# Darvin Patel

# Brisbane, QLD 4059 | +61 426908969 | [contact@darvinpatel.com](mailto:contact@darvinpatel.com) | [Linkedin](https://www.linkedin.com/in/darvinpatel/) | [Portfolio](https://portfolio.darvinpatel.com/) | [Website](https://www.darvinpatel.com/) | [Github](https://github.com/darvinpatel)

**Personal Profile:**

Dedicated Cybersecurity Analyst with a Master's Degree in Information Technology - Cybersecurity and a proven track record in Automation. Seeking the role of Threat Analyst at Cofense, leveraging extensive experience in Microsoft Azure Sentinel SIEM, along with a strong educational background and certifications.

**Education:**

• **Master of Information Technology Management** (2019 - 2021)

[The University of Sydney](https://www.sydney.edu.au/handbooks/archive/2023/engineering_pg/computer_science/information_technology_information_technology_management.html), Sydney, Australia

• **Master of Information Technology - Cybersecurity** (2019 - 2021)

[The University of Sydney](https://www.sydney.edu.au/courses/subject-areas/major/cybersecurity.html), Sydney, Australia

• **Bachelor of Computer Science and Engineering** (2014 - 2018)

[Nirma University](https://cse.nirmauni.ac.in/), Ahmedabad, India

**Certifications:**

• [Azure SC-900: Microsoft Security, Compliance, and Identity Fundamentals](https://learn.microsoft.com/en-gb/users/darvinpatel-6473/credentials/81efd02d41c7d0c5)

• [Azure SC-200: Microsoft Security Operations Analyst](https://learn.microsoft.com/en-us/credentials/certifications/exams/sc-200/) (In Progress: Projected February 2023)

• [Applied Skills: Configure SIEM security operations using Microsoft Sentinel](https://learn.microsoft.com/en-gb/users/darvinpatel-6473/credentials/b0b912c0de9aa8e5)

• [Applied Skills: Secure Azure services and workloads with Microsoft Defender](https://learn.microsoft.com/en-gb/users/darvinpatel-6473/credentials/adafbfd09e27ae7e)

• [LPI Linux Essentials](https://cs.lpi.org/caf/Xamman/certification/verify/LPI000433401/udjab7bdv6)

**Skills:**

• Scripting

• Firewalls

• Intrusion detection

• Incident response

• Threat assessment

• Threat detection

• Threat analysis

• Vulnerability management

• Malware analysis

• Security auditing

• Security assessments

• Risk management

• Forensic Analysis

• Compliance management

• Networking

• Cloud security

• Identity and Access Management(IAM)

• Splunk

• Azure Sentinel

• MS Defender for Endpoint

• Wireshark

• Security Information Event Management (SIEM)

• Security orchestration, automation, and response (SOAR)

**Home Lab/Projects:**

**-** [**Microsoft Azure Sentinel SIEM - Mapping live Brute Force global attacks**](https://github.com/darvinpatel/sentinelMap)

• Used custom PowerShell script to extract metadata from Windows Event Viewer to be forwarded to third-party API to derive geolocation data

• Configured Log Analytics Workspace in Azure to ingest custom logs containing geographic information (latitude, longitude, state/province, and country)

• Created Custom Fields in Log Analytics Workspace with the intent of mapping geo data in Azure Sentinel

• Built Azure Sentinel (Microsoft’s cloud SIEM) workbook to display global attack data (RDP brute force) on a world map according to physical location and magnitude of attacks

**-** [**Microsoft Azure Sentinel Walkthrough**](https://github.com/darvinpatel/sentinel-walkthrough/tree/main)

• Created Sentinel Log Analytics Workspace and configured Microsoft Sentinel Playbook

• Enabled Data connectors for Azure activity, Microsoft Defender for Cloud, Microsoft Defender Threat Intelligence

• Used custom analytics rules for incident management, threat hunting and intelligence

• Whitelisted IP addresses, created watchlists and bookmarks, and promoted bookmarks to incidents

• Explored Sentinel Content hub and deployed content from the catalog

**Professional Work Experience:**

**- Automation Engineer** (12/22 - Present)

[Planit](https://www.planittesting.com/au/home), Brisbane

• Deployed test scenarios using codeless AI-based tool - AccelQ

• Reviewed, estimated, and identified test conditions and objectives, while ensuring appropriate testing coverage

• Create relevant test plans and reports while contributing to high-level documentation

• Mentored internal and external peers across cross-functional teams to promote a culture of knowledge-sharing

• Demonstrated a solid understanding of modern application deployment methodologies and cloud infrastructures, with in-depth experience across the SDLC

• Deployed Agile development practices using Azure DevOps

**Technologies used:** [AccelQ](https://www.accelq.com/), Azure DevOps,

**Achievement:** Lead the team in the absence of the Team Lead. Managed to automate more than 70% of manual tests with over 90% stable tests in AccelQ

**-** **Technology Associate** (02/22 - 12/23)

[Infosys](https://www.infosys.com/australia/), Sydney

• Wrote clean, readable, and easily maintainable Java code for scalable and robust frameworks that can be used to automate tests

• Created Automated test cases from scratch for APIs and GUIs along with manual testing

• Prepared extensive test reports and documented all the analytical insights

**Technologies used:** Postman, IntelliJ, Java, Selenium

**Achievement:** Tested a feature end to end within a sprint working across global teams with minimal requirements and documentation

**- QA Engineer** (04/21 - 02/22)

[Effision](https://effision.com/), Sydney

• Worked on software testing for MPGS - MasterCard Payment Gateway Services as part of Continuous Integration, Continuous Delivery (CI/CD)

• Reviewed the product code throughout the development lifecycle with the highest integrity and security

• Performed automation testing - Unit, Functional, Performance, Integration, System, Regression, Smoke, and User acceptance testing

**Technologies used:** Jenkins, Splunk, Putty, Java, Selenium, Postman, Confluence

**Achievement:** Documented the entire regression testing process with one team and trained others using that document. Thus improving testing coordination, eventually saving 50% of the time that was consumed with requirement gathering and resolving the defects

**Membership:**

• Association of Professional Engineers Australia ([APEC](https://www.professionalsaustralia.org.au/))

* • Australian Computer Society ([ACS](https://www.acs.org.au/))

**Referees:**

[**Martin Schacher**](https://schacher.ch/)

CEO, Anooky

(Former)Senior Test Automation Consultant, Planit

Email: [martin@schacher.ch](mailto:martin@schacher.ch)

Ph no.: +41 788051213

[**Fabio Costa**](https://www.linkedin.com/in/fabio-costa-developer/)

Senior Full Stack Software Engineer, ASX

(Former)Java Application Developer, Effision

Email: [fabio.costa.ti@gmail.com](mailto:fabio.costa.ti@gmail.com)

Ph no.: +61 458960461