INTELLIGENT TECHNOLOGY SOLUTIONS

IT Sevice Management Company

CONVERGESolv SECURE NETWORKING SERVICESolv PROFESSIONAL SERVICES

IT Security Assessments

Are your networks secured?

The truth of the matter is this question cannot be answered with any degree of certainty unless your systems are either compromised, or preferably assessed/tested for vulnerabilities. Intelligent Technology Solutions offers a variety of services to evaluate the hardened stance of a "secured" IT infrastructure, serving to validate or invalidate the perceived security posture.

Vulnerability Assessments:

A vulnerability assessment is a process that defines, identifies and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability assessments can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are implemented.

Vulnerability Assessment - Complimentary

Intelligent Technology Solutions CONVERGESolv Secure Networks offers a complimentary vulnerability assessment of 1 to 5 of an organization's publically facing IP addresses. This assessment is a snapshot of a small portion of the environment and presents a high level insight as to the security posture. Optimally, we recommend a full vulnerability assessment of the entire network to present a more complete picture of the security posture and begin to correlate the organization's standing with regard to various industry compliance requirements.

Intelligent Technology Solutions has conducted more than 100 complimentary vulnerability assessments of 1 to 5 IP addresses per client. Alarmingly, less than 2% of client networks assessed passed with no known vulnerabilities. One network was cited with over 1,400 vulnerabilities associated with a single IP address.

Ordering information:

- SKU 4364118 – Complimentary vulnerability assessment (per IP) - quantity 1 to 5

Full Vulnerability Assessment

During a full network vulnerability assessment, a security engineer will scan both the internal and external network looking for any known vulnerabilities that exist in the client infrastructure. The engineer will further test to attempt to rule out any false positives.

Engineers will conduct social engineering, testing the company's employees for adherence to information security/privacy best practices. Often, employees are not properly trained on information security and social engineering testing will validate their training.

Custom professional service engagements can be crafted for your specific security needs.
For more information contact: sales@its-itsm.com

Finally, the assessment will include a compliancy audit, ensuring the organization is complying with any relevant regulations or standards like; GLBA, HIPAA, PCI-DSS, or ISO27001. These assessments can be conducted on-site or remotely, with on-site assessments also including a physical security review.

Ordering information:

- SKU 3158449 – External vulnerability assessment bundle – 20 IP addresses
- SKU 3158450 – External vulnerability assessment – Add'l IP addresses 21+
- SKU 3158451 – External vulnerability assessment bundle – 50 IP addresses
- SKU 3158452 – External vulnerability assessment – Add'l IP addresses 51+
- SKU 3158453 – External vulnerability assessment bundle – 100 IP addresses
- SKU 3158454 – External vulnerability assessment – Add'l IP addresses 101+

Network Penetration Testing

Network penetration testing is taking a vulnerability test to the next level and is a close simulation to a real world hack available. During a network penetration test a security engineer/ethical hacker will first scan the network for vulnerabilities and exploit those vulnerabilities to gain access to systems. From there the engineer will gain access to sensitive information or if allowed by the SOW, leave a marker to prove that they gained access. In many penetration tests, the engineer will use a tactic called pivoting to gain access through the perimeter on non-sensitive system and launch attacks on critical systems from the non-sensitive system behind the firewall.

- SKU 3158439 – External penetration test – 5 IP addresses
- SKU 3158440 – External penetration test – Add'l IP address
- SKU 3158441 – Internal penetration test – 5 IP addresses
- SKU 3158442 – Internal penetration test – Add'l IP address

Web Application Penetration Testing

Many companies have custom web apps that were developed in house or by a third party. These apps are typically not tested before they are deployed to see if any security holes exist. During a web application penetration test a security engineer/ethical hacker will attempt to gain access to the application as an authenticated user, using various testing means to attempt to extract or manipulate data in the application. It is best practice to have a web application penetration test before deploying any new applications.

- SKU 3158437 – External web application vulnerability assessment bundle – 3 IP addresses
- SKU 3158438 – External web application vulnerability assessment – Add'l IP address