

2025

seceon

Eastern Mediterranean Under Cyber Siege:

A Unified Response to Critical Infrastructure Threats

Protecting Healthcare, Critical Infrastructure, and Manufacturing Across Greece, Cyprus, Romania, and Israel

Prepared by Seceon, Inc. in partnership with CyberLion Ltd.

Executive Summary

The Eastern Mediterranean region—encompassing Greece, Cyprus, Romania, and Israel—faces an unprecedented convergence of cybersecurity threats targeting its most critical sectors. This strategically vital region has become a primary battleground for sophisticated cyber adversaries, with attack frequencies and sophistication levels that far exceed global averages.

> *"Seceon's AI-driven cybersecurity platform consistently demonstrates exceptional accuracy and responsiveness, helping our clients detect threats faster and with greater confidence. Their innovative technology raises the bar for enterprise-grade protection."*
> **Mr. Arie Wolman, EVP Sales, CyberLion Ltd.**

Current Threat Landscape:

Israel is the target of thousands of cyberattacks per day, mostly from Iran, Russia, and North Korea, though in 2024, Ukraine took top spot with 2,052 attacks, according to Radware's 2024 report. Meanwhile, Russian hackers targeted Romania's election systems with over 85,000 cyberattacks and leaked credentials on Russian hacker forums, and a ransomware attack affected over 100 healthcare facilities in Romania.

Key Regional Findings:

- **Healthcare Crisis:** Life-threatening ransomware attacks affecting over 100 healthcare facilities demonstrate the urgent need for specialized healthcare cybersecurity
- **Democratic Infrastructure:** Coordinated attacks on electoral systems with over 85,000 documented attack attempts
- **Critical Infrastructure:** Cyprus's critical infrastructure and government websites were targeted in a series of coordinated cyberattacks claimed by several pro-Palestine hacker groups
- **Economic Impact:** Regional attacks causing multi-million euro losses and threatening business continuity across strategic sectors

Business Impact:

- **Platform Consolidation:** Reduce from 15+ security tools to a single unified platform
- **Enhanced Detection:** AI-driven threat detection with dramatically reduced false positives
- **Automated Compliance:** Streamlined compliance for EU and national regulatory requirements
- **Regional Expertise:** Specialized understanding of Eastern Mediterranean threat landscape

Regional Threat Landscape

Geopolitical Targeting and Nation-State Actors

The Eastern Mediterranean's strategic importance makes it a focal point for sophisticated nation-state cyber operations and ideologically motivated attacks that exceed typical cybercrime patterns.

Coordinated Regional Campaigns:

The region faces sustained, coordinated campaigns that demonstrate clear strategic objectives rather than opportunistic attacks. A planned cyberattack targeting the infrastructure of Cyprus is scheduled for 17th October 2024, with potential tactics including distributed denial of service (DDoS), data breaches, and other exploitation techniques, illustrating the level of planning and coordination targeting regional infrastructure.

Multi-Vector Threat Environment:

Regional organizations face threats from multiple sophisticated actors simultaneously:

- **Nation-State Operations:** Radware warns of surge in Iranian cyber activity targeting Israeli industrial, critical systems
- **Electoral Interference:** Systematic attempts to undermine democratic processes with documented attacks exceeding 85,000 attempts
- **Ideologically Motivated Groups:** Coordinated campaigns by international groups targeting regional infrastructure
- **Advanced Criminal Organizations:** Sophisticated ransomware operations targeting high-value regional assets

Critical Sector Vulnerabilities

Healthcare Sector Crisis:

The region's healthcare infrastructure faces existential cybersecurity threats. The Romanian ransomware incident affecting over 100 healthcare facilities demonstrates the scale and coordination of threats facing regional healthcare systems. These attacks directly threaten patient safety and create cascading effects across national healthcare infrastructure.

