**Title:** Security Analyst

**Department:** Threat Hunting and Response

**Report To:** Security Operations Center Manager

**Summary**

As a security analyst at Pondurance you will monitor, evaluate and report on clients network traffic in an effort to help mitigate their risk of attack, as well as immediately contain threats that do penetrate their defenses.

**Job Description**

The successful candidate will assist in Incident Detection and Response as well as Vulnerability Management for our Threat Management Solution clientele. The candidate will be expected to perform duties to include both host-based and network-based forensic investigations after correlating events from the analyst console tool as part of our monitoring service. The analyst will use static and dynamic malware analysis to repeatedly identify detectable indicators of compromise and work with the team to develop countermeasures. The candidate will also be required to work with the team to resolve issues, tweak current processes, and develop/improve existing work instructions. The candidate will also need to research new threats to an enterprise environment and work with the team to develop effective countermeasures.

**Responsibilities:**

* Monitor and analyze large amounts of network traffic looking for attacker presence
* Analyze event and system logs, perform forensic analysis, implement incident response tactics, and analyze malware as it presents itself
* Identify threat vulnerabilities
* Document and escalate incidents
* Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity
* Provide weekly threat reports to clients
* Conduct monthly vulnerability scans of clients networks

### Education and Experience

### Degree in Computer Science, Engineering, or a related technical discipline or equivalent experience

### Skills and Qualifications

* Must have excellent oral and verbal communication skills
* Experience with system or network administration (Unix/Linux experience preferred)
* Experience and knowledge of information security, IPv4/v6 networks, network devices, proxies, IDS/IPS, and monitoring tools
* Experience with Windows OS
* Demonstrate experience with 2 or 3 of the following: Packet Capture (PCAP) analysis using Wireshark, Familiarity with commercial or open source log or SIEM solutions, Event analysis, correlation, reporting, and alerting, host-based analysis/detection, Service discovery tools such as nmap and vulnerability scanning tools such as Nessus, Nexpose, and/or Qualys
* Ability to communicate technical problems, vulnerability, and risk into a business context understood by the client.
* Ability to multi-task and work independently with minimal supervision
* Ability to make sound decisions and possess excellent problem-solving skills
* Demonstrate strong composure with a balance of urgency and intensity, as well as focus.
* Possess the desire to grow both technically and professionally in the information security field
* Experience with electronics social engineering exercises and campaigns, using social media, email, and phone.

**To Apply**

Please submit resume/CV and cover letter to info@pondurance.com.