

DIIPESH MISTRY

Security Engineer | Vulnerability Management · Security Posture Mgmt · Cloud & Infrastructure Security

Calgary, Alberta, Canada (Willing to relocate) • diipesh@gmail.com • 306-450-0421 • linkedin.com/in/diipesh

PROFESSIONAL SUMMARY

Security engineer with 10+ years in IT infrastructure and security, including 8+ years focused on finding, prioritizing and eliminating vulnerabilities across Windows, Linux and multi-cloud (Microsoft Azure, Google Cloud Platform) environments. Builds the automation, security design reviews and detection pipelines that make vulnerability discovery repeatable at scale, and has delivered penetration testing, ICS/OT risk assessments and malware analysis for enterprise and Government of Canada clients. CISSP-certified, with a Master of Engineering in Computer Networks and a learn-it-all approach to emerging attack techniques.

CORE COMPETENCIES

Vulnerability Discovery & Management · Penetration Testing · Security Design & Impact Review · Attack Surface Analysis · Threat Detection & Malware Analysis · Security Automation (Bash, PowerShell, API integrations) · Cloud Security (IAM, RBAC, Firewall) · DevSecOps / CI/CD Security · ICS/OT Security Assessment · Compliance (ITSG-33, PBMM)

PROFESSIONAL EXPERIENCE

Technology Lead – Security

Jan 2025 – Present

Infosys Public Services | *Government of Canada engagement* | *Remote*

- **Protect and harden** internet-facing web assets and the cloud platform hosting the client's most critical systems, closing misconfigurations before they can breach compliance baselines.
- **Drive vulnerability management:** run recurring scans, steer remediation with system owners, and report exposure through risk-management dashboards and executive briefings.
- **Detect and respond:** analyze Microsoft Sentinel telemetry to identify and block bot attacks, malicious crawlers and other hostile activity against client assets.
- **Analyze malware samples** and publish threat reports on phishing, DLP events and outages caused by insecure or misconfigured systems.
- **Designed phishing and vishing simulations** and awareness campaigns, with tracked-metric dashboards and an executive presentation showing program effectiveness.

Geotab Inc. | *Remote*

Senior Security Administrator

Nov 2024 – Jan 2025

Security System Administrator

May 2019 – Oct 2024

- **Automated vulnerability scanning and reporting** with Bash and secure API integrations to Tenable.io (Nessus) and Qualys, and automated Google Cloud firewall rule configuration and asset management, removing repetitive manual work.
- **Performed security assessments and penetration testing** and implemented security controls across AWS and GCP environments; led threat detection and timely remediation of discovered risks.
- **Ran security impact analysis** on proposed changes before release to expose risk to existing systems and planned enhancements, and worked with development and operations teams to integrate security into CI/CD pipelines.
- **Designed and enforced least-privilege access** on Google Cloud (IAM, RBAC, service accounts, Cloud Firewall) and automated role provisioning through an in-house portal using PowerShell and Bash.
- **Deployed and administered** CrowdStrike Falcon, Tenable Nessus agents, Duo MFA, Splunk SIEM and Zscaler; partnered with the SOC to roll out new security systems and policies.
- **Automated audits, patch management and system hardening** to sustain a consistent security baseline across servers, network devices and workstations.

- Designed site-assessment methodologies to expose risk, vulnerabilities and threat vectors in client industrial control systems, and produced compliance-ready consulting reports for instrumentation and safety systems.
- Created reusable templates for security posture assessments and report drafting; managed patch procedures and deployed advanced threat detection and prevention tooling.

Security Operations Center Analyst

Mar 2019 – May 2019

Uzado Inc. | *Vaughan, ON*

- Performed vulnerability assessment, remediation and compliance management with Qualys; analyzed SIEM, network-traffic and host-security logs and delivered data-driven recommendations to stakeholders.

Senior Systems Analyst**(Oct 2013 – Aug 2018) / Team Lead (Jun 2015 – Feb 2016)****WBM Technologies Inc.** | *Calgary, AB / Regina, SK*

- Resolved escalated and critical issues, monitored security trends, and operated firewall and IDS/IPS controls across business systems and a data center.
- Led province-wide deployment of the Government of Saskatchewan's Next Generation Desktop and Mobile Device Management solution for executives, managing the technician team, incident response, documentation, training and mock exercises.

EDUCATION**Master of Engineering, Computer Networks** – Toronto Metropolitan University (formerly Ryerson), Toronto Oct 2019**Post-Graduate Diploma, Information Technology Professionals** – Lambton College, Sarnia, ON Dec 2011**Bachelor of Technology, Computer Engineering** – Ganpat University, Gujarat, India Aug 2009

CERTIFICATIONS

- **CCNA** Routing & Switching, Security
- **MCSA** – Microsoft Certified Solutions Associate
- **CompTIA** Network+, Project+
- **CISSP** – Certified Information Systems Security Professional
- **Fortinet** - Network Security Engineer 1, 2 and 3

TECHNICAL SKILLS**Security Tooling:** Microsoft Sentinel, Splunk, AlienVault, CrowdStrike Falcon, Tenable.io / Nessus, Qualys, Aqua, Netsparker, Zscaler, Duo MFA, KnowBe4**Cloud & Platforms:** Google Cloud Platform, Microsoft Azure, AWS, Windows Server, Linux, VMware vSphere, Hyper-V, Citrix**Network Security:** FortiGate, SonicWall, Cloud Firewall, IDS/IPS, McAfee endpoint protection**Automation:** Bash, PowerShell, REST/API integrations, CI/CD security integration**Human Risk:** Phishing, vishing and smishing simulation; security training and awareness programs**Compliance Exposure:** CMMC Level 2, FedRAMP, ISO27001, SOC2

SECURITY COMMUNITY**Google Cloud Security CTF** – Worked challenges in network forensics, ICS/SCADA analysis and AI prompt injection.**Hack The Box & Try Hack Me** – Self learned platform where I practice security hands-on**Professional conference attendee** – Bsides Calgary and Bsides Edmonton