

# [Full name]

## 24 x 7 Security Operations Center Associate | OneStep Group

Perth WA | [Australian mobile] | [Email address]

*Fictional resume example. All credentials, experience and results are illustrative.*

### Professional profile

Early-career security analyst with one year of combined internship and hands-on lab experience monitoring alerts across endpoint, network and cloud environments. Comfortable triaging SIEM and XDR signals, collecting evidence, documenting incident timelines and escalating according to severity and customer impact. Brings practical Microsoft Sentinel and Defender XDR exposure, introductory KQL, PowerShell and Python, and a strong interest in detection engineering, threat hunting and security automation.

### Relevant skills

**SOC monitoring:** Alert triage, incident investigation, severity assessment, evidence preservation, case notes and escalation.

**Microsoft security platforms:** Microsoft Sentinel, Defender XDR, endpoint, network and cloud telemetry, dashboards and platform health.

**Detection and hunting:** KQL queries, detection-rule tuning, threat hunting, false-positive analysis and documented investigation methods.

**Automation and client support:** PowerShell, Python, automated workflows, integrations, technical documentation and clear managed-service communication.

### Relevant experience

#### Security Operations Intern | Example Managed Security Provider

Perth WA | November 2025 - August 2026

- Triaged 30 weekly Sentinel and Defender XDR alerts, recorded scope and evidence, and escalated confirmed or high-risk events to senior analysts.
- Investigated endpoint, identity, network and cloud telemetry using KQL, timelines and user context, distinguishing benign activity from suspicious patterns.
- Tuned five lab detection rules and documented before-and-after false-positive results without suppressing required security coverage.
- Built two supervised PowerShell and Python workflow helpers for enrichment and case formatting, retaining analyst review before any action.

- Prepared client-ready incident summaries with affected assets, actions, outstanding risk and next update time and joined roster handovers.

## **Selected projects**

### **Microsoft SOC Investigation Lab**

*Cyber security capstone | 2026*

- Built a 40-alert endpoint, identity and cloud dataset using Microsoft Sentinel, Defender XDR, KQL and incident-response workflows, with documented scope, assumptions and safe operating boundaries.
- Executed and recorded 40 investigation records and a severity-based escalation matrix, including expected results, exceptions, verification steps and escalation points.
- Presented the evidence to a supervisor or peer reviewer, incorporated feedback and published a concise handover for repeat use.

### **Detection and Automation Improvement Project**

*Security engineering project | 2026*

- Built five detection rules and two analyst-assist workflows using KQL, PowerShell, Python, false-positive analysis and documentation, with documented scope, assumptions and safe operating boundaries.
- Executed and recorded a tuning report, reviewed scripts and 20 regression tests, including expected results, exceptions, verification steps and escalation points.
- Presented the evidence to a supervisor or peer reviewer, incorporated feedback and published a concise handover for repeat use.

## **Education**

### **Bachelor of Cyber Security | Example University**

Completed 2026. Relevant study: security operations, incident response, network security, cloud security, digital forensics, Python, PowerShell and governance.

### **Availability and requirements**

Available for full-time work in Perth and rostered or after-hours support by agreement. Australian citizenship: [confirm status for potential government security-clearance eligibility]. Australian work rights: [confirm status].

### **References**

References available upon request.