White Paper

Securing your mission-critical operations

Improve your defenses against threats with cybersecurity services

MOTOROLA SOLUTIONS

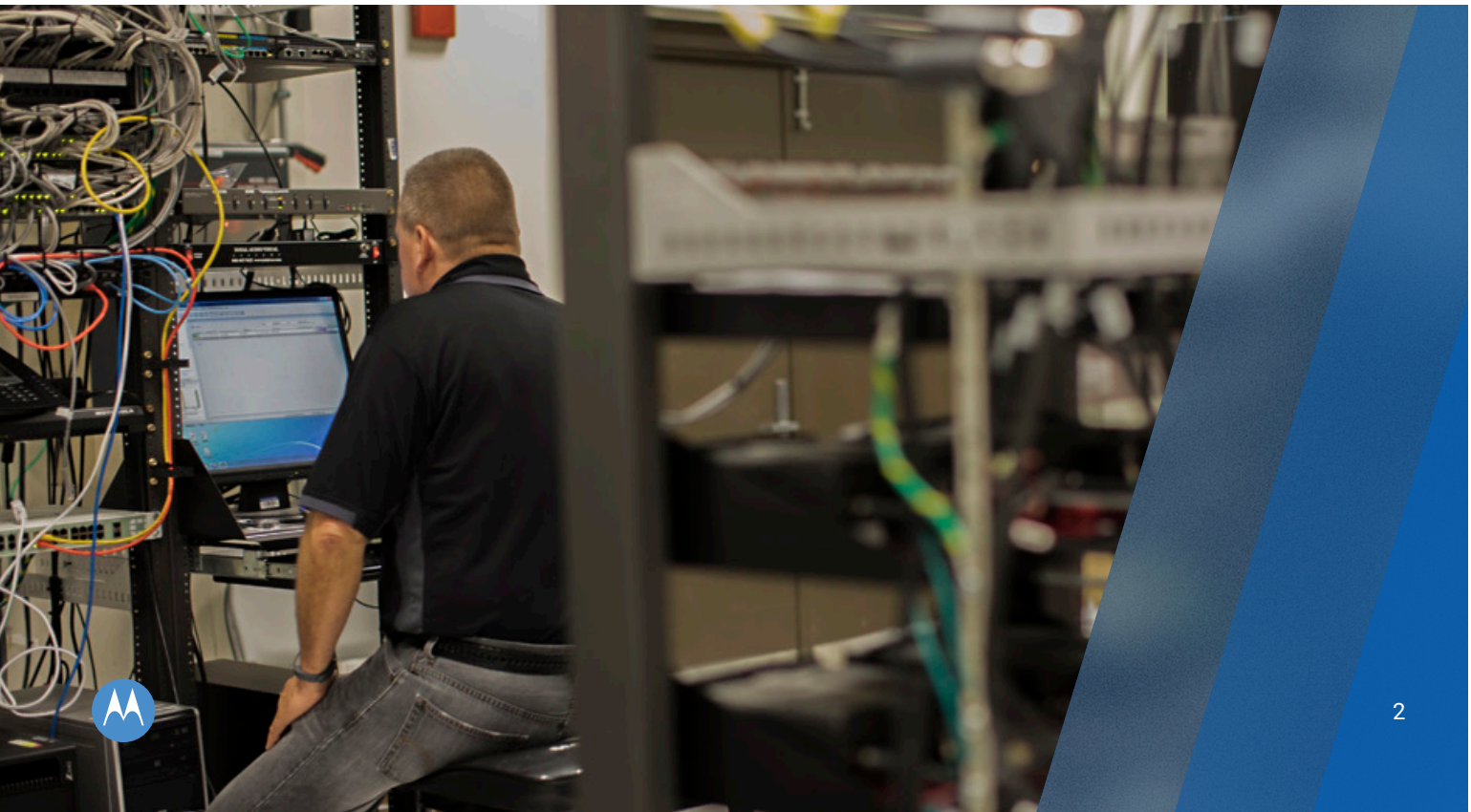
Cyber attacks are a reality. And the stakes are high.

For organizations tasked with mission-critical operations, system downtime can endanger lives. Failure is simply not an option. But cyber attacks continue to accelerate in number, frequency and impact. In fact, the annual cost of global cyber crime damage is expected to hit $10.5 trillion by 2025.[1]

Malware, ransomware, phishing, man-in-the-middle attacks, distributed denial-of-service attacks, SQL injections and zero-day exploits are some of the common attacks that can disrupt mission-critical operations without a moment's notice. Too often, security strategies are created to "check the box" on security compliance or as a reaction to a specific attack. Clearly, yesterday's strategies to secure mission-critical operations are inadequate to protect against today's advanced and accelerating cyber threats.

