DATASHEET

Managed Extended Detection and Response (MXDR) Services

Detect, investigate, and respond to advanced threats in your ICT environment

myCloudDoor Managed Extended Detection and Response (MXDR), powered by Microsoft Defender and Microsoft Sentinel, is a managed service provided by myCloudDoor SOC MYCD-CERT specialists, who monitor, detect, and respond to cyberattacks targeting your organization.

Introduction

Cyber threats are constantly evolving, with attacks becoming more automated, targeted, and difficult to detect. Ransomware, data breaches, and insider threats put business continuity at risk, while the expansion of hybrid and multi-cloud environments increases the attack surface.

Many organizations face a lack of visibility and resources to detect and respond to incidents in real-time. The shortage of cybersecurity talent, the complexity of managing multiple tools, and the need for continuous monitoring mean that reactive protection is no longer enough.

To mitigate these risks, enterprises need advanced detection and response capabilities, operating 24x7 and backed by threat intelligence and automation.

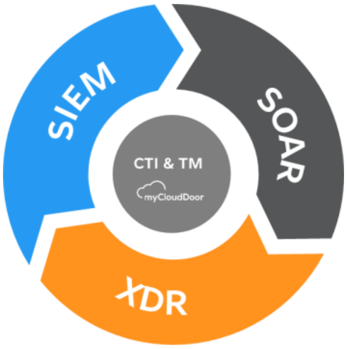
myCloudDoor MXDR 24x7: Continuous Protection Against Advanced Threats

To address today's challenges in cybersecurity, myCloudDoor MXDR 24x7 provides a managed extended detection and response (MXDR) service based on Microsoft technologies. Through a team of cybersecurity experts, we continuously monitor, analyze, and respond to advanced threats, ensuring effective protection against targeted attacks, ransomware, security breaches, and other emerging risks.

Our service combines the power of Microsoft Defender and Microsoft Sentinel with advanced threat intelligence, forensics, and response automation. Thanks to a complete integration with security data sources, we correlate events in real time to identify and neutralize incidents before they impact the organization. With a proactive and managed 24x7 approach, we help companies reduce risk, improve their resilience to cyberattacks, and optimize their security posture without the need to manage an internal SOC.

Key Benefits

- Stop ransomware and other advanced attacks with a 24/7 team of threat response experts.
- Have a managed ecosystem of Microsoft security technologies that is integrated and protects your development investment.
- Have a complete view of the attacker's end-to-end activity, knowing that all assets are accounted for and monitored.
- Achieve measurable reduction in cybersecurity risks by relying on contractual SLAs of 15-minute notification for critical alerts and 60-minute or less mean time to resolution.
- Achieve continuous alignment with high levels of security compliance.
- Maximize ROI in cybersecurity by improving the detection efficiency of threats mapped to the MITRE ATT&CK® framework.



Key features

myCloudDoor MXDR 24x7 offers different service levels and response options tailored to the needs of each organization. Our team of cybersecurity experts can handle complete incident response, work closely with your team to manage threats, or simply alert your internal teams as soon as suspicious activity is detected.

With our advanced threat detection, automation, and analysis capabilities, we quickly identify the source, scope, and methodology of an attack. Our agile response capability allows us to contain and mitigate threats in a matter of minutes, minimizing the impact on your business and ensuring continuous protection.

1 24x7 Detection and Response

- Continuous monitoring of cybersecurity events and threats in real-time.
- Advanced threat correlation using Microsoft Sentinel and Defender.
- Real-time human and automated response to contain incidents.

2 No Vendor Lock-In

- Ownership of your data and settings.
- Retention of valuable historical data, configurations, and artifacts.
- Customization of playbooks, reports, dashboards, and automation assets.

3 Security optimization

- Ongoing review and adjustment of Microsoft security platforms.
- Continuous evolution and tuning of detection and response rules in Defender.
- Deployment and evolution of the Microsoft Sentinel SIEM/SOAR platform.

4 Critical Incident Response

- Immediate 24x7 response and support to critical cybersecurity incidents.
- Coordination of the crisis and support for reporting to management by specialists.
- Input vector analysis, persistence, forensics, and recovery support.

5 Quality of Service Plan

- Assignment of a dedicated Service Manager and Technical Manager.
- Reports and committees for monitoring and continuous improvement of the service.
- Dashboards with the most relevant service indicators and SLAs.

6 Threat Hunting and Cyber Intelligence

- Automated Threat Hunting missions to uncover hidden threats.
- Integration with cyber intelligence feeds (TIP) to improve detection.
- Analysis of attack patterns and continuous threat modeling.

7 Expert Cybersecurity Support

- Direct access to cybersecurity experts via phone, email or Teams in 24x7 around myCloudDoor's international SOCs.
- Close collaboration to understand your environment and advise you on its safety.

