PLUMAS COUNTY **NEW: 06/2023**

NETWORK /EDR ADMINISTRATOR

DEFINITION

Under general direction of the Director of Information Technology to configure, maintain, and administer all County networks and EDR (endpoint detection & response) tools used by all County departments; and to perform related and other duties as required.

DISTINGUISHING CHARACTERISTICS

A Network/EDR Administrator is responsible for overseeing an organization's database networks to ensure proper maintenance and cybersecurity. Identifies threats to security and acts as lead on support response to the EDR platform. Duties include working with other IT staff and County employees to identify network or computer system needs, overseeing the installation of new hardware or software and using employee feedback to isolate issues. This position has access to and supports the County's financial and personnel systems with access to confidential information.

This position analyzes and monitors all ongoing activities for devices connected to the County's network and provides real-time threat detection and visibility for automated threat response for security teams for cybersecurity.

REPORTS TO

Director of Informational Technology

CLASSIFICATIONS DIRECTLY SUPERVISED

None

EXAMPLES OF DUTIES

- Administers and optimizes all County networks, troubleshooting and resolving network issues, implementing cybersecurity measures, and proactively optimizing network performance.
- Maintaining computer networks and systems including software, mainframes, VPNs, routers and other physical hardware.
- Combine and correlate full-spectrum endpoint visibility data across al devices to analyze activity and provide details about Indicators of Compromise (loC) as well as Indicators of Attack (IOA).
- Installing and configuring network equipment to update or fix hardware or software issues.
- Updating virus protection software to keep data and communications protected.
- Monitoring computer systems to improve network performance for computer systems and networks.
- Communicating networking issues to other employees and management, especially in training new users.
- Fixing software and hardware configuration issues for users on-demand or from inspection of the systems.
- Administers and optimizes County EDR (endpoint detections & response) tools.
- Administers county data backups and related tools.
- Works with state entities / vendors to understand network requirements and determines best practices to facilitate those needs while complying with county policies.
- Prepares thorough topologies and documentation on County networks.
- Prepares thorough and clear documentation on County EDR tools.
- Prepares & hardens county endpoint operating systems.
- Monitors new security risks and prepares reports / dashboards on these risks for the Information Technology Director.
- Continually monitor for necessary updates, ensuring optimal network performance and security.
- Installs and tests new computer hardware, software, and operating systems.
- Assists with county desktop support.
- Perform related duties as assigned.

TYPICAL PHYSICAL REQUIREMENTS

Sit for extended periods; frequently stand and walk; normal manual dexterity and eye-hand coordination; some kneeling and stooping; physical ability to lift and move objects weighing up to 50 lbs.; corrected hearing and vision to normal range; verbal communication; use of office equipment including computers, telephones, calculators, copiers, and FAX.

TYPICAL WORKING CONDITIONS

Work is performed in an office environment; some exposure to dust and electrical energy; continuous contact with staff and the public.

DESIRABLE QUALIFICATIONS

Knowledge of:

- Analyzing and figuring out the systems needs of a government County agency.
- Use of various data analytics techniques to detect suspicious system behavior.
- Installing hardware and software for the network.
- Antivirus (AV) and antimalware (AM) tools.
- Advanced threat detection and malicious activity detection.
- Containment of the cyber security threat at the compromised endpoint.
- Incident data search and investigations – alert triage with high fidelity alerting.
- Suspicious activity and remediation guidance.
- Threat hunting to protect the endpoint against future attacks.
- Keeping systems operating efficiently by performing any necessary upgrades and repairs.
- Planning a strategy to maintain system security on the computers and the network.
- Optimizing and evaluating the system regularly.
- Assigning and updating security permissions for the system network.
- Training or directing users on the correct use of software and hardware within the system.
- Performing problem-solving tasks when alerted by an employee user or monitoring system.
- Computer operating systems.

Ability to:

- Analyze user information system needs and develop systems to meet those needs.
- Proactively monitor, detect, and remediate or isolate threats on endpoint devices as they happen.
- Focus on endpoint security as a key part of the overall County's IT security strategy.
- Lead and oversee deployment, operation, and maintenance of the global EDR platform.
- Block malicious activities throughout the County's computer systems.
- Detect to contain, investigate, and eliminate invasive cybersecurity threats.
- Provide remediation options in response to threats to restore affected systems.
- Evaluate and prioritize projects under the direction of the Information Technology Director.
- Maintain the confidentiality at all times
- Communicate clearly and concisely, both orally and in writing.

Training and Experience:

A minimum of two (2) years' experience in TCP/IP, Cisco Training, familiarity with backup and recovery software and methodologies, and computer & server operating systems.

Specific knowledge of Cisco Meraki Administration, Firewall Configuration, Cohesity Backup Administration, Crowdstrike Administration, and Microsoft Windows.

Equivalent to completion of twelfth grade and additional college courses or specialized training in computer programming, operating systems, network operations, or related fields. A bachelor's degree in a related field is highly desirable.

Special Requirements:

Must possess a valid driver's license at time of application and a valid California Driver's License by the time of appointment. The valid California Driver's License must be maintained throughout employment.

All County of Plumas employees are designated Disaster Service Workers through State law (California Government Code Section 3100-3109). Employment with Plumas County requires the affirmation of a loyalty oath to this effect. Employees are Required to complete all Disaster Service Work related training as assigned, and to return to work as ordered in the event of an emergency.