



COMMON_d Security Assessment Technology Integration Practices (TIPs™)

identifies vulnerabilities that allow outside, untrusted networks to gain access to internal, trusted networks and systems and recommends solutions for improvements.

COMMON_d Security TIPs™ methodology gives you an accurate posture of your network security architecture. Our security services provide proactive protection of your IT infrastructure by identifying vulnerabilities in the network, web applications, and internet perimeter by prioritizing corrective actions to protect the confidentiality, integrity, and availability of your organization's assets and information. With our security assessment, you can:

- ❑ Identify unwanted exposure, including intentional or accidental access to IT assets and information
- ❑ Have the ability to define network vulnerabilities and block loopholes
- ❑ Enable regulatory compliance
- ❑ Increase productivity
- ❑ Enable optimization for network monitoring and analysis
- ❑ Provide accurate information and network platform for future security policy and technologies
- ❑ Develop a prioritized list of steps required to fix identified vulnerabilities
- ❑ Improve compliance with federal and state regulations that require security assessments
- ❑ Validate current security policies and practices against industry best practices and verifying areas that require security budget or staffing

Social Engineering and Physical Security

COMMON_d assesses the physical security posture for designated site(s), if applicable. The sites are surveyed for security breaches. Potential components to be examined are:

- ❑ Mailrooms
- ❑ Paper/media disposal process and paper records storage
- ❑ Dissemination and disposal
- ❑ Physical access to buildings with a focus technology related assets

COMMON_d also assesses your organization and reports findings pertaining to security social engineering. We examine the organization from a social engineering and administrative standpoint. COMMON_d attempts to obtain confidential information from trusted users. We attempt to exploit weaknesses with regard to passwords, email attachments, and protection of financial and related information by using increasingly sophisticated lures to "phish" users for information.

External Vulnerability

COMMON_d Security Technology Integration Practice (Security Tips™) allows our security team to perform a quantitative risk analysis and vulnerability assessment for your logical external network infrastructure.

We analyze, test and try to penetrate all access controls to determine the environmental (network) factors and perform a threat analysis. Our vulnerability examination of the network infrastructure is performed as seen from the PUBLIC internet. COMMON_d's security methodology provides analysis from the vantage points of both an internal or Internet-based hacker. During this phase, COMMON_d analyzes and documents your network architecture with particular attention paid to networks directly exposed to the Internet. This analysis is focused on points of presence and critical assets such as:

- ❑ Gateway Routers
- ❑ Firewall and Edge Protection
- ❑ VPN and Remote Access
- ❑ Web Protection
- ❑ Wireless
- ❑ Email
- ❑ Telecommunications
- ❑ Applications
- ❑ Database (s)
- ❑ Servers
- ❑ Local Area Network
- ❑ Work Stations

Scope of Services:

Our engineers identify and confirm the presence of systems and services visible to the Internet by:

1. Identifying the number of active systems and devices, including hosts behind filtering devices such as firewalls
2. Scanning TCP ports and User Datagram Protocol (UDP) ports to determine if any services are externally visible
3. Researching and confirming potential target systems, services, devices, and applications
 - a. Emulate typical hacker activities through nondestructive means to confirm the presence of vulnerabilities and the level of unauthorized access
 - b. Provide a detailed analysis of simulated attacks to identify critical vulnerabilities and compare assessment results with recommended industry best practices and policies, as well as the operational requirements of the organization
 - c. Prioritize the discovered risks and provide recommended actions to improve the security state of your network and meet your organizational security goals

From the data gathered, the deliverables from our experts minimize unknown technical security threats to your organization. Furthermore, we recommend best-in-class remediation solutions, with technical references, to deliver a set of functional and integrated network protections for your organization to:

- ❑ Detect and Identify
- ❑ Contain
- ❑ Prioritize
- ❑ Remediate
- ❑ Document
- ❑ Prevent

Benefits

With our Security Assessment, your organization can:

- ❑ Obtain a cost-effective, unbiased assessment
- ❑ Identify critical security threats
- ❑ Effectively simulate an internal attacker to compute the risks posed by threat sources
- ❑ Validate all security policies and practices against industry best practices
- ❑ Improve the overall security state of your network

Why COMMON_d

- ❑ **Outstanding People:** We have the very best consultants and professionals the industry has to offer
- ❑ **Integrity:** We do what is right, every time
- ❑ **Excellence in Everything we do:** Excellence in everything we do is about quality and exceeding client expectations during and after the engagement process
- ❑ **Focus:** Customer First, Last and Always
- ❑ **Performance Based:** By investing our financial resources up front, we eliminate financial risk for our client. Until completion of deliverables, our client has no financial obligation.
- ❑ **Best-in-breed:** COMMON_d Security TIPs™ guarantees the neutrality of our deliverables.

We give you a consistent and uniform set of service parameters and solutions without the disposition of vendors or brands.