CYBER DEFENCE CHALLENGE

COMPETITION EVENT 2017

The Canadian Cyber Defence Challenge (CCDC) competition is a challenging and exciting event program. You will be able to wear different hats and try a few roles from the IT security field.

The fundamentals of CCDC are based on the concepts of event-anchored learning. You will be immersed in a real-time security event. You are expected to detect the risk and the nature of the attack, isolate the attack vector and mitigate the risk. You will then analyze the business environment to determine whether any information assets have been compromised. Once you have assessed the information assets and the system environment, you will recommend to the business and implement preventive security measures designed to reduce the risk of future similar attacks from compromising the organization. The procedures that you will learn to implement are considered standard security industry best practices.

CCDC Competition Event Scenario

"A state of the art security alerting system noticed an anomaly in your network, and it has generated an alert. When someone evaluated the alert, there was an incident created. A group of security professionals were tasked with addressing the incident."

At least once a day, a security professional analyzes some suspicious data streams. It could be a binary file or a network flow. The most challenging and exciting time comes when there is a security breach. As you may guess, this is the time when all skills and knowledge come to play.

Responding to a security breach is an exciting challenge for a security professional. On one hand, it can be stressful and scary as the system and security controls have failed. On the other hand, it can be an exhilarating and adrenaline-filled adventure as you work against the clock to mitigate the risk. Time management and team organization play a big role in one's success in responding to the breach.

Can you imagine what may be discovered when you responding to an incident? Was there only one system compromised or others? How far-reaching was the compromise? Where did it come from? How do we stop it? What needs to be done to avoid such a compromise in the feature? You will now have a chance to experience all of these scenarios and answer these questions by preparing and participating in the upcoming CCDC competition event.

Continued on next page...

CCDC COMPETITION EVENT PRACTICES

The CCDC competition event is designed around the cyber security industry's Digital Forensics Incident Response (DFIR). DFIR is composed of six key steps:

1. Breach discovery
2. Incident containment and remediation
3. Determining how the breach occurred
4. Analyzing compromised and affected systems within the organization domain
5. Identifying and understanding what the attackers took or changed
6. Reporting and communicating to organizational leaders

In industry today, over 80% of all organizations that are breached by a cyber attack learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through their network undetected for months or even years.

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in the organization enterprise; they are compromising hundreds. Industry teams are strained and require additional services that help educate and equip them to properly identify compromised systems, provide effective containment of the breach, and ultimately rapidly remediate the incident.

The CCDC's competition event provides students with the appreciation, awareness, training and skills to walk through the DFIR process while dealing with critical incident in real time. Students will learn to hunt down, counter, and recover from a wide range of threats with a fictitious simulated enterprise environment. As part of the competition event, students will be given hands-on experience to identify where the initial targeted attack occurred and lateral movement through multiple compromised systems. Students will extract and create crucial cyber threat intelligence that can help you properly scope the compromise and detect future breaches.

As part of the CCDC's competition event, students will work in teams of four (or five) to:

- Utilize tools, techniques, and procedures necessary in order to effectively detect, contain, and remediate against a variety of adversaries.
- Determine how the breach occurred by identifying the spear phishing attack mechanisms.
- Recover data cleared using anti-forensics techniques.
- Learn how file systems work and discover powerful forensics artifacts.
- Identify lateral movement within the environment, showing how attackers transition from system to system without detection.
- Understand how the attacker can acquire legitimate credentials, including domain administrator rights - even in a locked-down environment.
- Track data movement as the attackers collect critical data.
- Recover and analyze proprietary files used by attackers to exfiltrate sensitive data from the enterprise network.
- Use collected data to perform effective remediation across the entire enterprise.

CYBER DEFENCE
CHALLENGE

May 16th, 2017 • Winnipeg, MB
cyberdefencechallenge.ca

Find us on

info@cyberdefencechallenge.ca