

Cisco Cybersecurity Workshop Service



Assess security gaps, operations, and mission readiness of your security infrastructure with a three-day Cisco® Cybersecurity Workshop.

Understand where your security gaps are, how to improve your security framework, and how to tackle enterprisewide security initiatives and challenges, using existing technology and processes to reduce risk and help meet compliance needs. The Cisco Cybersecurity Workshop can provide guidance and best practices direction on one of the following areas:

- Security operations
- Mission-centric security
- Security policy
- Compliance
- Virtualization or cloud computing
- Data center migrations or consolidations
- Telecommuting, voice, and video
- Infrastructure security (defense in depth)
- Wireless security

The Cisco Cybersecurity Workshop enables you to interactively discuss security approaches, projects, and challenges with a Cisco cybersecurity expert to help address and identify security gap impact and an approach to address a comprehensive security architecture with processes, multivendor technologies, and organizational personnel.

Organizations are increasingly looking for ways to reduce their security risks, stay informed about security incidents, and maintain visibility into situations, while reducing costs and protecting their critical mission systems and data necessary to fulfill business objectives. Through consolidation of older

environments, virtualization, expanding endpoint presences, and addressing wireless needs and multivendor technology sprawl, a larger awareness of risks and gaps may be identified and addressed across the enterprise. The use of cybersecurity technology, processes, and best practices can enhance the security, resilience, and manageability of the data and its infrastructure.

A high-level Cybersecurity Workshop review of your existing security process, infrastructure, and current security plans can identify gaps, provide actionable steps to help provide visibility into your risks, as well as provide guidance and strategy to align with your mission. Whether you are experiencing cyberattacks and data loss, identity and access problems, or are trying to understand where the go-forward security gaps will be, the Cybersecurity Workshop can provide direction and identify high-level approaches to addressing corrective security steps.

To provide insight into your challenges and top cybersecurity issues, Cisco will facilitate interactive discussions about the following:

- Architectural design
- Environments and topologies
- Operations and procedures
- Data center migrations
- Virtualization projects
- Interoperability
- Compliance

Cisco will also discuss infrastructure security and other security requirements, as well as best practices for security policy and processes, and provide recommendations for improvements. Deliverables of the Cybersecurity Workshop are a presentation of security findings and prioritized recommendations, recommended actions that include best practices and options to reduce risk, and suggestions on meeting compliance goals through ongoing assessments and monitoring. Recommendations will help you with future security planning efforts; identify immediate security needs with actionable steps; and provide guidance on addressing your challenges to better enable security threat reduction, mission security reliability, and security migration and consolidation plans.

Cisco and Partner Expertise

Cisco will provide a cybersecurity expert in one of the specific security technology areas:

- Security policy
- Security planning and assessment
- Secure data center
- Secure voice and video security

Our cybersecurity experts apply Cisco's deep expertise in security planning, design, and implementation and in operating and optimizing for risk reduction and to meet compliance requirements. Cisco's expertise and knowledge with cybersecurity enables us to provide you with the best solution to meet your needs. Cisco expertise is continually enhanced by hands-on experience with real-life security networks and broad exposure to the latest security technology and implementations.

Follow-On Services

Cisco has several in-depth follow-on assessment and operational services that address security architecture, risk, and compliance. Whether you are planning future programs, consolidating or modifying existing systems, or simply need to reduce security exposure, Cisco can help guide you through the security complexities.

Why Cisco Cybersecurity Services?

In today's complex and ever-changing threat landscape, gaps in a security solution can place data integrity, information confidentiality, business-critical applications and mission objectives at risk. You need visibility into those risks with actionable steps to remediate. Your infrastructure needs integrated security controls that provide protection in a dynamic threat and vulnerability environment, while at the same time remaining aligned with security policy and compliance requirements as your organization evolves. Cisco and our industry-leading partners deliver intelligent, personalized services that identify, address, and help to mitigate those security gaps.

Cisco takes an enterprisewide approach to help you reduce the risk and costs associated with achieving your mission objectives by helping you plan, build, run and measure the effectiveness of your security solutions.

Availability

The Cisco Cybersecurity Workshop Service is widely available. Contact your local Cisco account manager about availability in your area.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)