Critical Infrastructure Under Assault:

Regional critical infrastructure faces systematic targeting designed to maximize economic and social disruption:

- **Energy Systems:** Attacks on regional energy infrastructure designed to cause widespread outages
- **Transportation Networks:** Targeting of ports, airports, and logistics systems that serve as regional hubs
- **Financial Services:** Sophisticated attacks on banking and financial infrastructure
- **Government Services:** Coordinated attacks on government systems designed to undermine public confidence

Manufacturing and Supply Chain Risks:

Regional manufacturing faces increasing threats from supply chain attacks and industrial espionage:

- **Intellectual Property Theft:** Sophisticated campaigns targeting proprietary manufacturing processes and technologies
- **Supply Chain Compromises:** Attacks designed to infiltrate multiple organizations through vendor networks
- **Industrial Control System Targeting**: Attempts to disrupt or damage physical manufacturing infrastructure
- **Economic Espionage:** State-sponsored theft of competitive intelligence and strategic information

Cross-Border Attack Patterns:

Recent attacks have specifically targeted critical infrastructure, highlighting the need for robust defenses in Greece, while similar patterns are evident across all four nations. In Q3 2024, an average of 1,876 cyber attacks per organization was recorded, marking a 75% increase compared to the same period globally.

Traditional Security Failures

Fragmented Approaches and Tool Proliferation

Traditional cybersecurity approaches in the Eastern Mediterranean have created dangerous gaps that sophisticated adversaries exploit systematically.

Tool Proliferation Crisis:

Managing and Transforming Cybersecurity today feels like trying to juggle too many balls at once. Companies are forced to use a collection of tools, each focused on a single task, like threat detection. Organizations across the region typically deploy numerous separate security tools, creating:

- **Management Overhead:** Security teams are spending more time managing tools than responding to threats

- **Integration Gaps:** Critical security information isolated in different systems
- **Alert Fatigue:** Thousands of daily false positive alerts that mask real threats
- **Skills Requirements:** Multiple training requirements that strain limited cybersecurity personnel

Coordination Failures:

Despite facing coordinated regional threats, defensive efforts remain fragmented:

- **Information Silos:** Limited threat intelligence sharing creates blind spots that attackers exploit
- **Response Delays:** Slow coordination between organizations and agencies enables attack progression
- **Resource Duplication:** Inefficient resource allocation as organizations develop separate capabilities
- **Standards Inconsistency:** Different approaches that complicate regional business operations

Inadequate Protection for Critical Systems

Traditional enterprise security tools fail to address the unique requirements of critical infrastructure and healthcare environments prevalent throughout the region.

Operational Technology Gaps:

Legacy industrial control systems across the region cannot support traditional IT security approaches:

- **Availability Requirements:** Critical systems that cannot be taken offline for security updates
- **Real-Time Constraints:** Security controls that cannot interfere with real-time operations
- **Protocol Limitations:** Industrial protocols that traditional security tools cannot monitor effectively
- **Legacy Dependencies:** Aging systems that cannot support modern security software

Healthcare-Specific Challenges:

Regional healthcare systems face unique cybersecurity requirements:

- **Medical Device Security:** Connected medical devices that often lack adequate security controls
- **Emergency Access Requirements:** Need for rapid access to patient information during emergencies

- **Regulatory Complexity:** Multiple overlapping compliance requirements across different jurisdictions
- **24/7 Operations:** Healthcare facilities that cannot shut down systems for security maintenance

Seceon's Unified Regional Solution

Open Threat Management Platform Architecture

Seceon's aiXDR360 platform, powered by SERAai addresses the fundamental limitations of traditional security approaches by providing a unified, AI-powered security architecture specifically designed for the Eastern Mediterranean's unique challenges.

Consolidated Security Functions:

Seceon's OTM Platform (including aiSIEM™, aiXDR-Pmax™, aiSecurityCard360™, aiSIEM-Cguard™) integrates multiple security capabilities into a single, unified solution:

- **aiSIEM**: Advanced security information and event management with regional threat intelligence
- **aiXDR**: Extended detection and response optimized for multi-vector regional threats
- **aiSOAR**: Security orchestration and automated response with cross-border coordination capabilities
- **UEBA**: User and entity behavior analytics tuned for regional threat patterns
- **NDR/NBAD:** Network detection and response with specialized OT/ICS monitoring

AI-Powered Threat Detection:

Advanced artificial intelligence capabilities provide:

