Dimiter Todorov

Senior Cyber Security & Integration Specialist

Toronto, Ontario · Remote todorov.ca linkedin.com/in/dimiter-todorov-94248213 github.com/dimitertodorov

Senior cyber security and integration specialist with 15+ years across datacenter automation, the Ontario government's first Azure hosting, red teaming and security operations, and now full-stack apps built with AI agents. I bring a generalist's view: architecture, integration, code and the screens people use, with security as the thread that runs through all of it. Open to consulting and speaking on security integrations, ServiceNow SecOps and AI-assisted engineering.

EXPERIENCE · ONTARIO PUBLIC SERVICE

Senior Cyber Security & Integration Specialist

Jun 2020 – present

Ontario Treasury Board Secretariat, Cyber Security Division

Started in offensive security; since 2021, ServiceNow security operations engineering and architecture.

- Red-team exercises, penetration tests and web and network vulnerability assessments across province-wide I&IT, with custom tooling, C2 and Splunk apps, and reports for senior management.
- Led the ServiceNow Security Incident Response (SIR) implementation, from the platform assessment to production: Splunk and Microsoft Sentinel ingestion, Sentinel playbooks, phishing email-to-incident automation and Remedy ticket synchronization.
- Led the Vulnerability Response / USEM (CTEM) implementation: Microsoft Defender (TVM, XDR, Defender for Cloud), Qualys, IBM Guardium and BitSight into ServiceNow, with CMDB matching, risk scoring and assignment.
- Designed an explainable, seven-component vulnerability risk model and the Risk Model Workbench used to edit, validate and preview it on real CIs before activating it.
- Re-platformed the Remedy ↔ ServiceNow integration in 8 days with agentic AI (Claude Code): about 24K lines, 320 unit tests and 3 ATF suites.
- Substantially improved CMDB matching for scanner data with new CI lookup rules, and projected a 40% cut in Defender TVM import volume through filtering before persistence.
- Built the team's ServiceNow DevOps foundation: SDK/Fluent scoped apps, Azure DevOps pipeline templates, ATF in CI, and Bicep-managed Entra ID identities with GitHub OIDC, so no long-lived secrets.
- Championed AI-assisted engineering: wrote the team handbook, guardrails and the "prompt → human review → pull request → DEV install and ATF → evidence" delivery path.
- Also contributed to Recorded Future ↔ Splunk threat intelligence, the SOC dashboard architecture, a critical-incident reporting portal, and the SIR escalation integration with an external cyber partner.

Senior Automation & Integration Specialist (Development)

Oct 2016 – Jun 2020

Ontario Treasury Board Secretariat

- GoCloud: founding member and lead automation and integration developer of the government's first off-premise hosting, on Microsoft Azure. Built a PowerShell and Azure-native automation framework, a Jenkins pipeline farm, and integrations with ITSM and operations tooling.
- NMDB: lead developer of the network management database re-platform, from MS Access and SQL to Ruby/JRuby and ClojureScript, with an OpenAPI REST API, BMC Remedy and Atrium CMDB integration, deployed as containers.
- Wrote nsg-parser, an open-source microservice that turns Azure NSG flow logs into Syslog for the ArcSight SIEM.
- Owned the operations tooling: the HP / Micro Focus ITOM suite, GitLab CI, Docker Enterprise and Jenkins.

Senior Systems Analyst, Datacenter Operations, Tools & Automation

Jan 2010 – Oct 2016

Ontario Ministry of Government Services

- Led the enterprise HP Server Automation rollout across 8,000+ servers (Windows, AIX, SunOS, RHEL): a highly available, geographically distributed design, enterprise patch management and PCI compliance policies.
- Led Operations Orchestration as a clustered runbook-automation platform: private-cloud deployment, bare-metal provisioning, and Remedy ↔ HP UCMDB change, incident and configuration flows.
- Led the Closed Loop Incident Process, automating incident creation, assignment and resolution across tools, and a Rails API and dashboard over Remedy, HPSA, McAfee ePO, HP Operations Manager, HPNA and Active Directory.

Operating Systems Support

May – Sep 2009

Ontario Ministry of Government Services

PROJECTS

CheriBase: H3OK rights for a prosthetics center · 2026, ongoing · architect and lead developer

A web app for Allegro Prosthetics, a prosthetics and orthotics center in Bulgaria, working beside its legacy programs with byte-for-byte parity: an engine for patients' rights under H3OK, the national health insurer, with versioned rule sets, every entitlement explained in plain language, and a worklist that turns it into a call, a case and a claim. AI coding agents wrote most of the code under contracts and build-enforced boundaries I reviewed. In use. Kotlin, Ktor, React, TypeScript, Firebird, Entra ID, Azure.

Klide: a local ServiceNow emulator · 2026 · personal tooling

Runs ServiceNow server-side JavaScript on Rhino against PostgreSQL, emulating GlideRecord, business rules, scheduled jobs, Scripted REST and IRE, verified against live responses, so apps can be built and tested offline. 141 tests. Kotlin, Ktor.

Popfold · 2026 · open source

A scroll-driven 3D engine for the web, with a studio and a Blender pipeline, built with Claude Code; it runs todorov.ca. github.com/popfold/popfold. three.js, TypeScript.

Microsoft 365 and Cloudflare · consulting

Microsoft 365 security and compliance configuration, and a full Cloudflare tenant set up and integrated with Entra ID for a medium-sized business operating in an EU jurisdiction.

SKILLS

ServiceNow	Security Incident Response, Vulnerability Response, USEM / CTEM, CMDB and CSDM, IRE, MID Server, SDK / Fluent, ATF, Scripted REST, Flow Designer
Security	Microsoft Defender (TVM, XDR, Defender for Cloud), Microsoft Sentinel, Splunk Enterprise Security, Recorded Future, Qualys, IBM Guardium, BitSight, MITRE ATT&CK, penetration testing, red teaming
Cloud and identity	Microsoft Azure, Bicep, Entra ID, Key Vault, Managed Identity, Microsoft Graph, GitHub OIDC, Microsoft 365, Cloudflare
ITSM and automation	BMC Remedy and Atrium CMDB, HP Server Automation, Operations Orchestration, HP UCMDB, Jenkins, GitLab CI, Docker
Delivery	Azure DevOps, GitHub Actions, Vitest, unit-test-first design, technical handbooks
Languages	TypeScript, JavaScript, Kotlin, Python, PowerShell, KQL, SQL, Ruby / JRuby, ClojureScript, Vue 3
AI engineering	Claude Code, GitHub Copilot agents, MCP, AGENTS.md guardrails, human review with test evidence

EDUCATION

Georgian College · 2008 – 2010

LANGUAGES

English · Bulgarian · German