Vishant Patel

Professional Experience

Microsoft Corp. - Redmond, WA

Digital Crimes Unit/Microsoft Legal & Corporate Affairs **August 2012 – Present**
Senior Manager of Investigations

- Developed, implemented, and managed investigations regarding botnets, malware and computer intrusions impacting Microsoft and its customers, products and services
- Developed evidence and participated in legal actions directed at identifying and disabling botnet infrastructure.
- Responded and investigated the System & Network incidents
- Evaluated and implemented Security Event Management (SEM), Network Forensics', and Incident Management technologies.
- Communicated Cyber tools, techniques, & trends on vetted information sharing groups
- Acted as liaison with local, federal and international law enforcement and industry groups in prosecuting organized crime groups.

Citigroup Inc - New York, NY

Cyber Investigation & Response Team **February 2011 – August 2012**
Senior Investigator / Vice President

- Developed, implemented, and managed enterprise level Anti-Phishing & Anti-Trojan solutions to meet Citi framework. These solutions anticipate all aspect of Phishing & Trojan threats and takes systematic counter measures to mitigate threats.
- Participated in development of new group called Citi Cyber Intelligence Centre (CIC). CIC collects, analyzes, and exchanges actionable Cyber intelligence that increases threat awareness and decrease risk posture.
- Responded and investigated the System & Network incidents involving DDoS, Advance Persistent Threat (APT), ZERO day, Policy Violation, & Data leakage.
- Advised monthly and on ad hoc basis about Cyber threats to Senior Management by performing Risk Assessments on CIRT incidents.
- Interacted with Information Technology Risk Management group to mitigate gaps identified within the process and technology controls through CIRT investigation.
- Managed third party security vendors to ensure they are in compliance with Citi policies, standards, procedures, and service level agreements.
- Evaluated and implemented Security Event Management (SEM), Network Forensics', and Incident Management technologies.
- Communicated Cyber tools, techniques, & trends on vetted information sharing groups such as FS-SIAC, DPN, UK Payment Councils, FIRST, & Botnet take-down task force.
- Acted as liaison with local, federal and international law enforcement and industry groups in prosecuting organized crime groups.
- Participated in working groups to update Citi information security policies, standards, and procedures involving CIRT components.
- Developed & conducted Cyber investigation training to Investigators & new hires.
- Managed team of three individuals to ensure CIRT investigation meets industry best practices.
- Interacted with Citi fraud risk group in development of multilayered risk strategies to mitigate emerging social engineering, online banking, mobile, and carding fraud.
- Acted as liaison with forensics, vulnerability assessment, intrusion detection, and anti-virus group to mitigate Zero day vulnerabilities impacting Citi globally.

Cyber Investigation & Response Team **February 2005 – February 2011**
Investigator / Assistant Vice President

- Designed and implemented controlled lab environment to perform runtime and reverse engineering of Malware.
- Developed and automated customized parsing scripts to extract and normalize the compromised credentials captured by Phishing and Malware.
- Developed a self service portal to disseminated compromised credentials to respective fraud risk group in real time.
- Published routine comprehensive intelligence reporting of internal and external Cyber threats to Citi businesses.
- Developed strategic partnership with ICANN & Internet Service Provider to detect and mitigate Phishing & Malware threats.
- Advised Security Operation Center in development of framework to detect and track emerging Cyber threats.

CompUSA – New York, NY

Lead Network & Computer Technician **January 2000 - February 2005**

- Acted as a network team lead in migration and integration of New York stores.
- Configured and deployed store Point of Sale systems.
- Designed and implemented secured WiFi networks.

CERTIFICATIONS

- Malware Artifacts 2006
- XANALYS Link Explore
- A+ Technician

EDUCATION

Stony Brook – Computer Science: New York, NY **May 2002**

Degree: Bachelor of Computer Science

Programming Languages

- C++
- Java
- HTML
- SQL
- Perl
- Python

Operating System

- Windows
- OS X
- Linux
- Android

Application / Appliances

- i2 Workbench
- SharePoint
- MS Suite
- ArcSight
- Netwiness
- Source Fire

Personal Accomplishments

Certificate of Appreciation from Federal Bureau of Investigation