- **Dynamic Threat Modeling:** Continuous learning and adaptation to evolving regional threat patterns
- **Contextual Analysis**: AI models that understand regional business and threat contexts
- **False Positive Reduction:** Significant reduction in false alarms through advanced AI filtering
- **Predictive Analytics:** Early warning capabilities for emerging threats based on regional intelligence

CYBER SIEGE

Eastern Mediterranean Under Attack

GR	CY	RO	IL
Greece	Cyprus	Romania	Israel

Current Threat Level: CRITICAL



2,052
Annual cyberattacks
Israel faces daily coordinated attacks



85,000+
Election system attacks
Romania's democracy under siege



100
Healthcare facilities hit
Ransomware threatens patient lives



75%
Attack increase
Above global average

Current Problems

- 15+ separate security tools
- Fragmented defenses
- Thousands of false alarms
- Slow response times
- No coordination between countries
- Complex compliance management

vs.

Seceon Solution

- Single unified platform
- AI-powered threat detection
- 90% fewer false positives
- Automated response
- Regional threat intelligence
- Automated compliance

Transform Your Cybersecurity

15→1
Tools Consolidated

90%
Faster Detection

24/7
AI, ML & DTM Protection

Don't wait for the next attack.
Secure your organization with Seceon's unified AI, ML & DTM platform today.

Regional Customization and Specialized Capabilities

Geopolitical Threat Intelligence:

- **Regional Threat Feeds**: Specialized intelligence focusing on Eastern Mediterranean threat actors
- **Government Coordination:** Integration capabilities with national cybersecurity agencies
- **Cross-Border Intelligence:** Threat intelligence that accounts for regional interconnections
- **Real-Time Updates:** Continuous updates on emerging threats and geopolitical developments

Sector-Specific Adaptations:

- **Healthcare Protection**: Specialized capabilities for medical device security and patient data protection
- **Critical Infrastructure:** Advanced OT/ICS monitoring and protection capabilities
- **Manufacturing Security:** Supply chain risk management and intellectual property protection
- **Financial Services:** Enhanced fraud detection and regulatory compliance capabilities

Multi-National Compliance Integration

EU and National Regulatory Support:

- **NIS2 Directive Compliance:** Automated compliance management for enhanced cybersecurity requirements
- **GDPR Integration:** Comprehensive data protection compliance with automated breach notification
- **National Regulations:** Support for country-specific cybersecurity and data protection requirements
- **Sector Standards:** Industry-specific compliance for healthcare, financial services, and critical infrastructure

Automated Compliance Reporting:

- **Multi-Jurisdiction Reporting:** Automated generation of compliance reports for different authorities
- **Audit Trail Generation:** Comprehensive logging and documentation for regulatory audits
- **Policy Enforcement:** AI-powered enforcement of security policies across different frameworks
- **Risk Assessment**: Continuous assessment of compliance risks and regulatory gaps

Business Case and ROI Analysis

Platform Consolidation Benefits

Traditional Security Costs:

Regional organizations face significant challenges with fragmented security approaches:

- **Multiple Tool Licensing:** Substantial annual costs for numerous separate security tools
- **Management Overhead:** Majority of security staff time spent on tool management rather than threat response
- **Integration Complexity:** Custom integration projects to connect disparate security systems
- **Training Requirements:** Multiple training programs for different security tools and interfaces

Seceon Platform Advantages:

Seceon offers Zero Trust architecture, real-time threat intelligence, and comprehensive cybersecurity services for CISOs, Security Architects, SOC Managers, and IT Leaders:

- **Unified Platform:** Single platform replacing multiple security tools and reducing complexity
- **Operational Efficiency:** Significant reduction in security management overhead
- **Enhanced Detection**: AI-driven threat detection with improved accuracy and speed
- **Streamlined Compliance:** Automated compliance management across multiple regulatory frameworks

Competitive Advantages

Regional Market Leadership:

Seceon's comprehensive approach provides significant advantages in the Eastern Mediterranean market:

- **Threat Intelligence:** Deep understanding of regional threat landscape and attack patterns
- **Technology Innovation:** Advanced AI and machine learning capabilities for enhanced threat detection
- **Platform Maturity**: Proven platform with established track record across diverse environments

