

SECURITY SERVICES

EXTERNAL VULNERABILITY SCANNING SERVICE

ESI will provide perimeter security tests utilizing public IP network scans. Testing helps to assure that security upgrades and patches are applied and changes in the network do not create new vulnerabilities. Testing will also provide the reports and documentation needed for compliance. Reports are provided either monthly or quarterly per the agreement.

1. An external vulnerability scan including analysis of web servers and perimeter security devices.
2. A security report with vulnerability analysis including risk levels.
3. Technical recommendations for remediation.

INTERNAL VULNERABILITY SCANNING SERVICE

Vulnerability Scanning will enhance security posture through proactive identification and remediation of vulnerabilities. ESI will test all devices providing internal IP network scans. Testing helps to assure that security upgrades and patches are applied and changes in the network do not create new vulnerabilities. Testing will provide the reports and documentation needed for regulatory compliance. Reports are provided either monthly or quarterly per the agreement. The main elements of the service are:

1. An internal vulnerability scan including analysis of network, servers and workstations.
2. A security report with vulnerability analysis including risk levels.
3. Technical recommendations for remediation.



SECURITY ANALYSIS

The remote security assessment produces recommendations to mitigate vulnerabilities for information systems. Testing is available with adherence to security standards from ISO 17799 and ISO 27001. Security is also assessed for information privacy compliance.

A risk based methodology is used to determine the appropriate countermeasures for information systems. Countermeasures are audited and recommendations are produced to mitigate risks. Technical approaches are utilized for the internal, external vulnerability tests and detailed reports of vulnerabilities are produced. The assessment process is facilitated by the on-line Security Portal. The Portal provides reports and a venue for collaboration for the client and ESI to assess risks and provide recommendations for remediation. Reports include response areas for clients to input responses and facilitate documentation to incorporate an integrated risk based approach to the client's security program. The report is helpful for internal audit and regulatory examiners. In addition, there is a management summary to provide an appropriate update for senior management.

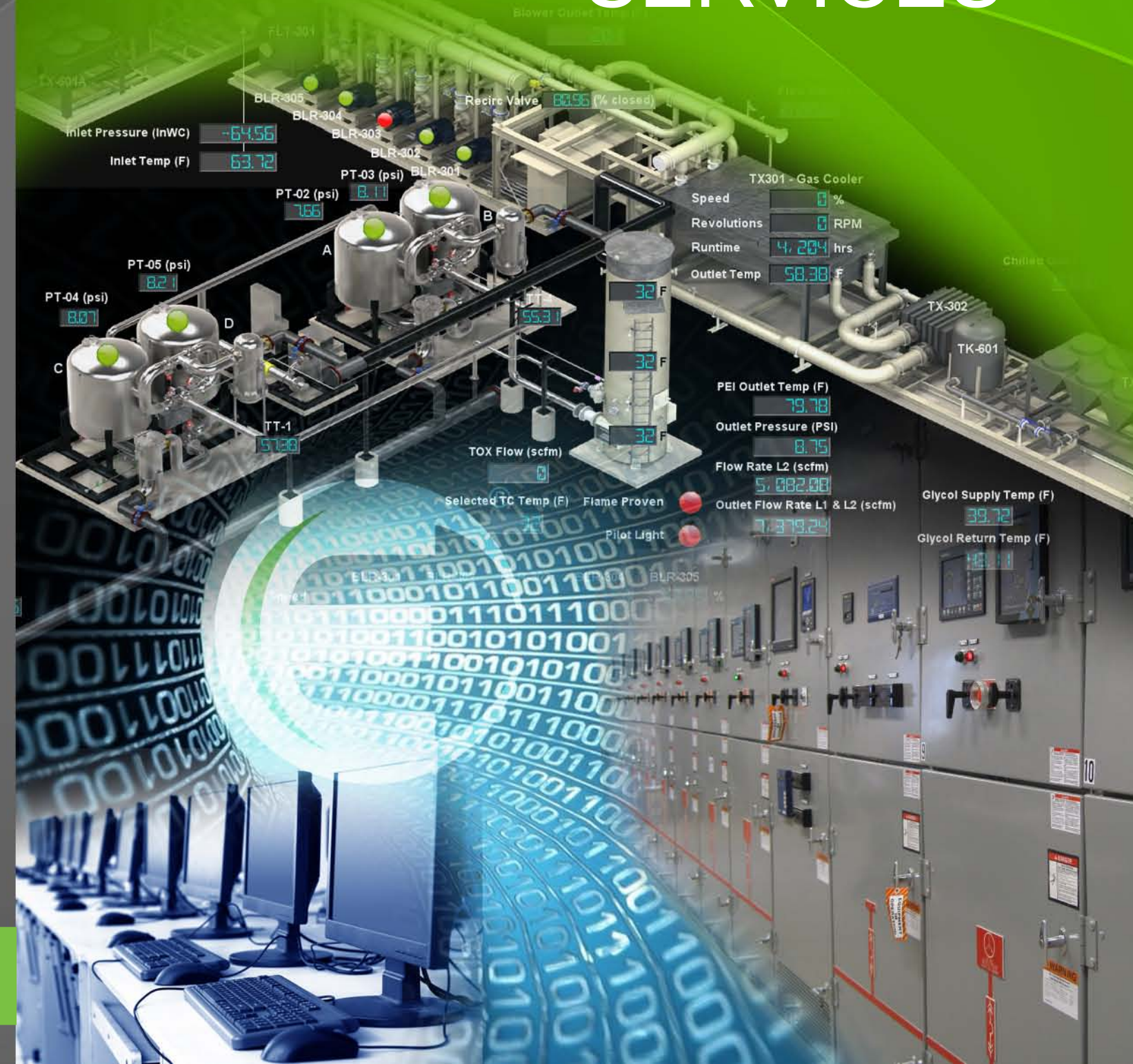
- **Administrative Controls** - Assessment recommendations will support your companies operational risk management program in developing appropriate countermeasures to mitigate the risks in the following areas:
 - IT Controls review for current regulatory compliance.
 - Information Systems Strategy, Planning and Personnel
 - Relationship with Outsourced Vendors
 - Disaster Recovery / Business Continuity Planning
 - Information Systems Operations
 - Network Support & Security
 - Hardware & Operating System Support
 - Application Development and Maintenance
 - Information Systems Security
 - Organization Controls
 - Information Security Risk Assessment Program
- **Internal Technical Controls** - analysis of firewall, IDS / IPS, servers and workstations. Tests of the internal control objectives are performed to identify vulnerabilities associated with internal network and system assets. The review of the internal

