Position: Senior Tactical Threat Analyst - Tokyo

Role Overview

Responsibilities:

- Review incoming security events to perform initial triage of events primary from our FortiEDR technology
- Identify and analyze events that appear highly suspicious and notify customs of malware infections
- As needed conduct host-based analysis and forensic functions on Windows, Linux, and Mac OS X systems
- Work on escalated events and help to assist other team members
- Assist in enhancing and tuning Fortinet's Cloud Services and Automated Incident Response (AIR) system
- Review firewall, web, database, and other log sources to identify evidence and artifacts of malicious and compromised activity
- Leverage our FortiEDR platform to conduct investigations to rapidly detect, analyze and contain security threats
- Perform memory forensics and file analysis as needed
- Monitor FortiGuard Labs data and open-source intelligence outlets to maintain proficiency in latest threat actor tactics and techniques
- Perform reverse engineering of threat actor's malicious tools

Requirements:

- Experience with at least one scripting language: Shell, Ruby, Perl, Python, etc
- Strong knowledge of operating system internals, endpoint security experience an active directory a must
- Experienced with EnCase, FTK, X-Ways, SIFT, Splunk, Redline, Volatility, WireShark, TCPDump, and open-source forensic tools a plus
- Demonstrate relevant experience as a contributing member of a security operations, threat intelligence or incident response team
- Experience with malware analysis tools such as IDA Pro, OllyDbg, Immunity Debugger is a plus
- Hands-on experience dealing with APT campaigns, attack Tactics, Techniques and Procedures (TTPs), memory injection techniques, static and dynamic malware analysis and malware persistence mechanism
- Hands-on experience with memory forensics
- Excellent written and verbal communication skills a must
- Reading and writing skills of non-English languages such as Chinese and Russian a plus
- Analysis of Linux and MAC binary files and the understanding of MAC internals is a plus but not required.
- Highly motivated, self-driven and able to work both independently and within a team
- Able to work under pressure in time critical situations and occasional nights and weekends

- Bachelor’s Degree in Computer Engineering, Computer Science or related field or 5 to 8+ years experience with incident response and or Forensics
- GCFA, GCIH, GCFE, GREM or any other related GIAC certification is a plus

Fortinet is an equal opportunity employer.

We will only notify shortlisted candidates.

Fortinet will not entertain any unsolicited resumes, please refrain from sending them to any Fortinet employees or Fortinet email aliases.
Should any Agency submit any resumes to Fortinet, these resumes if considered, will be assumed to have been given by the Agency free of any related fees/charges.

<#LI- XW1>