MALWARE

Malware or Malicious Software is malicious code or a file that is intentionally introduced to a network and is designed to cause disruption of an information system. Some forms of malware are solely for destructive purposes, others are designed to steal information, track keystrokes, gain unauthorized access to network systems, and compromise the privacy and security of the organization. GSIS offers a variety of services to help protect your organization from modern day threat actors.

GSIS

To learn more, contact us today:

GSIS
1401 H St NW
Suite 875
Washington, DC 20005
202.888.2360
www.gsis.us

REMOTE ENVIRONMENT DIAGNOSTIC SERVICES (REDS)

CYBER POSTURE RATING

GSIS offers a company an excellent way to limit their cyber risk as well as improve their own cyber hygiene through a non-intrusive scan of a company's IP address(es). These tools provide a critical view of technical assets exposed to potential criminals/hackers via the internet, thereby identifying a pathway to reducing risk

CYBER SECURITY RISK ASSESSMENT AND STRATEGIC IMPLEMENTATION PLAN

GSIS, in full collaboration with a client, conducts a full-scale cybersecurity assessment to determine system and program proficiency against established industry frameworks. GSIS goes the distance by providing a roadmap for improvement based upon a client's risk posture and budget to further reduce the risk of malware.

TECHNICAL SERVICES

GSIS provides technical assessment capabilities: such as internal and external network vulnerability scanning, web application vulnerability scanning, external and internal pen testing, phishing training and testing, and web application firewall, cloud configuration, and code reviews.

CISO as a SERVICE (CaaS)

EXECUTIVE CISO SERVICES

GSIS provides E-CISO services that include Strategic Plan Implementation project management, SOCaaS technical monitoring and oversight, and cybersecurity advisory services.

CRISIS MANAGEMENT

CRISIS MANAGEMENT PLAN

GSIS can enable an organization to effectively manage a crisis through timely and informed escalation to speed the decision-making process, including incident escalation procedures, communications across organizational components and with outside agencies and media. This capability is critical to any organization facing a natural disaster, major cyber event, or internal crisis that requires immediate and effective action.