SUMIT ATRE, CISSP

CYBER SECURITY ENGINEER | CLOUD SECURITY & INFRASTRUCTURE

Location: Greater Toronto Area, ON | **Email:** resume@sumitatre.com | **LinkedIn:** linkedin.com/in/sumitatre | **Portfolio:** sumitatre.com

EXECUTIVE PROFILE

High-impact Cyber Security Engineer with proven expertise architecting and securing multi-tenant Azure, hybrid cloud, and SASE enterprise environments. Specialized in FinOps-aligned telemetry architecture, DevSecOps pipeline automation, Identity & Access Management (Entra ID), Zero Trust Network Access (ZTNA), and infrastructure-as-code (Terraform) governance. Proven track record collaborating with senior leadership and cross-functional engineering teams to remediate systemic vulnerabilities, establish cloud security baselines, and drive enterprise-scale OpEx reduction. Holds active **CISSP** and **Azure Administrator Associate (AZ-104)** credentials, underpinned by foundational **Azure Solutions Architect Expert (AZ-305)** and **Enterprise Administrator Expert (MS-102)** milestones.

CORE COMPETENCIES

Cloud Architecture & Platform Security: Azure, AWS, AKS, Terraform (IaC), Zero Trust Architecture, CIS Benchmarks, CSPM.

SecOps & SOAR Automation: Microsoft Sentinel, Log Analytics (LAW), Logic Apps / SOAR, DCRs, FinOps Telemetry, BlueVoyant MDR, KQL.

Identity, SASE & Zero Trust Governance: Entra ID, Cato Networks SASE, ZTNA, Dual-Control Conditional Access, PIM, FIDO2, Managed Identities.

Data Protection, AI Security & GRC: Microsoft Purview (DSPM/DLP), Enterprise AI Data Boundaries (M365 Claude), SOC 2 Type II, ISO 27001, NFRs.

PROFESSIONAL EXPERIENCE

Cyber Security Engineer | GS1 Canada

April 2025 - Present | Greater Toronto Area, ON

- **Cloud FinOps & Telemetry Re-Architecture:** Architected and implemented an enterprise-wide Azure Log Analytics and Sentinel ingestion overhaul, reducing monthly workspace ingestion overhead by over 90%, realizing over **$100K+ CAD in annual recurring OpEx savings** without degrading detection fidelity.
- **Kubernetes Telemetry Optimization:** Engineered surgical Azure Monitor Data Collection Rules (DCRs) to filter high-volume, low-signal container stdout/stderr at the edge, retaining actionable security and control plane telemetry while eliminating non-security operational noise-slashing container telemetry ingestion costs by over 70% ($50K+ annually).
- **Enterprise Identity & Zero Trust Transit:** Architected enterprise Conditional Access dual-control frameworks (Intune Compliance + MFA) and automated Graph API identity lifecycle governance, eliminating remote SASE/Cato SSO transit deadlocks.
- **Enterprise AI & Data Security Governance:** Engineered enterprise AI data boundaries (M365 Claude integration), authoring custom Microsoft Purview DSPM Sensitive Information Types (SIT) and automated Defender App Governance circuit breakers.
- **Proactive Threat Defense & SOAR Automation:** Engineered high-fidelity KQL detection analytics and automated SOAR pipelines in Sentinel for supply-chain vendor compromises (EmailEvents correlation with automated entity consolidation).
- **Data Lifecycle & Ingestion Governance:** Redesigned retention policies across 15 core security tables from 365-day interactive storage into a 90-day interactive / 275-day archive tier, with an expanded plan capturing an additional 11 high-throughput tables.
- **Executive Security Visibility & Governance:** Authored FinOps capacity models, data lifecycle policies, and architectural cost-efficiency baselines for senior technical leadership, establishing foundational KPIs for enterprise platform modernization.
- **Infrastructure-as-Code Hardening:** Conducted end-to-end security reviews of Terraform deployments and Azure Functions execution models (Run From Package tokenization), authoring automated guardrails and migrating legacy SAS tokens to Azure Managed Identities.
- **MDR & Threat Attribution:** Technical escalation lead partnering with BlueVoyant MDR; executed cross-platform investigations correlating external vendor ingress with Entra ID tenant telemetry and Azure DevOps pipelines to eliminate false positives and drive root cause remediation.

