INFORMATION SECURITY ANALYST – NETWORK SECURITY

Dillard's is seeking an Information Security Analyst in Little Rock, Arkansas.

Dillard's is seeking an Information Security Analyst to lead the practice of Network Security in Little Rock, Arkansas. As an Information Security Analyst, you will be responsible for leading the team in the discipline of Network Security, including serving as a security consultant for Information Technology. You will advise business process owners, functional area representatives, and other IT personnel on the information security risks within their respective areas of responsibility and help to architect end-to-end solutions with a Network Security focus. There are other responsibilities included with this role that relate to other Security disciplines such as Endpoint Security, Penetration Testing, and Event Correlation.

ROLES and RESPONSIBILITIES

- Inspect and assess current solutions on Network Security risks.
- Find security gaps by performing routine audits of change management and vulnerability management of Network devices.
- Analyze intelligence continuously to identify indicators of compromise and detection signatures.
- Create effective SIEM rules and other tools' alerts to notify staff of network threats and correlate across environments.
- Gather evidence regarding cyber offenses including the forensic analysis of network traffic, packets, and log files.
- Ensure security controls are in compliance with applicable laws, regulations and policies to minimize risk and audit findings.
- Architect/design security controls and analysis processes.
- Train others on the team in network security concepts.
- Identify areas where IT processes need to be established or improved.
- Participate in on-call rotation.

QUALIFICATIONS and EXPERIENCE

- Authorization to work in the United States without sponsorship.
- Experience analyzing risk in accordance with regulations including PCI, HIPAA, and Sarbanes-Oxley.
- Experience creating processes, procedures and solutions that reduce technical risk and increase operational efficiency.
- Knowledge of networking infrastructure concepts including routers, switches and firewalls, network vulnerabilities, wireless networking, LAN/WPA security, intrusion detection/prevention, perimeter security, vulnerability analysis, VPN, IPSEC, IDS, Firewalls, Cisco IOS, Next-Generation Firewalls, Snort.
- Understanding of security threats and solutions for IT systems.
- Ability to work independently and in teams, while meeting multiple deadlines.
- Strong interpersonal and communication skills with proven decision making skills.
- Desire to troubleshoot and lead investigations.
- History of and commitment to ethical behavior and ethical full disclosure.
- Background in several of the following areas: cyber security, intrusion detection/prevention, OS architecture, malicious network traffic identification, malicious code detection/prevention, security auditing, security architecture, security awareness education, databases, application security architecture for web environments, identity management, PKI, encryption methods/standards, event correlation, authentication services, advanced incident handling and forensics best practices, PKI.