Datasheet

Managed Detection and Response for PremierOne CAD

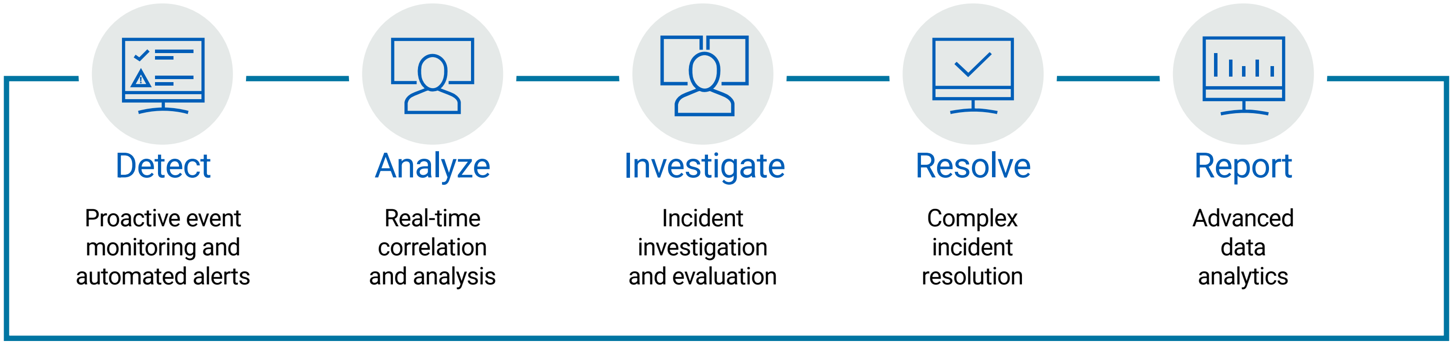
Enhanced security and resilience for your PremierOne CAD system

In today's complex cybersecurity landscape, public safety agencies relying on mission-critical systems like PremierOne Computer-Aided Dispatch (CAD) face increasing cyber threats. These threats, such as ransomware attacks, can severely impact system availability, compromise sensitive data and disrupt emergency communications putting lives at risk.

Motorola Solutions' Managed Detection and Response (MDR) service for PremierOne CAD leverages Endpoint Detection and Response (EDR), log collection and analytics, a network intrusion detection system and the advanced ActiveEye security platform. Experienced security analysts provide 24/7 monitoring, threat detection and rapid response capabilities. All designed to protect your PremierOne CAD environment and the surrounding IT infrastructure.

MDR helps public safety organizations enhance their cybersecurity posture, maintain operational continuity and work towards CJIS compliance requirements. Designed and tested specifically for PremierOne, it ensures compliance while maintaining your system's high availability and performance. So you can spend less time worrying about security and more time focusing on your mission.

Systematic approach to mitigate risks



Detect
Proactive event monitoring and automated alerts

Analyze
Real-time correlation and analysis

Investigate
Incident investigation and evaluation

Resolve
Complex incident resolution

Report
Advanced data analytics

Key features

24/7 Security Operations Center

Our Security Operations Center (SOC) provides 24/7 monitoring and expertise and is staffed with experienced, highly trained and certified cybersecurity experts who continuously monitor your PremierOne system for suspicious activity. These analysts are experienced in public safety threats and are prepared to investigate and initiate a response when necessary, including actions against ransomware.

ActiveEye Security Platform

The ActiveEye Security Orchestration, Automation and Response (SOAR) platform serves as the central hub for security operations. It collects and analyzes security data from your PremierOne system and connected IT systems, differentiating between malicious and routine traffic to focus on actual threats.

ActiveEye Co-Managed Portal

The ActiveEye web-based portal provides visibility to threat insights, event investigations, security reports, threat advisories and the status of any security cases. The platform provides a “single pane of glass view” offering full visibility into cybersecurity activity across your CAD system, enterprise networks and endpoints. As a co-managed platform, ActiveEye synchronizes security efforts between your security team and our SOC analysts, ensuring you have 24/7 visibility and can see what our SOC analysts see. Giving you access to review security data, configure alerts and notifications, perform security investigations, and generate custom reports. The ActiveEye portal allows users to save queries, customize reports and set up daily email summaries of key security statistics, including alert counts and security cases. ActiveEye also allows you to set-up and receive automatic alerts or notifications via email or other communication channels.

