Shirsh Gupta

shirshgupta99@gmail.com • *+91-8887893568* • *Portfolio* • *LinkedIn*

EXPERIENCES

Jul. 2024 - Present **Accenture technologies** **Senior Security Analyst**

a. *Worked with Accenture Security delivery team to handle vulnerability management and Security Incident management operations for Canada retail company* ***Sobeys.***
b. ***Handled transition activities*** *for the client and* ***created vulnerability management process from scratch****.*
c. *Utilized* ***CrowdStrike Falcon*** *and* ***Qualys*** *for vulnerability management and prioritization of vulnerabilities.*
d. *Helped remediation team in prioritization of remediation of large number of vulnerabilities (20.1 M) by providing insights on the assets, CVEs to be targeted with least efforts.*
e. ***Provided IOCs, Yara Rules and Additional workaround*** *to* ***threat hunt team*** *for quick action until remediation is performed.*
f. *Performed Vulnerability Management, including supporting scan tools, implementing vulnerability scans, performing analysis, creating vulnerability report and recommending / tracking mitigation/ exceptions.*
g. *Managed the day-to-day triage of* ***cyber alerts****, analyzing and* ***prioritizing*** *threats/vulnerabilities using* ***VULNDB*** *and* ***Virus Total****.*
h. ***Analyzed*** *&* ***validated*** *security vulnerability data to identify applicability,* ***false positives and exceptions.***

Apr. 2023 – Jun. 2024 **Cognizant Technology Solutions** **Sr. Security Engineer**

a. *Worked in* ***Cognizant CIS team****, focusing on* ***Vulnerability Management*** *for client infrastructure using* ***Qualys*** *and* ***Rapid7 Nexpose.***
b. *Registered the assets in the scanning tool and perform scanning as per the agreed schedule.*
c. ***Analyzed*** *&* ***validated*** *security vulnerability data to identify applicability,* ***false positives and exceptions;*** *recommended corrective actions and applied it on* ***Qualys*** *and* ***Rapid7 Nexpose*** *tools, ensuring the* ***generation of accurate vulnerability reports****.*
d. **Tracked** and provided **remediation steps of vulnerabilities** by using **agreed-upon action plans** and timelines with responsible technology developers and support teams.
e. ***Automated processes,*** *including the* ***conversion of IP ranges to IP addresses*** *and the* ***segregation of IP addresses****, using* ***'Bash scripts'****.*
f. *Validated and updated the* ***authentication records*** *to resolve the failure issues to conduct* ***authenticated vulnerability scans.***
g. ***Developed option profiles*** *and* ***Static/Dynamic search lists*** *on* ***Qualys*** *for* ***customized scanning*** *based on Security team advisories.*

Nov. 2020 - Mar. 2023 **Infosys technologies Ltd.** **Senior System Engineer**

a. *Worked in Infosys* ***CyberSecurity Vulnerability Management*** *team collaborating with* ***Mercedes Benz & Daimler Trucks security teams*** *on* ***Vulnerability Management*** *&* ***Assessment*** *using* ***Qualys Cloud Platform*** *&* ***Qualys Agent****.*
b. *Collaborated with Mercedes Benz Security team for* ***Qualys agent roll-out*** *activities on* ***servers*** *and* ***endpoint devices****.*
c. *Possess strong knowledge and experience in* ***security assessment****,* ***vulnerability management****,* ***risk-based threat analysis****, and* ***security mitigation*** *techniques. Proficient in using tools like* ***Qualys Scanner and Qualys Agent****.*
d. ***Lead a data analytic team****, and utilized Infosys internal offering '****CyberGaze'*** *and* ***Jupyter Notebook*** *to generate visuals, providing key insights on Compliance and Operational KPIs using* ***flowcharts, graphs****, and other visuals through* ***Python****,* ***SQL****, and* ***KPI templates*** *(prepared in* ***Excel*** *and* ***Python****)*
e. *Analyzed project metrics related to* ***Vulnerability Management****,* ***Patch Management****,* ***Risk Management****,* ***SLA adherence, Software Currency****.*

SKILLS

Languages	*Python3 (Scapy), Advance SQL, Bash Scripting, HTML5, CSS3, JavaScript, Node.js.*
Tools	*Qualys, CrowdStrike Falcon, Splunk, Nexpose, OpenVAS, Nikto, SQLmap, MS Defender, Wireshark. Nmap, Hashcat.*
Platforms	*Ubuntu, Kali Linux, Windows*
Policies/ Frameworks	*GDPR, ISO/IEC 27001, PCI-DSS, HIPAA, NIST*
Relevant Skills	*Sniffing & Spoofing, DNS Based attacks, ARP Spoofing attack, Basic Networking, Shell Scripting, Governance, Risk Management, Compliance, Vulnerability Management, Data Analysis (Pandas, Matplotlib, Seaborn), programming & Scripting, Cloud Security.*

CERTIFICATION & BADGES

Certification Name	*Issued By*	*Links*
Ethical Hacker	*Cisco*	*Link*
Ethical Hacking Essentials (EHE)	*EC Council*	*Link*
Specialist in Vulnerability Management	*Qualys*	-
CrowdStrike Falcon Vulnerability Management	*CrowdStrike*	-
Networking Essentials	*Cisco*	*Link*
ISO/IEC 27001 Information Security Associate	*Skillfront*	*Link*
AZ-900 (Azure Fundamentals)	*Microsoft Azure*	*Link*
Python Essentials-I	*Cisco*	*Link*
Cybersecurity Essentials	*Cisco*	*Link*
Qualys Cloud Agent	*Qualys*	-
Specialist in Assetview and Threat Protection	*Qualys*	-

EDUCATION

Jul. 2023 - Present **Birla Institute of Technology and Science, Pilani**
Master Of Technology in Software Systems (Cyber Security) ***CGPA:*** *9.0*

Aug. 2016 - Sep. 2020 **Dr. A.P.J. Abdul Kalam Technical University, Lucknow**
B*achelor Of Technology in Electronics & Communication Engineering* ***C.G.P.A:*** *8.25*

Aug. 2014 - Jul. 2016 **M.P.V.M Ganga Gurukulam, Prayagraj**
12th in Physics, Chemistry, Maths, English and Computer Science. ***Percentage:*** *87.8%*

Jun. 2013 - Jul. 2014 **M.P.V.M Ganga Gurukulam, Prayagraj**
10th in Maths, Science, Social Science, Hindi, English and IT. ***Percentage:*** *96%*

HONORS

a. ***Won 'Accenture Excellence Award' in 2024*** *for excellence and prioritizing the critical tasks for vulnerability management.*
b. ***Won 'Insta Award' in 2022*** *for excellence & on time delivery to Mercedes Benz and Daimler Trucks.*
c. ***Won 'Insta Award' in 2021*** *for providing interesting insight using Visuals and insights (Using CyberGaze and Jupyter Notebook) on Project's compliance and operation to Mercedes Benz and Daimler Trucks security teams.*