

Security Protocol Research Consultant, Toronto - SAL01805-12

Description

Position Overview:

The Application Protocol Team supports a global customer base including leading security product vendors, software and high-tech manufacturers, telecommunications providers, and large enterprise customers, with a set of industry-leading technical data feeds, research products, and engineering services.

Responsibilities:

- As a Consultant - Application and Protocol Research, you will be part of a team that develops detection signatures for providing application visibility and control.
- You will work on developing detection signatures of peer-peer clients, instant messaging, media streaming, authentication protocols, and common business and data center protocols by deep packet inspection and other means of behavioural analysis and research.

Responsibilities and duties of this position include:

- Create and analyze network traffic and model application behavior using regular-expression and Snort.
- Analyze and describe complex application behaviours
- Analyse software to reverse engineer protocols, Internet application, and malware attack methods.
- Effectively communicate the results of your analysis to management and clients.
- Analyse new applications, protocols, malware, networking and software vulnerabilities.
- Learn and use new detection signature languages and regular-expression based grammar.
- The role includes participation in delivery activities as well as involvement in product strategy and pre-sales support.

Qualifications

Required Knowledge:

- The successful candidate will possess:
- In-depth knowledge of TCP/IP and other networking protocols.

- RFC-level understanding of popular protocols like HTTP/FTP/SMTP/CIFS.
- Some experience with Snort, Wireshark, Fiddler and VMware.
- Ability to analyze and describe complex application behaviours.
- Knowledge of operating system internals.
- Extensive knowledge and experience with Networking protocols, Internet security paradigms, Application Security, and Cryptography.
- Experience in application and protocol reverse engineering is a big plus
- Deep knowledge of multiple modern operating systems.
- Programming Skills in languages like Python, UNIX shell, Perl and JavaScript.
- Excellent oral and written communication skills.
- Excellent client management/soft-skills.
- Terrific attention to detail and personal QA.
- Willing to take initiatives and get things done independently.
- Be able to work within a team but self-directed, self-motivated, self-starter able to work with minimal supervision.

Required Skills & Abilities:

- The successful candidate will possess:
- In-depth knowledge of TCP/IP and other networking protocols.
- RFC-level understanding of popular protocols like HTTP/FTP/SMTP/CIFS.
- Some experience with Snort, Wireshark, Fiddler and VMware.
- Ability to analyze and describe complex application behaviours.
- Knowledge of operating system internals.
- Extensive knowledge and experience with Networking protocols, Internet security paradigms, Application Security, and Cryptography.
- Experience in application and protocol reverse engineering is a big plus
- Deep knowledge of multiple modern operating systems.
- Programming Skills in languages like Python, UNIX shell, Perl and JavaScript.
- Excellent oral and written communication skills.
- Excellent client management/soft-skills.
- Terrific attention to detail and personal QA.
- Willing to take initiatives and get things done independently.
- Be able to work within a team but self-directed, self-motivated, self-starter able to work with minimal supervision. Optional Skills & Abilities:

Preference will be given to the candidate that also possesses:

- Familiarity in C/C++ and or x86 Assembly language
- Expertise with common malware analysis tools for surface analysis, run-time analysis, and reverse engineering.
- Strong knowledge of malware, rootkits, software protection schemes is highly desirable
- Understanding of security vulnerability exploits.

- In depth knowledge of the general security concerns facing large enterprises.
- Experience writing attack detection and protocol signatures for commercial security devices and systems.
- Familiarity with QA processes and their implementation.
- In depth knowledge of the inner-workings of operating systems in general and UNIX & Microsoft specifically.
- Good knowledge of the inner-workings of web servers in general and Apache and IIS specifically.

Required Professional Designation/Certification:

- Bachelor's or Master's degree in computer science, engineering or a related field preferred.

Required Experience:

- Preferred to have at least 2 years industry experience performing similar technical role but not required.
- Desire to work in information security environment is a plus.

In order to be considered on a vacancy:

- You must be performing at standard in your current role for a minimum of 12 months*
- The opportunity should align with your CCDP
- You are responsible for notifying your support person of your application
- You must apply online

*Or in accordance with applicable collective agreement

Job: Sales & Professional Services

Primary Location: ON-Toronto

Organization: TELUS Customer Solutions

Posting Date May 9, 2012, 7:30:21 PM

Hiring Manager: Thayaparen Thankarajah