JONATHAN DAVIS

CLOUD SECURITY ENGINEER

✉ bigdavis@gmail.com

☎ 501-765-3925

📍 Little Rock, Ar 72201

PROFESSIONAL SUMMARY

Technically sophisticated and dedicated cloud security engineer with 20 years of experience administering, monitoring, maintaining, and operating security solutions for high profile corporations and securing their cloud computing deployments to protect sensitive data. Cybersecurity specialist aligning architecture plans and processes with security standards and business goals using experience in supporting, developing, and testing security framework for cloud-based software.

EXPERIENCE

Secureworks – Cloud Security Engineer
10/2017 - Present

- Formulate, implement, and operate written controls to secure cloud-based systems.
- Utilize cloud-based APIs when appropriate to write network/system level documentation for securing cloud environments.
- Developed a cloud assessment tool to check customer cloud environments to ensure security best practices and/or regulatory controls are being implemented for multiple platforms such as Azure, o365, and AWS.
- Developed AWS Config Rules and policies to monitor production systems for unencrypted volumes and overly permissive security groups in all accounts and configure Lambda functions to automatically remediate findings.
- Created a cloud-based security platform that monitored and analyzed data from multiple sources to identify potential threats.
- Discuss Root Cause Analysis with clients after incidents.
- Discuss technical requirements for contracted services with clients and complete implementations of managed services.
- Meet with customers on a set cadence to provide program utilization review, security guidance, and deliver strategic recommendations that will help improve their security posture.
- Collaborate with customers to learn about established security controls within their environment and the value they will add to security event analysis.

SKILLS

- Cloud Security Infrastructure
- Regulatory Compliance
- Solutions Deployment
- Architectural Standards
- Cloud Computing
- Identity & Access Management
- Microsoft Entra ID

CERTIFICATIONS

- CYSA+
- CASP+
- CCSP
- CCSK
- AWS Security Specialty
- AWS Certified Developer
- AWS Solutions Architect
- AWS Sysops Administrator
- Azure Administrator
- Azure Security Engineer

Atos - Network Security Engineer
Little Rock, Ar • 01/2013 - 03/2017

- Designed, created, and implemented policies for IDS and IPS devices for multiple fortune 500 clients which included clients in the financial sector, energy, oil\gas, and medical.
  Fostered and cultivated collaborative working relationships to effectively establish connectivity and open firewall rules between devices.
- Collaborated with application and infrastructure teams to design and architect infrastructure (network, OS, databases) and applications to protect against attackers.
- Responded to audits from SOX, HIPAA, PCI, as well as internal security audits. Understood and followed NERC CIP requirements.
- Ensured adequate security solutions and controls are in place throughout client's Cloud platform, services, and solutions.
- Manage and coordinate major rollouts for McAfee, SourceFire IPS. Fortigate, Cisco Firepower Next Gen Firewalls, Fireeye Advanced Malware, and Cisco ACS TACACS.
- Met with clients on a regular basis to go over security posture and make improvements.

SAIC - Security Systems
Little Rock, Ar • 01/2002 - 03/2013

- Primary HIPS Engineer with the responsibility of designing and creating policies, granting exceptions and exclusions to policies for Host Based Intrusion Detection using McAfee ePO.
- Functioned as a Tier III engineer\architect for Identity management and Active Directory. Determined access levels and set policies\processes.
- Closely collaborated with security architects in developing cloud security frameworks for the enterprise. Provided thought leadership on monitoring, alerting, reporting, and blocking.
- Acted as a quality assurance by conducting annual penetration test.
- Scan and test all applications using IBM Rational Appscan software.
- Met with clients to provide guidance and direct technical engineering support teams and developers on mitigating risks found during risk assessments.
- Provided subject matter expertise in network security configurations.
- Collaborated with functional-area specialists and security specialists to design, configure and/or develop security solutions