- **Scalability**: Architecture that scales from small businesses to large enterprises and government agencies

Technology Differentiation:

- **AI Integration:** Advanced artificial intelligence capabilities integrated throughout the platform
- **Platform Consolidation:** Unique ability to consolidate multiple security functions without performance degradation
- **Customization**: Flexible platform that adapts to specific sector and organizational requirements
- **Real-Time Response:** Advanced automation and orchestration capabilities for rapid threat response

Implementation Success Metrics

Security Effectiveness Metrics:

- **Threat Detection:** Enhanced detection capabilities for regional threat patterns
- **Response Time:** Faster mean time to detection and response for security incidents
- **False Positive Reduction:** Significant reduction in false alarms that waste security team resources
- **Compliance Status:** Improved compliance with applicable regulatory requirements

Business Impact Metrics:

- **Operational Efficiency:** Reduction in security management time and complexity
- **Cost Optimization:** Lower total cost of security ownership through platform consolidation
- **Business Continuity:** Improved uptime for critical business systems during security operations
- **Risk Reduction**: Measurable reduction in successful security incidents and their business impact

Implementation Strategy

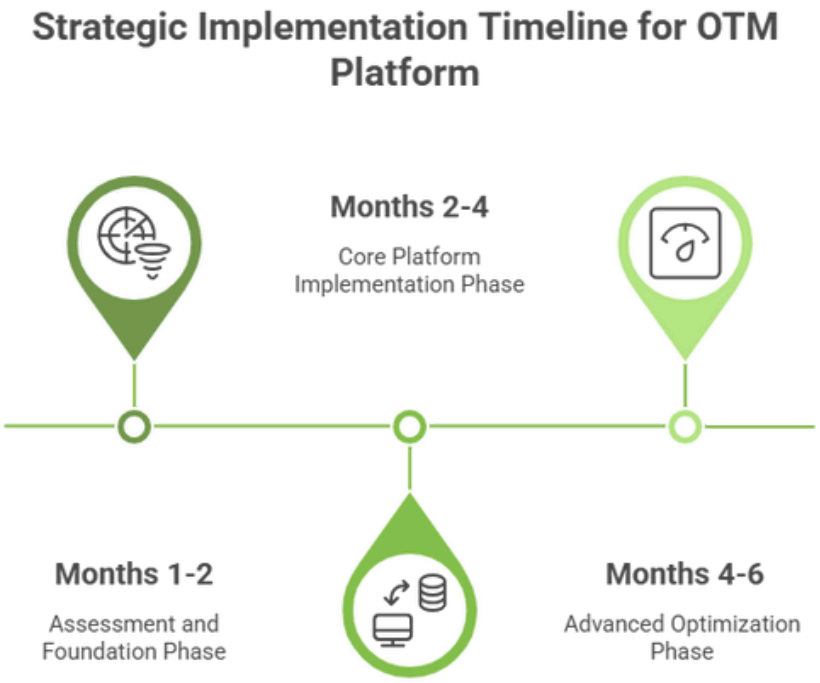
Phased Regional Deployment

Phase 1: Assessment and Foundation (Months 1-2)

- **Regional Threat Assessment:** Comprehensive analysis of specific threats facing the organization's operations
- **Current State Analysis:** Evaluation of existing security tools and their effectiveness
- **Compliance Gap Analysis:** Assessment of regulatory compliance status across applicable jurisdictions
- **Stakeholder Alignment:** Coordination with operational teams and management

Phase 2: Core Platform Implementation (Months 2-4)

- **Platform Deployment:** Installation and configuration of core OTM platform capabilities
- **Data Integration:** Connection and normalization of existing security data sources
- **AI Model Configuration:** Customization of AI models for organization-specific requirements
- **Team Training:** Comprehensive training on platform capabilities and regional threat landscape



Phase 3: Advanced Optimization (Months 4-6)

- **Automation Enhancement:** Implementation of advanced automated response capabilities
- **Threat Intelligence Integration:** Integration with regional threat intelligence sources
- **Continuous Optimization:** Ongoing tuning based on operational experience and threat evolution
- **Performance Validation:** Comprehensive testing and validation of all security capabilities

