

GABRIEL SANTA ROSA LESSA

Vancouver, BC, Canada

Phone: [REDACTED] | Email: [REDACTED]

LinkedIn: <https://www.linkedin.com/in/gabriel-santa-rosa-lessa/>

Portfolio: <https://lessa-github.github.io/gabriel-portfolio/> | GitHub: <https://github.com/lessa-github>



SUMMARY OF QUALIFICATIONS

- 1+ year of hands-on academic experience in cybersecurity, threat intelligence, cloud infrastructure, and risk management through CCTB coursework, applied projects, and technical labs.
- Architect and maintain a 24/7 dedicated Proxmox VE HomeLab hosting 12+ isolated LXC containers, OPNsense firewall routing, Wazuh SIEM telemetry, and WireGuard Zero Trust mesh VPN.
- Practical knowledge of the Software Development Life Cycle (SDLC), with security considerations across planning, analysis, design, implementation, testing, deployment, and maintenance.
- Developed cloud-based security lab environments on AWS EC2 using Ubuntu Linux, Amazon Linux, and Windows Server, including distributed monitoring and log-analysis infrastructure.
- Practical experience conducting Cyber Threat Intelligence (CTI) investigations, mapping complex adversary tactics (credential dumping, spearphishing attachments, Pass-the-Hash) to the MITRE ATT&CK framework.
- Hands-on proficiency with network reconnaissance, packet crafting, and traffic analysis using Nmap, Scapy, Wireshark, tcpdump, and pfSense on Kali Linux environments.
- Knowledge of enterprise security architecture and SOC operational workflows, designing defense-in-depth frameworks, RACI matrices, and incident response procedures aligned with NIST CSF 2.0 and NIST SP 800-61.
- Strong background in network administration and API automation, connecting Python/Django backends with REST APIs (Cisco DNA Center, OpenRouteService) under Git version control.
- Operating systems and tools: Windows, Linux (Ubuntu, Kali, Debian), Proxmox VE, OPNsense, Wazuh, WireGuard, AWS EC2, Cisco Packet Tracer, Nmap, Scapy, Wireshark, tcpdump, pfSense, Python, Django, MongoDB, Bash, and Git.

TRANSFERABLE SKILLS

- Analytical Problem-Solving & Troubleshooting: Proven capability to perform root-cause analysis, diagnose complex network/system anomalies, and isolate technical faults systematically under operational pressure.
- Technical & Cross-Functional Communication: Experienced in translating intricate technical findings, CTI reports, and risk assessments into clear, actionable documentation for non-technical stakeholders.
- Process Adherence & Security Compliance: High rigor in following standard operating procedures (SOPs), defense-in-depth frameworks, NIST guidelines, and maintaining documentation hygiene.
- Incident Prioritization & Composure: Strong ability to triage concurrent alerts, handle escalation workflows efficiently, and maintain professional focus in time-sensitive incident response scenarios.

RELEVANT EXPERIENCE:

2025 – Present

Personal Cybersecurity Infrastructure Vancouver, BC

Enterprise Zero-Trust HomeLab & SOC Infrastructure - Technical Project

Architected and maintain an enterprise-grade virtualization homelab on dedicated hardware, implementing Zero Trust access, endpoint telemetry, and network isolation to simulate production security operations.

- Deployed and manage 12+ production microservices on Proxmox VE 9.x across isolated, unprivileged LXC containers and security virtual machines.
- Virtualized an OPNsense firewall with VLAN segmentation, NAT masquerade, and air-gapped subnets for safe malware analysis and traffic isolation.
- Configured Wazuh SIEM/XDR agents across Linux and Windows hosts for centralized log collection, rule-based alerting, and proactive threat detection.
- Enforced Zero Trust access via encrypted WireGuard mesh VPN, eliminating public port exposure, paired with Ed25519 SSH keys and Authentik SSO (WebAuthn / Passkeys MFA).
- Engineered a Zero-Knowledge secret management architecture (lab-vault Python/Bash CLI) with blind in-memory injection, canary traps, and real-time output sanitization to govern autonomous AI agents and automation scripts.
- Tools utilized: Proxmox VE, OPNsense, Wazuh SIEM, WireGuard, Authentik SSO, lab-vault (Zero-Knowledge Engine), Python, Bash CLI, Docker, and Debian.

