IT Analyst, Operational Technology and Cyber

Do you want to join a team that values Service, Collaboration and Excellence?

Do you want to work with an organization that is committed to serving its customers and community by providing clean, reliable, and affordable energy to Long Island and the Rockaways?

Is being part of a value-driven organization important to you?

If yes, please check us out!

Who We Are

We are a team of motivated, engaged, and exceptionally talented self-starters, willing to roll up our sleeves and do what is necessary to get the job done. If you are interested in joining this dynamic team and have a passion to learn, develop, and want your experience to make an immediate impact, please apply.

To find out more about us, please visit our website: www.lipower.org

What We Offer

We offer an environment of continuous development and growth with a thriving company culture, exceptional colleagues, and exceptional benefits. Our benefit package includes:

- Hybrid work options available and flexible hours
- Excellent health insurance
- No employee cost for dental and vision insurance
- Paid holidays and generous paid time off
- Professional development opportunities
- Educational assistance opportunities
- Multiple retirement plan options with company contribution
- Short-term and long-term disability coverage
- Flexible spending account with company contribution
- Life Insurance
- 529 College Savings Program
- $300 Wellness Reimbursement

LIPA's Corporate Values
Service: Our work is service. Everything we do is for the benefit of our customers.
Collaboration: Operate as one LIPA team. Everyone is included.
Excellence: One plan, with relentless implementation. Clear performance goals.

What You'll Do At LIPA

The IT Analyst, Operational Technology (OT) and Cyber is responsible for the oversight of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) environments, and the protection of operational technology assets from cyber threats. This role focuses on identifying vulnerabilities, monitoring security events, supporting incident response, and ensuring the resilience of critical infrastructure systems in use by the Operating Services Company.

The IT Analyst works closely with internal and Operating Company engineering, IT, operations, and compliance teams to strengthen cybersecurity across industrial environments while maintaining system availability, safety, and regulatory compliance.

The IT Analyst, OT and Cyber will:

- Monitor the Service Provider's performance of managing the OT environments for cyber threats, anomalies, and suspicious activity using security tools and platforms and consult with, and advise, the Service Provider's OT group for any issues observed.
- Analyze alerts and incidents affecting industrial systems, including SCADA, PLCs, HMIs, DCS, and related infrastructure.
- Conduct risk assessments and vulnerability reviews for OT assets and industrial networks. Partner with the OT Cyber group to ensure all incidents are fully investigated and appropriate response measures are taken to remediate risks.
- Support incident response efforts for cybersecurity events impacting operational environments.
- Assist in developing, documenting and maintaining OT cybersecurity policies, standards, and procedures to minimize system risks and vulnerabilities.
- Collaborate with engineering and operations teams to resolve issues, implement security controls and assist in the annual testing for the OT environments with minimal disruption to production.
- Maintain accurate and current asset inventories, network diagrams, and system baselines for OT environments.
- Evaluate and recommend security technologies for industrial systems.
- Participate in security audits, compliance assessments, and regulatory reporting.
- Track emerging OT cyber threats, vulnerabilities, and industry best practices and provide recommendations on what practices should be modified to ensure LIPA and the service provider align with best practices.
- Support disaster recovery, business continuity, and resilience planning for operational systems.
- Perform other related duties, as necessary.

What We Need

- Bachelor's degree in Cybersecurity, Information Technology, Engineering, Computer Science, or related field or equivalent experience.
- Three (3) years of experience in cybersecurity, industrial control systems, or operational technology environments.

- Experience in critical infrastructure sectors such as utilities, manufacturing, transportation, or energy.
- Experience with threat intelligence and industrial cyber risk management.
- Experience conducting risk assessments, incident response, and forensic analysis in operational environments.
- Must possess at least one (1) of the following industry certifications: GIAC GICSP, CISSP, Security+, or ISA/IEC 62443 certifications.

- Knowledge of Windows, Linux, and embedded industrial systems.
- Familiarity with network segmentation, zero trust principles, and secure remote access solutions.
- Knowledge of OT/Industrial Control Systems (ICS) protocols such as Modbus, DNP3, OPC, IEC 61850, or similar.
- Familiarity with SCADA systems, PLCs, Remote Terminal Units (RTUs), and industrial networking concepts.
- Understanding of cybersecurity frameworks such as NIST, ISA/IEC 62443, or NERC CIP.
- Experience with SIEM platforms, intrusion detection systems, vulnerability management, and endpoint protection tools.
- Strong analytical, problem sensitivity and problem-solving skills.
- Skill in analyzing and evaluating systems.
- Critical thinking skills.
- Excellent written and verbal communication skills.
- Interpersonal and collaboration skills and the ability to work well with others.
- Knowledge of regulatory requirements and audit processes related to critical infrastructure protection.

What We Want (Preferred Qualifications)

- Advanced degree in Cybersecurity, Computer Science, Engineering, Information Technology, or a related field.
- Five (5) years of experience in cybersecurity, with at least two (2) years supporting Operational Technology (OT), Industrial Control Systems (ICS), or SCADA environments.
- Possess multiple professional certifications such as: CISSP, GICSP, Security+, CISM, or ISA/IEC 62443 credentials.
- Hands-on experience with industrial protocols including Modbus, DNP3, OPC, IEC 61850, or Profinet.
- Understanding of industrial network architecture, segmentation strategies, and secure remote access controls.
- Knowledge of cloud-connected industrial environments and IIoT security considerations.
- Familiarity with scripting or automation tools such as PowerShell, Python, or Bash for security operations.
- Demonstrated ability to balance cybersecurity priorities with operational uptime and safety requirements.

Salary Range

- $ 86,400 - $105,600

LIPA's Corporate Values
Service: Our work is service. Everything we do is for the benefit of our customers.
Collaboration: Operate as one LIPA team. Everyone is included.
Excellence: One plan, with relentless implementation. Clear performance goals.

How You Can Apply:

- Interested parties should submit their cover letter and resume to Gary Martens, Director, Human Resources and Administration, at **2026ITanalyst@lipower.org**

LIPA is an equal opportunity employer.

All people with disabilities are encouraged to apply.

If you require a reasonable accommodation in completing this application, interviewing, completing any pre-employment testing, or otherwise participating in the employee selection process, please direct your inquiries to Gary Martens, Director, Human Resources and Administration.