Arkansas Supreme Court

Administrative Office of the Courts
Job Description

|  |  |  |  |
| --- | --- | --- | --- |
| Job Title: | AOC Security Analyst | Grade: | IT06 |
| Division: | Court Information Systems – Operations Team | Revision Date: | August 23, 2022 |
| POSITION SUMMARY:The Administrative Office of the Courts (AOC) is an agency within the judicial branch of government that works to support the state courts on behalf of the Arkansas Supreme Court. The Court Information Systems Division (CIS) is responsible for providing technological support to the state’s courts, making court information available to the public, and developing and implementing online, court-related services. CIS is a team-based organization using the Disciplined Agile framework. You may view our Statement of Core Values at <https://www.arcourts.gov/modernization/statement-core-values>.The AOC Security Analyst works with the Chief IT Security Officer and Chief IT Security Architect to secure the AOC network and cloud environments. This position will monitor security devices, run vulnerability scans, respond to events and incidents, and assist in vulnerability management. The AOC Security Analyst is a member of the Operations Team and works closely with the System Administrators, Desktop Support, Database Administrators, and Network Engineers. **JOB DUTIES:*** Scan network and cloud environments for vulnerabilities using Tenable products.
* Compile/create vulnerability reports of interest for briefing leadership.
* Perform monitoring and data correlation to events of interest using multiple tools such as system event logs, SIEM, IPS/IDS logs, network traffic, anti-virus console and client end-point software to determine if there is an incident.
* Assist in maintenance of security tools, appliances, and other devices as necessary.
* Assist in tuning SIEM appliance, creating rules, and integrating intelligence feeds and log sources
* Recognize attacker and APT activity, tactics, and procedures as indicators of compromise (IoCs) that can be used to improve monitoring, analysis, and incident response.
* Analyze network traffic to identify anomalous activity and potential threats to the network.
* Tune IDS and in-line malware tools based on threat feeds, trust and reputation data, incidents, or vulnerabilities and exploits of downstream systems.
* Identify and escalate events and supporting evidence for incident response.
* Develop and build security content, scripts, tools, or methods to enhance the incident investigation processes and vulnerability remediation.
* Perform basic forensic activities (e.g., conducting examinations of computers, system logs, applications, and networks to locate evidence).
* Perform threat hunting and assist in penetration testing.
* Assist security architect in evaluating security settings and conducting periodic firewall reviews.
* Research and stay up to date on current security threats and vulnerabilities to relevant information systems.
* Assist in vulnerability management and patching.
* Other duties as assigned.

**QUALIFICATIONS:*** Education
	+ Bachelor’s Degree in Computer Science or related field.
* Experience
	+ 3 years of experience supporting complex security environment, to include hands-on investigation and log analysis
	+ May substitute certifications and additional experience for the required education. Acceptable certifications include: CompTIA Security +; ISC2 certs such as: CISSP, SSCP, CCSP; GIAC certs such as: GCIH, GCIA, GCDA, GSOC; EC-Council certs such as: CSA, CEH, CTIA, CPENT, APT, ECIH, CNDA
* Knowledge, Ability and Skills
	+ Sound understanding of OS (Unix/Linux, Windows), IPS/IDS, VPN, Firewalls, Application Security.
	+ Familiarity with NIST/CIS standards.
	+ Familiarity with MITRE ATT&CK framework.
	+ Knowledge of handling and mitigating attacks related to viruses, spoofing, hoaxes, malware.
	+ Knowledge of emerging security threats and their attack vectors especially web application attacks.
	+ Knowledge of threat hunting.
	+ Knowledge of SSL/TLS, certificates, and encryption methods.
	+ Ability to use security tools (including Web application security scanning, Tenable products, Snort IDS, Wireshark, Data Loss Prevention software).
	+ Ability to analyze logs and alarms.
	+ Experience with commonly used tools such as PowerShell, Office 365 Admin Center, SCCM, Active Directory, Python, SSH, etc.
	+ Must have extensive experience in multiple security areas such as SIEM, IDS and Vulnerability Scanning/Remediation.
	+ Must work well both individually and within a team-oriented, collaborative environment.
	+ Strong analytic and problem-solving skills.
	+ Excellent interpersonal, verbal, and written communication skills.
 |
| Last Updated By: | Dain Couch |