

Brochure



Prevent attacks, meet compliance requirements and respond quickly to security incidents

Strengthen your defenses and mission-critical system resilience



MOTOROLA SOLUTIONS

Table of contents

Safeguard your organization	2
Risk assessments	4
Penetration testing	5
Incident response planning	6
Tabletop exercises	7
Compliance assessments	8
Building a cyber defensive mindset	9
Resources	10

Safeguard your organization

To protect your systems, it's critical to have a complete understanding of where you might be vulnerable and which regulatory and compliance frameworks impact your organization.

Motorola Solutions Cybersecurity Services bring together an integrated portfolio of Managed Detection and Response (MDR) and Advisory Services aligned to the National Institute of Standards and Technology (NIST) framework.

As a trusted partner, we help you develop roadmaps to safeguard your information, employees and systems.

Our security advisors can assess your organization and deliver critical insights so you can make informed decisions on the best security procedures and controls to implement and build a robust cybersecurity strategy and roadmap in line with your business needs and industry best practices.

Our Cyber Assurance Program (CAP) is designed to help you improve your defenses even further once your MDR service is deployed. The program includes a suite of professional services delivered annually to strengthen your security response plans and overall program. They include Tabletop Exercises, Incident Response (IR) Planning, Risk Assessments, Vulnerability Scans and Penetration Testing (aka ethical hacking). The program is tailored to your specific environment. A multi-year package provides a cost-effective approach.



Cybercrime costs organizations an average of \$2.9 million¹ every minute, with global ransomware costs predicted to exceed \$265 billion² by 2031.

Motorola Solutions 90+ years of skilled experience, collaborative approach and use of scenario-based drills will prepare your organization to detect and respond quickly in the event of a cyber attack.



