Security Operations Center
Build, Transition, Management and Transformation Services

THE CHALLENGE
Every organization faces the challenge of balancing the risks and benefits of operating in cyberspace. As society’s dependence on technology and its vast capabilities has increased, so too have the number of adversaries who use technology to disrupt, steal, damage or destroy. Cyber threats have morphed from small groups of curious hackers into sophisticated, organized crime and nation state-sponsored consortiums. As a result, technology is increasingly being used as a weapon in asymmetric attacks, and government organizations are all too often the target.

THE SOLUTION
For more than eleven years SRA has been a leader in cyber defense; helping government agencies secure and defend their computer networks through reliable, trustworthy Security Operations Centers (SOCs). We leverage a unique combination of innovative technologies, proven methodologies and multi-disciplined cyber expertise to stay ahead of ever-evolving cyber threats. We train our engineers and analysts to exacting standards to design and build operation centers based on our customers’ individual needs, operational structure and applicable governing policies using SRA’s SOC Maturity Model (SOCMM).

SRA ADVANTAGE
SRA takes a proactive approach to SOC development and management that allows us to perform detection, collection, analysis and remediation activities more rapidly, efficiently and effectively – thereby closing our customers’ gap to exposure. We have a dedicated group of experts specifically focused on intrusion analysis and we leverage threat fusion to promote shared situational awareness and guide incident prevention activities. Our robust defensive strategies and cyber expertise, coupled with our structured methodology for continuous improvement, result in unparalleled SOC services.

FEATURES
- SIEM Integration, Tuning and Management
- Vulnerability Management
- Incident Response
- Event Monitoring and Notification
- Situational Awareness
- Cyber Security Engineering and Architecture (Protect, Detect, Respond)
- Virus Software Application(s)
- Monitoring and Management of SOC Security Devices
- Testing and Validation of Security Monitoring/Detection Services
- Cyber Threat Analysis and Fusion
- Cyber Intelligence and Focused Operations
- Forensic Analysis
- Reverse Engineering Malware Analysis
- RED/BLUE Teams and Penetration Testing
STAY AHEAD OF THE THREAT

Even the most advanced SOC must evolve to respond to ever-changing cyber threats. As a result we’ve adopted a disciplined approach to SOC maturity. Our dedication to continuous performance improvement combined with our years of experience establishing and operating federal SOCs has resulted in a comprehensive SOC Maturity Model (SOCM) that guides maturity within six key areas:

- Physical Facilities
- Processes
- SOC Performance Management
- Staffing/Personnel Management
- Technology Use
- Analytical and Operational Services.

MODELING SUCCESS

The SOCM helps organizations assess their current state of security operations, prioritize enhancements, and build a roadmap for operational improvement. Our roadmaps outline incremental capability improvements in each of the six areas with the goal of optimizing SOC operations. The model provides a means to articulate what capability advancements are needed at each level and what gains will be provided to the organization. Individual functions and capabilities within the six key areas are tailored to fit each customer’s organizational mission and goals.

Having a roadmap and plan that continuously seeks to enhance cyber defense capability is integral to achieving cyber security goals for any organization. Our SOCM and continuous improvement strategies have been paramount to our customer’s continuing success.

THOUGHT LEADERSHIP

SRA has long been a trusted partner in cyber security because we understand the most sophisticated cyber threats and how to mitigate them. As a thought leader in this area, we have helped to develop a number of cyber security best practice guidelines for the federal government including the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the Industry Compendium to the National Strategy to Secure Cyberspace. We have also provided support for the establishment of requirements for the NSA Centers of Excellence in Information Security Education. We apply the latest and most relevant developments in cyber defense occurring throughout government, academia and industry to advance cyber security operations.

OUR CLIENTS

SRA has designed and developed SOCs for a variety of public and classified programs spanning more than 20 federal agencies. In addition, we have constructed and successfully relocated major cyber security command centers. We operate some of the largest and most complex SOCs within the U.S. federal government, and we continue to develop proven, repeatable operations centers that successfully combat the most pervasive cyber threats facing our nation today.

FOR MORE INFORMATION

To learn more about our services and capabilities, please contact us at (703)653-5360 or info@sra.com.

About SRA International, Inc.

SRA is dedicated to solving complex problems of global significance for government organizations serving the national security, civil government, health and intelligence markets. Founded in 1978, the company has expertise in such areas as cloud, cyber security; disaster response planning; enterprise resource planning; environmental strategies; energy systems and sustainability; IT systems, infrastructure; learning technologies; logistics; mobile workforce; public health preparedness; strategic management consulting; and systems engineering.

SRA, SRA International, Inc., Honesty and Service and the SRA logo are registered trademarks and service marks owned by SRA International, Inc. All rights reserved.

sra.com