business unit, and addressing technical challenges for prioritizing the remediation over business dependency.
- Handling vendor product Vulnerability assessment, restructure EOL/EOS model to map overall risk factor.
- Currently handling governance of enterprise certificate management posture. Helping process optimization to reduce any certificate outage etc.
- In a secondary role – Handling e-mail security part of Threat response auto pull feature (TRAP) in Proofpoint, including deployment and operation governance.
- Handling security incident response and manage triaging the incident.
- Changing entire Vulnerability management tool across organization in multiple phased approach – Onprem, Cloud.
- Deployment of Qualys VM tool across the enterprise, Cloud environment, starting with POC, Deployment architecture, VM program coverage etc.
- Responsible to run POC for new technology aligned to Threat and VM program/E-mail security etc.

Wipro Limited:

Jan 2014 – May 2021

- Engaged with multiple customer (Finance/Retail etc.) during Wipro tenure in managing Threat and Vulnerability Program across enterprise.
- Responsible to re-architect and deployment of Rapid 7 Nexpose VM tool across enterprise, including On-prem and Cloud section.
- As security IR lead, managing end to end incident life-cycle for any cyber security incident from a single or series of security events.
- Investigate and qualify possible incidents received from SOC Security Analysts & limit or mitigate the impact of identified incidents by working with operations teams & resolver groups.
- Be the escalation point for any Cyber security incident and invoke customer Incident Response Process for severity 1 and severity 2 reported incidents.
- Extensive working experience in various domains - Infrastructure/Application Security, Vulnerability and Threat Management, Security Incident monitoring, SIEM technology etc.

- Perform application security manual and automated penetration testing on OWASP top 10 threat, and providing analysis to business stake holder. Work as Application vulnerability remediation SME and connect customer for offshore deliverables.
- Designed and operationalized vulnerability management programs for multiple clients leveraging solutions from Rapid7 and Nessus.
- Complete architecture review on all Nexpose engine, console deployment across geo for Infra Vulnerability Management coverage and scan methodology.
- Deployment of 50+ Nexpose scan engine and 4+ Nexpose console in AWS, On-Prem as dedicated project lead and SME for infrastructure Vulnerability Management.
- Defining the entire infrastructure vulnerability management remediation process aligned with regular patch management including RACI Metrix, risk, process flowchart, SOP etc.
- As Firewall audit lead, completed 80+ Cisco and Juniper Firewall rules audit using Nipper, consolidated findings and driven with Network stake holder for closer.
- Implemented proactive threat monitoring process including zero-day vulnerability, adhoc threat, out of band patch management, security incident management etc.

Infosys Limited:

Dec 2012 – Jan 2014

- Operated as a Security Lead for customer environment from offshore, which included the responsibilities of handling Vulnerability management lifecycle, SIEM Incident management, IDS even monitoring etc.
- Complete responsibilities in performing periodic VA scanning to critical devices through Qualys Guard.
- Monitor all adhoc vulnerability in operating system and application, analysis and report to management. Complete remediation driven project was executed.
- SIEM Integration (ArcSight) with all available log sources for monitoring. Work as L3 administrator for ArcSight SIEM deployment includes, onboarding log sources, configuring dashboard, filter, channel, co-related evets, notification etc.
- Implemented 24x7 incident and traffic monitoring, management by creating SIEM traffic dashboard, account login, filter, notification etc.
- Performed administration of application access review and filtering of Cisco Iron Port Proxy. Delivered security threat analysis using IPS event and managing day-to-day operation.
- Implementation of Sourcefire IDS for sensing the outbound traffic as part of threat management.
- Management and implementation of Security control in client environment.
- Preparation and presentation of Security metrics data on weekly/monthly basis.
- Meeting with team on weekly basis regarding security control in in entire environment.

Serco Global Services Pvt Limited:

July 2011 – Dec 2012

- Worked as Security Administrator for Integrating ArcSight for all remote location Log monitoring and security incident response through IBM IPS.
- Complete end-to-end project for ArcSight included Connector, filters, Dashboard etc. Performed implementation of Checkpoint VPN setup for remote location.
- Preform manual penetration testing for security vulnerability across infrastructure and application. Made sure the identified vulnerability is captured in ArcSight dashboard.
- Performed daily McAfee ePO and WSUS report review for compliance. Including rogue system, DAT level etc.
- Checkpoint VPN setup for remote location, including log forwarding to SIEM loggers.
- IPS event analysis for daily, weekly, monthly and present security metrics data.
- Change management review and promote to Tripwire for new baseline configuration.
- Complete security analysis and maintain security incident for all global location.

Rolta India Ltd:

May 2008 – Nov 2010

- MPLS WAN Link monitoring, link troubleshooting and complain booking for all corporate offices and branch.
- Configuring the Sonic wall firewall for IPSEC VPN, Access rules for almost 4000 users, including end user VPN.
- Cisco ASA firewall configuration for migrating existing access rules from Sonic wall.
- Installation and configuration of Router, Switches, Firewall (Cisco, 3Com, SonicWall). Worked 2in 4x7 NOC.
- Installation and configuration of Switches L2, L3 and testing of all routing table, VLAN access issues etc.
- Installing the software and other networking products for Windows AD server, Exchange Server etc.
- Worked on projects, meeting with ISP to get complete details and installation any new WAN Router.
- Completely involved in Network development and Network Security.

eRoads Technology

Feb 2007 – May 2008

- MPLS WAN Link monitoring, link troubleshooting and complain booking.
- Configuring the Sonic wall firewall for IPSEC VPN, Access rules for almost 4000 users.
- Cisco ASA firewall configuration.
- Installation and configuration of Router, Switches, Firewall (Cisco, 3Com, Sonicwall)
- Installation and configuration of Switches L2.L3
- Installing the software and other networking products.
- Worked on different projects, meeting with ISP.
- Completely involved in Network development and Network Security.

Training

- SANS Security leadership for Enterprise and Cloud Vulnerability Management Program.
- Proof point certified Insider Threat Specialist.
- IBM Certified Associate Security QRadar V7.0
- 5 Days hands on training on ArcSight from Paladion.

Professional Qualification

Degree:	**B-Tech.**
Area:	Electronics & Communication Engineering.
Institute:	B.I.E.T Suri (Birbhum), West Bengal. West Bengal University of Technology
Year:	2006.

Personal Details

Date of Birth:	- 26th Sept, 1982
Gender:	- Male
Marital Status:	- Married
Nationality:	- Indian
Languages Known:	- English, Hindi, Bengali.

Current Address

3000 Grand Summit Blvd, Apt 3112. Concord, NC 28027