https://www.iconnectitbs.com/careers/web-application-firewall-engineer/

Description

We are seeking a skilled Web Application Firewall Engineer with expertise in web application firewalls (WAF), specifically AVI WAF or similar technologies. The ideal candidate will have a strong background in network and application security, VA/PT assessments. This role requires a proactive approach to security, ensuring our web applications are protected against evolving threats.

Responsibilities

Deployment and Configuration:

• Implement and configure AVI WAF solutions in on premises and cloud environments.

Integration:

• Integrate AVI WAF with existing systems and applications to ensure compatibility and seamless operation.

Monitoring and Optimization:

• Monitor WAF performance, analyse traffic patterns, and optimize settings for enhanced security and efficiency.

Troubleshooting:

• Identify and resolve issues related to WAF deployment, configuration, and operation. Support incident response and remediation efforts.

Documentation:

• Create and maintain comprehensive documentation for WAF configurations, procedures, and best practices.

Collaboration:

• Work with cross functional teams (IT, security, development) to implement and integrate WAF solutions effectively.

Compliance:

• Ensure WAF implementations comply with organizational security policies and industry standards.

Training and Support:

• Provide training and support to team members and end users on WAF usage and best practices.

Qualifications

• Proven experience with AVI WAF or similar web application firewall technologies.

Hiring organization

iConnect IT Business Solutions

Job Location

Dubai

Date posted

November 14, 2024

- Hands on experience with network security, application security, and firewall configurations.

- Familiarity with cloud platforms (AWS, Azure,) and virtualization technologies.

- Experience in deploying, configuring, and maintaining on-prem/cloud native web application firewalls.

- Strong knowledge of web application security and threat mitigation.

- Proficiency in scripting and automation (Python, PowerShell).

- Experience with load balancing, traffic management, and SSL/TLS configurations.

- Knowledge of static and dynamic application security testing, mobile application security testing, and software composition analysis.

- Familiarity with risk management frameworks, intrusion prevention/detection, and security event response.

- Experience in API security with cloud environments.

- Experience with Zero Trust Architectures

- Security Information and Event Management (SIEM) platforms experience is required.

- Experience with tools for web application testing (e.g., Cymulate) and extensive knowledge of networking protocols.

- Experience with vulnerability assessment (VA) and penetration testing (Pentest).

- Skills in packet and traffic analysis.