Research Engineer – Detection and Response

Talos wants YOU! Talos is a dynamic environment that inspires employees to create opportunities by honing their talents and skills every day. Employees are self-motivated, results driven and engaged. We recognize and reward quality results and commitment to our company's purposes and principles.

Summary:

As a member to the Detection Response Team, you will research vulnerabilities in software and network protocols, how they are exploited, be responsible for creation of detection content for the technologies Talos supports, and act as a trusted security partner within the Talos organization and Cisco. You will learn to take a Proof-of-Concept (PoC), verify it exploits the vulnerable condition, create a PCAP of the network traffic created during exploitation, and write detection content to detect that exploitation, while not generating False Positives. You will join a team of subject matter experts in a wide range of fields & technologies, as well as newbies fresh out of college or the local CTF competition!

Essential Duties and Responsibilities:

- Analyze 0days and new security threats and tools
- Analyze malware samples using static/dynamic analysis, debuggers
- Create advanced detection content for Snort, ClamAV, AMP, and Security Intelligence
- Write detailed technical advisories on new vulnerabilities
- Capture network traces from exploits for testing IPS and IDS security effectiveness
- Develop small tools as necessary (this is not a software development position)

Job Requirements:

- Bachelor's degree in Computer Science, Cyber Security, or other tech-related degree preferred, but not required (experience may substitute)
- Solid base knowledge of networking, transport, and application layer protocols, such as IP, TCP, UDP, and HTTP - Experience with vulnerability analysis
- Experience with common methods of exploitation, such as Buffer Overflows, Cross-site Scripting, etc.
- Experience with the structure of common file formats, such as PDF, DOC, and SWF
- Experience with OllyDbg or IDA Pro
- Experience working in both Windows and Linux
- Experience with network traffic dissectors such as Wireshark
- Experience with Perl, Python, or Ruby
- Solid technical writing skills
- Excellent Analytical and problem-solving skills
- Excellent organization, decision making, and verbal and written communication skills
- Ability to work independently with minimum supervision and take on additional tasks as required
- Ability to work with small teams to solve complex problems

Work Conditions:

- Works closely with software reverse engineers and research analysts to quickly develop detection content for all our core applications
- Moderate to high levels of stress may occur at times
- Fast paced and rapidly changing environment
- Extremely talented and experienced team members and mentors
- No special physical requirements
- Constant internal training, heated discussions, and ice cream

If interested, please contact Chris Langer and Chris Carpenter with your resume and/or CV at carp13@cisco.com and chrlange@cisco.com.