Change Management for Multi-National Operations

Organizational Alignment:

- **Executive Sponsorship:** Clear executive support and involvement throughout implementation
- **Cross-Functional Teams:** Integration of security, operations, compliance, and business teams
- **Communication Strategy:** Regular communication about implementation progress and benefits
- **Success Recognition:** Recognition and celebration of implementation milestones and achievements

Technical Implementation:

- **Phased Deployment:** Gradual implementation to minimize operational disruption
- **Backup Procedures:** Comprehensive backup and rollback procedures to ensure business continuity
- **Testing Protocols:** Thorough testing of all capabilities before production deployment
- **Documentation**: Complete documentation of configurations, procedures, and best practices

Conclusion: Regional Cybersecurity Resilience

The Eastern Mediterranean region faces cybersecurity challenges that traditional approaches cannot adequately address. The evidence demonstrates coordinated, sophisticated threats that require unified, comprehensive responses.

The Scale of Regional Threats:

The statistics demonstrate the urgency of the situation:

- Israel facing 1,550 documented cyberattacks in a single year
- Romania experiencing over 85,000 coordinated attacks on electoral systems
- Healthcare systems across the region under sustained ransomware assault affecting over 100 facilities
- Critical infrastructure facing coordinated attacks with international coordination

Traditional Security Approaches Have Failed:

Companies are forced to use a collection of tools, each focused on a single task, creating dangerous gaps that sophisticated adversaries exploit systematically. Seceon's comprehensive platform includes more than 15 tools consolidated into a unified solution that addresses these fundamental challenges.

Seceon's Regional Solution:

Seceon's aiXDR360 platform, powered by SERAai and the comprehensive OTM platform provides the unified, AI-powered security architecture that the Eastern Mediterranean requires:

Proven Platform Benefits:

- Consolidated security functions replacing multiple fragmented tools
- AI-driven threat detection with enhanced accuracy and reduced false positives
- Automated compliance for complex multi-jurisdictional regulatory requirements
- Specialized capabilities for healthcare, critical infrastructure, and manufacturing

Regional Advantages:

- Deep understanding of Eastern Mediterranean threat landscape and geopolitical factors
- Advanced threat intelligence capabilities tailored to regional attack patterns
- Proven platform scalability across diverse organizational requirements
- Comprehensive support for critical sector security requirements

The Strategic Imperative:

Organizations across Greece, Cyprus, Romania, and Israel cannot afford to maintain fragmented security approaches in the face of coordinated, sophisticated regional threats. Seceon offers Zero Trust architecture, real-time threat intelligence, and comprehensive cybersecurity services for CISOs, Security Architects, SOC Managers, and IT Leaders.

Next Steps:

Contact Seceon today to begin your organization's transformation from vulnerable, fragmented security to unified, AI-powered cybersecurity resilience. The Eastern Mediterranean's strategic importance and threat environment demand immediate action to protect critical business operations and national infrastructure.

Regional Competitive Advantage:

Organizations that implement comprehensive cybersecurity platforms gain significant advantages:

- **Enhanced Security Posture**: Advanced protection against sophisticated regional threats
- **Operational Efficiency:** Streamlined security operations through platform consolidation
- **Regulatory Compliance:** Automated compliance management across multiple jurisdictions
- **Business Resilience:** Improved ability to maintain operations during cyber attacks

The future of Eastern Mediterranean business depends on cybersecurity decisions made today. Seceon provides the proven platform and expertise to transform cybersecurity from a source of risk and complexity into a strategic business enabler.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 680 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

About the Author

Shikha Pandey

Principal, Product Strategy & Partnerships, Seceon Inc.



Shikha has led product strategy, partnerships, and technical programs at Seceon and Meta. At Meta, she drove a core infrastructure program powering Facebook, WhatsApp, and Instagram, enabling teams to boost productivity with automation, advanced tooling, and GenAI. Now at Seceon, she leads product strategy, marketing, and partnerships—building brand presence, scaling channel growth, and driving data-driven campaigns to strengthen market impact.

© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.