

EWA–Canada's CanCERT™ SERVICE OFFERINGS

CanCERT™ is Canada's first national Computer Emergency Response Team. Operated since 1998 by EWA–Canada Ltd. CanCERT™ provides trusted and timely *information* and *support* related to secure IT systems operations. We are committed to and understand client confidentiality, privacy and legal concerns.

PUBLIC SERVICES

International Coordination – provides a Canadian focus for coordination with international Computer Emergency Response Teams (CERTs) through the Forum for Incident Response Security Teams (FIRST).

Limited Incident Response – provides initial incident response service to Canadian government, business and academic organizations.

CLIENT SERVICES

Informational Reports

Provides three timely reports to help an organization secure their networks:

- A1 **Daily Threat and Vulnerability Report** – provides a daily summary of, and pointers to, threat and vulnerability information including defence strategies, tools and early warning indications of possible attack methods gathered from publicly available sources. The document is delivered via email by 2:00 p.m. EST/EDT Monday to Friday excluding Canadian holidays.
- A2 **Weekly Threat and Vulnerability Report** – provides a similar, but more streamlined, version of A1 that covers a full week. The document is delivered via email by 4:00 p.m. EST/EDT Tuesday, excluding Canadian holidays.
- A3 **Cyber Trends & Analysis Report** – provides a monthly overview and interpretation of threat and vulnerability trends, including regular updates of CanCERT™ incidents and statistics. The report targets senior level managers, and is delivered on the first Friday following the end of the month.

Network Attack Detection Statistics

EWA–Canada has designed and developed a Network Attack Detection System (NADS) that detects malicious activity and traffic from external sources and provides meaningful statistics of these activities. Gathered at EWA–Canada's perimeters throughout Canada and the world, this consolidated, analyzed data provides a *unique* Canadian perspective of attacks. Also included are statistics at a world-wide level. An understanding of attack patterns allows remedial action to be implemented and is invaluable for comparison to a client's own data.

- B1 **NADS Canadian and World-wide Statistics** – provides a statistical report delivered via email by 2:00 p.m. EST/EDT Tuesday, excluding Canadian holidays.

Help Desk

Knowledgeable staff is available to help with emergencies or to answer ad hoc IT security inquiries. Possible forms of assistance include identifying whether intruders have compromised a system; how the penetration occurred; how much damage has been done; how to recover; log and event file interpretation; and how to prevent an emergency type of incident from recurring. Additional assistance is available in establishing communications with authorities, agencies and experts; and coordinating with other sites, incident response teams, Internet service providers and law enforcement agencies as requested when resolving security related matters. On-site assistance is available through EWA-Canada Consulting Services.

- C1 **Emergency Inquiry** – provides a *premium* 7/24 telephone service intended to handle the most critical situation.
- C2 **Ad hoc Inquiry** – provides advice and answers during business hours.

Certificate Authority (CA)

- D1 **CanCERT™ Certificate Authority** – provides a highly trustworthy Public Key Infrastructure to support authenticated and secure communications between CanCERT™ and its clients. Up to four CanCERT™ PKI certificates are available to clients at no charge.

INFORMATION EXCHANGE SERVICE

The importance of sharing information on IT threats and incidents among various stakeholders in public and private sector communities (e.g., healthcare, banking and finance, telecommunications, utilities, etc.) has increased as everyone has become more reliant on networked computer systems. Information about threats and incidents experienced by others can help stakeholders identify trends, understand the risks, determine appropriate responses and implement effective preventative measures. EWA-Canada recognizes that many clients share IT security concerns with others in their sector. CanCERT™ provides its clients with a comprehensive forum for executive and technical information exchange amongst peers who have similar interests. For those clients who have already purchased the Daily Threat and Vulnerability Report, the following packaged service is available.

E1 Sector Threat Monitoring – provides threat monitoring based on sector requirements, for example, SCADA for the energy sector or SS7 for the telecom sector. The same criteria for escalating and for delivering Threat and Vulnerability information is used to issue this sector specific information.

Anonymous Data Consolidation – based on clients' local implementations of Intrusion Detection Systems as well as firewalls and virus scanners, Anonymous Data Consolidation provides a meaningful view of the cyber activity confronting the sector. If the NADS Canadian and World-wide Statistics service has been purchased, the Anonymous Data Consolidation adds the missing sector focus upon which comparisons can be made. In order to receive maximum benefit from this service, clients are strongly encouraged to provide analyzed IDS, firewall and virus data in a format defined by CanCERT™ by 8:00 a.m. EST/EDT Tuesday (for consolidation for the bi-weekly Information Exchange Forum).

Security Information Exchange Forum Conference Call – designed to facilitate information sharing, the bi-weekly Security Information Exchange Forum conference call provides access to highly trained security experts to discuss more fully the daily or weekly threat and vulnerability report and analysis, and the consolidated data statistics and trends. Liaison with all involved parties, key management, agenda creation and distribution, conference call management, and chairing and facilitation are included.

Email List Server – hosted by CanCERT™, the Email List Server is intended to provide a convenient mechanism for clients and CanCERT™ staff to exchange and share hints and best practices.