The uncertainty and the financial implications of a cyber attack have made cybersecurity a top concern for organizations. Advancement in cyber attack techniques and an ever-evolving IP-based system are putting relentless pressure on in-house resources. There is a constant need to update skills and expertise in order to manage a complex environment and bolster cyber resilience. In addition, investments in next-generation security tools to prevent and combat sophisticated threats continues to pose a challenge, as organizations face shrinking budgets.

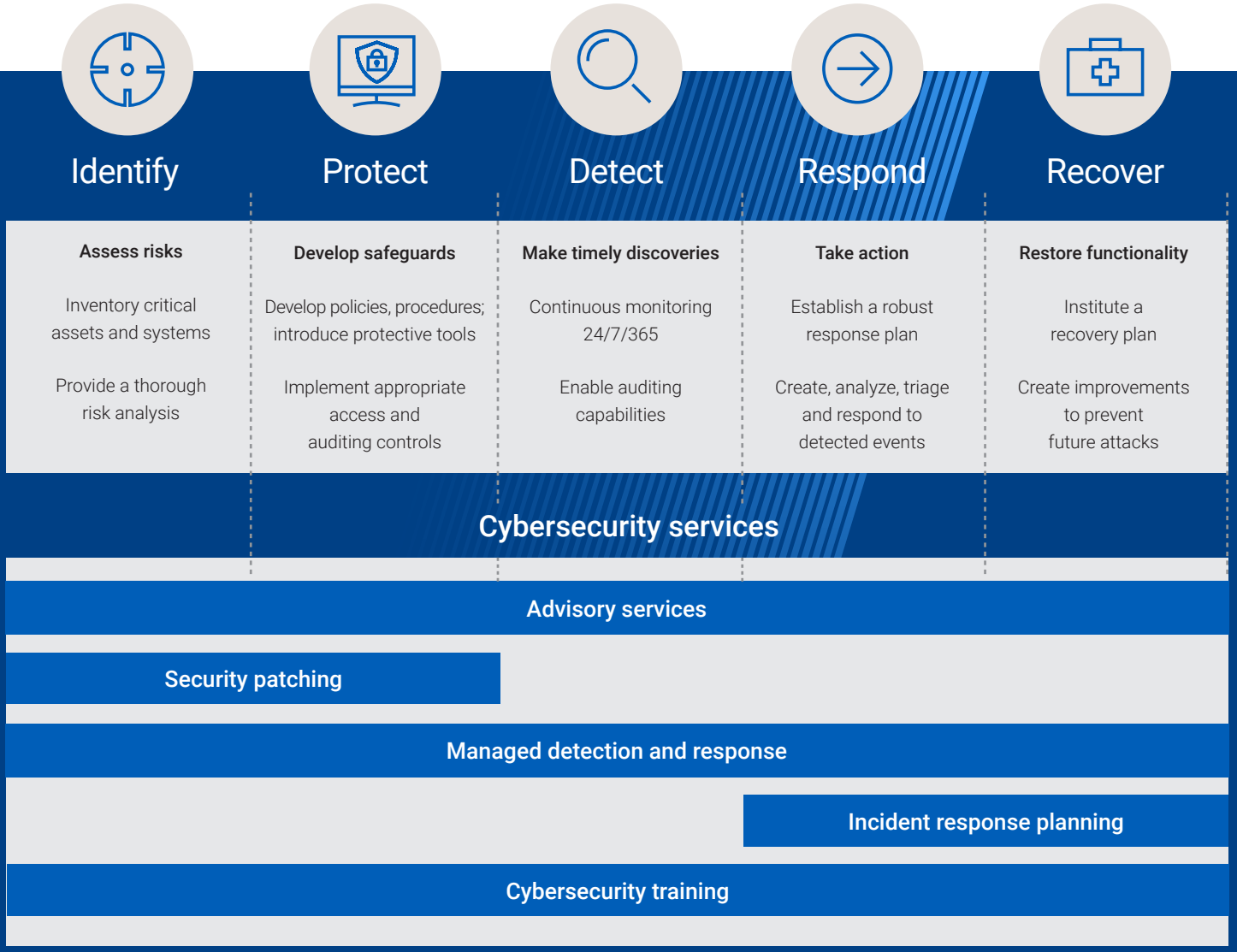
What's needed? A holistic approach to cybersecurity centered around a risk mindset, that focuses on mitigation options, continuous monitoring, diagnosis and remediation. We can help. We bring a range of security products and services that span your mission-critical ecosystem – networks, command center software, video and radios. We're continuously evolving our portfolio to ensure you have the cyber resilience to stay a step ahead of increasingly sophisticated attacks. With the seamless orchestration of highly specialized talent, industry-leading security processes and cutting-edge tools, we help manage the complexity of cybersecurity so you can focus on your core mission.



