PHILIPS RHOGUNS

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

Security Analyst | SOC Tier 1 / Level 1 | CompTIA Security+ | AWS Certified

SUMMARY

Computer Science student with experience in a 24/7 campus security operations centre, first as an operator and then as a team lead: triaging alerts, deciding what to escalate to police and emergency services, and writing incident reports that hold up in investigations. CompTIA Security+ and AWS certified. Run a home SOC lab on Wazuh and Microsoft Sentinel and have built log monitoring and alerting in AWS and Azure. Looking for a SOC analyst or security analyst role in Toronto.

CERTIFICATIONS

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

SKILLS

Security operations: SIEM (Wazuh, Microsoft Sentinel, Splunk), Sigma rules and pySigma, alert triage and escalation, incident response and reporting, MITRE ATT&CK, Sysmon, Suricata, Wireshark, Windows Event Logs, syslog

Cloud security: AWS (CloudTrail, VPC Flow Logs, GuardDuty, IAM, EventBridge, Lambda), Azure (Entra ID, Log Analytics, Defender for Cloud)

Systems and networking: Linux (Ubuntu, RHEL), Windows Server 2022, Windows 10/11, Active Directory, Group Policy, pfSense, TCP/IP, DNS, VLANs, VPN

Scripting and analysis: Python (pandas, scikit-learn), PowerShell, Bash, KQL, SQL (DuckDB, PostgreSQL)

EXPERIENCE

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

- Led a shift of control room operators monitoring CCTV, access control, and alarm systems across two campuses, around the clock, for a campus community of more than 50,000 students and staff.
- First point of escalation on shift: decided when to dispatch mobile security, call Toronto Police, Fire, or EMS, and notify university management.
- Reviewed and signed off on operators' incident reports and shift logs; wrote the reports for serious incidents myself, in enough detail to be used in investigations.
- Trained new operators on SOPs, monitoring systems, and escalation paths.

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

- Monitored live CCTV, door access alerts, and alarm panels, dispatched mobile units by radio, logged every call in the incident management system, and pulled footage and access records for investigations.

PROJECTS

Home SOC Lab *Wazuh, Sysmon, Suricata, pfSense*

- Wazuh SIEM on Ubuntu collecting Sysmon and Windows event logs from a Windows 11 VM, syslog from a Linux host, and firewall and IDS alerts from pfSense and Suricata.
- Custom detection rules for brute-force logins, new local admin accounts, and suspicious PowerShell, mapped to MITRE ATT&CK and tuned to cut false positives.
- Ran simulated attacks (Hydra, Mimikatz) in an isolated network and wrote each one up as a Tier 1 ticket: what fired, what I checked, what I would escalate.

SOC Alert Analytics (github.com/prhoguns/soc-alert-analytics) *SQL, DuckDB, Wazuh, MITRE ATT&CK*

- SQL analysis of 45K Wazuh alerts and triage logs (noisy-rule tuning, time-to-triage SLAs, ATT&CK coverage gaps, attack-chain reconstruction) plus Isolation Forest anomaly detection with per-host baselines, evaluated against planted incidents: all three ranked in the top 65 of 13,675 host-hours, including a quiet lateral movement no volume rule finds.

Sigma Detection Pack (github.com/prhoguns/sigma-detection-pack) *Sigma, pySigma, Splunk SPL, Sentinel KQL*

- Eleven detection rules covering an intrusion chain (encoded PowerShell, LSASS access, privileged group changes, Cobalt Strike pipes, Defender tampering, SSH root from external), converted to SQL, SPL and KQL with pySigma and tested in CI against a corpus with planted positives and near-misses: every rule must match exactly.

AWS Security Monitoring *CloudTrail, GuardDuty, Lambda, Python*

- CloudTrail and VPC Flow Logs from two accounts to a central logging account; EventBridge and GuardDuty alerts for root logins, security group changes and public S3 buckets.

EDUCATION

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