Global scale & experience

300+

Security experts focused on 24/7 monitoring and response

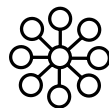


People

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

9B

Security events proactively monitored each day



Process

Services aligned to the NIST Cybersecurity Framework

20+

Years of experience developing cybersecurity solutions



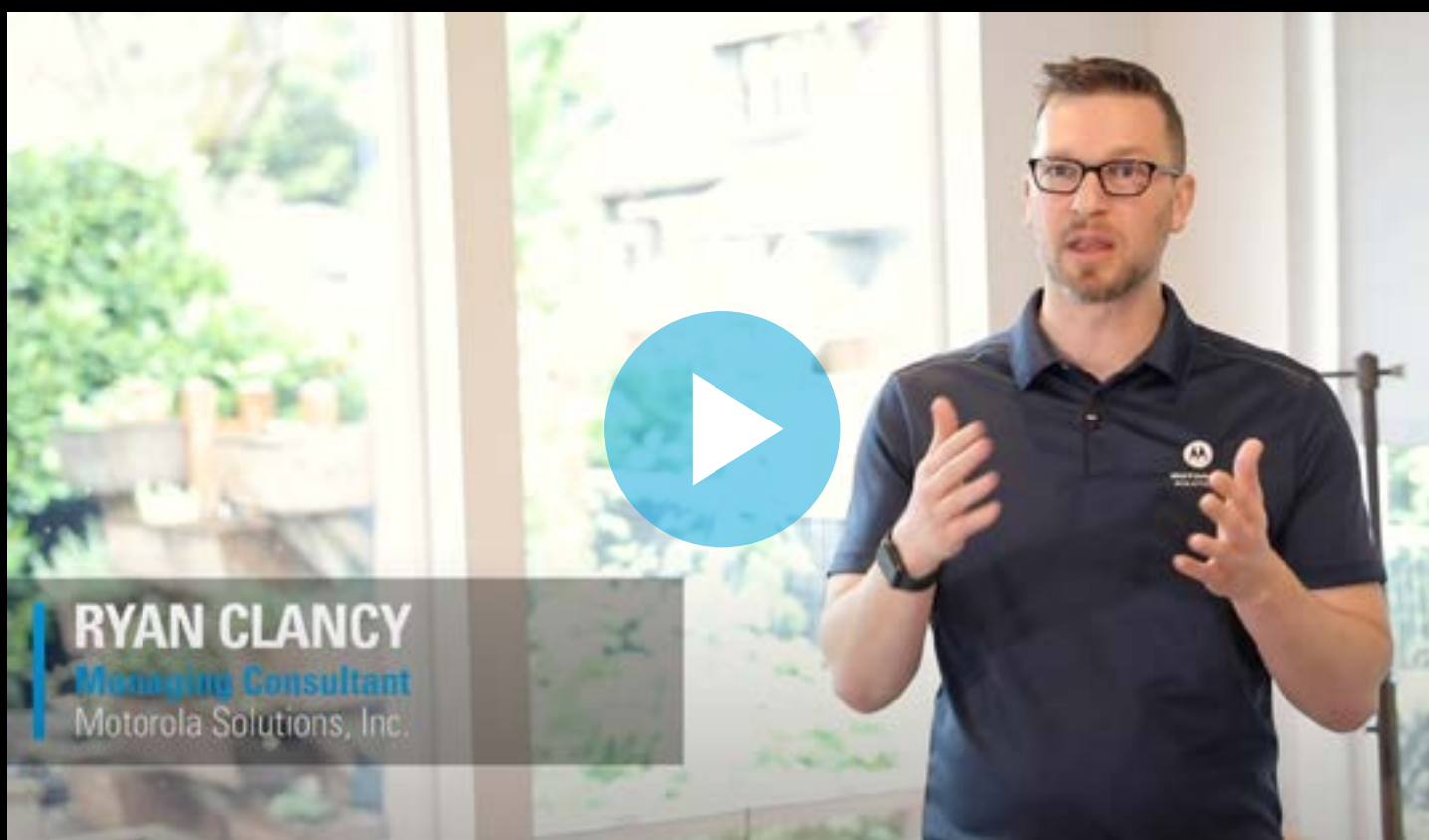
Technology

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



Risk assessments

Our assessments provide your organization with useful insights by analyzing your current environment, systems and security program to identify critical vulnerabilities and gaps that need to be addressed. We use this information to develop a robust cybersecurity strategy that is mapped to key regulatory frameworks and provide a prioritized list of risks and vulnerabilities.



Pre-assessment

Together we define the scope and agree on the desired outcome to meet your operational needs. Our cybersecurity experts collaborate with your team to define the statement of work and all deliverables. We develop an end-to-end understanding of your business operations including network architectures, security policies and controls, compliance and governance frameworks to finalize engagement scope and timelines.

Onsite assessment

Our onsite assessment, which includes data gathering and documentation, starts with one-on-one interviews with key stakeholders, understanding business profiles and analyzing annual statements and existing approaches to security. Workshops are conducted to close out any knowledge gaps. We can perform regulatory assessments along with vulnerability and threat intelligence assessments to evaluate network, applications and endpoints.

Post-assessment

Once our consultants have collected the data, they distill it using a set of sophisticated programs including a Risk Scorecard report indicating low, moderate, high and critical severities for each finding. Then, working with your team, we produce a set of roadmaps and recommendations to strengthen your system's cyber resilience.



Penetration testing

Our experts evaluate the security of your IT and communications infrastructure by trying to exploit its vulnerabilities. By probing your systems for any potential gaps, we can reveal issues that could leave your organization at risk and recommend how to close them before a malicious actor exploits them. Motorola Solutions offers penetration testing, also known as pentesting or ethical hacking, to ensure that your organization is aware of potential risks and how to best address them.

Types of pentesting

External

An external network pentest is designed to test the effectiveness of perimeter security controls to prevent and detect attacks, such as physical premises security and digital authentication soundness. It can also identify weaknesses in internet-facing assets such as web, mail and FTP servers.

Wireless

A wireless pentest is performed by ensuring that all wireless connections between the business WiFi network and devices are secured from attacks.

Internal

An internal network pentest helps organizations detect what an attacker could achieve with insider access to their network. An internal network pentest can mirror threats that can come from within an agency, such as an employee intentionally or unintentionally performing malicious acts or an external malicious threat actor who gains access to the same privileges as an employee.

Web application

A web application test ensures that any public facing web application, such as a website, is secure and that any data connected or submitted to that page is safe.

Phases of pentesting

Pre-engagement



Establish Rules of Engagement (ROE)

Engagement



Perform pentests aligned with ROE

Post-engagement



Document and submit applicable findings



Incident response planning

With cyber attacks on the rise, it's increasingly important to have an incident response (IR) plan ready in the event that your systems are compromised. Our incident response services are tailored to your needs and organizational structure to optimize how your agency will handle a cyber attack. Motorola Solutions custom IR plans are designed to be the best fit for your employees, processes and technology so you have a well-defined plan in the time of need.

