The Canadian Cyber Incident Response Centre (CCIRC)

OAS-FIRST Cybersecurity Symposium

September 2016
What is a CSIRT?

● “A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client”.

  - **National CSIRTs** provide incident handling services to a country.
  - **Coordination Centers** coordinate and facilitate the handling of incidents across various CSIRTs.

*CERT SEI Definition*
CCIRC’s Operational Cycle

- What kind of data does CCIRC use?
- Where/who does it come from?
- What is the value of this process?
- How do the results influence the input?
- How do we disseminate the results?
- Which products or services do we provide?
- What tools and resources do we use to process the information?
CCIRC’s Incident Management Process

Victims

Other national CSIRTs

Open Source and Industry

CCIRC’s Incident Handling Team

Automated Analysis Tools

National Cyber Threat Notification System

Takedown Requests, Advisories, Advice and Guidance

Victim notifications

Other national CSIRTs

Open Source and Industry

National Cyber Threat Notification System

CCIRC’s Incident Handling Team

Automated Analysis Tools

Takedown Requests, Advisories, Advice and Guidance

Victim notifications

Other national CSIRTs

Open Source and Industry

National Cyber Threat Notification System

CCIRC’s Incident Handling Team

Automated Analysis Tools

Takedown Requests, Advisories, Advice and Guidance

Victim notifications

Other national CSIRTs

Open Source and Industry

National Cyber Threat Notification System

CCIRC’s Incident Handling Team

Automated Analysis Tools

Takedown Requests, Advisories, Advice and Guidance

Victim notifications

Other national CSIRTs

Open Source and Industry

National Cyber Threat Notification System
Automating the CSIRT

Data Sources
- Feeds

Ingest  Process  Dynamic Reporting

Goal: Assess in real-time the Canadian Cyber Health

Automation

Notifications

Knowledge

Strategy

Action

Impact Assessment
Malware vs. Vulnerable Services

Score Card

Canadian Cyber Incident Response Centre (CCIRC)

Malware (per 1,000 IPs Owned)
ICT

Vulnerable Services (Per 1,000 IPs Owned)
ICT

*No malware to report in this period
Red indicates above average and green indicates below average.

*No vulnerable services to report in this period
Red indicates above average and green indicates below average.
Automated Information Sharing: STIX/TAXII

- Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)
  - Two protocols to develop a standardized language to represent and share structured cyber threat information
  - Serves as a new way of sharing the same information CCIRC traditionally shares with its partners, but more actionable and timely format

STIX/TAXII Project (September 2016)
- Successfully operating a working model using STIX/TAXII with 30+ organizations
  - Shared indicators of compromise for active network defence and monitoring
Contact Us

cyber-incident@ps-sp.gc.ca

www.publicsafety.gc.ca/ccirc