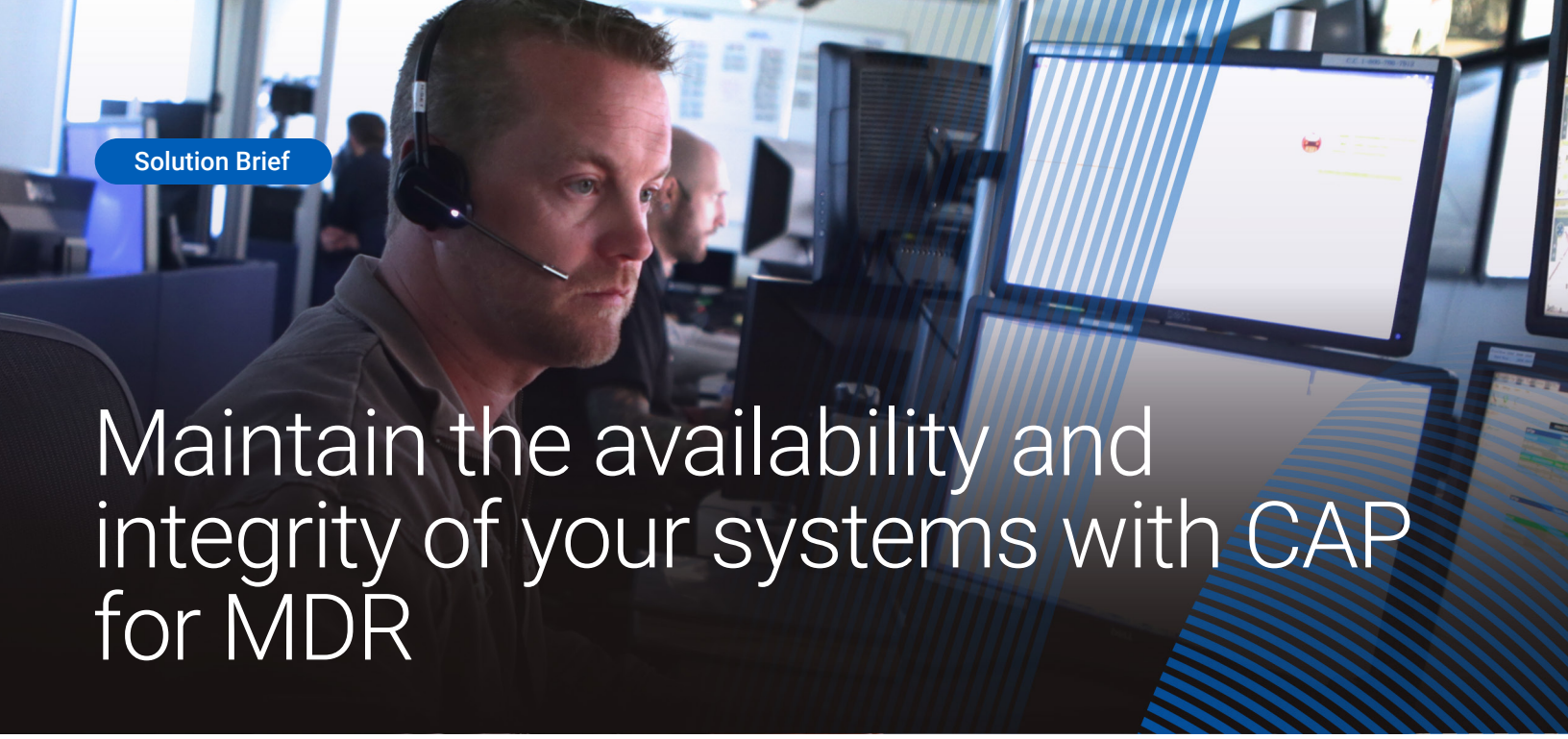


Solution Brief

Maintain the availability and integrity of your systems with CAP for MDR

Strengthen your security with our Cyber Assurance Program for MDR

Maintain the availability of your systems by combining Managed Detection and Response (MDR) with professional services. Powered by our ActiveEye security platform, our MDR service provides 24/7 coverage through our Security Operations Center (SOC) to continuously monitor your network. Implementing our Cyber Assurance Program (CAP) on top of your MDR service engages Motorola Solutions experts to work with your team to reduce your risk of cyber threats further and strengthen the resilience of your system against them. CAP is a structured program of cybersecurity professional services that complements your MDR service, significantly enhancing your organization's cybersecurity and ensuring the confidentiality, integrity and availability of your mission-critical systems. When you combine our CAP with your MDR service, you gain the insights and expertise of our professional services team, along with rapid threat detection and response.

Seamlessly integrate MDR into your operations with CAP

Our Cyber Assurance Program is designed to optimize your MDR service. Once MDR is deployed on your network, we can help you integrate it seamlessly into your daily operations. This will provide you with actionable expert advice and clear recommendations, which can help improve your organization's ability to detect and respond to cybersecurity incidents.

