Lucas Buchli

425-442-7120 • lucasbuchli23@gmail.com • LinkedIn

Experience

Information Security Intern, *Port of Seattle* *2/2025-2/2026*

- Administered Archer GRC platform for vendor risk management during enterprise implementation, mapping 7 vendor profiles and 10 organizational risks with CIS controls using NIST CSF 2.0, configuring RBAC for 8 departments, and resolving 50+ critical configuration errors across 3 environment migrations
- Compiled and validated 200+ IoCs (IPs and URLs) from threat intelligence feeds and OSINT using reputation databases for Microsoft Defender EDR ingestion to enhance threat detection, blocking, and hunting capabilities
- Researched and profiled 6 APT groups (Scattered Spider, SideWinder, Syrian Electronic Army, APT32, APT36) through campaign analysis and cross-referencing TTPs with MITRE ATT&CK framework using SOCRadar intelligence, informing threat intelligence strategies
- Conducted 33 software security assessments across all Port departments in 4 months, leveraging CVE/CISA databases and OSINT to identify critical vulnerabilities, compiled vendor risk documentation (ToS, EULA, privacy policies), and delivered risk-based recommendations for procurement decisions
- Designed and developed web-based incident response tabletop exercise simulating AI-enabled denial of service scenario using a Python script to demonstrate attack progression for executive leadership and InfoSec stakeholders

Trainings & Professional Development

Airport Cybersecurity Training (Certified), *Department of Homeland Security* *9/11-12/2025*

- Completed hands-on wireless security assessment training at Seattle Paine Field Intl Airport (PAE), identifying simulated vulnerabilities and security gaps through packet capture and RF traffic analysis (Aircrack-ng, Wireshark, Kali Linux)
- Analyzed wireless network traffic to identify encryption protocols (WEP/WPA2), deauthentication attack patterns, and WiFi access point misconfigurations in controlled training scenarios

ThinkCyber UW Chapter, *University of Washington* *10/2025-Present*

- Won zero-day vulnerability tabletop exercise among competing teams, presenting incident response strategy to cybersecurity professionals from Boeing and Microsoft
- Served dual Blue Team and Red Team roles for 4-person team, analyzing proof-of-concept SQL injection exploit, investigating indicators of compromise, and developing comprehensive risk management plan for simulated cloud platform breach
- Participated in Blue Team IR Workshop (CrowdStrike) covering healthcare breach simulation, incident triage, containment, and recovery phases

TryHackMe *9/2025-Present*

- Active participant in hands-on cybersecurity training labs covering pen testing, network security, and threat detection

Technical Skills

- Security Tools: Microsoft Defender for Endpoint, Archer GRC, Shodan, Wireshark, Aircrack-ng, Cisco Talos, URLScan.io, SOCRadar, CVE Details, CISA Known Exploited Vulnerabilities, SIEMs
- Frameworks & Standards: MITRE ATT&CK, NIST CSF 2.0, CIS Controls
- Programming/Scripting & Version Control: Python, Java, R, HTML/CSS, SQL, React, Git/Github
- Networks and Systems: Windows, Linux, Networking Basics
- Security Concepts: Threat Intelligence, Privileged-access Concepts, Incident Response, Log Analysis, Vulnerability Management, Risk Assessment, Open Source Intelligence, GRC, Threat Modeling

Education

The University of Washington, *Seattle* *Expected Graduation: June 2026*

- BS in Informatics: focus in Cybersecurity, GPA: 3.82