Executive Profile

Utpal Mondal
Cyber Security – Threat & Vulnerability Manager
utpal.mondal@hotmail.com
https://www.linkedin.com/in/utpalmondal/
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 Threats and vulnerability for large enterprises along with Cyber threat management, security incident management, and remediation governance across business units for on-premises and cloud instances.
- Extensive experience in Vulnerability management process with Qualys/Rapid7, which includes architecture & deployment across on-premises and AWS cloud instances, along with remediation process & threat prioritization, etc.
- Deploying CSMP (AWS Cloud Security Posture Management) – Assessment, monitoring & governance.
- Integration of Vulnerability management program for Amazon cloud, cloud inventory management, real-time threat detection, and mitigation for misconfiguration in cloud instances.
- Shifting the traditional Vulnerability management methodology for AWS cloud instances to Snapshot-based scanning of all EC2 instances across the organization.
- Implement risk-based Vulnerability remediation process, zero-touch patching, automation, and governance across multiple technologies and domains.
- Implement cross-functional work culture from a Vulnerability management leadership point of view, to enable and expedite proactive remediation processes across multiple business units.
- Deployment and standardization of CIS standards across technologies, and business units, aligned to the audit board.
- Evaluation of new technology, running POC for cloud vulnerability scanning, remediation governance, etc.
- Deploying a 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 that violate organization information security policies, acceptable use policies, or standard security practices.
- Leverage industry standards and best practices to collect data during response efforts, seek to minimize incident impact and work to continually improve incident response capabilities.
- In a technical consultant role, managing and delivering application security assessment of various types E.x- Penetration Testing, Application Security Testing, and OWASP standard security testing. This includes automated and manual penetration testing for all applications, 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, e.g. – McAfee, Crowdstrike, etc.
- Deployment of Proofpoint e-mail security, specialized in the deployment of Threat Response Auto-Pull (TRAP) solution.

Specialization Areas	Industry Expertise	Geo Coverage
• Security Architecture Reviews and Implementation. • Threat & Vulnerability Program Manager. • Amazon Cloud instances Vulnerability Management • AWS Snapshot scanning • Cloud security posture management (CSPM) • 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 Incident Management. • Application Penetration Testing (OWASP). • Security Event and SOC Expertise, Incident Management. • Firewall audit, Monitoring, and Incident Management. • IPS, Endpoint 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 for handling business relationships and deploying cross-functional vulnerability remediation processes for various types of Vulnerabilities identified in different compliance requirements.
- Continuous maturity of the VM program across the organization aligns with overall risk mitigation, compliance regulations, and security incident management.
- Deployment of snapshot-based scanning for AWS cloud instances, including continuous monitoring of cloud instance misconfiguration and real-time threat detection.
- Integration of Qualys and Divvy cloud for cloud instances part of Cloud Security Posture Management (CSPM).
- VM program maturity from reactive to proactive approach and business enablement to prioritize the risk-based Vulnerability assessment and remediation.
- Helping deploy risk-based remediation across multiple business units and addressing technical challenges for prioritizing the remediation over business dependency.
- Handling vendor product Vulnerability assessment, and restructuring the EOL/EOS model to map overall risk factors.
- Currently handling governance of enterprise certificate management posture. Helping process optimization to
- reduce any certificate outage etc.
- In a secondary role – Handling the e-mail security part of the Threat response auto pull feature (TRAP) in Proofpoint,
- including deployment and operation governance.
- Handling security incident response and managing triaging the incident.
- Deployment of Qualys VM tool across the enterprise and cloud environment, starting with POC, Deployment
- architecture, VM program coverage, etc.
- Responsible for running POC for new technology aligned to Threat and VM program/E-mail security etc.

Wipro Limited:

Jan 2014 – May 2021

- Engaged with multiple customers (Finance/Retail etc.) during Wipro tenure in managing the Threat and Vulnerability Program across the enterprise.
- Responsible for re-architecting 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 cybersecurity incident and invoke the 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 threats, and provide analysis to business stakeholders. Worked as an Application vulnerability remediation SME and connected customers 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, and console deployment across geo for Infra Vulnerability Management coverage and scan methodology.
- Deployment of 50+ Nexpose scan engines and 4+ Nexpose consoles 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 audits using Nipper, consolidated findings, and driven with Network stakeholders for closer.
- Implemented proactive threat monitoring process including zero-day vulnerability, ad-hoc 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 the Vulnerability management lifecycle, SIEM Incident management, IDS events monitoring, etc.
- Complete responsibilities in performing periodic VA scanning to critical devices through Qualys Guard.
- Monitor all ad-hoc vulnerabilities in the operating system and application, analyze, and report to management. A 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 the dashboard, filter, channel, co-related events, notification, etc.
- Implemented 24x7 incident and traffic monitoring, and management by creating an 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 events and managing day-to-day operations.
- Implementation of Sourcefire IDS for sensing the outbound traffic as part of threat management.
- Management and implementation of Security control in the client environment.
- Preparation and presentation of Security metrics data on a weekly/monthly basis.
- Meeting with the team on a 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 including Connector, filters, Dashboard, etc. Performed implementation of Checkpoint VPN setup for remote location.
- Perform manual penetration testing for security vulnerability across infrastructure and applications. Made sure the identified vulnerability was captured in the ArcSight dashboard.
- Performed daily McAfee ePO and WSUS report reviews for compliance. Including rogue system, DAT level, etc.
- Checkpoint VPN setup for a 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 incidents for all global locations.

Rolta India Ltd:

May 2008 – Nov 2010

- MPLS WAN Link monitoring, link troubleshooting, and complaint booking for all corporate offices and branches.
- 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, and Firewall (Cisco, 3Com, SonicWall). Worked 2in 4x7 NOC.
- Installation and configuration of Switches L2, and L3 and testing of all routing tables, 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 of 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 complaint booking.
- Configuring the Sonic wall firewall for IPSEC VPN, Access rules for almost 4,000 users.
- Cisco ASA firewall configuration.
- Installation and configuration of Router, Switches, and 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

- Pursuing CISSP certification.
- 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 of 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.

Current Address

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