CSCSS

CENTRE FOR STRATEGIC
CYBERSPACE + SECURITY SCIENCE

BAY3000

# CyberImmersion Workshop Program

**CyberImmersion surrounds you with real world extensive cyber based education**

# CyberImmersion: In today's world, cybersecurity lessons are hard won in rapidly evolving threat landscapes.

CSCSS in our role in cyberspace through our CSCSS Intelligence Services (CIS) mounts projects and delivers cyber + intelligence services, associated projects and operations globally in support of the CSCSS mission, vision, partner objectives and requirements.

Experience, knowledge and expertise are keys to individual success as well as organizational security. The CyberImmersion workshop is dedicated to and focused on providing a realistic stage for learning and gaining valuable experience.

# Module 1

# Security Penetration Testing Management

**Security Penetration Testing Management** is a workshop designed to address skills, methodologies and knowledge required to properly conduct information assurance testing in a structured manner. It will empower managers to fully understand the impact and pitfalls of penetration testing and engagement management.

Security penetration testing is an excellent method for determining the strengths and weaknesses of a network and its architecture. However, the process of performing a penetration test is complex, and without due diligence and care can have disastrous effects on the systems being tested. This workshop will lead participants through the processes involved in proposals, scoping, contractual elements, and NDA requirements. It will cover the fundamentals of testing, spanning the relative phases of penetration testing and 'attack', leading to reporting and document preparation and security.

Penetration testing is best performed by a team, which delivers several benefits from both a technical and a managerial standpoint ensuring a successful test.

- Understanding basic definitions and elements of security testing including legal requirements
- Learn how to run and manage testing through teams to ensure efficiency and accountability
- Essential components of security tests and methodologies
- Understanding the various phases of a security test and information feedback
- Application of elements, including legal agreements, tools, technologies, scoping, attack planning and project management
- Engagement management and communications, in test and post engagement reporting, delivery, expectations and data security

## Key Takeaways:

- Discover and incorporate lessons into your specific security testing methodologies
- Understand the attack process, and associated management
- Understanding the tools, technologies, their employment, and placement in the process of conducting a security test
- Deliver and understanding to think strategically and incorporate testing into an ongoing program
- How to effectively assess, scope, plan and deliver a security test
- Understand the potential ramifications and impact of testing, during and after testing has taken place
- Tie in lessons learned: understand what your company can do to prevent an attack
- Gain insight into the mindset of Threat Actors and how they look at your network
- Learn key concepts associate with cybersecurity testing, trends and terminology and their application

CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE | BAY3000

# Module 2

# Intelligence: The Planners Strategic Edge

## A deep dive into employing intelligence in your environment

**Intelligence: The Planners Strategic Edge** is an expert led, interactive workshop. The purpose of the workshop is to familiarize participants with intelligence and how to integrate cyber intelligence into their cyber security profile.

When correctly employed, intelligence including 'threat intelligence' as described by the computer security industry, provides focus for:

- Long-term planning (strategic intelligence);
- Direction in the current cyber environment (using intelligence for operational management)
- Providing situational awareness and tactical intelligence supporting defence against current attacks, cyber, social and/or physical.

Participants will learn how executive direction is translated by the intelligence team in order to deploy specific products to specific management levels in the organization. This workshop provides project managers, security leaders and system integrators with the tools to deploy and utilize intelligence in their organizations.

A key feature of the workshop is the integration of intelligence into security processes and the distribution of intelligence products. Participants should be able to discuss examples of: corporate organizations, IT security organizations as well as cyber security policies. Participant examples will be used in discussions on how-to implement intelligence processes and procedures.

**Key Takeaways:**

- Learn critical definitions of Intelligence and intelligence processes
- Understand the difference between 'threat intelligence' and integrated intelligence
- Gain insight into the differences between 'analysis' and 'intelligence'
- Project managers will learn to integrate cyber + intelligence into security processes
- Learn the prerequisites required BEFORE intelligence processes can be initiated
- Learn the importance of getting intelligence direction from your CEO/President
- Discover the different types of intelligence reporting.
- Learn the distinctive elements of a thorough intelligence report.
- Learn what you should expect from an intelligence provider.
- Know what an intelligence team will expect of your organization.
- Tie in your lessons learned to maximize the return on investment for your security investment

CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE | BAY3000

**About CSCSS**

The Centre for Strategic Cyberspace + Security Science (CSCSS) is a multilateral, international not-for-profit organization that conducts independent cyber-centric research, development, analysis, and training in the areas of cyberspace, defence intelligence, cyber security, cybercrime, and science while addressing the threats, trends, and opportunities shaping international security policies and national cyberspace cyber security initiatives.

CSCSS, as a strategic leader in cyberspace, works jointly with key partners to address, develop, and define cyber technologies, cyber defence force capabilities, information dominance, and concept operations. We deliver practical recommendations and innovative solutions and strategies to advance a secure cyberspace domain.

**About Bay3000**

Established in 1991, Bay3000 helps organizations excel in the execution of operational excellence through improved project, program, portfolio management, and continuous improvement by offering standard and customized training & professional development consulting solutions. Our specialists are educators and active practitioners who bring industry experience in the fields of project management, business analysis, lean, six sigma, technical, soft skills and leadership development.

Bay3000's client list includes many of Canada's most respected organizations spanning all sectors, including financial services, government services, healthcare services, & manufacturing. Bay3000 is an accredited, registered education provider for PMI and the IIBA.

CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE | BAY3000

# Registration

Price for Both Modules
**$1,595 Full Price**
**$1,395 Early Bird**
**Register by November 3, 2017**

To register, please call
**905.947.8562**
**info@bay3000.com**

**Venue Location**

**The Thornhill Club**
7994 Yonge St.,
Thornhill, ON L4J 1W3

**Contact Us**

For more information on the CyberImmersion Workshop, or to book this course please contact us

**Bay3000 Consulting Inc.**
200 Town Centre Blvd, Suite 402-200
Markham ON L3R 8G5
905.947.8562
info@bay3000.com

CSCSS.org