Endpoint Security Engineer

Summary/Objective

As a member of the Vigilant team, the Endpoint Security Engineer works alongside our Application Development, Security Research and Internal Hunt Teams to implement highly scalable distributed data solutions including the continuous delivery, optimization, monitoring, release management and support for all production and development application systems. This is an exempt position reports directly to the Head of Detection and Response Services.

Primary Responsibilities

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. The Endpoint Security Engineer provides highly visible customer facing service delivery and engineering support services for our Managed Endpoint Protection Service.

- The ideal candidate is an experienced subject matter expert in endpoint detection, prevention, and Active Response.
- Will oversee the entire release management process for deployments, upgrades, updates, and hotfixes across all feature sets to include customer communications, planning, testing, deployment, and monitoring.
- Will administer production and development environment application servers, to including ePolicy Orchestrator (ePO), Agent Handlers, DXL Brokers, TIE Servers and other Windows and McAfee Linux Operating System (MLOS) based systems.
- May have some non-technical responsibilities including project effort estimating, proposal
- generation, and license reporting.
- May participate in sales and proposal presentations in addition to supporting Customer Integration and Sales Team's requests for support.
- Identifies additional product/services opportunities in the customer's organization.

Technical and Functional Skills

The Endpoint Security Engineer will need to bring multi-disciplinary expertise to the role across a wide array of "endpoints" not limited to;

- Servers, workstations, laptops, virtual machines, thin clients, mobile devices, virtualized and cloud hosted resources running various operating systems including Windows, Macintosh, Linux, UNIX, iOS, and Android.
- Engages in hands-on lab testing for detection efficacy, new feature evaluation, or problem resolution.
- Manage all 3rd party vendor support escalations on behalf of customers in ticketing systems and provide periodic updates to stakeholders and leadership.
- Experience deploying and using host based live response tools in multi-platform environments.

Requirements/Qualifications:

The following knowledge, skills and abilities have been identified as those that would most enable an individual to be successful in this role. Applicants will possess a strong combination of all or most of the skills to be competitive in the selection process.

- 5+ years detailed knowledge and hands on experience with McAfee ePO and ePO managed products such as: ENS Endpoint Security, Active Response, Data Exchange Layer (DXL), DLP, Application Control, Device & Removable Media Control, and Endpoint Encryption products in a mid-range or larger environment (Managed Service Provider preferred).
- 5+ years demonstrated mastery in log file analysis, fault isolation and diagnostic/assessment actions including root cause analysis, followed by the determination and self-directed execution of corrective actions.
- Understanding of malware analysis and ability to perform basic static and dynamic analysis.
- Sufficient scripting skills with python, perl, or bash to automate analysis tasks as needed.
- Strong interpersonal & communication skills working with remote peers over IM, phone & video.
- Ability to speak authoritatively and confidently while balancing respect & tact with customers.
- Customer focused, building first-name relationships and protecting their networks as your own.
- Experience providing similar Managed Services to multiple customers is a plus.

Other Requirements

This role leverages a flex-schedule that may involve nontraditional working hours. Must be willing to participate in occasional after-hours maintenance windows and be on-call as needed.

Required Education and Experience

- B.S. in Computer Science, or equivalent experience.
- 10+ years of work experience.

The above statements describe the general nature and level of work being performed by individuals assigned to this classification. This is not intended to be an exhaustive list of all responsibilities and duties required of personnel so classified.