Secured by Motorola Solutions: services for cyber resilience

Our approach to cybersecurity includes a holistic set of services spanning Risk Assessments, Security Patching, Advisory Services and Managed Detection and Response (MDR). All of our offerings closely follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is aimed at helping organizations manage cyber risk awareness, detection, response and recovery.

Industry-leading NIST Cybersecurity Framework



Risk Assessments

Based on decades of experience working closely with public safety, government and enterprise customers we've refined a systematic and reproducible risk management assessment that helps you better understand your specific security environment. This spans your technology ecosystem including the command center, LMR networks, radios and video cameras, as well as your IT network.

Our Risk Assessments provide a structured approach for identifying, assessing and managing infrastructure and software cyber risks. We start with a series of interviews, surveys and workshops to develop a thorough understanding of your requirements and current environment.Then we use a time-tested scorecard methodology that measures your objectives against your cyber resilience readiness, with a focus on identifying anddefining specific risk elements unique to your environment. We deliver a readiness dashboard that addresses vulnerabilities, business process and skills alignment based on your technology attributes, security architecture and governance policies.

At the conclusion of the assessment, you receive a risk scorecard report that prioritizes each finding based on low, moderate, high and critical severity. A remediation or risk acceptance recommendation follows each finding. Finally, based upon the gaps identified, we can introduce new technologies and provide services that help you withstand security threats on an on-going basis.

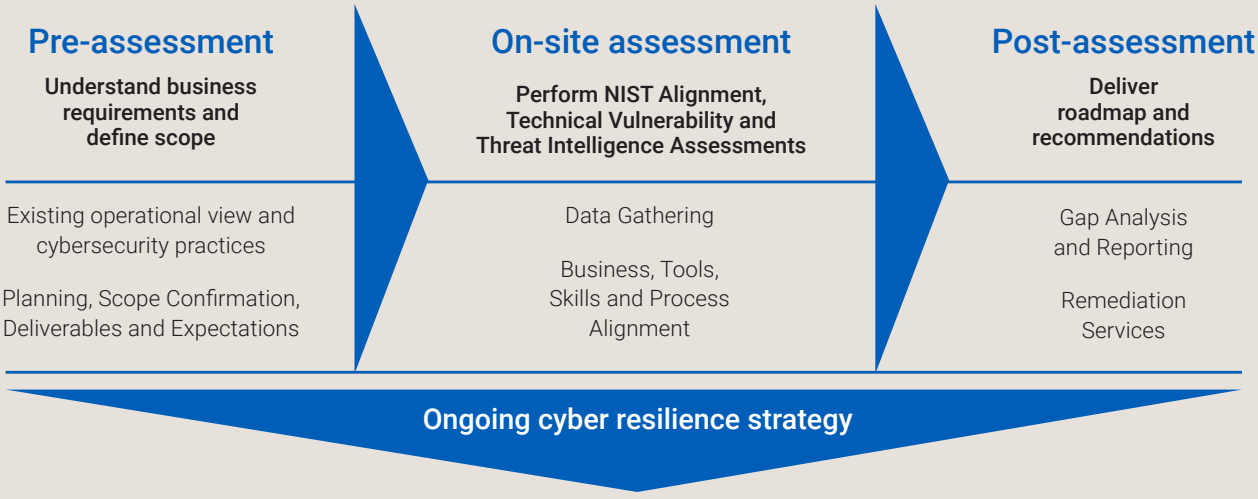
Security Patching

Security patching is one of the most important, but often overlooked, tools to defend against cyber attacks. All software, systems and devices need continuous patching to stay secure. We work with you in three phases – identification, testing and installation – to ensure your patching procedures are as efficient and secure as possible.

