Dhruvil Pathak

Dhruvil.Pathak5241@gmail.com | +1 (647)-393-7666 | www.linkedin.com/in/dhr5241

Objective

Skilled and analytical cybersecurity professional with expertise in cryptographic algorithm, using different industry-standard tools, patching security devices, analyzing security events, and event handling. Polished communication and presentation skills with the ability to work in an environment where timeline and accuracy matter the most.

Skills

- **Operating System**: Windows, Mac, Parrot, Unix/Linux,Solaris etc.
- **SIEM Tools**:Symantec, SolarWinds, SPLUNK and IBMQradar.
- **Programing languages**:C, C++, Perl, Python, MYSQL, PowerShell, Bash etc.
- **Forensics Digital Investigation tools**: FTK imager, SANS SIFT, KAPE,EnCase,RedLine, Registry Viewer, Volatility,Cyber Triage etc.
- **Network and host**: LDAP, TCP/IP, subnetting, DNS, DHCP, SSL/TLS, VoIP, SMTP, SSH, Telnet, FTP.
- **Offensive/Defensive Security tools**: Wireshark, Nmap, Tshark, tcpdump, Metasploit,BEeF, MS office exploits, Tenable Nessus, OpenVas, SolarWinds etc.
- Vulnerability management, risk management, incident response, latest cyber trends, DLP management.
- **Cryptography**: PKI certificates, symmetric/asymmetric keys, hash functions, HSM, KMS, Docker etc.
- **Security Architecture**:PaloAlto, MS azure, CISCO, Fortinet, ModSec, Security Onion, Solarwinds. OWSAP, AWS etc.
- **Industry-standard security compliance and framework**: NIST,ISO2700,MITRE,GDPR,SOX,CIS. PHIPA.

Experience

IT Operational Assistant | EFLYN-Ambianz.inc | Mississauga — **Aug 2020 – Feb 2021**

- Providing TIER3 technical support to different clients for infrastructural issues.
- Working extensively on Windows Active Directory, creating & managing Group Policy objects.
- Repairing/Troubleshooting hardware as well as software-related issues for both endpoint devices and kiosks.
- Providing support to different clients in both the automotive and medical industries.
- Handling G-Suite for backend POS and Kiosk applications.
- Providing support to POS and kiosk customers in retail and restaurant.
- Designing secured infrastructure for migration of data from onsite to cloud. This includes implementing secure architecture, work according to PHIPA security compliance, migration of all users, and client accounts/details.
- Managing email domains for different clients.
- Configuring RAID levels on SSDs for failover backups.
- Creating PowerShell and shell scripts to automate day-to-day configuration and backups.
- Managing and configuring different kinds of Web-based Firewalls, Physical Firewalls, Switches, and Routers.

Intermediate Security Analyst |BMO Financial Group| COOP, Toronto — **Jan 2020 – April 2020**

- Cloud and Security Architecture Management with emphasis on encryption and key management.
- Monitored security events using the SIEM tools such as the SPLUNK and Palo-Alto redlock, for cloud-based applications and on-prem HSM.
- Implemented data security controls, creating IOCs, and analyzing malicious emails.
- Worked proactively with the SOC team, to derive a secured architecture for the banking systems.
- AWS cloud setup (S3, DaynamoDb, KMS, RDS, Cloud Trail, Lambda Functions, API gateway, VPC)
- Classified data according to the banking standards and norms depending on their level of confidentiality.
- Minor application development using Python, HTML, and PHP.

Education

Computer Security and Investigation | Sir Sandford Fleming College, Peterborough — **Jan 2018 – April 2020**

- 3-year advanced diploma in the field of Cyber Security, Digital and Forensics Investigations, and some aspects of project management.

Academic Projects.

❖ POC for measuring the Decryption rate for AWS cloud management. Jan 2020-April 2020

- Developed a secured design for the banking system using different artifacts of the AWS.
- Implementing the security artifacts for the backend application and the database.
- Configure Lambda function for serverless functioning of web application.
- Understanding the IAM roles for different users and assigning privileges accordingly to the PCI/PII data.
- Managing and Maintaining the AWS resource usage, billing details, Application development status, Log analyzing tool usage using different tools such as Tableau.

❖ Cryptography Jan 2019-April 2019

- Understanding and Generating PKI certificates, protocols used for data security & data sharing.
- Understanding the concept behind the internet key exchange protocols and the security for the different versions of the SSL and TLS protocols.
- Working with HSM and different cloud-based key storage devices.

❖ Security Architecture Management Sept 2019 - Dec 2019

- Understanding the concept behind Active Directory, implemented SCCM server, Zabbix monitoring tools.
- Developed a project for simple office infrastructure that includes making GPO’s for different users in the active directory, making a kiosk mode computer, and control the users using the main SCCM server.
- Implemented system log forwarding for both Unix and Windows using the WinRm and other industry-standard tools.
- Azure cloud management and configuration of the cloud to host a small web-based application.

❖ Software DevOps For Security Jan 2018-Dec 2018

- Made a Perl ARP scanner for discovering the alive host on the network.
- Python Flask and Django-based backend application, this included minor application development and major security analysis of the application.
- Handling of SQL database for getting the info for the port scanning utility and filter them according to the user demand.