AMANDEEP SINGH VIRDI

amandeepvirdi1992@gmail.com ● +91 9717575262 ● Bangalore, India

PROFILE

- Solutions-driven IT professional with deep theoretical knowledge and hand-on experience in **threat modelling**, **DevSecOps**, **cloud security**, **incident response**, **vulnerability assessment**, and **system operations**.
- Experienced in working in cross-functional teams; adept at working in shifts and turning in deliverables in a high-criticality environment of varying daily workload.
- **M.S. in Security and Mobile Computing (NordSecMob)**. Coordinated by Aalto University: first year at **KTH Royal Institute of Technology** in Stockholm, Sweden; second year at **Norwegian University of Science and Technology (NTNU)** in Trondheim, Norway.

SKILLS

- Focus area: Threat Modelling, DevSecOps, Cloud Security
- Operating systems: Windows, Linux, MacOS
- Programming languages: Bash, Python, Java, C++
- Cloud computing platforms: Amazon Web Services (AWS), Google Cloud Platform (GCP)
- Security tools: Zscaler, Rapid7, CrowdStrike, Endpoint Protector, ManageEngine, Black Duck, Polaris, GitHub Advanced Security
- Miscellaneous: Git, Terraform, Docker, Kubernetes, Datadog, Puppet, Monit, SQL, MongoDB, iptables, Microsoft Office, HTML, OpenVPN, LDAP

WORK EXPERIENCE

Cyber Engineer • IKEA • Bangalore, India **Mar 2023 – Present**

- Conducted comprehensive threat modelling for multiple products, proactively assessing evolving risk profiles and safeguarding critical infrastructure across diverse environments.
- Designed and implemented a threat modelling automation pipeline with **TerraformC4Gen** (for infrastructure visualization and diagram generation), **augurAI** (for AI-driven threat identification), and **Cerberus** (for vulnerability correlation and data deduplication), significantly enhancing efficiency.
- Strengthened the organization's DevSecOps practices by integrating security-first workflows using tools such as **Black Duck**, **Polaris**, and **GitHub Advanced Security**, streamlining vulnerability detection and remediation.
- Engineered scalable cloud security monitoring solutions to enhance the efficiency of cloud infrastructure vulnerability reporting and triaging by enhancing incident response capabilities and reducing alert fatigue.
- Developed and scaled the organization's **security champions** program, designing comprehensive training materials and workshops that empowered teams with the skills to adopt security-first practices, fostering a strong culture of security awareness.

Security Operations Engineer • SHL • Gurgaon, India **Feb 2021 – Mar 2023**

- Responsible for designing, implementing, and supporting the security controls and software required to protect the company's infrastructure from evolving cybersecurity threats using a variety of tools such as **Zscaler, CrowdStrike, Rapid7, Endpoint Protector**, **ManageEngine**, etc.
- Recognizing areas for security improvements, wrote scripts and set up CI/CD pipelines, using **Bamboo**, for automated compliance and alerting; improved monitoring and reporting of incidents and requests by better integration of disparate tools such as **Rootshell Prism** and **Jira**; set up data loss prevention and cloud app control policies to protect company data.
- Reviewed security requirements for new IT solutions and performed security review of new solutions and vendors.

Operations Engineer • Placester, Inc. • Remote **Dec 2019 – Feb 2021**

- As a member of the extended operations engineering staff for Placester, provided thorough support and problem resolution for all DevOps-related issues
- Maintained infrastructure automation and delivery using **Puppet** for 200+ servers; used **Monit** for process monitoring, management, and alerting; implemented **Datadog** for full stack metrics and alerting; wrote scripts and launched servers for efficient process and cost optimization.
- Responsible for the maintenance and further development of the **'Placester AWS Inventory Tool'**; that used **boto3**, the AWS SDK for Python, to query the cloud environment and present, using HTML toolkits such as **Bootstrap** and **DataTables**, an internal-only website, offering a detailed listing of the company's infrastructure.

Security Engineer • foreseeti AB • Stockholm, Sweden (link) **Nov 2018 – June 2019**
Master Thesis Student • foreseeti AB • Stockholm, Sweden (link) **Jan 2018 – Jun 2018**

- The primary goal of the thesis project was to adapt and extend securiCAD™ by foreseeti to the **AWS (Amazon Web Services)** cloud environment. Thesis title: *AWSLang: Probabilistic Threat Modelling of the Amazon Web Services environment* (link)
- Conducted a survey of the AWS domain; compiled a taxonomy of possible attacks on clouds; built a feature matrix that maps the elements of the AWS environment with the assets in **securiCAD™** and beyond.
- Keeping my previous work in the field as the foundation, worked with developers from various cross functional teams to write, parse, automate, design the next-generation of threat modelling tools: **securiCAD Vanguard** – a **fully-automated threat modelling and attack simulation solutions for cloud**.