2026

Canadian College of Technology and Business Vancouver, BC

Cyber Threat Intelligence (CTI) & Adversary Intrusion Assessment - Academic Project

Analyzed a multi-stage enterprise intrusion scenario involving spearphishing attachments (.docm), PowerShell execution, and SAM registry credential dumping to mitigate risk and recommend defensive controls.

- Evaluated risk exposure associated with Pass-the-Hash attacks (T1550.002), SAM registry credential access (T1003.002), and lateral movement across internal networks.
- Mapped threat actor tactics and techniques directly to the MITRE ATT&CK framework across initial access, execution, persistence, and credential access phases.
- Authored a comprehensive CTI assessment report recommending immediate host isolation, forensic evidence preservation, credential rotation, and proactive detection rules.
- Applied incident response workflows aligned with NIST SP 800-61 and NIST Cybersecurity Framework 2.0 to establish containment and remediation strategies.
- Tools utilized: MITRE ATT&CK, Cyber Threat Intelligence (CTI), PowerShell, Registry Analysis, NIST SP 800-61, and NIST CSF 2.0.

2026

Canadian College of Technology and Business Vancouver, BC

Enterprise Security Architecture & SOC Operating Model - Academic Project

Designed a secure, multi-site enterprise network architecture and operational framework to protect a central HQ Data Center, DMZ environment hosting 200 VMs, and 7 remote branch locations.

- Implemented strict network segmentation between internal LANs, DMZ zones, and remote branch links to enforce defense-in-depth security principles.
- Defined a complete Security Operations Center (SOC) operational framework, establishing a detailed RACI matrix across Tier 1–3 analysts, Threat Hunting, DFIR, and Detection Engineering functions.
- Integrated enterprise security controls including Palo Alto WildFire sandboxing, Thinkst Canary honeypots, Proofpoint email protection, and Microsoft Defender for Endpoint.
- Developed incident response escalation procedures and detection engineering workflows aligned with NIST Cybersecurity Framework 2.0.
- Tools utilized: Defense-in-Depth, SOC Operating Model, RACI Matrix, NIST CSF 2.0, Palo Alto NGFW, Thinkst Canary, and Proofpoint.

2025-2026

Canadian College of Technology and Business Vancouver, BC

AWS Cloud Infrastructure & Database Security Automation - Academic Project

Built and deployed multi-tier web applications on AWS EC2 instances, establishing secure database connectivity between Python/Django backends and remote MongoDB nodes.

- Provisioned and configured AWS VPC subnets, DHCP Option Sets across EC2 instances, Application Load Balancers (Least Connection algorithm), and granular Security Group inbound rules.
- Developed Python scripts to integrate external REST APIs (Cisco DNA Center, OpenRouteService), utilizing Git version control with multi-branch workflows (main, dev, feature1).
- Configured Linux server environments (Ubuntu, Amazon Linux) and managed services, firewall rules, ports, permissions, and environment variables via Bash CLI.
- Validated API endpoints, database queries, and load balancing traffic distribution under simulated client workloads.
- Tools utilized: AWS EC2, VPC, Load Balancing, Python, Django, MongoDB, REST APIs, Git/GitHub, and Linux CLI.

EDUCATION

2025 – 2028 Canadian College of Technology and Business Vancouver, BC

Cybersecurity Risk Management with Co-op Diploma (Expected May 2028)

- Relevant study: SIEM, incident response, network security, threat intelligence, cloud security, Linux and Windows security, risk management, and business continuity.

2020 – 2022 Estácio de Sá University Brazil

Associate Degree in Cyber Defense