8 Efficiency and Productivity

- It improves cyber resilience, security posture, and return on investment, while reducing threat response time and organizational effort.
- Predictability of costs and reduction of TCO by up to 30%.

Integrations Included

Naturally, directly, and at no additional cost, security data from the following Microsoft sources can be integrated so that the myCloudDoor MXDR cybersecurity team can use it for service delivery. Microsoft feeds, naturally integrated on top of the Defender XDR platform, emit telemetry, used to increase visibility into your entire ICT environment, generate advanced threat detections, and deploy automated response capabilities.

Defender for Endpoint

Detect malicious behavior and respond to advanced threats across all endpoints (endpoints, servers, and mobile).

Defender for Office 365

Protect the collaboration environment from phishing attacks and advanced threats on email, Teams, Sharepoint, and OneDrive.

Defender for Cloud Apps

Detect and protect access to unauthorized SaaS platforms, data exfiltration, and detect Shadow IT on the organization.

Defender for Cloud

Detect threats and protect cloud payloads and services from attacks and assess cybersecurity posture on an ongoing basis.

Defender for Identity

Detect, investigate, and respond to advanced threats in Entra Id and AD, identifying, identity attacks or unauthorized access.

Entra Id

Identity and access management platform that provides secure authentication, access control, SSO, and threat protection.

Intune

Unified device management to manage and protect PCs, mobiles through security policies and access control.

Defender EASM

Identify and monitor the organization's external attack surface, detecting exposed assets, vulnerabilities, and risks.

Purview

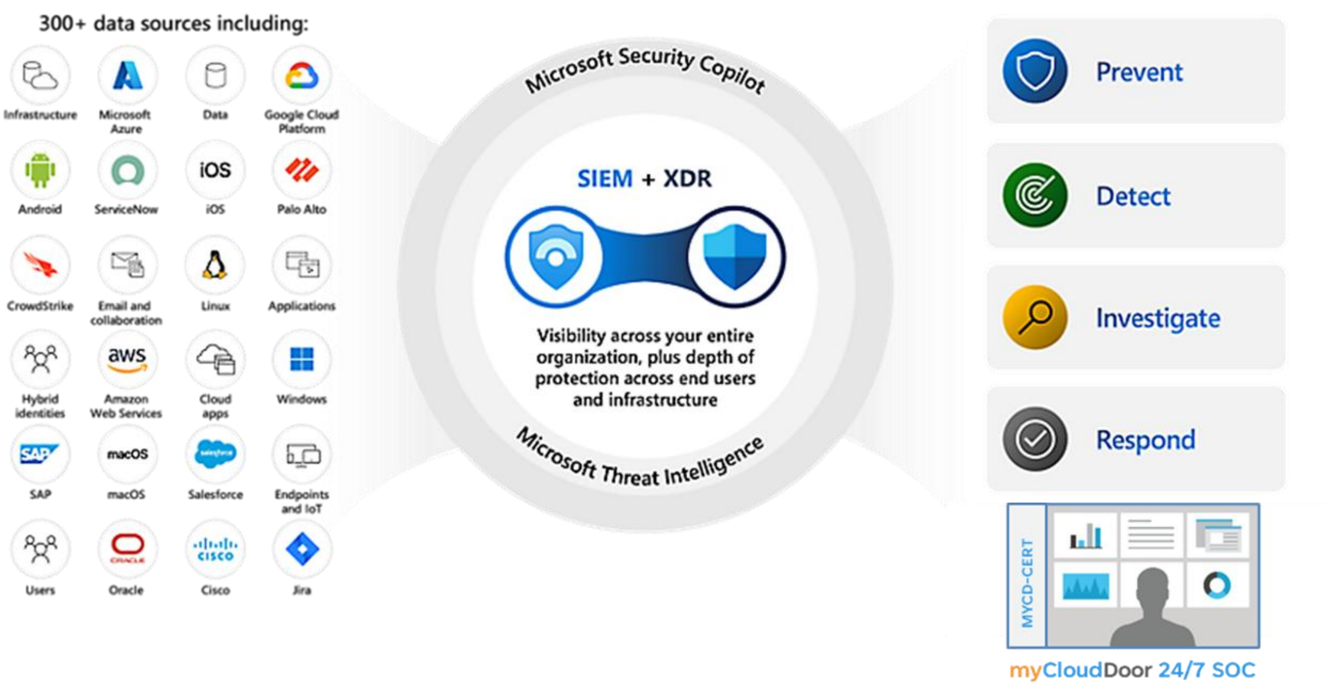
Data protection and compliance that allows sensitive information to be classified, audited and protected, guaranteeing privacy and security.

