WISTON LESTIN

Cybersecurity Professional – Detection & Response | Security Automation | Cloud Security

Sorel-Tracy (Quebec), Canada | Mobile: 514 655-9924 | Email: wislest@gmail.com

LinkedIn: www.linkedin.com/in/wiston-lestin | Languages: French (native), English and Spanish (professional working proficiency)

PROFESSIONAL SUMMARY

Cybersecurity professional specializing in Detection Engineering, Incident Response, and security automation across enterprise and cloud environments. Proven track record in building scalable detections, implementing Detection-as-Code, leading high-pressure incident investigations, and developing SOAR playbooks that reduce MTTR significantly. Skilled in Microsoft Security Stack (Sentinel, Defender XDR, Defender for Cloud), with adaptability to AWS and GCP. Strong advocate for blameless incident culture, proactive threat hunting, and aligning detection strategy with business objectives.

CORE COMPETENCIES

Detection & Response: Detection-as-Code, behavioral analytics tuning, false positive reduction, MITRE ATT&CK mapping
Incident Response: Incident command, containment & remediation, forensic investigation, root cause analysis
Threat Hunting: Hypothesis-driven hunts, advanced KQL queries, cross-platform telemetry analysis
Security Automation (SOAR): Playbook design (Microsoft Sentinel, Logic Apps), automated triage, enrichment & containment
Cloud Security: Azure (expert), AWS & GCP (rapid adaptation), cloud logging & monitoring, GuardDuty, CloudTrail
Programming & Tools: KQL, Python, PowerShell, Terraform, CI/CD, EDR tools, Splunk, Elastic, Microsoft Graph API

CERTIFICATIONS

- CompTIA CASP+ (Advanced Security Practitioner)
- CompTIA Pentest+ | CompTIA CySA+ | CompTIA Security+
- Microsoft Azure Fundamentals (AZ-900)
- ISC^2 Certified in Cybersecurity
- ICSI Certified Network Security Analyst

PROFESSIONAL EXPERIENCE

Security Analyst - Detection & Response Operations

TC Transcontinental | Jan 2023 – Present

• Developed and optimized Sentinel detection rules, reducing false positives by 40%.
• Built automated detection pipelines and SOAR playbooks, cutting MTTR by 50%.
• Led incident response for critical security events across 7,000+ endpoints.
• Integrated threat intelligence for proactive threat-based detections.
• Enhanced security logging and visibility in collaboration with infrastructure teams.

Security Detection Analyst

Desjardins | Apr 2022 – Nov 2022

• Created and tuned detection rules for financial sector threats, reducing false positives by 50%.
• Managed high-volume alerts in a regulated environment.
• Collaborated with IT and compliance teams to enhance response capabilities.

Information Security Specialist - Detection Engineering

Hitachi Systems Security | Oct 2021 – Apr 2022

• Developed enterprise SIEM detection rules and runtime security monitoring.
• Conducted proactive threat hunting using MITRE ATT&CK.
• Managed EDR platforms and performed forensic investigations.

PROJECTS

• Network Share Enumeration System– Built automated PowerShell tool that analyzes permissions, integrates with CMDB systems, and auto-generates remediation workflows in ServiceNow.
• DefenderHunter Detection Framework– Developed comprehensive PowerShell-based threat hunting and detection system integrated with Microsoft Defender XDR and Sentinel for automated threat investigations.
• AuditCloud360 – Automated Azure & AWS security audit tool with reporting and alerting (In Development).
• SecureOrbit360 – SOC workflow automation integrating Logic Apps and n8n (In Development).

TECHNICAL EXPERTISE

Detection & Response Platforms: Microsoft Sentinel, Defender XDR, Splunk, QRadar, MITRE ATT&CK
Cloud & Infrastructure: Azure, AWS, GCP, GuardDuty, CloudTrail

Programming & Automation: PowerShell, Python, Bash, Terraform, API integration
Security Operations: Digital forensics, threat intelligence enrichment, runtime security

EDUCATION

• Certificate in Industrial Internet of Things – Polytechnique Montreal (In progress)
• Certificate in Cybersecurity Architecture and Management – Polytechnique Montreal (2022–2023)
• Certificate in Computer Network Security – Polytechnique Montreal (2020–2021)

KEY ACHIEVEMENTS

• 75% reduction in investigation time via automated detection frameworks.
• 60% faster MTTD through custom behavioral analytics.
• 50% reduction in false positives through intelligent automation.
• 40% faster incident response through standardized automation.

Available for immediate remote work across Canada | Excited to contribute to 1Password's mission of digital safety