



XPERTECHS Job Description

Job Title: Cloud Security Engineer/Architect (Office 365)	Location: Ellicott City
Department: Service Delivery & Operations	FLSA Status: Salary, Exempt
Reports To: VP of Service Delivery	Compensation: Base Pay + Bonus; includes medical, STD, LTD, life insurance, 401k and vacation plan

Summary

Office 365 EMS Technical Lead will be the chief architect and technical leader of advanced Office 365 functionality for an organization. The successful candidate will have significant knowledge of Office 365 platform, services, and associated configurations. Will provide expert consultation and leadership to the Office 365 Enterprise Mobility + Security suite of services (Identity and Access Management, Cloud Application, Azure Active Directory and Mobile Device Management solutions). Key responsibilities include architecture, configuration, best practices, and risk management strategies to support Office 365 operational KPIs. Will also provide expertise in Office 365 governance and work within an ITIL service delivery model. The Office 365 EMS Technical Lead will support the Service Manager in gathering and analyzing requirements, solution design, and execute a high level of security and risk management, while delivering high customer satisfaction. Additionally, the candidate must possess strong creative communication, and collaboration skills.

Essential Duties and Responsibilities

- Review vulnerabilities and track resolution
- Security assessments of client Office 365 implementations or planned implementations
- Security assessments of related SaaS products and services
- Perform SaaS security assessments using domain knowledge and automated tools (CASB etc)
- Security Information and Event Management (SIEM)
- Monitor SOC Alerts queues and continually process, prioritize, and automate resolution of issues
- Review and process threat intel reports and sources
- Perform customer security assessments
- Develop, Draft, and Publish internal SOC policies and procedures
- Deploy and maintain security sensors and tools
- Monitor security sensors and review logs to identify intrusions
- Develop and deploy custom monitoring solutions according to client and applications requirements
- Manage and execute the monthly/bi-monthly summary & detailed client network health reports

Supervisory Responsibilities

No direct reports. Vendor management required.

Work Environment

XPERTECHS has an interactive, fast-paced work environment. Responsibilities require an adjusted work schedule and/or evening/weekend hours in order to satisfy customer needs as well as position requirements. The Cloud Security Engineer position offers the flexibility of remote worker arrangements.

Minimum Qualifications

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- **Education and/or Experience:** This position requires a minimum of an Associate's Degree (with a Bachelor's degree preferred); at least 3 years' recent IT support or SOC experience to the small or mid-sized business market; or an equivalent combination of education and/or experience. Must be able to effectively communicate in specific terms about technologies used by our clients, including Windows Server, Network Security, Scripting, Event Logs, Backup, Virtualization, and LAN/WAN architectures.
- **Knowledge, Skills and Abilities:** The must have a strong aptitude in Office 365 enterprise mobility and security tools.
- **Physical Demands:** While performing the duties of this job, the employee is regularly required to communicate with and present information to others and access information using a computer for several hours at a time. Employees must have mobility throughout the office and may occasionally drive or ride up to 30 miles to other service locations.
- **Emotional Demands:** The employee must be emotionally mature and be able to handle difficult and complex client and work-related situations. Candidates must possess strong problem solving, conflict resolution, and interpersonal skills. They must be self-driven and possess a positive mental attitude.
- **Collaboration/Teamwork:** The Cloud Security Engineer creates commitment to common goals; identifies competing interests and finds ways to balance them; values contributions of all team members and other constituencies; values team accomplishments over individual accomplishments; leverages others' strengths and experiences to achieve team goals; co-operates with colleagues and shares resources.
- **Intellectual Demands:** Excellent written and verbal communication skills are essential, as well as effective organizational, multi-tasking, and prioritization skills. Candidates must be able to read, analyze, and interpret general industry periodicals, technical procedures and governmental regulations. They must be able to interpret a variety of instructions furnished in written, oral, diagram, or schedule form. They must be able to effectively present information and respond to questions from clients, vendors, and employees.

All job requirements are subject to possible modifications. This job description in no way states or implies that these are the only duties to be performed by the employee occupying this position. Requirements are representative of minimum levels of knowledge, skills, and/or abilities to perform this job successfully; the employee must possess the abilities or aptitudes to perform each duty proficiently. Continued employment is on an "at-will" basis. Employee must be able to relate to other people beyond giving and receiving instructions: (a) can get along with other co-workers or peers without exhibiting behavioral extremes; (b) perform work activities requiring negotiating, instructing, supervising, persuading or speaking to others; and (c) respond appropriately to constructive criticism from a supervisor.