Be prepared for any situation



Industrial control incidents



Natural disasters



Internal/external threats

Proven approach to security incident management

Motorola Solutions can help contain or prevent an incident by recommending and implementing safeguards. Through an array of technologies and skill sets around cloud analytics, endpoint threat hunting, log and data analytics, system forensics, malware analysis and more, our incident response planning provides assistance developing an integrated response to cyber attacks and data breaches. This can also include advanced threat hunting and post-incident analysis.



Tabletop exercises

Tabletop exercises are a type of emergency preparedness planning exercises that enable a broad group of participants to evaluate the effectiveness of your organization's incident response plan, as well as walk through the who, what, when, where and how of a situation in a safe environment.

Cyber exercises like this provide a valuable real-world scenario to see how prepared your team is and where improvements should be made, as well as ensuring that key stakeholders across the organization understand their role in the event of an emergency. These exercises improve the team's ability to detect, respond and recover to cybersecurity incidents faster.

20%

Of employees are likely to click on phishing email links³

95%

Of cybersecurity breaches result from human error⁴

Be prepared for any threat



Ransomware



Phishing



Malware



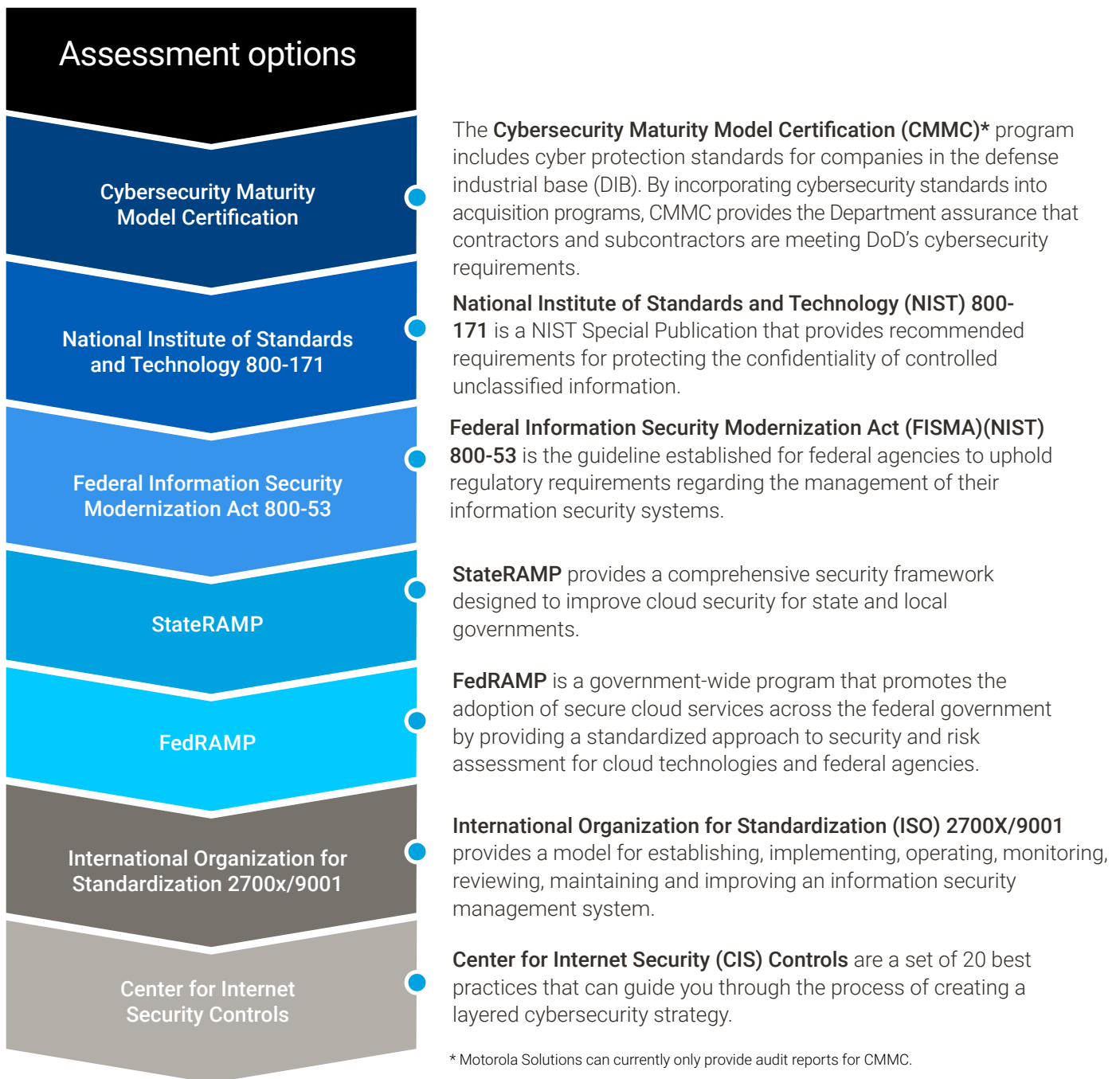
Data breach



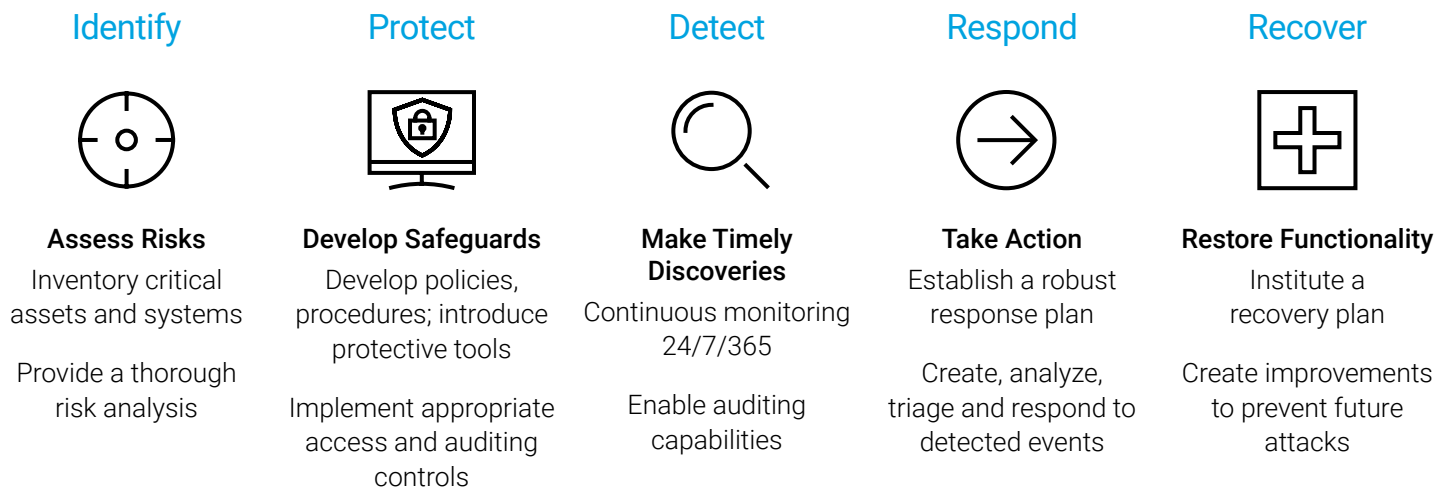
Compliance assessments

Our compliance assessments give you data-driven, prioritized recommendations to inform better cyber risk management and decision-making. We ensure your team adheres to the regulatory cybersecurity requirements that are in line with your unique organizational needs and follow industry best practices.

Our experts can provide gap analysis preparation and pre-audit verification. Audit reports* evaluate the strength and thoroughness of compliance preparations, security policies, user access controls and risk management procedures over the course of a compliance audit. Our experts are also approved to assess your agency or organization as meeting certain compliance certifications.



Industry-leading NIST cybersecurity framework



Building a cyber defensive mindset

When a cybersecurity incident occurs, what will you do? With cyber attacks growing in number and intensity, businesses and public safety agencies must be prepared to keep critical operations running smoothly by detecting and handling security incidents and breaches. Our experts are ready to work with your agency to create a comprehensive cybersecurity strategy plan.

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions Cybersecurity Services empower agencies to take control of their security and instill confidence in employees to handle cyber risks.





Resources

- 1 <https://www.forbes.com/sites/joeljohnson/2020/08/11/what-costs-29-million-every-minute-and-how-to-protect-yourself-from-it/?sh=509e33ed7764>
- 2 <https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/>
- 3 <https://www.techrepublic.com/article/phishing-emails-more-than-25-of-american-workers-fall-for-them/>
- 4 <https://www.cybintsolutions.com/cyber-security-facts-stats/>



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](https://www.motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2024 Motorola Solutions, Inc. All rights reserved. 03-2024 [EV06]