SANDS CORP CYBER JOB

Posting ID: E051616
Company: Las Vegas Sands Corp
Job Title: Vulnerability Management Analyst
Position Type: Full-Time, Entry Level
College Major(s): Computer Science

Company Website: http://lvissa.org/jobs/
Work Location: Las Vegas, NV
Salary: N/A
College Level(s): Graduates

OVERVIEW
The primary responsibilities of the Vulnerability Management Analyst is performing the vulnerability and configuration scanning and mitigation processes and procedures.

All duties are to be performed in accordance with departmental and Las Vegas Sands Corp’s policies, practices, and procedures.

Essential Duties & Responsibilities

Key Responsibilities

- Ability to use automated tools and analysis to assess operating systems, applications, databases, servers, and network equipment for vulnerabilities and secure configurations
- Knowledge of and familiar with identity and authentication management and their architecture
- Ability to architect solutions for cross domain solutions to include Microsoft, Linux, IBM, SCADA, and Gaming
- A working knowledge of vulnerabilities and configuration settings and their exploitation in order to gain access to networks, applications, hosts, and desktops. (White hat only)
- Security engineering
- Malware analysis
- Forensics analysis
- Reverse software engineering
- Wireless security architectures, scanning, rogue detection and prevention and secure configurations
- Threat/Vulnerability Research
- Source Code Scans
- Red Team engagements
- Excellent writing and speaking skills
- Red Team and Tabletop exercise experience
- Ability to gather and report meaningful metrics

Key Processes

- Lead and coordinate the activities of vulnerability and configuration scanning and mitigation.
- Align vulnerability and configuration mitigation functions with the organization’s overall business objectives by reducing information technology's exposure to vulnerabilities.
- Work closely with IT and Cyber peers to architect patching strategies for potential vulnerabilities ensuring information security policy and best-practices are enforced globally.
- Work with internal business units to drive enterprise-wide patching efforts for approved third party software, manage expectations and set service level agreements.
- Work with internal business units to drive secure configurations in images used for desktops, servers, network devices, and wireless network devices.
- Produce meaningful metrics and reports in accordance with direction from the Director of Vulnerability Management and Penetration Testing.
- Participate in incident response activities as needed
- Knowledgeable in change management processes and participate in change control process as needed.
- Coordinate with Cyber Architecture and Engineering in the completion of a risk register.

Consistent and regular attendance is an essential function of this job

Performs other related duties as assigned

Minimum Qualifications

- 21+ years of age
- Proof of authorization/eligibility to work in the United States
• Associate’s degree in Information Systems or equivalent in relevant discipline preferred.
• At least five years of experience in Information Security and Technology with expertise in configuring and using scanning tools, verifying found vulnerabilities, researching found vulnerability mitigation solutions, and working with varied business units to mitigate valid vulnerabilities, and creating secure images.
• Five years’ experience in hands-on vulnerability and configuration scanning and mitigation can be substituted for a certification.
• This position is responsible for planning, scheduling, running and mitigating vulnerability and configuration scans in accordance with direction from the Director of Vulnerability Management and Penetration Testing.
• The ability to communicate and work effectively with all facets of the corporation is expected along with expertise in communicating with Management. It’s essential that this position have the ability to explain in plain English what each vulnerability and insecure configuration is and what activity it could allow in the LVSC environment.
• Expertise in promulgating risk to the business by correlating vulnerabilities, configuration settings, by performing an assessment of the risks that considers the threats, our vulnerability to those threats, the likelihood that vulnerabilities will be exploited, the impact that exploitation will have on the company, and finally what the residual risk will be after the vulnerabilities, and insecure configuration settings are remediated.
• Possess an information security certification such as CISSP, or GISP plus two years’ experience in vulnerability scanning and mitigation.

Work Environment

• Work in a fast-paced, results-oriented and ever-changing environment
• Able to maintain composure under pressure and consistently meet deadlines with internal and external customers and contacts
• Maintain physical stamina and proper mental attitude while dealing effectively with guests, management, team members, and outside contacts

Job Segment: Manager, Network, Information Systems, Telecom, Telecommunications, Management, Technology