SECURE HALO
SECURING THE ENTERPRISE

WE EXAMINE VULNERABILITY ACROSS SIX CRITICAL DOMAINS

Secure Halo believes that an all-encompassing and proactive approach is the ideal way to understand risk, make strategic investments, and maintain business continuity. We look beyond traditional technical controls to understand the business and user complexities that are often overlooked. That's why we examine holistic vulnerability across six critical domains.

INSIDER THREAT

There's no way around it – insiders pose the greatest threat to information security. We examine threats that arise from the human element, whether deliberate or inadvertent in nature. To do that, we look for technical and non-technical patterns that may indicate attempts to commit sabotage, theft of intellectual property, espionage, or fraud. We also review your organization's approach to communicating with and training employees about cyber risks, since even savvy employees can be fooled into opening the door to hackers intent on gaining access to company networks.

PHYSICAL SECURITY

We assess your organization's physical security strategy as it relates to the protection of data and examine the allocation of resources relative to threats against your highest priority assets. In addition to analyzing the potential for physical intrusion and unauthorized access to priority locations such as a server room or R&D lab, we assess procedural vulnerabilities that endanger sensitive information. We approach every review from the perspective of the adversary, identifying low-cost, high-impact solutions.

MOBILITY

We explore the security of data during times when it is at its most vulnerable: during transit. Our mobility domain focuses on threats to intellectual assets that are present during foreign travel as well as from mobile device management practices such as Bring Your Own Device (BYOD). These challenges may occur from lost, stolen, or compromised devices, or as a result of poor travel security practices.

DATA SECURITY

We search for and find the risks stemming from the use of enterprise IT resources. To do so, we examine the programs and technology that secure the network and the information assets that reside upon it. Our data security assessment reviews network and security device configurations; identity and access management policies and implementations; vulnerability and patch management systems; operating system, database and application monitoring programs; and perimeter and endpoint defenses.

INTERNAL BUSINESS OPERATIONS

Do you have processes and policies in place that form the backbone of security strategy? In our review of internal business operations, we measure the effectiveness of initiatives that manage internal administrative vulnerabilities. For example, we assess contingency operations, evaluate internal risk management policies, and scan for vulnerabilities to critical assets resulting from personnel, organizational or business processes.

EXTERNAL BUSINESS OPERATIONS

Organizations large and small rely on external partners, suppliers, and/or service providers in key enterprise functions. This expansion of external parties, and therefore access to your enterprise internal information, is a necessary complication to modern business operations. We uncover the hidden vulnerabilities you may face due to third party risk by examining your security strategy, policies and procedures, and threat universe resulting from external engagements.