



Criterion Systems provides full life-cycle security services for our clients in the government, financial services, energy, telecommunications, and life sciences market sectors.

Criterion has relationships with leading technology solutions companies such as Microsoft, IBM, Citirx, vmWare, HP, and Access Data.

Criterion has a strong history of delivering some of the most innovative and cost effective security solutions in the marketplace today.

## **MATCHING RISK TO REWARD**

The pace of technology change has outstripped many IT manager's ability to keep up with the dynamic security requirements of the enterprise. Product development becomes a production environment without the benefit of a careful review to ensure security holes are closed and affected systems are secure. Above all, customer privacy is at stake. Names, addresses, and even personal financial information are all stored on electronic media, often within reach of the Internet hacker. Controlling these risks becomes more difficult in light of the very competitive nature of business today. Customer delight hinges on instant and accurate access to information, as well as the ability to do commerce on the Internet at any time. Success depends upon meeting these objectives while avoiding the pitfalls posed by faulty security.

## **STRIKING THE BALANCE**

Good business is about successfully setting and executing priorities. A solid security policy process includes planning, design, and implementation; and updating procedures to operate and update these policies, must address the most likely threats. Operations must implement the design and faithfully carry out the procedures to ensure no vulnerabilities are created. Constant reevaluation is the only way to gauge the accomplishment of this continually shifting equilibrium as new vulnerabilities are introduced.

## **RISK AND THREAT PROFILE**

The first step in a Managed Security program is to understand threats, risks, and their tradeoffs. Understanding the threat environment is an important part of the service, and it goes to the heart of why security is required. An accurate IT asset inventory, along with an assessment of the current operations, security practices, and configuration management practices, sets the stage for further alignment of these environmental elements to drive operational efficiencies, synergies and

productivity. Moreover, security must be continually updated based on the changing nature of organizations, and the threats existing in their operating environment.

## **RISK MANAGEMENT**

The risk and threat profile results in a risk assessment from which management actions are developed. This is a prioritized action plan for investing in a security program that fits the organization's threat environment. It combines threat with vulnerability and technical engineering. It steers the decisions for allocating resources between people, tools or services. Many security tasks that are handled by tools can also be addressed by educating and training staff. Security monitoring is often a process that should be outsourced.

## **About Criterion HPS**

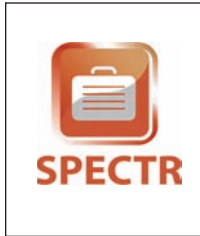
Headquartered in Vienna, VA, Criterion HPS is a wholly-owned subsidiary of Criterion Systems, Inc. a leading provider of information technology services to Government and commercial clients. Criterion HPS mission is to help our customers deploy high performance solution sets to the operational edge. Enabling organizations to efficiently deploy high performance solutions anywhere, anytime and anyplace – computing @ the edge - will forever change the way business is conducted. For more information on Criterion HPS please visit [www.criterion-hps.com](http://www.criterion-hps.com).

# Cyber Teams



## SRT

**Special Response Team:** A specialized team that has the training and experience to perform special operations outside the current operational abilities of a client. These operations include cyber investigations, digital forensics, and incident response.



## Specter

**Insider Threats Team:** A highly trained team that specializes in stealthy and discrete Network Operations and/or Operations Centers (Op Center) activities focusing on insider threats. Specter manages professional activities that are based on aggressive proactive and reactive information collection, analysis, investigations and operations to identify and neutralize espionage, foreign intelligence, and/or terrorist activities.