Endpoint Detection and Response

Endpoint Detection and Response (EDR) agents are deployed on PremierOne client workstations and servers to look for anomalies, detect previously unknown attacks and identify potential insider threats. Integration with the ActiveEye platform enables security analysts to respond quickly to attacks by isolating hosts, blocking or removing malicious files and viewing integrated threat intelligence.

ActiveEye Remote Security Sensor

The physically deployed ActiveEye Remote Security Sensor (AERSS) provides remote collection of logs, network intrusion detection and vulnerability scanning for your PremierOne system. The AERSS monitors network traffic for real-time signatures of malicious activity and analyzes traffic for anomalies. It also collects logs from various system components and forwards them to the ActiveEye platform for analysis.

Log Collection and Analytics

The platform collects log data from systems, applications, networking components and security systems within your PremierOne environment. Analytics components and security policies process this data to identify policy violations and suspicious activity, providing critical context for tracking the origin of threats and identifying new attack patterns. Collected events are stored for a defined period, allowing for threat hunting and historical analysis.

Network Intrusion Detection System

A Network Intrusion Detection System (IDS) is deployed within your PremierOne network to perform real-time signature and anomaly detection. The NIDS analyzes network traffic at both packet and flow levels to identify malicious activity and anomalous behavior.

External Vulnerability Scanning

External Vulnerability Scanning (EVS) regularly scans the internet-facing, external network interfaces of your PremierOne system for new software component vulnerabilities and insecure system or network settings. Scans identify vulnerabilities, provide risk scores using the Common Vulnerability Scoring System (CVSS) and recommend actions for remediation.

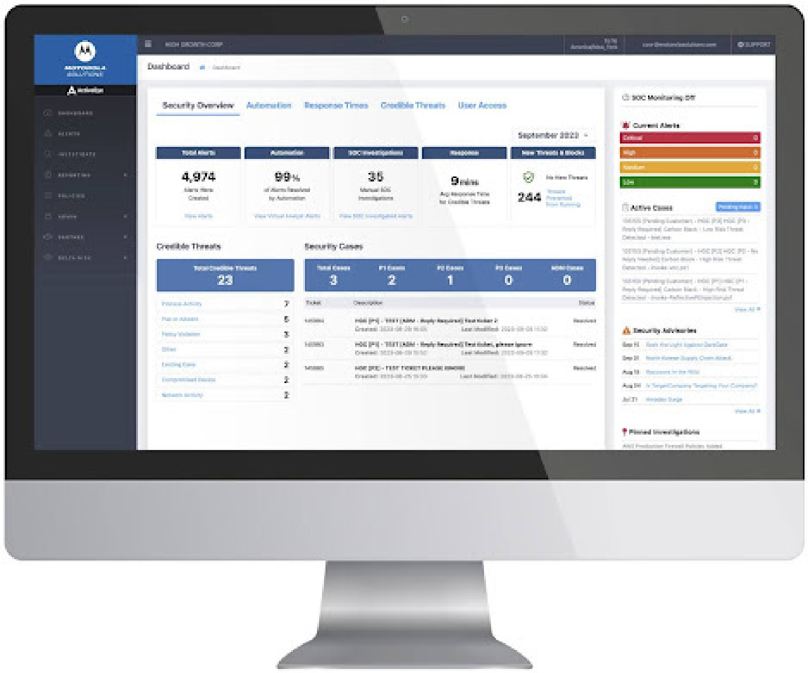
Incident Response Support

When a security incident is detected, our SOC analysts will engage with your team, participate in status calls, perform compromise assessments and provide guidance on recovery approaches. They leverage the data available in ActiveEye to determine the extent of malicious activity and recommend mitigating actions.

