**Title:** Mid-Tier Security Analyst

**Department:** Threat Hunting and Response

**Report To:** Security Operations Center Manager

**Company Profile**

Pondurance was founded in 2008 and has since become one of the leading information security solution providers in the Midwest. Our experts set, follow and develop the latest industry trends and cutting-edge security technologies. Our breadth of experience allows the team to provide clients with a formidable yet entrepreneurial ally in information security. We are proud to call many of the leading companies throughout the Midwest our clients, partners and trustees.

At Pondurance we thrive on a culture of excellence by adhering to the following core values:

* Champion Others: Our foundation is rooted in a tenet of servant leadership.
* Be Genuine: Pondurance is built on strong relationships fostered by a culture of integrity and trust.
* Pursue Balance: We must pursue balance in everything we do; work/life, data/emotion, confidence/humility, risk/tolerance.
* Creative Collaboration: We are problem solvers at heart and none of us exist on an island. The team partners with one another and our clients to solve problems together.

**Summary**

As a Security Analyst at Pondurance you will serve as a support system for lead analysts on cyber threats, evaluate and report on client’s network traffic and system logs; 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 also be able to analyze IOCs and work with the team to develop countermeasures. The candidate will also be will be required to work with the team to resolve issues, tweak current processes, and 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:**

* Perform threat hunting on client’s networks and logs, looking for attacker presence
* Serve as support to lead investigator on Digital Forensics Incident Response to include performing forensic analysis, implement incident response procedures, and analyze malware as it presents itself
* Identify and attack vectors, threat tactics and attacker techniques
* Understand customers’ intelligence needs and wants
* Regularly assist with the review and provide reports on observed threats.

### Education and Experience

The Security Analyst position requires a Bachelor’s degree or 1 to 3 years of experience in a related field.

### Skills and Qualifications

* Knowledge of threat hunting and incident response procedures
* Knowledge of Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) tools and applications
* Knowledge of network forensics and host-based forensics is a plus
* Strong understanding of OS behaviors
* Experience and knowledge of information security, IPv4/v6 networks, network devices,

proxies, IDS/IPS, and monitoring tools

* Demonstrate experience with one or more of the following: packet capture (PCAP) analysis using Wireshark or similar tools, familiarity with commercial or open source log or SIEM solutions, event analysis, correlation, reporting, alerting, and host-based analysis/detection, service discovery tools such as Nmap and vulnerability scanning tools such as Nessus, Nexpose, and/or Qualys. *\*Endgame knowledge is a plus*
* Experience with system or network administration (Unix/Linux experience preferred)
* Experience with electronics social engineering exercises and campaigns, using social media, email, and phone
* Skill in evaluating information for reliability, validity, and relevance
* Skill in securing network communications
* Ability to recognize and analyze malware
* Ability to exercise judgement when policies are not well-defined
* Ability to adjust and adapt in a fast pace and dynamic environment.
* Ability to communicate technical problems, vulnerability, and risk into a business

context understood by the client

* 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

**To Apply**

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