AYUSH BABARIA

ayushbabariya601@gmail.com | (306)-550-9931
Regina, SK, Canada | LinkedIn

PROFESSIONAL SUMMARY

Third-year Computer Science student at the University of Regina with foundational cyber security knowledge and hands-on SOC-style lab practice in alert triage, basic investigation, and clear incident documentation, plus frontline POS/kiosk troubleshooting experience.

Skills and Abilities

- **Security:** SIEM (Elastic/Splunk – lab), alert triage, incident documentation, phishing analysis, MITRE ATT&CK, basic hardening, runbooks/playbooks
- **Platforms:** macOS, Windows, Linux; PowerShell (basic); Git; zsh/Bash basics.
- **Networking:** TCP/IP, DNS, HTTP; basic packet analysis
- **Programming:** Python, SQL, JavaScript; Flask for internal tools

Projects

- **SOC Alert Triage & Playbooks**
  - **Context:** Personal lab; Python, Pandas, JSON/CSV logs, MITRE ATT&CK, Markdown runbooks.
  - Triaged 300+ simulated endpoint and network alerts across brute force, suspicious script execution, and new admin creation use cases; prioritized by severity with simple rules.
  - Reduced false positives by 28% after two tuning iterations and enrichment of macOS Unified Log exports and user/account context.
  - Cut average time-to-triage from 6.5 to 3.8 minutes using standardized playbooks and a Python enrichment script.
  - Authored 3 incident playbooks and a handoff-ready incident report template with MITRE technique mapping.
    - **Technologies:** Python, CSV/JSON logs, Regex; macOS Unified Log (log show) exports; optional osquery for process/auth artifacts; Git.
- **Phishing Simulation & Takedown Workflow**
  - **Context:** Personal lab/club test; mailbox triage checklist, training one-pager, decision tree.
  - Ran 4 small-scale phishing simulations (120 sends total) and tracked open/click/report metrics to iteratively improve messages and training.
  - Improved report rate from 22% to 46% after two training iterations and clearer reporting instructions.
  - Standardized a 10-step phishing triage and takedown checklist covering header review, SPF/DKIM/DMARC note, URL expansion, and purge steps.
  - Defined containment communications templates and escalation triggers to SOC/IT with ticket linkage.
    - **Technologies:** Apple Mail/Gmail, email headers, SPF/DKIM/DMARC checks, curl for URL expansion, zsh/Bash basics, Git.
- **Endpoint Hardening & Compliance Tracker**
  - **Context:** Flask, SQLite; weekly compliance scoring and reports.
  - Extended an asset tracker to capture patch currency, AV status, full-disk encryption, remote access exposure, and local admin presence using CIS-style checks for macOS (e.g., FileVault, Firewall, auto updates).
  - Generated weekly compliance reports and raised baseline compliance from 62% to 88% in a lab by prioritizing updates and remote-access hardening tasks.
  - Cut asset lookup time by 40% with filterable views and JSON exports for audit snapshots.
    - **Technologies:** Python, Flask, SQLite; macOS baseline checks (FileVault, Firewall, auto updates, admin group); simple RBAC; JSON export; Git.

WORK EXPERIENCE

Team Member | BarBurrito — April 2024 - Present

- Diagnosed POS/kiosk incidents and escalated with clear replication steps and logs, reducing average downtime during busy periods.
- Followed structured procedures for configuration and cash-out reporting; created one-page job aids that reduced repeated questions across shifts.
- Communicated technical issues to non-technical staff clearly and calmly in a fast-paced environment, supporting teamwork and service quality.

Sandwich Artist | Subway Restaurants — January 2024 – March 2024

- Troubleshot POS errors under time pressure and escalated per workflow to minimize order delays.
- Maintained accurate cash handling and closing reports aligned to documented procedures.

Education

Bachelor of Science – Computer Science Major — January 2024 - Present

University of Regina, Regina, SK

Certifications and labs

- Udemy/Self-study: SOC Fundamentals (in progress); macOS logging and hardening labs (Unified Log, FileVault, Firewall).
- Hands-on labs: Alert triage, phishing analysis, incident documentation, endpoint hardening (20+ hours).

Extras

- Activities: Member, University cyber club; Volunteer tech support at campus events.
- Languages: English, Hindi.

References

Dr. Lisa Fan
Instructor
University of Regina, Regina, SK
Lisa.Fan@uregina.ca

Manak Singh
Instructor
University of Regina, Regina, SK
msz916@uregina.ca

Sathyajit Loganathan
Instructor
University of Regina, Regina, SK
slv958@uregina.ca

Kamlesh Vaghasia
Manager
BarBurrito, Regina, SK
+1 (306) 209-9711