

Cybersecurity

Managed Detection & Response (MDR)

THE CHALLENGE

Presidio's Managed Detection and Response (MDR) solution brings traditional detection and response up to the level of modern threats. Organizations are increasingly concerned about their advanced threat management. A proliferation of security applications, alarms and alerts can overwhelm a security team, delaying an effective response and putting their business at risk.

THE SOLUTION

Presidio MDR introduces a new approach to threat mitigation efficiency. It integrates with traditional security point-products and consolidates decisions through an intuitive platform. Presidio MDR with Active Response integrates seamlessly to automatically initiate protective action in seconds, not minutes or hours.

Visibility and Control

Presidio MDR goes beyond just opening tickets for a client's cyber team to investigate and resolve. The intuitive dashboard gives clients control over responses to threats including options to:

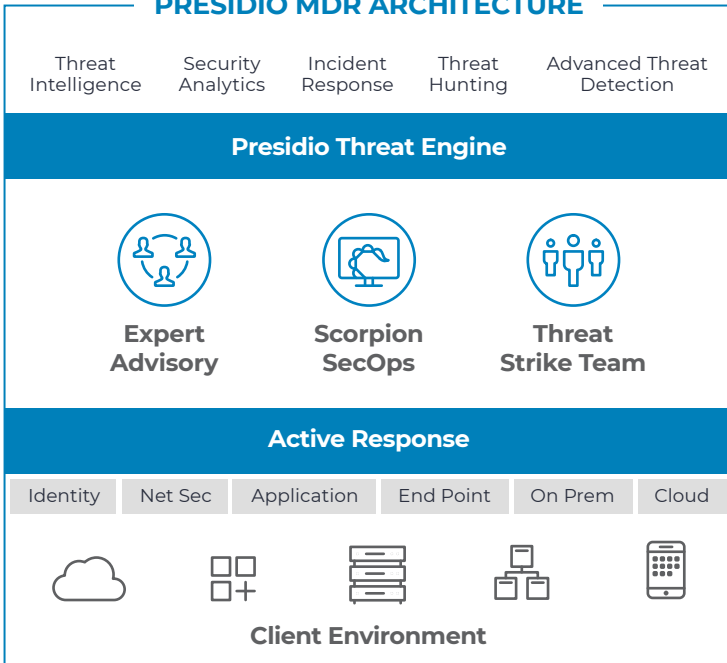
- ◆ Disable accounts
- ◆ Remove phishing emails
- ◆ Add/remove indicators from whitelist or blacklists

The Presidio MDR approach aligns with multiple security frameworks to ensure the right coverage for end-to-end threat mitigation across the entire infrastructure. It constantly learns to protect against the ever-evolving threat landscape. It offers actionable security insights and has a real-time dashboard to consolidate and simplify a remediation plan including Active Response to automatically protect a business.

KEY BENEFITS

Presidio enables our clients to defend their evolving vulnerabilities. Organizations face greater risk exposure due to the adoption of cloud, IoT and mobility, along with an increase of cyber-attacks.

PRESIDIO MDR ARCHITECTURE



Enhanced Visibility
Consolidates threat intelligence across multiple systems for the latest protections.

Reduced Mean Time to Detect / Mean Time to Respond
Reduces initial responses from hours to seconds, not just with notifications but with active responses to immediate cyber threats.

Security Framework Alignment
Aligns with multiple security frameworks to ensure the right coverage, and constantly evolving for today's threat landscape – operating non-stop 24 x 7 x 365.

Managed Detection & Response (MDR)

Presidio MDR Mitigates Key Challenges in Cybersecurity:

- ◆ **Lack of Skilled Personnel** – retaining skilled cyber resources that are hard to find. Keeping current with the latest risks and certified on multi-vendor technology innovations.
- ◆ **24 x 7 x 365 Coverage** – managing services, monitored and operated every minute of every day to support the highest levels of security and to respond to incidents in seconds.
- ◆ **Alert Prioritization** – ending alert spam with our proprietary Presidio Threat Framework that specifically targets the latest threats, reducing incidents and breaches.

What Makes Us Different

Presidio is a trusted partner to our clients, securing their infrastructure, employees, customers and assets from ever-growing cyber threats. Our clients trust Presidio:

- ◆ **End-to-End Protection** – Presidio MDR is a powerful platform, integrating with the broad spectrum of cyber products to support the entirety of the cyber infrastructure, from the border, through the network, down to every endpoint.
- ◆ **Cyber Intelligence** – Presidio's cyber intelligence data is comprised of knowledge from thousands of data sources, dozens of cyber products, transactions, and events supporting rapid detection and response in a managed services deployment. In addition to our own accumulated intelligence, we have intelligence sources familiar with Classified (government) and Dark Web threats.
- ◆ **Speed and Accuracy** – Presidio's deep knowledge of every layer of the It and cyber architecture, combined with proven methodologies supports responding in record time to potential threats. Response can be deployed in seconds instead of hours or days.

WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready. Our clients benefit from:

- ◆ Services methodology built on recognized industry standards including NIST, CIS, and ISO
- ◆ Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- ◆ Multi-discipline experts provide for a broad view of client's potential vulnerabilities
- ◆ Deep security services bench and broad security services solutions provide domain expertise and consistent deliverables

INFORMATION SECURITY

- CISA Certified Information Systems Auditor
- CISM Certified Information Security Manager
- CRISC Certified in Risk and Information Systems Control
- CGEIT Certified in the Governance of Enterprise IT
- CISPP Certified Information Security Professional
- CISSP Certified Information Security Specialist
- CCSP Certified Cloud Security Professional
- ISSMP Information Security Service Management Professional
- ISO 27001 Information Security Management System Certified
- PCI Security Standard Council Qualified Security Assessor
- G2700 Global 2700 Security
- SABSA SABSA

INFRASTRUCTURE SECURITY

- CISCO PARTNER Master Security Specialized
- CCDE CISCO CERTIFIED DESIGN
- CCIE CISCO CERTIFIED ROUTING AND SWITCHING
- CCIE CISCO CERTIFIED SECURITY
- CCNP CISCO CERTIFIED NETWORK SECURITY
- paloalto Palo Alto Networks
- f5 F5
- CITRIX Citrix
- vmware VMware
- NDA Certified Network Defense Architect
- RSA SECURITY RSA
- vmware CERTIFIED IMPLEMENTATION EXPERT NETWORKS VIRTUALIZATION
- paloalto PCNSE Palo Alto Networks
- aws certified Security Specialty
- GCED Global Cyber Intelligence Center of Excellence
- GCWN Global Cyber Warfare Network
- MCSE Microsoft Certified Professional
- MCSE Microsoft Certified Professional
- MCSE Microsoft Certified Professional

TECHNICAL ASSESSMENT

- GPEN Global Penetration Tester
- GXPIN Global XPIN
- GWAPT Global Web Application Penetration Tester
- GAWN Global Advanced Web Network
- GREM Global Red Team
- GCTI Global Cyber Threat Intelligence
- OSCP Offensive Security Certified Professional
- CEH Certified Ethical Hacker
- CompTIA CASP+ Certified Advanced Security Practitioner
- CISA Cyber-Infrastructure

Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. Getting started with Presidio is easy. Let's explore how we can secure your business.

Visit us online today or call us at 800.235.6259