First, our dedicated Information Assurance Lab identifies and validates required security updates to identify any gaps in your system patches. All hardware and software assets, network and communication flows and dependencies are identified, mapped, classified and managed according to criticality. While it's important to apply patches as soon as possible once released, for mission-critical systems it's absolutely essential to thoroughly test them before deployment. Motorola Solutions' Security Update Service pre-tests the latest anti-malware definitions and all applicable software patches in dedicated testing labs. Once validated as safe, we work closely with you in the installation phase. We either make the updates for you or make them accessible on our secure extranet for implementation, so your organization can easily deploy them on its own terms.

You cannot effectively patch aging systems. Today's IP-based mission-critical networks require periodic upgrades to stay current. Motorola Solutions provides system upgrades to enable both software and hardware technology refresh across your infrastructure while ensuring system availability.

Repeatable process, continuous awareness and evaluation



Managed detection and response

Ensure your mission-critical systems are resilient to cyber attacks and threats. Our managed security services for public safety provide a complete solution to identify, remediate risks, detect and respond to cybersecurity threats 24/7.

Security expertise

Our security operations center (SOC) is staffed by highly skilled analysts who continuously monitor your devices and systems to quickly detect and remediate cyber threats.

Co-managed platform

Our advanced ActiveEye platform provides real-time, 24/7 visibility into what our SOC analysts see for better insights and collaboration.

Integrated solutions

Our Managed Detection and Response (MDR) service is integrated with Motorola Solutions systems and devices, providing unparalleled compatibility and access to our engineers.

Robust reports

ActiveEye's ad hoc reporting capabilities enable you to investigate and hunt active threats, and to view historical data sets. Reports provide a simple, consistent view of collected event data. Pre-defined templates organize the data and display the most important attributes of event types. Users can customize these standard reports to display and summarize different attributes when needed.

Advanced Threat Insights

ActiveEye Advanced Threat Insights expand upon the standard SOC monitoring services. Advanced Insights provide in-depth research to give you a more complete picture of how secure your systems are.

Cyber Assurance Program

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.

Public Safety Threat Alliance

Motorola Solutions established the Public Safety Threat Alliance (PSTA) in 2022, a cyber threat Information Sharing and Analysis Organization (ISAO) recognized by the Cybersecurity and Infrastructure Security Agency (CISA). The PSTA is designed to provide public safety agencies with the knowledge they need to better defend against risks like ransomware and data breaches. It operates as a single organization focused on the collection, analysis, production and sharing of actionable cyber threat information. Our global reach, combined with more than 90 years of experience supporting public safety customers and the communities they serve, allows us to rapidly establish a network of trusted partners and share information and intelligence on the most pressing cyber threats to public safety delivery status from a single web-based platform.

Your Motorola Solutions edge: people, process and tools

Effective cybersecurity goes beyond technology. Our industry-leading talent, security processes and cutting-edge tools are part of an integrated approach that streamlines complexity and makes it easier for your organization to manage risk.

People

Lack of cybersecurity expertise is a constant challenge facing many organizations today. This can slow adoption and implementation of the critical tools and processes needed for effective cybersecurity protection.

Our people are the driving force of our security culture, one that's fully integrated in everything we do. Our experts guide the entire range of our solutions, constantly striving for more predictive and proactive cybersecurity. They hold top industry certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+ (Security+), Certified Ethical Hacker (CEH) and GIAC Security Essentials Certification (GSEC), and stay sharp with comprehensive, ongoing training.

We created the Motorola Solutions Cyber Champions Program, which instills cybersecurity principals and knowledge at a grassroots level throughout every facet of the company.

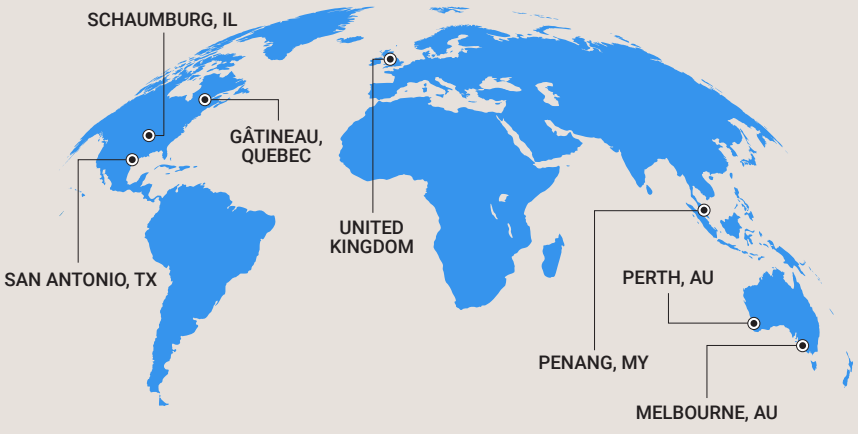
We continuously invest in cyber education and training because when our cybersecurity experts are set up for success, so are you. We use the NIST Cybersecurity Workforce Framework to guide our cyber education and training efforts.

