Darsh Patel

470-641-4432 pateldarsh467@gmail.com Darsh Patel pateldarsh.com

Education

Purdue University *Bachelors of Science in* ***Cyber Security*** *(Minor in* ***Forensic Sciences****)* Aug 2020 - May 2024 | West Lafayette, IN

Center for Education and Research in Information Assurance and Security - Student Ambassador

Computer and Information Technology Student Council - General

Executive Forum - Student Host

Experience

Security Engineer, *Amazon LLC.* June 2025 – Present | New York, NY

- Co-authored a **GenAI AppSec certification framework** based on **OWASP LLM Top-10**, **NIST AI RMF**, and **Amazon Security Policy**, and operationalized it as a repeatable certification process enabling secure GenAI adoption across internal and external applications
- Performed extensive application security review on **IMDb Pro iOS App, Impression, Point, Click(IPC) services, Amazon Ads Console Monitoring and logging services, IMDb GenAI Web Application Features** involving **manual and automated code review, threat model review** and **mitigation testing** and creating **Incidence Response plans** with **MTTR of 2-3 weeks**
- Shipped **auto-remediation and containment guardrails** using **AWS Config**, **EventBridge**, and **Lambda** for public **S3**, wildcard **IAM**, and permissive **security groups**, reducing auto-remediation **MTTR from 1 day to 5 minutes**
- Built application-specific **threat models** using **STRIDE** and **PASTA** and authored **incident-response playbooks** covering containment, communications, **CloudTrail Lake** queries, and rollback criteria to ensure teams are incident-ready pre-launch
- Embedded with product design to mitigate **GenAI** and **RAG** risks including prompt injection, data exfiltration, model and **PII minimization and redaction**, cutting hallucination-related defects and saving **75 engineering hours per quarter**
- Shipped a **Next.js** and **TypeScript** SecOps app unifying **SIRT**, **pentest**, **bug bounty**, and critical-incident reporting with IR runbooks, reducing manual load and boost engineer productivity with MTTD by **70%**

Customer Success Engineer, *Verkada Inc.* June 2024 – June 2025 | San Mateo, CA

- Automated high-volume customer **(H&M** and **Burlington)** workflows with **Python** including bulk audit exports, policy checks, and resource management, saving **160 engineering hours per quarter** and reducing manual touches
- Built cross-source log correlation in **Splunk**, **Datadog APM**, and **AWS Athena** to link auth, device, and user activity, improving **MTTD** and **lowering false positives** for faster bug triage and investigation
- Resolved over **990+** client cases per quarter, addressing diverse technical issues across **11+ product types** with a **97%** customer effort score
- Identified **upsell opportunities** by recommending complementary products (cellular modules for remote deployments, PTZ cameras for expanded coverage), contributing to account expansion
- Delivered **30+** technical product demonstrations across cameras, access control, intercoms, and alarms, educating customers on integration capabilities and driving product adoption

Assistant Network Assistant, *Purdue University* Dec 2022 – May 2024 | West Lafayette, IN

- Deployed **802.1X EAP-TLS** with **dynamic VLANs** across **2,480** access ports to enforce device identity and segmentation, cutting unauthorized port use by **68%**
- Built detections and dashboards in **Splunk** and **SolarWinds** for auth anomalies, link instability, security events and network traffic analysis, accelerating incident detection
- Implemented **SNMPv3** telemetry with **python** to counter system errors and alert on threshold breaches for CPU consumption, temperature and backup power level to prevent service outages
- Designed micro-segmented **VLAN** topology for **HPC**, **IoT labs**, and academic networks with ACLs and QoS, reducing lateral-movement exposure and passing an internal audit
- Deployed containerized applications for **HPC research** using **Docker** and **Kubernetes** for scalable and cloud-based workflows

Information & Technology Associate, *Purdue University* Dec 2021 – May 2024 | West Lafayette, IN

- Integrated **Grafana** and **ELK** for real-time container troubleshooting and performance insights
- Authored **SOPs in Confluence** for VLAN provisioning, firewall change windows, and incident triage used by **18** student assistants, cutting onboarding time **31%**
- Implemented **RBAC** aligned to **least privilege** for service accounts and CI/CD, removing **36** over-permissive roles and eliminating privilege-escalation findings in two consecutive quarterly reviews

