Canadian Insider Risk Management Centre of Excellence

Practical Certificate in Insider Risk Management
Open Source Research and Intelligence
ONLINE

***Completion of this certificate in conjunction with the Practical Certificate in Insider Risk Management – Foundations for Screening and Risk Factors, Investigations, and Organizational Integration will result in the issuance of a Professional Certificate in Insider Risk Management**

Workshop Overview

The Canadian Insider Risk Management Centre of Excellence (CInRM CoE), in collaboration with Carleton University's Norman Paterson School of International Affairs (NPSIA PT&D) Office of Professional Training and Development, has designed a virtual two-day workshop to enhance participants' skills in using Open Source Intelligence (OSINT) to address and reduce the risks of insider threat. As insider threats grow more complex, leveraging OSINT and intelligence methodologies has become crucial for organizations aiming to detect early warning signs of insider threat activity. This proactive approach allows organizations to intervene before harm occurs, enhancing overall security and resilience.

OSINT practices emphasize the collection of publicly accessible data, such as social media activity, indicators of financial stress, and external affiliations, that could signal potential insider risks. By combining this external information with internal behavioral insights, organizations can create comprehensive risk profiles, identify unusual patterns, and assess employee vulnerabilities. Early detection and intervention are key, with a focus on mitigating internal threats. Key OSINT techniques include behavioural monitoring, sentiment analysis, anomaly detection, and linking external digital footprints with internal behaviours.

The continuous nature of OSINT allows for ongoing monitoring of embedded insider threats within the organization, helping to understand the full scope of a potential adversarial network. OSINT and complementary intelligence activities provide critical insights that clarify the impact of an incident, guide decision-makers, and support more informed strategies for incident recovery.

Learning objectives of the workshop:

- gain a comprehensive understanding of the personal risks associated with social media presence,
- discover how OSINT methodologies and intelligence techniques can be implemented by organizations to safeguard against insider threats and strengthen risk management practices,
- apply OSINT techniques to gather publicly available data that aids in behavioral monitoring and early warning detection,
- explore how OSINT can identify potential risks during security clearances and support administrative investigations,
- understand how OSINT and related intelligence processes contribute to assessing the scope and impact of insider threats and incidents.

*This course also provides 12 ASIS Continuing Professional Education (CPE) Credits - Aligns with ASIS Certified Protection Professional (CPP), Associate Protection Professional (APP), and Professional Certificate Investigator (PCI) certification programs

Fee: $700.00 + HST

If interested, please contact CanadianInsiderRiskManagementCOE@carleton.ca and provide your: 1) Full Name, and 2) E-mail

Our featured Instructor: Daniel Bertrand

Mr. Bertrand retired from public service with over 35 years of experience in law enforcement and federal investigations, including service as an Officer of the Royal Canadian Mounted Police (RCMP). Throughout his career, he specialized in organized crime and national security with a strong emphasis on intelligence and technical expertise. Mr. Bertrand led numerous intelligence teams, including the foundational Open Source Intelligence Section within the RCMP National Security Program.

His extensive service includes assignments across Canada, in the United States, and internationally with the United Nations as part of a peacekeeping mission in Haiti. With a background in computer forensics, Mr. Bertrand continues to expand his expertise, now focusing on the integration of artificial intelligence applications into intelligence and security practices.