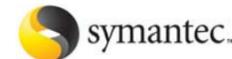


LOCKHEED MARTIN

THE LOCKHEED MARTIN CYBER SECURITY ALLIANCE

ENHANCING THE SPEED OF SOLUTIONS DELIVERY
THROUGH PARTNERSHIP AND INNOVATION



Lockheed Martin Information Systems & Global Services
700 North Frederick Avenue
Gaithersburg, MD 20879
(301) 240-6000
cyber.security@lmco.com
www.lockheedmartin.com

"By bringing the combined strengths of market leading technology companies to the Lockheed Martin NexGen Cyber Innovation and Technology Center, we can accelerate development of solutions without boundaries or limitations. Our adversaries operate in sophisticated criminal ecosystems that enable and enhance their attacks. To defend against such organized and purposeful opponents we need to build effective security ecosystems based on collaboration, knowledge sharing and industry best practices."

Art Coviello, Executive Vice President, EMC and President, RSA, the Security Division of EMC

THE LOCKHEED MARTIN CYBER SECURITY ALLIANCE

Lockheed Martin is a global security company, and cyber security is a critical component of integration and sustainment of advanced technology systems, products, and services.



CYBER SECURITY ALLIANCE

The Lockheed Martin Cyber Security Alliance integrates the best commercial security offerings to serve the cyber security needs of government. It combines the strength and expertise of market leading cyber security companies, domain knowledge, and “systems-of-systems” integration into a unique environment called the NexGen Cyber Innovation and Technology Center. NexGen is a world-class cyber security center designed for customer and partner collaboration and innovation.

THE VISION

At Lockheed Martin, cyber security is more than a core competency – it’s a way of life. We understand it, we apply it, and more importantly, we deliver it by integrating and embedding security into everything we do, and every solution we develop. We’ve brought together the right team, the right processes, and the right technologies to provide our customers with mission resilient systems.

“We face significant known and unknown threats to our critical infrastructure. We not only need solid defenses, but also the right technologies to predict and prevent future threats. Innovation and collaboration are key to ensuring mission resilience and securing cyberspace.”

Charles Croom, Vice President, Cyber Security Solutions, Lockheed Martin

THE CHALLENGE

The current cyber security threat is driven by highly motivated individuals and groups, to include organized crime syndicates, terrorists’ organizations and nation states for the purpose of political, technological, or economic gain. Analysis of cyber incidents shows trends of recurring, related activities over a period of years. These advanced, persistent threats use both sophisticated technical approaches and social engineering. Many of today’s cyber security solutions are focused on defensive blocking to address threats with known signatures. Additionally, the number of unique cyber security threats is increasing dramatically. According to the Symantec Global Internet Security Threat Report, Volume XV, Symantec wrote almost 3 million new malicious code signatures in 2009— which is more than all their previous 15 years combined. This data suggests that there are more unknown than known threats. Today’s manual processes and point solution technologies that make up most of our customer operations are not sufficient to handle the magnitude of threats.

Federal government information technology systems and networks are often a consolidation of many systems and networks acquired and built to different technology and standards over time. The security solutions for these systems and networks were not built in from the beginning, but acquired later in a piecemeal fashion. To compound the problem, the applications on these systems often did not follow secure coding processes and frequently contain security vulnerabilities.

Commercial off-the-shelf solutions play a critical role, yet often leave “seams” in defenses. Inadequate talent, training, and processes further contribute to a porous security fabric as security operators have poor visibility across the enterprise making identification and recovery from incidents slow. This slow and predictable response becomes an opportunity for our adversaries and can result in loss of mission availability.

Even with the hard challenges facing our digital infrastructure, there are solutions. It begins with a mature process with a proactive enterprise approach that leverages a better integration of tools, and continues with collaboration among industry, partners, and customers.

THE SOLUTION

The Lockheed Martin Cyber Security Alliance members collaborate on solutions that can help provide early threat detection, protection, and multi-layer self-healing capabilities to solve customers’ hard problems and meet future challenges.

These technology partners are engaged in customer-focused solutions, experiments, and end-to-end systems integration pilots. Alliance companies include: APC by Schneider Electric, CA Technologies, Cisco, Dell, EMC Corporation and its RSA Security Division, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, VMware, and Symantec.

Lockheed Martin’s world-class NexGen Center fosters an agile environment where alliance companies and customers can rapidly and virtually collaborate and develop new capabilities. The center is a global security asset for innovation. NexGen is also the central site for Lockheed Martin’s global cyber innovation range that enables safe attack and defense testing to simulate customer environments, enhancing the speed, security, and innovation of real world solutions development.

A fully integrated and tested solution is paramount to address the persistent, very sophisticated threat that now faces our customers. Because speed of recovery is essential for mission success, organizations need better platforms for assimilation libraries of security event data, and fusing multi-source intelligence and network operations data. This will demand significantly increased integration of tools to achieve network domain awareness to facilitate selecting courses of action to prioritize remediation across global networks.

An alliance approach to cyber security implements end-to-end solutions that close the seams between product solutions and adds layers of protection from targeted advanced threats. Lockheed Martin’s relationship with world-class partners and its team of certified security professionals brings increased confidence for mission assurance.

LM CYBER SECURITY™
ALLIANCE