Information Security Intern, *Penske Entertainment(INDYCar)* May 2023 – Aug 2023 | Speedway, IN

- Monitored **200+ switches** and **750+ access points** with **Suricata** and **SolarWinds** to analyze traffic and reduce MTTD **rogue AP**, **beacon flood**, and **MDNS abuse**
- Executed a **firewall migration** from **Cisco ASA** to an **ESXi-virtualized** core with state sync and **failover under 1 minute** during race-season

- Automated **Azure AD** lifecycle tasks with **PowerShell**, reducing onboarding and offboarding time and eliminating orphaned accounts for seasonal staff and vendors
- Segmented **20+ VLANs** for teams, media, and operations with **QoS** and rate limits to reduce broadcast storms and congestion and validated **TLS** and **DTLS** integrity using **Wireshark**

Projects

Metasploitable 2 Hardening & Network Defense — *Metasploit, Samba, UFW, Snort, Suricata, ELK Stack*

- Used **Nmap** NSE scripts and a custom **SMB fuzzer** to identify misconfigured shares and weak NTLM authentication settings
- Migrated from default **ufw** rules to a stricter **iptables**-based approach, applying egress filtering and network segmentation
- Deployed **Suricata** sensors for in-depth packet inspection, shipping logs to **Elasticsearch** for real-time dashboards in **Kibana** (visualizing intrusion attempts, Samba exploit attempts, etc.)
- Drafted a **post-incident report** linking **MITRE ATT&CK TTPs** to each exploit, recommending more granular firewall egress filtering

Reverse Shell Exploitation & Credential Harvesting — *DVWA, msfvenom, msfconsole, Burp Suite, Meterpreter*

- Generated a **msfvenom** payload to exploit **DVWA**'s file upload vulnerability, establishing a **reverse shell** via **msfconsole** to enumerate PHP version, processes, open ports, and user accounts
- Analyzed session token randomness using **Burp Suite**'s sequencer for both **POST** (high entropy) and **GET requests**, and executed command injection in **DVWA** to extract (/etc/group) data and create directories
- Performed **XSS attacks** and exploited **CSRF** to reset DVWA admin credentials via crafted URL parameters
- **Harvested** saved Chrome browser **credentials** using a Meterpreter post module (post/windows/gather/enum_chrome)
- Produced a **Penetration Testing Report** to **justify each exploitation technique**, demonstrate **attack impact**, and **recommend secure coding practices**

Multi-VPN Architecture & Secure Remote Access — *pfSense, VyOS, IPsec, L2TP, OpenVPN, Wireshark*

- Configured **IPsec Site-to-Site** tunnels with **IKEv1** and **AES-256** encryption between **VyOS** and **pfSense**.
- Implemented **IPsec Client-Access** on **pfSense** using **RADIUS** authentication for DMZ resource access and **AD-based sign-on**
- Established **OpenVPN Site-to-Site (SSL)** tunnels to securely bridge two DMZ networks, ensuring redundancy and fault tolerance.
- Conducted traffic captures with Wireshark, verifying secure key exchanges (TLS handshake analysis)

Technical Skills

Skills: Vulnerability and Threat Analysis, Systems Designing, Secure Code designing, Intrusion Detection, Penetration Testing, Firewall Management, Network Security, Automated Scripting, Incident Response, Risk Assessment, Cyber Forensics, Cryptography

Tools: AWS S3/EC2/Athena, Nessus, Nmap, Metasploit, BurpSuite, Linux, Splunk, Suricata, Grafana, Datadog, Wireshark, Docker, Github

Frameworks & Compliance: MITRE ATT&CK, NIST CSF, GDPR, HIPAA, SOC 2

Network & Access: 802.1X (EAP-TLS), NAC, IPsec/OpenVPN, STP, BGP/ACLs, VLAN, QoS

Languages: Python, BASH, PowerShell, SQL, Rust*(learning)*

Certifications: Google Cybersecurity Professional Certificate, CompTIA Security+ (*In progress*)