CAP for MDR also enables you to develop and test your incident response plan, as well as evaluate how you incorporate your MDR solution. These services are available for both public safety and commercial organizations and can be provided as one-time engagements or multi-year packages that test your program over time.

Cyber Assurance Program

- Tabletop exercises
- Incident response planning
- Risk assessments
- External penetration testing
- Vulnerability scanning

MOTOROLA SOLUTIONS

Proactively identify risks

The CAP Services can be conducted as one-time engagements. However, a multi-year Cyber Assurance Program package will enable you to test and adjust your cybersecurity plan on an ongoing basis, providing even greater value.

Tabletop exercises

Evaluate your ability to respond and recover from an attack. Guided by a facilitator, this discussion-based exercise will allow you to evaluate the readiness of your incident response plan. This exercise will not only test your organization's knowledge of your incident response plan, but also how your MDR service supports the plan. This occurs without requiring any action on your live systems.

Incident response planning

Ensure that your incident response plan is effective, meets your agency's needs and incorporates your MDR solution. We can help develop your incident response plan based on guidelines established by the National Institute of Standards and Technology (NIST) and any best practices relevant to your organization.

Risk assessments

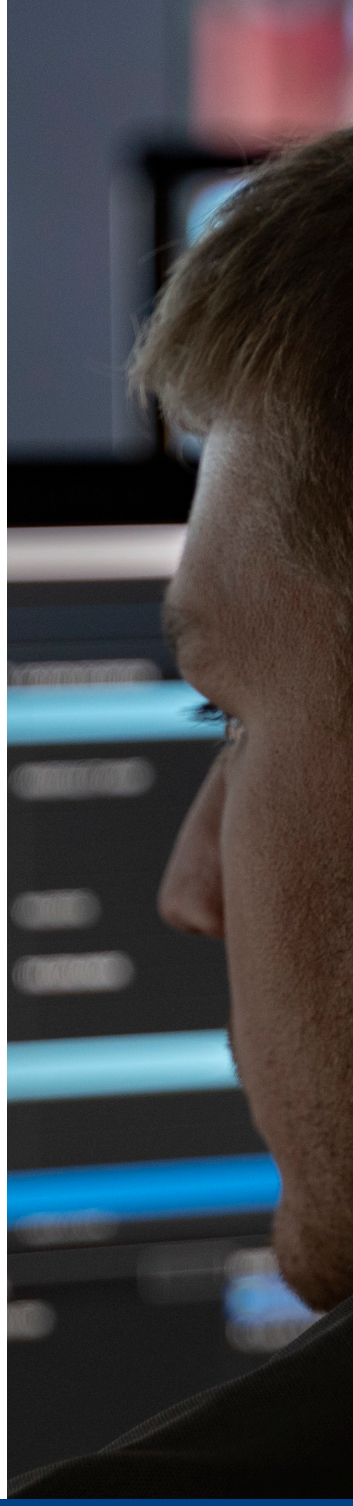
Evaluate every element of your organization's security program, including the policies, standards, procedures and technologies. A risk assessment will compare your program against a best practices framework, provide you with experience in responding to alerts from your MDR solution, and identify any areas that may need attention. This includes interviews, site visits, network assessments and firewall reviews to ensure any existing gaps are identified.

Penetration testing

Penetration testing, also known as pentesting or 'ethical hacking,' can help you evaluate how your organization responds to alerts from your MDR system, as well as identify which elements of your cybersecurity program will be effective during an attack. Testers will attempt a no-harm breach of your network security controls, including physical security assessments, to determine if and where a program may need to be strengthened. Pentesting can be executed from an external or internal perspective and threat vector.

Vulnerability scanning

Vulnerability Scanning (internal & external) will identify any known technical vulnerabilities in your system that could be exploited, either by internal threat actors or through unauthorized external access. This provides a clear understanding of your current vulnerability posture, with findings prioritized and delivered in comprehensive reports and debriefings.



Industry-leading NIST cybersecurity framework

Identify

Assess Risks
Inventory critical assets and systems

Provide a thorough risk analysis

Protect

Develop Safeguards
Develop policies, procedures; introduce protective tools

Implement appropriate access and auditing controls

Detect

Make Timely Discoveries
Continuous monitoring 24/7/365

Enable auditing capabilities

Respond

Take Action
Establish a robust response plan

Create, analyze, triage and respond to detected events

Recover

Restore Functionality
Institute a recovery plan

Create improvements to prevent future attacks

Get the most out of your MDR Service

Our MDR service provides a comprehensive view of your organization's overall security posture and support from our 24/7 SOC experts. Our Cyber Assurance Program for MDR can help you maximize its benefits.

Strengthen your overall cybersecurity posture and better defend against cyber threats.

Global scale & experience

300+
Security experts focused on 24/7 monitoring & responses

9B
Security events proactively monitored each day

100%
Co-managed approach for visibility and control

20+
Years of experience developing cybersecurity solutions

For more information on CAP, how it can be combined with your existing MDR subscription and our Cybersecurity Services, contact your Motorola Solutions representative or visit us at:
www.motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A.