Maintain the availability and integrity of your system

Strengthen your security posture with our Cybersecurity Essential Services

Maintain the confidentiality, integrity and availability of your systems with the insights and expertise of the cybersecurity advisory services team. Motorola Solutions experts can work with your team to reduce your risk of cyber attacks and strengthen the resilience and integrity of your system against them.

Cybersecurity essential services

Cyber health check

Incidedent response plan development

Tabletop exercise

Risk assessment

Onsite security update service

MOTOROLA *SOLUTIONS*

Proactively identify risks

Our cybersecurity advisory services provide your organization with a comprehensive approach to managing cyber risk. We offer both one-time engagements and ongoing cyber assurance packages to continually assess and enhance your cybersecurity posture.

Our team of experts will work closely with you to identify vulnerabilities, assess potential threats, and develop a customized plan to mitigate risks. Through a combination of advanced tools and proven methodologies, we will thoroughly examine your systems, networks and applications to uncover any weaknesses that could be exploited by cybercriminals.

The services are aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a widely recognized industry standard for managing cybersecurity risk. By adhering to this framework, we ensure that your organization is equipped to effectively identify, protect against, detect, respond to and recover from cyberattacks.

By partnering with us, you can be confident your organization is taking proactive steps to protect its valuable assets and sensitive data from cyber threats. Our team of experts will provide you with actionable insights and clear recommendations to help you strengthen your cybersecurity defenses and reduce your risk of a cyberattack.

Cyber health check

Our cyber health check service is designed to evaluate your organization's security posture by assessing it against 42 cybersecurity best practices. These best practices have been proven to effectively mitigate risks and protect your systems against cyber attacks.

The cyber health check includes an examination of both your Information Technology (IT) and Operational Technology (OT) systems. This includes a firewall review to assess the effectiveness of your network's perimeter defenses, a vulnerability scan to identify and prioritize potential weaknesses in your network and a physical security assessment to evaluate the physical safeguards protecting your critical infrastructure and sensitive data.

The cyber health check service can be performed either remotely or onsite by our team of experienced cybersecurity professionals.

Incident response plan development

Our team of experts can assist your organization in developing and implementing a robust incident response plan that is not only aligned with industry best practices but also adheres to the stringent guidelines set forth by the National Institute of Standards and Technology (NIST). This comprehensive approach encompasses the definition, development, rigorous testing and seamless implementation of best-practice procedures designed to effectively manage a wide array of cybersecurity events.

Additionally, we will help you identify key stakeholders and document their roles in incident response to enable your organisation to prepare for, detect, analyze, contain, eradicate, recover from and learn from security incidents.

By partnering with us, you can strengthen your organization's cybersecurity defenses and establish a robust incident response framework that safeguards your critical systems and minimizes the impact of cyber attacks.

Table top exercise

Test your team and your incident response plan by letting our experts guide you through a structured, real-world cyber attack scenario. A tabletop exercise enables a broad group of participants to evaluate the effectiveness of your organisation's incident response plan and walk through the who, what, when, where and how of a situation in a safe environment.

A tabletop exercise tests how prepared your team is and identifies where improvements should be made and ensures that key stakeholders across the organisation understand their role in the event of an emergency. This improves the team's ability to quickly detect, respond and recover from cybersecurity incidents.

Risk assessment

Our risk assessment service, based on decades of experience working closely with public safety, government, and enterprise customers, provides a systematic and reproducible evaluation which gives you a deeper understanding of your specific security environment. The assessment encompasses the various areas of your infrastructure, such as command and control rooms, communications networks, OT and IT systems.
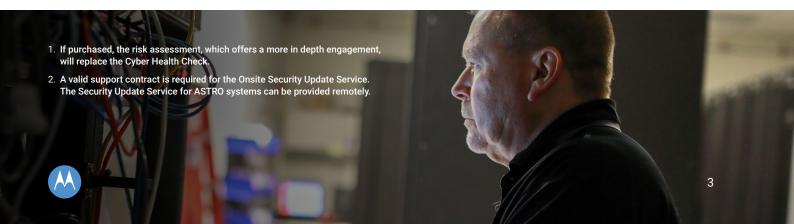
The risk assessment service offers a more thorough analysis of your cybersecurity protection than a cyber health check. Through interviews, site visits, network assessments and firewall reviews, we evaluate elements of your organization's security program, including policies, standards, procedures and technologies. We compare your cybersecurity posture against a best practices framework, identifying areas that may need to be addressed and ensures that any gaps are identified and addressed.[1]

Onsite security update service

Motorola Solutions' Security Update Service (SUS) tests and verifies the latest anti-malware definitions and applicable operating system software patches in dedicated testing labs to validate their compatibility with Motorola Solutions mission critical systems. Once tested and released, we then work closely with you to schedule and implement the update.

Our team manages the deployment of your operating system and antivirus file definitions and reboot patched workstations and servers. Post deployment a report is provided of patched appliances.

Operating security patching is critical for protection against cyberattacks, but it's often overlooked. All software, systems, and devices require continuous patching to maintain security.[2]

Global scale & experience

300+

Security experts focused on 24/7 monitoring response

9B

Security events proactively monitored each day

20+

Years of experience developing cybersecurity solutions

People

Experts with top industry certifications work hand-in-hand to ensure system availability and security

Process

Services alligned to the NIST Cybersecurity Framework

Technology

Network to security operations, security orchestration and automation - designed to accelerate service response

For more information on our Cybersecurity Services, contact your Motorola Solutions representative or visit us at **www.motorolasolutions.com/cybersecurity**

MOTOROLA *SOLUTIONS*