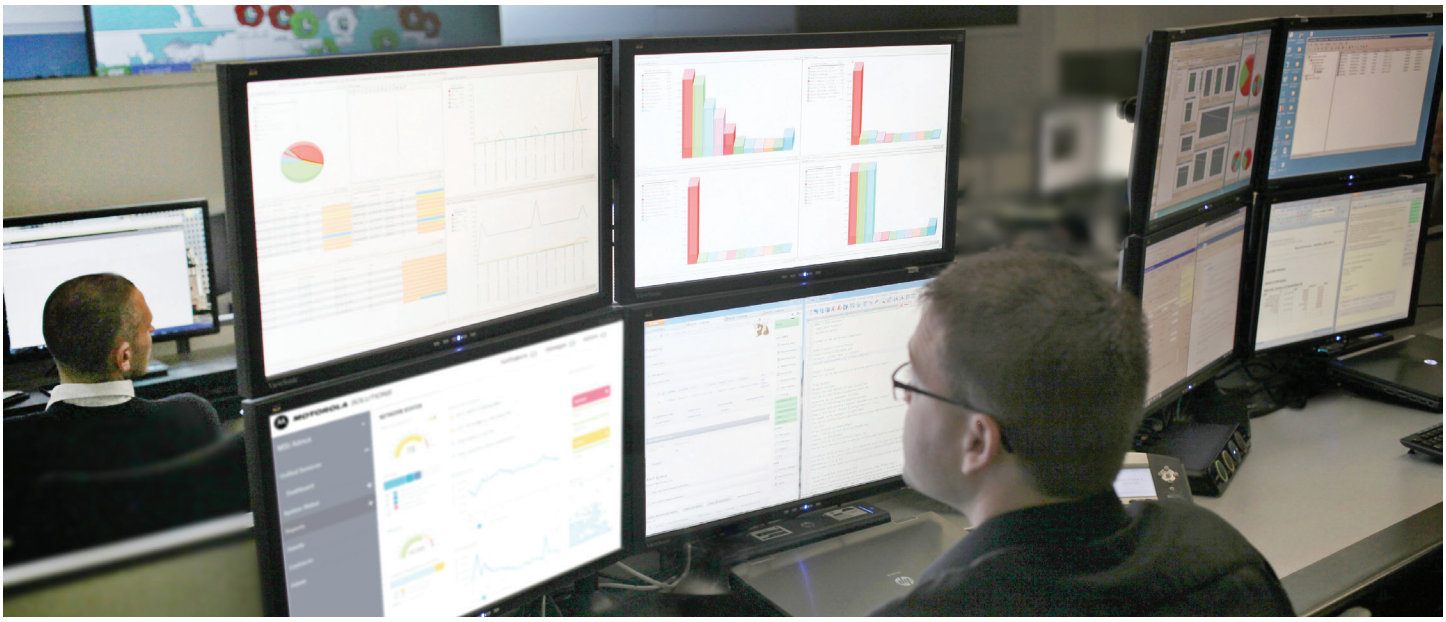
PROACTIVELY PROTECT MISSION-CRITICAL INFRASTRUCTURE FROM CYBER ATTACKS AND THREATS

24 X 7 REAL-TIME REMOTE SECURITY MONITORING



COMMUNICATION SYSTEMS FACE INCREASED SECURITY RISK

IP-based systems face an increasing risk of intrusion and system compromises that are constantly evolving. As mission-critical communications networks become interconnected to other IP-based systems, they are just as exposed to cyber threats and require proactive risk management.

Having security elements like anti-malware, firewalls or intrusion detection systems inspecting traffic traversing the network are not enough. Enterprise systems must be constantly monitored by experienced security professionals trained to detect, characterize and respond to security events. Proactive security monitoring helps you stay a step ahead of threat detection and mitigation to maintain optimal network performance.

Included with our Premier Services and optional in our Essential and Advanced Services packages, Motorola's Security Monitoring service provides a comprehensive methodology to identify, protect, detect, respond and recover mission-critical communication systems and IT networks from cybersecurity incidents.

By relying on Motorola for security monitoring, you are partnering with the global leader and innovator of mission-critical communications solutions providing unmatched experience, expertise and support for protecting land mobile radio systems and enterprise networks.

- **Identify** assets to be monitored, categorized and risk-prioritized.
- **Protect** all networks from attacks with proactive security updates and monitoring for suspicious activity.
- **Detect** suspicious system faults, network traffic anomalies and potential security threats real-time, 24 x 7.
- **Respond** to suspicious events by performing remote investigation, diagnostics and if necessary take action to neutralize the threat.
- **Recover** by restoring affected components or the entire system to proper operational state.

In 2014, the National Institute of Standards and Technology (NIST) issued the Framework for Improving Critical Infrastructure Cybersecurity, which outlines drivers to guide cybersecurity activities and serves as a basis for organizations to formally consider cybersecurity risk as part of their risk management process. The framework provides a blueprint of activities to achieve specific cybersecurity outcomes and consists of five concurrent and continuous functions: identify, protect, detect, respond and recover.

Motorola applies this framework to deliver comprehensive Security Monitoring and Management services.

REAL-TIME REMOTE MONITORING BY CERTIFIED PROFESSIONALS

Experienced, highly trained and certified security professionals are staffed 24 x 7 at Motorola's Security Operations Center (SOC) dedicated to monitoring the secure state of your IT systems. The skilled technologists are continuously updated on the latest cyber threat intelligence and apply event correlation and analytics tools to assess the monitored environment for potential threats and ready to take immediate action to protect network integrity. Remote security monitoring covers:

- Management of firewalls, intrusion detection sensors, authentication and logging servers
- Worm, virus, phishing, social engineering and other malicious activity
- Network vulnerabilities
- Abnormal network activity
- Compromised host command and control communication
- Web content filtering of domains and management of exemptions
- Email security with spam filtering and data loss protection (DLP) through email
- Full-packet capture that stores and analyzes all network traffic at the Internet Point of Presence (IPOP)
- Advanced behavioral analytics for internal data theft and extrication

Potential incidents are investigated by security analysts who thoroughly research and analyze the event. If the event is a confirmed incident, the technologists will conduct remote diagnostics to remedy the situation immediately or dispatch a local technician to the site. The dedicated security team continues to monitor the event until fully resolved. Many times, security events are caught and resolved before impacting the network helping you minimize maintenance costs and ensuring reliable system performance.

PROACTIVE COUNTERMEASURES FOR RISK MITIGATION

As attacks become more sophisticated, prevention is critical for a successful security strategy. Motorola's monitoring of customer networks enables the ability to rapidly identify emerging security threats that may potentially impact other customers. This visibility makes it possible to recommend proactive countermeasures to help mitigate network security risks. As soon as an issue is identified, the Security Operations Center has test labs to duplicate the issue and develop a resolution before it's made available for deployment on the customer's network.

ANALYTICS FOR CONTINUOUS PROTECTION

Monthly reports are generated to keep you informed on the overall security risk posture of your system with details related to your operational environment. When investigation is deemed necessary, our certified forensics experts can extract and examine critical intelligence for use as evidence or to establish future preventative safeguards.

For more information about our Security Monitoring Service, contact your Motorola representative or visit motorolasolutions.com/cybersecurity.

MOTOROLA SOLUTIONS