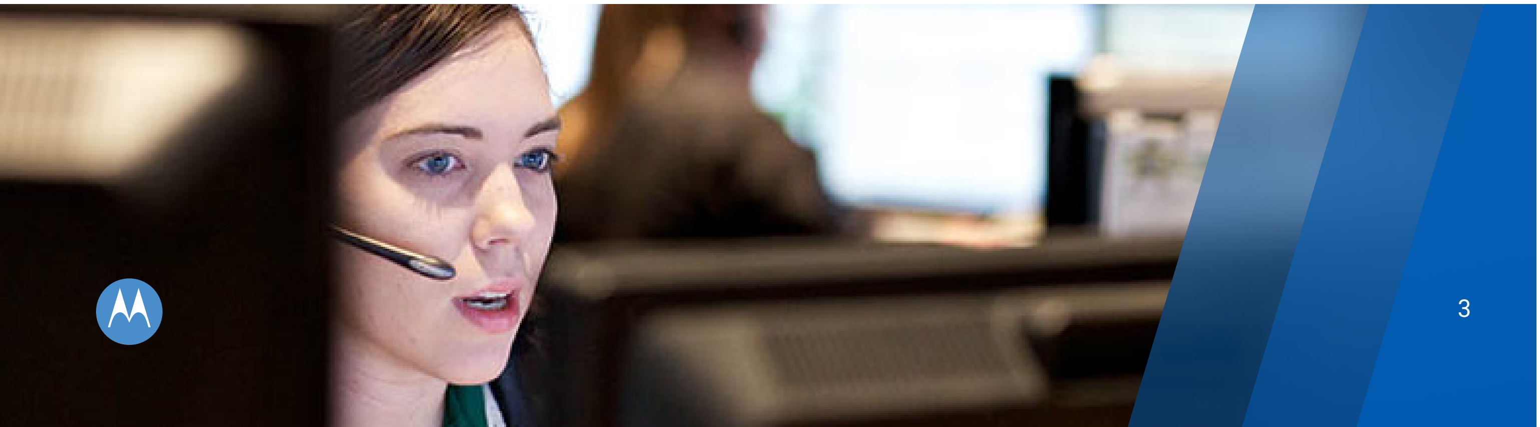
Advanced Threat Insights (Optional)

With the optional Advanced Threat Insights (ATI) our highly trained SOC analysts provide threat intelligence and alerts specific to your industry and organisation. You will also have a named cybersecurity analyst to provide knowledge and expertise on how to best take action against a threat.

Key benefits



- **Reduced cybersecurity risk**
  By providing continuous monitoring and addressing vulnerabilities across your PremierOne CAD system and IT infrastructure MDR significantly strengthens your overall security posture and reduces the risk of successful cyber attacks and impacts on your system availability, integrity and confidentiality.
- **Helps meet compliance requirements**
  The expanded MDR capabilities, including log analytics, network intrusion detection and the ActiveEye portal's reporting features can significantly assist in achieving compliance with regulations such as the CJIS Security Policy.
- **Enhanced threat detection and response**
  The combination of EDR, the ActiveEye platform's advanced analytics, real-time threat intelligence and 24/7 expert monitoring enables better identification of threats and a more rapid and effective responses to mitigate cyber attacks before they cause significant damage.
- **Reduced burden on your teams**
  Managing a comprehensive cybersecurity program can be challenging and resource-intensive. Our MDR service supplements your in-house skills with 24/7 expertise, freeing up your teams to focus on other critical tasks.
- **Complete visibility and control**
  The co-managed ActiveEye portal provides complete transparency into your security environment, allowing you to see detected threats, understand the actions being taken and generate customized reports.
- **Cost-effective security**
  Outsourcing your 24/7 security monitoring and response needs through our MDR service can be significantly more cost-effective than building and staffing an in-house Security Operations Center.
- **Access to cybersecurity insights and expertise**
  Our SOC is staffed with trained and accredited cybersecurity professionals experienced in mission critical systems and threat insights, log analytics and external vulnerability scans provide proactive identification of threats.



Motorola Solutions — Your trusted partner

As a leading provider of mission-critical solutions, we understand your mission can only be as secure as your partners enable you to be. Our goal is to provide you with transparency, accountability and security that's built-in from the start.

Our expert team, industry certifications, robust policies, and advanced technology uniquely position us to provide superior cybersecurity solutions that meet your current and future needs.

By choosing Motorola Solutions' Managed Detection and Response service for PremierOne CAD, you gain a trusted partner dedicated to protecting your mission-critical operations with cutting-edge technology and expert analysis.

Global scale & experience

300+
Security experts focused on 24/7 monitoring and 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 aligned to the NIST Cybersecurity Framework

Technology

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

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