PHILIPS RHOGUNS

Toronto, ON | orhogun@gmail.com | linkedin.com/in/philips-rhoguns-266748180 | github.com/prhoguns

Junior Security & Network Engineer | SOC, Detection Engineering, Cloud Security, Network Automation

SUMMARY

Computer Science student with two and a half years in York University's 24/7 security operations centre, first as an operator and then as team lead. Since then I have been building the technical side and can show it running: a six-router OSPF/BGP lab with automated tests, AWS auto-remediation for GuardDuty and Config findings, a Sigma detection pack, Zeek-based threat hunting and a KEV/EPSS vulnerability queue. CompTIA Security+ and AWS Certified DevOps Engineer – Professional.

SKILLS

Security operations: SIEM (Wazuh, Microsoft Sentinel, Splunk), alert triage, incident response and reporting, threat hunting, MITRE ATT&CK, NIST CSF, Sigma rules, Sysmon, Zeek, Suricata (IDS/IPS), Wireshark
Cloud security: AWS (CloudTrail, GuardDuty, Config, EventBridge, Lambda, IAM least privilege), Azure (Entra ID, Sentinel, Defender for Cloud), Terraform, Bicep
Networking: TCP/IP, OSPF, BGP (route-maps, prefix-lists, local-preference, aggregation), DNS, DHCP, VLANs, VPN, firewalls (pfSense, Palo Alto, Cisco ASA/Meraki), FRRouting, packet analysis
Systems: Linux (Ubuntu, RHEL), Windows Server, Active Directory, Group Policy, Intune, Docker
Vulnerability management: Trivy, CVSS, EPSS, CISA KEV, patch prioritization, container image hardening
Automation: Python (boto3, scapy, pandas), PowerShell, Bash, SQL, KQL, Jinja2, GitHub Actions, pytest

CERTIFICATIONS

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

PROJECTS

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

- Six-router lab in Docker: OSPF backbone, iBGP full mesh, and eBGP to two upstream ISPs with bogon filtering, aggregate-only advertisement and local-preference steering. All configs come from one YAML file through a Jinja2 template.
- 22 tests run against the live routers and check adjacencies, sessions, policy and end-to-end reachability. CI boots the whole topology on every push.

AWS Security Auto-Remediation *Terraform, Lambda, EventBridge, GuardDuty, Config*

- CloudTrail, GuardDuty and Config findings route through EventBridge to a Lambda that blocks public S3 buckets, revokes world-open ingress on risky ports without touching legitimate rules, and deactivates keys on credential-compromise findings. Root logins are alert-only on purpose.
- Least-privilege IAM, a dry-run switch, every action logged to SNS. Nine tests against mocked AWS.

Sigma Detection Pack *Sigma, pySigma, Splunk, Sentinel KQL*

- Eleven detection rules for an intrusion chain (encoded PowerShell, LSASS access, privileged-group changes, Cobalt Strike named pipes, Defender tampering, SSH root from external), converted to SQL, SPL and KQL. CI tests each rule against a corpus with planted positives and near-misses.

PCAP Threat Hunting *Zeek, DuckDB, scapy*

- Eight hours of synthetic office traffic with a planted C2 beacon, DGA and exfiltration, run through Zeek and hunted in SQL. Beacon found by timing regularity, DGA by DNS entropy, exfil by byte asymmetry. None would trip a signature; all three ranked first.

Vulnerability Prioritization *Trivy, CISA KEV, EPSS*

- Scanned ten container images (3,934 findings) and tiered them with KEV and EPSS: 95 need action, 47% have no fix. A current nginx image was shipping HTTP/2 Rapid Reset, marked LOW by the distro but in KEV.

SOC Alert Analytics *Wazuh, SQL, scikit-learn*

- Noisy-rule tuning, time-to-triage SLAs, ATT&CK coverage gaps and attack-chain reconstruction over 45K alerts, plus Isolation Forest anomaly detection checked against planted incidents.

EXPERIENCE

Security Operations Centre Operator, then Team Lead | York University, Toronto, ON *Jul 2022 – Jan 2025*

- Monitored CCTV, access control and alarm systems for two campuses. As team lead: first point of escalation, decided when to bring in Toronto Police, Fire or EMS, signed off incident reports and shift logs, trained new operators.

EDUCATION

Bachelor of Science, Computer Science | York University, Toronto, ON *Expected December 2026*