

Vulnerability Assessment Services

Internal &
External
Vulnerability
Assessments

Let us Help you
Understand Your
Risks & Alternatives

Risk Assessment Checklist

- Security Reviews
- Security Tests
- External Scans
- Internal Scans
- Penetration Tests
- Phishing Tests
- VOIP Tests
- Wireless Tests

Call Us Today!

At eSecurity Solutions, security is our only business. Since 2003, we have focused exclusively on products, services and managed services especially for business. We don't sleep until your data and business is secure and compliant.

Compliance Level Risk Assessment Solutions for All Businesses



Security reviews and risk assessments are essential to discovering risk and for defining appropriate security and risk mitigation strategies that fit your company's objectives. Security reviews provide a complete process for defining risk strategies based upon your objectives, security posture and status.

Risk assessment tests like vulnerability scans and penetration tests are partially automated tests that can be run internally or externally to your network to discover vulnerabilities at your gateway or internally on your endpoints.

External Vulnerability Scans

External vulnerability scans are run from our data center examining your externally facing IP addresses looking for exposed firewalls, Web servers and other publically facing devices. These test expose easy to exploit vulnerabilities by hackers and are typically required to be compliant with most security regulations such as PCI, HIPAA and financial.

Internal Vulnerability Scans

Internal Vulnerability Scans scan networks from the inside looking at all endpoints and network devices for risks. These tests provide in-depth testing of each scanned device in your network looking for device vulnerabilities. Since roughly 50% of threats occur from the inside, it is essential to test your network both externally and internally.

Why do you need some type of vulnerability scan for your network and devices?

- **To be compliant with most security regulations**
 - PCI: Quarterly External Scans
 - Health, Financial and Privacy Regulations
- **Vulnerability scans are an essential part of any security audit**
- **Increase your security by providing automated auditing of:**
 - Asset Inventory (What is attached to your Network)
 - Mobile Devices
 - Botnet/Malicious Process/Antivirus
 - Patch Management Systems (Verifies applied patches against patch management systems) - Optional
 - Sensitive Content (credit card, financial, personal, copy-written and other types)

Penetration Tests

In addition to vulnerability scans, many companies either must, or want to, also perform aggressive testing of the outside internet gateway to see if targeted attacks can penetrate your network. Penetration Testing, also known as ethical hacking, is conducted to determine the true risk of vulnerabilities identified through exploitation by attempting to gain root or administrator-level access to the target systems or other trusted user account access. These tests include External Vulnerability Scans but go beyond that to truly stress test your network security.


Security Reviews & Gap Analysis

The most important part of the suite of components in the risk assessment process is clearly the Security Review & Gap Analysis. It is the glue that ties the entire risk assessment solution set together. As with a security audit, there must be a process for assessing a company's risk profile. While it is possible to run specific tests to assess specific security vulnerabilities, understanding a company's overall security posture is also important.

Vulnerability Assessment Services

The table below shows how vulnerability assessments are a part of risk assessments and how they fit into the risk mitigation equation. eSecurity Solutions can help with all areas of risk assessment. See our *Risk Assessment White Paper* for more detailed information about risk assessment alternatives.

Comparing Risk Assessment Alternatives & Features

| RISK ASSESSMENT / AUDIT OPTIONS | | | | |
|---|---|--------------------------------|----------------------------------|----------------------------|
| Risk Assessment Process Steps  | ① | ② | ③ | ④ |
| | Security Review & Gap Analysis CORE REVIEW | Core Risk Assessment BETTER | Advanced Risk Assessment BEST | Functional Tests SELECT |
| 1. Security Review & Discovery <ul style="list-style-type: none"> Complete Set of Interviews and fact finding See Process Description for Detail | X | X | X | |
| 2. Perform Risk Tests | | | | |
| A. Ext. & Internal Network VULNERABILITY Tests | | X | X | Opt |
| B. Ext. & Internal Network PENETRATION Tests | | Opt | X | Opt |
| C. Web Application Penetration Testing | | | X | Opt |
| D. Social Engineering Tests (Phishing & Other) | | | X | Opt |
| E. Wi-Fi Penetration Testing | | | X | Opt |
| F. Security Configuration Testing and Analysis | | | Opt | Opt |
| G. Physical Security Tests | | | Opt | Opt |
| H. VOIP or Other Tests | | | Opt | Opt |
| 3. Risk & Gap Analysis <ul style="list-style-type: none"> Determine Risk Areas & Prioritize based upon level of discovery and tests performed Define Prioritized Remediation Alternatives | X | X | X | |
| 4. Report & Management discussion re: findings and recommendations | X | X | X | |
| 5. Remediation implementation (Security consulting to implement or configure new products, current products, policies or procedures) [To be Quoted after initial risk assessment] | Opt | Opt | Opt | Opt |
| Employee awareness training & education | Opt | Opt | Opt | Opt |
| Quarterly or Annual Follow-up & retest | Quote | Quote | Quote | Quote |