SIEM

Sentinel Centralize and automate security operations with 90 days of retention included.

Complementary Integrations

Security telemetry and alerts from various third-party sources can be integrated into myCloudDoor MXDR by purchasing additional integration modules. These telemetry feeds expand visibility into your environment, improve the accuracy of threat detections, and help identify new threats. In addition, they facilitate proactive threat hunting and enable additional incident response capabilities.



FIREWALL AND NETWORK

- Fortinet
- Palo Alto
- Cisco Firepower
- Barracuda
- F5
- Sophos
- WatchGuard
- Darktrace
- ExtraHop
- Zscaler
- Cisco Umbrella
- ...

MAIL AND CLOUD

- Proofpoint
- Fortinet
- Barracuda
- Cloudflare
- Trend Micro
- Forcepoint
- Mimecast
- Checkpoint
- Amazon AWS
- Google Cloud
- Google Workspace

...

OTHER SOURCES

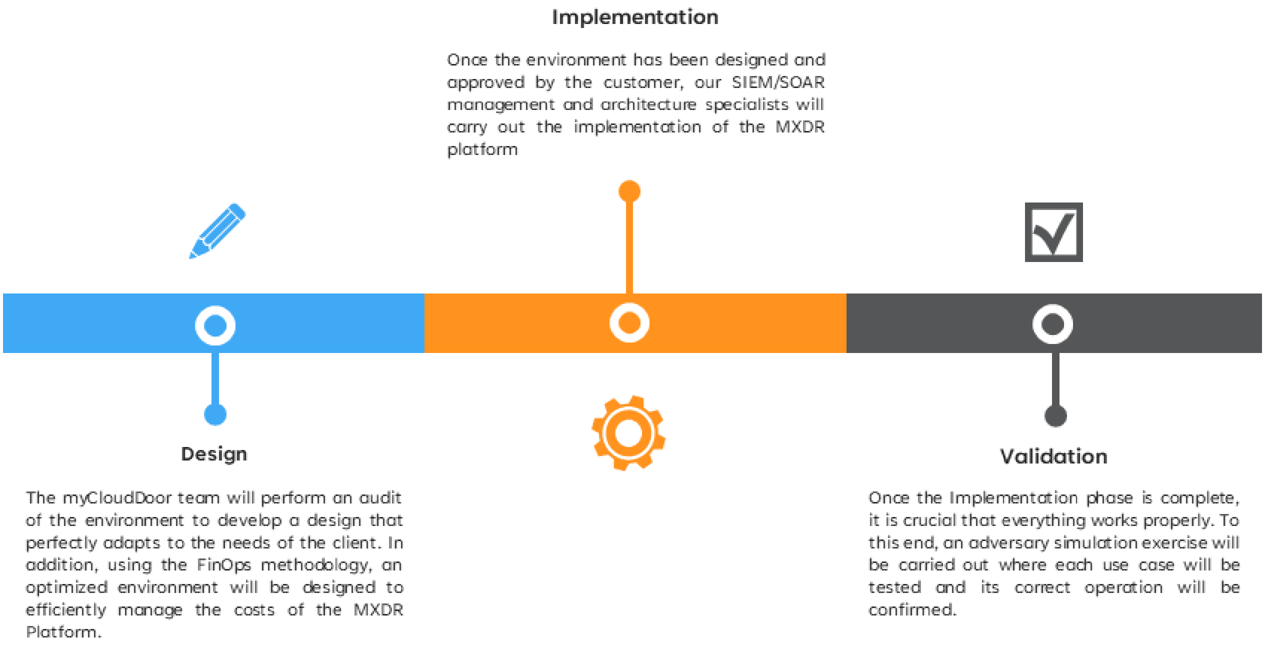
- VMWare
- Oracle
- Armis
- Cisco DUO
- Okta
- Claroty
- Commvault
- CCN RNS Gold
- CyberArk
- Dynamics
- SAP
- ...