control objectives includes vulnerability scanning and evaluation of security in the following areas:

- Network Design
- Wide Area Network
- Local Area Network
- Voice System
- Internal Firewall
- Internal Servers
- Internal Printers
- Wireless facilities
- Modems
- Vendor and Partner Connectivity
- Logging and Network Time
- Data in Transit and Portable Devices
- **External Technical Controls** - analysis and testing of the firewall, IDS / IPS, border routers and Internet services in the following areas:
 - Internet Design
 - Internet Services
 - Internet Border Devices
 - Internet Intrusion Detection / Prevention System (IDS / IPS)
 - Internet Firewall
 - Remote Access
 - Internet Servers
- **Web Security Test** - An analysis of the data provided on website for regulatory compliance. Domain extension fraud will also be analyzed.
- **Remote Social Engineering Tests** - The goal of social engineering is to create an inappropriate trust with an employee in order to acquire sensitive information. ESI will use a number of techniques to heighten the awareness of your organization and improve operational security. ESI tests how employees interact with outside contacts. The tests include attacks by physical and technical approaches to obtain unauthorized disclosure of information.
- **Executive summary** - key recommendations for presentation to the senior management.
- **Conference call** - consultation call to the IT Staff to explain the details of the assessment and answer questions about remediation.



IT SUPPORT SERVICES



ANY QUESTIONS? WE HAVE ANSWERS!

PH. 541.549.8766 | FX. 541.549.1901
15820 BARCLAY DRIVE | SISTERS, OR 97759
WWW.ENERGYNEERINGSOLUTIONS.COM

IT SUPPORT SERVICES

Energynearing Solutions (ESI) has the expertise to effectively manage your SCADA system, perimeter security, and virtual environment protecting your assets from today's threats. We can be your complete IT solution provider; has managed security services are available as turn-key services or co-managed services to assist your IT staff; and offers virtual infrastructure solutions integrated to provide a complete Disaster Recovery solution providing the highest uptime possible.

SCADA SYSTEMS MANAGEMENT

ESI SCADA systems management includes the following services:

- Online ticket creation and on-site systems administration with an emphasis on security.
- Server support that includes performance tuning and secure implementations.
- Systems backup management, implementation, and testing.
- Server security and health monitoring.
- New software implementation consulting.
- Antivirus software management.
- Software updates implementation.
- Hardware and software maintenance contract management.
- Management documentation including End User Agreements and Security Policies
- VMware Disaster Recovery Solutions.
- IT assets management and life cycle planning

NETWORK DEVICE MANAGEMENT

ESI is pleased to offer clients Network Device Management the following services includes:

- Maintenance administration, device upgrades, patches and incident response.
- Backup of device configurations for Disaster Recovery.
- Software maintenance – Administer applicable software upgrades. Client to pay the cost of the manufacturer's software maintenance.
- Hardware maintenance – Administer manufacturer maintenance and provide time and material response to on-site maintenance needs. Client to pay the cost of the manufacturer's maintenance.
- Online reports including ticket history, change control, audit trail.
- Change control online approval mechanism.
- Archiving of files including policies, procedures, and configurations.