Our experts are here to help you navigate a complex technology environment so that your people can focus on the mission, not the technology.

Security Operations Centers (SOCs)

Motorola Solutions' Security Operations Centers (SOCs) can monitor networks, applications, and devices for security threats 24/7 via ActiveEye. Our SOC analysts possess deep technical skills on both the offensive and defensive side of security. Based on their broad security experience, our SOC analysts recommend security device configurations that optimize threat detection and implement playbooks to cut through the noise and quickly address the most critical threats.

This puts our focus on identifying activity that could be a potential security risk or incident.



Process

Our cybersecurity processes are guided by three core objectives: confidentiality, integrity and availability. Data and information must be confined to people authorized to access it and not be disclosed to others; data must be kept intact, complete and accurate, with IT systems operational; and all information must be available to authorized users whenever needed. While many organizations simply focus on prevention, in today's threat climate, every enterprise must be thoroughly prepared for a "worst-case" cyber attack scenario.

With the NIST Cybersecurity Framework at its core, our approach to cybersecurity focuses on mitigation options, continuous monitoring, diagnosis and remediation to secure and protect systems and networks. Our experienced team draws on extensive global knowledge to develop a service delivery model, architecture and policies that meet your needs.

Tools

Cybersecurity analysts face an overwhelming number of challenges, and one of their day-to-day issues is filtering through and addressing a large volume of alerts. Although these security alerts are important to safeguarding your organization, they are generated by many different devices, platforms and applications, making it difficult to quickly identify actual threats. A managed cybersecurity platform like ActiveEye, which powers Motorola Solutions Managed Detection and Response (MDR) services, solves this problem. ActiveEye allows all of these alerts to be collected in one place, filters out unimportant threats and leaves only critical alerts to examine. Additionally, our SOC analysts continually monitor your systems and network for potential attacks and remediate them as needed so your security team can focus on other important tasks.

A key feature of ActiveEye is Security Orchestration, Automation and Response (SOAR) that is critical in identifying cyber threats and resolving alerts faster. SOAR allows ActiveEye to pull in data from IT networks, endpoints and cloud environments, as well as mission-critical solutions like PremierOne®, Flex®, VESTA® 9-1-1 and ASTRO® systems.

In addition to threat intelligence curated from multiple third-party sources, the ActiveEye platform is continuously updated with the latest cyber threat intel provided by the Public Safety Threat Alliance (PSTA). Security analysts are given even more context as needed and this further speeds response times. The platform uses machine learning capabilities as well to understand and apply what our human analysts do, and to automate those responses. This saves countless hours of time that would otherwise be spent on manual work.

Cyber resilience done right

Cyber attacks can happen to anyone at any time. Are you ready? Our cybersecurity services offer the expertise, cutting edge technology and responsiveness to help you get there. Partnering with Motorola Solutions allows your team to focus on your mission instead of worrying about security. We manage the complexity for you, which means you are always on pace with innovation at a predictable cost. Our team of specialists partner with your team, holistically securing your most important communication assets, anticipating issues before they become problems and continuously improving plans to prevent future attacks.

Motorola Solutions is the mission-critical communications leader for a reason. We bring the same trust and commitment you've relied on for over 90 years to every cybersecurity service we offer. With industry-leading people, processes and tools we're redefining what it means to ensure resilience for mission-critical operations.

Global scale and 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

Aligned to the National Institute of Standards and Technology (NIST) Framework

Technology

Real-time visibility into threats via our ActiveEye Security Orchestration, Automation and Response (SOAR) platform

[1]cybersecurityventures.com

See how Motorola Solutions can help keep your organization secure.
To learn more, visit: **www.motorolasolutions.com/cybersecurity**

MOTOROLA SOLUTIONS

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

Availability note (for example: Not available in Canada. Only available in Australia. Available in Europe.)