TRY OUR MANAGED RISK MITIGATION SOLUTIONS

- Managed Firewalls
- Log Monitoring/SIEM
- Intrusion Detection
- Backup & BDR
- 2-Factor Authentication
- SaaS Email
- SaaS Web
- Endpoint

Contact us for a quote or information today:

886-661-6685

sales@eSecuritySolutions.com

www.eSecuritySolutions.com

Many companies start with external and internal scans and add Security Reviews and penetration tests to complete the risk analysis and to get a more complete set of risk mitigation recommendations.

Vulnerability Assessment Services

eSecurity Solutions can provide scanning, penetration and audit services to match your company's requirements. Our security experts know how to interpret the results and provide you with mitigation alternatives that match your risk profile and budget.

Vulnerability Scanning Features by Scan Type

| VULNERABILITY SCAN FEATURES | <u>External Scan</u> | <u>Internal Scan</u> |
|--|------------------------------|------------------------------|
| Test Externally Facing IPs <ul style="list-style-type: none"> - Firewall Vulnerabilities - Web App. Server Vulnerabilities | ✓ | |
| Asset Discovery <ul style="list-style-type: none"> - # of Type of Devices, OS Used, Apps Installed | | ✓ |
| Regulation Compliance <ul style="list-style-type: none"> - FFIEC, FISMA, GLBA, HIPAA/HITECH, NERC, PCI, SCAP, SOX | ✓ | ✓ |
| Configuration Compliance <ul style="list-style-type: none"> - CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, IBM iSeries, ISO, NIST, NSA | | ✓ |
| Patch Auditing (Optional) <ul style="list-style-type: none"> - IBM® TEM for Patch Management, Microsoft® SCCM and WSUS, Red Hat® Network Satellite Server, and VMware® Go | | ✓ |
| Sensitive content auditing: <ul style="list-style-type: none"> - PII (credit card numbers, SSNs) and intellectual property | | ✓ |
| Mobile device auditing: <ul style="list-style-type: none"> - Lists iOS, Android™, & Windows Phone 7 devices accessing network - Detects mobile vulnerabilities | | ✓ |
| Vulnerability scanning for: <ul style="list-style-type: none"> - Network devices: Firewalls - Web applications: Web servers, web services, OWASP vulnerabilities | Externally Facing Devices | Internal |
| Vulnerability scanning for: <ul style="list-style-type: none"> - Network devices: Juniper, Cisco, Palo Alto Networks, Firewalls, Etc - Virtual hosts: VMware ESX, ESXi, vSphere, vCenter - Operating systems: Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM iSeries - Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL - Web applications: Web servers, web services, OWASP vulnerabilities - Compromise detection: Viruses, malware, backdoors, hosts communicating with botnet-infected systems, web services linking to malicious content - Credentialed scanning detects local vulnerabilities and conditions - Uncredentialed network scanning finds new hosts & vulnerabilities | | Internal |
| Minimal Impact to Customer Environment <ul style="list-style-type: none"> - Internal Scans use Agentless Client Scanning - Easy to Plug in Internal Scan Appliance - External Scans Require no Client Side Implementation | Zero Impact | ✓ |
| Easy to Read Scan Reports <ul style="list-style-type: none"> - Low, Medium, High & Critical Risk Results | ✓ | ✓ |
| Expert Analysis & Recommendations | Included With Review Service | Included With Review Service |

The eSecurity Solutions Advantage

- 13 Years in Security
 - CISA Certified
- Complete Security
 - Risk Assessments
 - Products
 - Managed Security
- Top Vendor Partners
- Affordable SMB – Enterprise Solutions

Peace of Mind

Contact us for a quote or information today:

886-661-6685

sales@eSecuritySolutions.com

www.eSecuritySolutions.com

Contact us today to see how we can help you with your risk assessment and mitigation needs.