Graduate Engineer Trainee • HCL Technologies Ltd. • Noida, India **Aug 2014 – May 2016**

- Member of the extended IT support staff for **H&M**, as part of the fixed period employment tenure with HCL in India.
- Provided thorough support and problem resolution for issues related to **Windows**, network connectivity, and application issues; assisted with troubleshooting of **Citrix** VDIs (Virtual Desktop Infrastructure) and XenApps, maintenance of the **SCCM (System Center Configuration Manager)** and the **Active Directory**.
- Awarded 'Comnet Jewel' as one of the top performers of the entire project thrice within a six-month period.

CERTIFICATIONS

- AWS Certified Cloud Practitioner • Nov 2019 (link)
- AWS Certified Solutions Architect - Associate • Sept 2020 (link)
- AWS Certified Security – Specialty • Jun 2021 (link)
- Zscaler Certified Cloud Administrator - Private Access (ZCCA-PA) • Jan 2022
- Zscaler Certified Cloud Administrator - Internet Access (ZCCA-IA) • Jan 2022
- GCP Cloud Digital Leader • Aug 2023 (link)
- GCP Associate Cloud Engineer • March 2024 (link)

EDUCATION

Master of Science • Security and Mobile Computing (NordSecMob) **2016 – 2018**

- Coordinated by Aalto University: first year at **KTH Royal Institute of Technology** in Stockholm, Sweden; second year at **Norwegian University of Science and Technology (NTNU)** in Trondheim, Norway.
- Advanced Networking | Internet Security and Privacy | Building Networked Systems Security | Wireless Network Security

Bachelor of Technology • Electronics and Communication Engineering **2010 – 2014**

- Four years of studies coordinated by the **Guru Gobind Singh Indraprastha University** in New Delhi, India.
- Circuits & Systems | Computer Networks | Network Technology | Telecommunication Networks | Mobile Communication

PROJECTS

Research poster: "Protect your Privacy in Big Electrical Data" (link) **Nov 2017**

- Presented a research poster titled "Protect your Privacy in Big Electrical Data" at the **NordSec2017: Nordic Conference on Secure IT Systems** in Tatru, Estonia.
- Conducted a literature review of smart grid communications technology and the use of cloud computing for smart meters; surveyed **Cryptonite** and the **StrongBox** model of key management; studied **Privacy Preserving Data Mining** mechanisms.Offered potential mitigations to privacy concerns of smart meters by using a combination of Searchable Encryption and Privacy Preserving Data Mining.

Software Defined Networking and Network Functions Virtualization project **April 2017 – May 2017**

- The project was undertaken with the objective of familiarizing oneself with modern networking design and implementation using **Software Defined Networking (SDN)** and **Network Functions Virtualization (NFV)** principles.
- Implemented a network design controlled by a **POX SDN** controller via **OpenFlow v1.0** protocol; added more advanced network functions using the **Click NFV** framework for Phase 2 of the project.
- Submitted a **Mininet** topology implementation along with the SDN application; wrote **Python** scripts to test the network.

ACME Secure Network Implementation **Jan 2017 – Mar 2017**

- **Building Networked Systems Security** is a project-/implementation-/lab- based Masters course targeted at implementing networked systems security solutions, addressing specific security requirements and system constraints.
- The project provided a secure network for a fictional business organization. The network could provide employee authentication (using both **two-factor authentication** and certificates), had strong **firewalls** and Intrusion Detection System (IDS), etc. All communication across the network was secured using **OpenVPN**.
- Designed and implemented the network; responsible for installation and configuring of the **IDS using Snort**, the **Log Server using Graylog**, in addition to the using standard Ubuntu procedures for the **DHCP** (Dynamic Host Configuration Protocol) server, the **DNS** (Domain Name System) server, and the **NTP** (Network Time Protocol) Server of the design.

SOCIAL MEDIA

- LinkedIn: linkedin.com/in/thatvirdiguy
- GitHub: github.com/thatvirdiguy

LANGUAGES

Hindi (native), Panjabi (native), English (fluent), Swedish (intermediate proficiency)