

PHILIPS RHOGUNS

DATA AND INFRASTRUCTURE ENGINEER

Toronto, ON | orhogun@gmail.com | github.com/prhoguns | LinkedIn | Portfolio

PROFILE

I build data pipelines and the systems that run them: PostgreSQL warehouses, dbt and Airflow workflows, Linux server automation, cloud infrastructure, and security monitoring. My work includes tested recovery and failover drills, live data loads, and detection rules with repeatable checks. Previously led a shift in York University's 24/7 campus security control room, with responsibility for escalation, incident reports, and operator training.

TECHNICAL SKILLS

Data engineering: SQL, Python, PostgreSQL, DuckDB, dbt, Apache Airflow, pandas, PySpark, Databricks, Delta Lake, Kafka/Redpanda, dimensional modelling, data quality testing, Power BI, MLflow

Infrastructure and cloud: Linux (Ubuntu, RHEL), Bash, Ansible, Docker/Compose, Terraform, Bicep, GitHub Actions, AWS (EC2, S3, Lambda, IAM, CloudTrail), Azure (ADLS Gen2, Data Factory, Synapse, Key Vault)

Databases and identity: PostgreSQL replication, WAL archiving, point-in-time recovery, indexing, EXPLAIN ANALYZE, roles and grants; Windows Server, Active Directory, Group Policy, Intune, PowerShell

Security and networking: Wazuh, Microsoft Sentinel, Splunk, Sigma/pySigma, MITRE ATT&CK, Zeek, Suricata, Wireshark, Trivy, CISA KEV, EPSS, TCP/IP, DNS, OSPF, BGP, pfSense

Business tools: Power Apps, Power Automate, Dataverse, Microsoft 365, osTicket, Tableau, Excel; incident documentation and stakeholder communication

PROFESSIONAL EXPERIENCE

York University | Security Operations Centre Team Lead | Toronto, ON | Mar 2023 – Jan 2025

- Led a 24/7 control-room shift supporting two campuses and a community of more than 50,000 students and staff; monitored CCTV, access control and alarm systems.
- Served as first point of escalation; coordinated mobile security and decided when to involve Toronto Police, Fire, EMS, and university management.
- Reviewed and signed off incident reports and shift logs, wrote serious-incident reports, trained new operators on systems and escalation procedures, and coordinated equipment-fault repairs.

York University | Security Control Room Operator | Toronto, ON | Jul 2022 – Mar 2023

- Answered emergency and non-emergency calls, documented incidents, dispatched mobile units by radio, and retrieved footage and access records for investigations.

Larry the Liquidator | Floor Manager | Scarborough, ON | Sep 2021 – 2022

- Supervised daily store operations, staff, inventory, opening and closing, and cash reconciliation.

SELECTED ENGINEERING PROJECTS

Toronto Open Data Pipeline | Python, PostgreSQL, dbt, Airflow, FastAPI

- Built a City of Toronto ELT pipeline with PostgreSQL loading, 11 dbt models, 40 data-quality tests and Airflow orchestration; documented run results and limitations.
- Added a prototype TTC delay model and compared it against a historical-rate baseline; retained the unsuccessful comparison in the project documentation.

PostgreSQL DBA Toolkit | PostgreSQL 16, Docker, replication, PITR

- Built a primary/replica lab with WAL archiving. Recovery drill restores a dropped 500,000-row table to a target time; failover drill promotes the standby and verifies writes.
- Wrote diagnostics and DBA runbooks; identified an unindexed foreign key and measured a query improvement from 24.9 ms to 0.2 ms after indexing.

Ansible Server Baseline | Ansible, Ubuntu, CIS checks

- Created eight roles for Linux users, SSH, firewalls, storage, auditing, patching and monitoring. Verified a second run made zero changes and 41 selected hardening checks passed.

Azure Toronto Data Platform | Bicep, Data Factory, ADLS Gen2, Databricks, Synapse

- Rebuilt the Toronto pipeline with managed identities and bronze/silver/gold PySpark notebooks; checked output row counts against the local dbt build.

TTC Real-Time Pipeline | GTFS-Realtime, Kafka, PostgreSQL

- Streamed TTC vehicle positions through Kafka into an idempotent PostgreSQL sink; exposed route activity and derived speed in SQL views.

Toronto Crime SQL Analytics | DuckDB, SQL, Plotly

- Answered 20 business questions over a decade of Toronto crime data with reproducible SQL, a findings report and an interactive dashboard.

Credit Default Risk | PySpark MLlib, MLflow

- Compared logistic regression and boosted trees on a 30,000-customer dataset; tracked parameters and metrics in MLflow and registered a model for batch scoring.

SECURITY, NETWORK AND SUPPORT PROJECTS

Sigma Detection Pack | Sigma, pySigma, Splunk SPL, Sentinel KQL

- Authored 11 intrusion-chain detection rules, converted them across query languages and tested each against planted positives and near-misses in CI.

SOC Alert Analytics | SQL, Wazuh, scikit-learn

- Analysed 45,000 SIEM alerts for noisy rules, triage time and ATT&CK gaps; evaluated anomaly detection against planted incidents.

Network Automation Lab | FRRouting, OSPF, BGP, Jinja2, pytest

- Generated six-router configurations from YAML and verified adjacencies, routing policy and reachability with 22 live-topology tests.

Vulnerability Prioritization | Trivy, CISA KEV, EPSS, SQL

- Scanned 10 container images, then reduced 3,934 findings to a 95-item P0/P1 action queue using exploit and fixability signals.

Directory Services Lab | Samba AD, Kerberos, LDAP, winbind

- Provisioned a domain and Linux client with user lifecycle controls; 30 checks cover authentication and offboarding behavior.

AWS Security Auto-Remediation | Terraform, GuardDuty, Config, Lambda

- Built event-driven remediation for public S3 access and risky security-group ingress with least-privilege IAM, dry-run support and mocked tests.

PCAP Threat Hunting | Zeek, DuckDB, scapy

- Analysed synthetic network traffic for planted C2 beaconing, DGA lookups and exfiltration using timing, entropy and traffic-asymmetry features.

Home SOC and Help Desk Labs | Wazuh, Sysmon, Windows Server, Intune, osTicket

- Built lab workflows for SIEM triage, Active Directory account support, workstation policy and common service-desk tickets; documented simulated incidents and escalation decisions.

CERTIFICATIONS AND EDUCATION

Certifications: CompTIA Security+ | AWS Certified DevOps Engineer – Professional | Microsoft Certified: Power Platform Developer Associate (PL-400) | Google Cybersecurity Professional Certificate

Education: Bachelor of Science, Computer Science | York University, Toronto, ON