



02/01/2017 Barcelona (Spain)

Job Overview

This position is responsible to assist in the research of systems, applications, and network devices for vulnerabilities and malicious code (threat content), attack techniques, and write detection signatures for the same in support of eTrust security products. Content is for all eTrust products that have a continual content flow including anti-virus, vulnerability management, intrusion detection, policy compliance, and anti-spam.

Key Responsibilities

- Monitor public/private sources of information for vulnerabilities and/or malicious code.
- Correlate threat content to industry peers.
- Disassemble and analyze malicious code/exploits.
- Create system detection and clean procedures and/or scripts to mitigate malware or vulnerability risk in accordance with established procedures.
- Test and validate threat content through lab testing in accordance with established procedures.
- Provide detailed documentation for threat content descriptions and mitigation strategies.
- Maintain internal and external network of relationships within the field.

Typical Role Definition

Works under general supervision. Has learned the fundamental concepts, practices, and procedures of a particular field of study, not yet the formal application of these concepts, practices, and procedures.

Job-Specific Authority and Scope

- Manager is consulted for decisions.
- Typically has no direct reports.
- Typically has no total staff.
- Typically has a global geographic focus.
- Typically does not manage a budget.

Business Travel and Physical Demands

Business travel of approximately 10 or less percent yearly is expected for this position.

Physical demands:

- Office environment. No special physical demands required.

Preferred Education

Bachelor's Degree or global equivalent in Computer Science or related field.

Work Experience

Typically 0 to 2 years of work experience. Ability to work independently and within a team environment. Highly self motivated and can perform research on technical issues. Security experience with some of the following is preferred: Microsoft Windows NT, 2000, XP, 2003 and/or Unix, transport protocols (TCP/IP, IPX/SPX, NetBEUI), wireless, Ethernet, WAN switching technologies, firewalls, intrusion detection, PKI, routers, switches, etc.

Skills & Competencies

Ability to de-compile program executables and analyze abnormalities. Basic knowledge of x86 assembler, BIOS, and DOS interrupts and different file formats. Basic knowledge of trade tools and utilities (disassemblies, debuggers, compilers). Basic knowledge of networking, traffic analysis and packet decomposition. Experience with scripting, Internet protocols and vulnerability techniques. Working knowledge of Windows/Linux/Unix operating systems. Proven ability to meet/exceed deadlines. Ability to succeed in a team based and/or autonomous environment. Excellent oral and written communication skills.

For further questions regarding the job position don't hesitate to reach out to me through mail:
ricin01@ca.com

technologies