THREAT HUNTER

TRAININGS
RECRUITMENTS
CONSULTANCY

eppc

EPPC Albania on behalf of its client, *a worldwide leader in the customer service sector*, is currently recruiting a ***Threat Hunter.***

The focus of Threat Hunter is to proactively investigate security events in an effort to identify artifacts of a cyber-attack with expectation to also participate in several different areas within Security Operations and Incident Response process. Threat Hunter is responsible for reviewing system log events and data packets to proactively detect advanced threats that evade traditional security solutions.

Major responsibilities:

- Track threat actors, their tactics, techniques, and procedures (TTPs), and their associated Indicators of Compromise (IOCs);
- Capture intelligence on threat actor TTPs/IOCs and coordinate with SecOps pods to develop countermeasures;
- Provide forensic analysis of network packet captures, DNS, proxy, net flow, malware, host-based security and application logs, as well as logs from a variety of security sensors;
- Perform Root Cause Analysis of security incidents to develop enhancements to existing alerting tools;
- Compile detailed investigation and analysis reports for internal SecOps consumption and delivery to management;
- Assist in incident response activities such as host triage and retrieval, malware analysis, remote system analysis, end-user interviews, and remediation efforts;
- Develop advanced queries and alerts to detect adversary actions.

Requirements for this position are:

- **Bachelor's (Preferred) or relevant work experience;**
- Previous experience in Information Security and Forensic Analysis;
- Previous experience with the incident response process, including detecting advanced adversaries, log analysis using SIEM and malware triage;
- Experience with packet analysis and usage of deep packet inspection toolsets.
- Knowledge and experience working with the Cyber Kill Chain Model, Diamond Model or MITER ATT&CK Matrix.

How to apply:

To apply for this opportunity, please fill your application at: **https://aplikim.eppc.al**

You will be contacted by eppc only if your CV will be qualified by our recruitment team.