MANAGED FIREWALL SERVICE

Firewall management provides the basic device services included in network device management as described in Network Device Management, as well as the following specialized services:

- Firewall documentation on demand including security diagram and firewall rules with business purpose for each rule.
- Firewall changes included. Services or troubleshooting beyond firewall management are billable.
- Firewall change control procedure with customer authorization for all changes.
- Quarterly managed security services conference call with Company staff.
- Monitor uptime with SNMP.
- VPN configuration and management.
- Monitor and gather syslog information and alert on security events of interest.
- Reports emailed to client weekly and archived on the Security Portal.

BUSINESS VALUE

ESI's service will reduce risk, improve performance, and manage cost by:

- Providing a way to track all help-desk requests and provide quarterly reports.
- Ensure your SCADA Systems are secure and performing properly.
- Monitor and manage system backups to ensure quick recovery.
- Monitor and manage antivirus software to ensure proper functionality.
- Track hardware maintenance agreements to ensure the proper coverage.
- Establish the needed systems documentation to protect your company in the event of a security breach.

BUSINESS VALUE

ESI's service will reduce risk, improve performance, and manage cost by:

- Providing accounting of assessments to determine where costs can be cut.
- Eliminating costly downtime by quickly recovering IT assets.
- Applying performance and security patches in a timely manner.
- Ensuring downtime is minimal by organizing and maintaining maintenance agreements and providing first response.

BUSINESS VALUE

ESI service will reduce cost, improve performance, and manage risks by:

- Providing a way to track VPN connectivity access.
- Ensure secure remote connectivity for end users and remote locations.
- Monitor and manage system backups to ensure quick recovery.
- Track hardware maintenance agreements to ensure the proper coverage.
- Establish the needed documentation so your company is protected in the event of a security breach.



DEVICE MONITORING

The service includes 24-hour real-time remote monitoring and fault management for network devices, firewalls, servers and work-stations. The key features of proactive monitoring services are as follows:

- Comprehensive fault, performance and security monitoring, using the following channels SNMP, Syslog, WMI, and specific services.
- Intrusion monitoring – Monitor login/logout activity by user/device, failed login details, and account modification activity.
- Full control over alerting & alert severities.
- Proactive alert notification following Client escalation procedure.
- Default policies to implement best practices for IT infrastructures.
- Integrated knowledge base to re-mediate alerts.

PHYSICAL TO VIRTUAL SOLUTIONS

ESI can help you implement and manage VM environments by providing the following services:

- Assessment and capacity planning with variable growth ratios.
- Virtual infrastructure design based on best-practice implementation guidelines.
- Quick implementation times with complete training and documentation packages.
- Disaster recovery planning, implementation, and test simulations.

COLOCATION SERVICES

ESI can help you secure your IT investments:

- ESI provided lockable racks.
- Remote hands for onsite needs.
- Power in a variety of formats, AC and DC
- Network connectivity in house or customer provided, including fiber optic solutions.
- Physical security including surveillance, bad access and logging.
- Real-time monitoring of all functions for failure.
- Per unit or per rack pricing is available
- Cooling protection with expandable systems to fit growth needs

PROCEDURES AND SLA

INFORMATION SECURITY INCIDENTS

The Client incident escalation procedure is designed to be coordinated with ESI. The baseline procedure is as follows:

- Contact Company staff with security issue and request approval.
- Follow documented escalation procedure.
- If a component is vulnerable, disconnect component and diagnose for exploits.
- Replace component after remediation.
- Verify that recommendations have been applied to components under attack.
- Send pertinent information to offender and request to track down problem.
- Update Client on response.
- Provide documentation through the Security Portal.

BUSINESS VALUE

ESI service will reduce cost, improve performance, and manage risks by:

- Providing first response and escalation management to mitigate downtime.
- Creating a security audit trail on network devices for forensic investigation.
- Providing a centralized logging solution to rapidly troubleshoot issues.
- Creating a buffer between alerts and IT staff to ensure peace of mind.

BUSINESS VALUE

ESI service will reduce cost, improve performance, and manage risks by:

- Providing a scalable server infrastructure that performs reliably with minimal management.
- Leaves your company holding all of the management keys.
- Reducing downtime while drastically improving performance and power utilization.
- Server virtualization offers substantial hardware and management savings.

BUSINESS VALUE

ESI service will reduce cost, improve performance, and manage risks by:

- Higher reliability provide by redundant systems
- Lower network latency and higher bandwidth availability
- On-site management of all systems.
- Easy access from off-site locations.
- Security Services

INCIDENT RESPONSE SERVICE LEVEL AGREEMENT

- Response to monitoring alert: 2 hours from alert – assess problem, assign to on-call engineer, resolve remotely or dispatch engineer
- Response time to on-site location: 4 hours plus travel time
- Equipment replacement – Administer manufacturer replacement – Four hour, next business day to 2 days depending on device coverage
- Install an available spare – 4 hours plus travel time
- Time and material maintenance response available for services not included under contract.