Senior Systems & Security Administrator | IT Business Advisors (ITBA) August 2021 - March 2025 | Greater Toronto Area, ON

- Spearheaded cloud infrastructure, security posture, and identity engineering for **40+ multi-tenant hybrid environments** across financial, healthcare, legal, and manufacturing clients (**800+ total seats**).
- Guided multilayered technical controls and audit readiness supporting successful **SOC 2 Type II compliance** and **ISO/IEC 27001 certification** programs for enterprise clients.
- Re-architected client operating environments into cloud-first configurations using Microsoft Entra ID, Intune, Conditional Access, and Microsoft Purview DLP, driving **40%-60% reductions** in on-premises infrastructure maintenance costs.
- Designed and deployed automated PowerShell automation engines for zero-touch provisioning and role-based lifecycle access, reducing employee onboarding and deprovisioning cycles by **40%**.
- Directed incident response and remediation operations across major industry threats (including zero-day **Kaseya VSA CVE-2021-30116**), containing lateral movement and eliminating blast radius across exposed customer tenants.
- Hardened cloud and hybrid environments to **CIS Level 1/Level 2 benchmarks**; instituted centralized enterprise PKI, enterprise domain certificate authorities, and RADIUS authentication over 802.1X.

Systems & Security Administrator | IT Business Advisors (ITBA) March 2020 - August 2021 | Greater Toronto Area, ON

- Monitored, investigated, and triaged multi-tenant security events across modern EDR/XDR and SIEM tools (Rapid7, Sophos XDR, Okta, Duo, ConnectWise).
- Led technical discovery, scoping, and deployment for complete on-premise-to-cloud migrations into Azure and Microsoft 365.
- Standardized infrastructure configuration policies, authoring runbooks and technical documentation for system hardening and disaster recovery.

Systems Administrator | Some IT Guy January 2008 - December 2019 | Greater Toronto Area, ON

- Maintained, secured, and administered Windows Server environments (2008-2019), Active Directory Group Policy, DNS, DHCP, and enterprise backup/DR platforms (Veeam).
- Managed third-party external penetration testing engagements, translating technical findings into prioritized vulnerability remediation roadmaps.
- Implemented physical and network security baselines across multi-site branch operations.

CERTIFICATIONS & CREDENTIALS

ACTIVE INDUSTRY CREDENTIALS

- **CISSP** - Certified Information Systems Security Professional ((ISC)² · Active)
- **Microsoft Certified: Azure Administrator Associate (AZ-104)** (Microsoft · Active)

ARCHITECTURAL CREDENTIALS & MILESTONES

- **Azure Solutions Architect Expert (AZ-305)** (Microsoft Certified)
- **M365 Enterprise Administrator Expert (MS-102)** | **Security+**

TECHNICAL SKILLS SUMMARY

Cloud & Platforms:	Microsoft Azure, AWS, Azure Kubernetes Service (AKS), Terraform (IaC), Docker, CSPM, CI/CD Security Integration.
SecOps & SIEM/SOAR:	Microsoft Sentinel, Log Analytics Workspaces (LAW), Kusto Query Language (KQL), Logic Apps / SOAR, BlueVoyant MDR, Defender for Cloud.
Identity & SASE:	Microsoft Entra ID, Cato Networks SASE, Zero Trust Network Access (ZTNA), Conditional Access, Intune MDM/MAM, PIM, FIDO2/Passkeys.
Data Security & AI:	Microsoft Purview (DSPM/DLP), Sensitive Information Types (SIT), Defender App Governance, Enterprise AI Data Boundaries (M365 Claude).
Automation & Code:	PowerShell, Python, Bash, Microsoft Graph API, Azure Resource Manager (ARM), JSON / REST APIs.
Networking & Edge:	Cato Cloud SD-WAN, Next-Gen Firewalls (Azure Firewall, SonicWall, pfSense), 802.1X RADIUS, DNS/DHCP, TCP/IP, IPsec.