Service Levels

	MXDR Standard	MXDR Advanced
Review, tuning, and manage Microsoft Defender for Endpoint and Microsoft Defender for Office 365 security	✓	✓
Deploy and configure Microsoft Sentinel as customer-owned SIEM/SOAR	✓	✓
24x7 cybersecurity threat monitoring, investigation, and response	✓	✓
Direct phone support with experts during incidents	✓	✓
Deployment of a personalized Dashboard with the relevant service indicators	✓	✓
Regular Automated Threat Hunting Missions	✓	✓
Integrated Additional Cyber Intelligence Feed (IoC/IoA)	Standard	Advanced
Integration of third-party information sources into Sentinel (firewall, NDR, ZTNA, CASB, Cloud, etc.)	Complement	Complement
Deploying and Evolving SIEM Detection Use Case Catalog with Threat Modeling	Standard	Custom
Deployment and evolution of the catalog of notification, enrichment, containment, and response automations on SOAR	Standard	Custom
Service Manager and Technical Manager assigned to the service	✓	✓
Sending periodic reports with data on the service (trends, SLA compliance, etc.) and continuous improvement	Bimonthly	Monthly
Periodic monitoring committee for service monitoring, research and continuous improvement	Bimonthly	Monthly
24x7 digital surveillance and exhibition area management service	Complement	Complement
Ongoing vulnerability management and risk mitigation support powered by Microsoft Defender	Complement	✓
Critical Incident Response Service (DFIR) with dedicated N3 team until incident eradication, crisis cabinet, entry vector analysis, forensic analysis and cyber incident coordinator. Reusable in other services if not consumed.	40 hours/year	80 hours/year
Technical cybersecurity office for recurring activities, security analysis or bastioning	Complement	Complement

Agile service deployment

Thanks to our expertise and methodology, we are able to deploy the myCloudDoor MXDR Standard service in just two weeks*, ensuring fast and effective integration of information sources, deployment of use cases, and the construction of initial automations.



Implementation

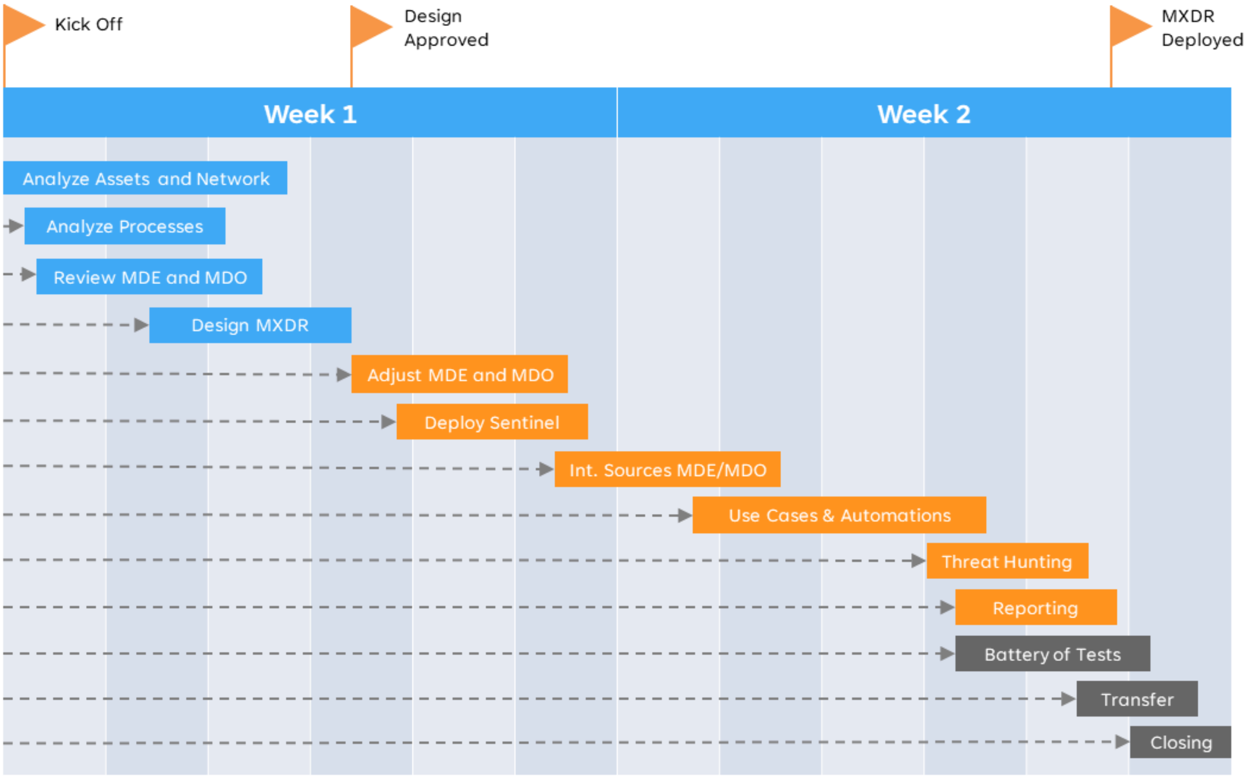
Once the environment has been designed and approved by the customer, our SIEM/SOAR management and architecture specialists will carry out the implementation of the MXDR platform

Design

The myCloudDoor team will perform an audit of the environment to develop a design that perfectly adapts to the needs of the client. In addition, using the FinOps methodology, an optimized environment will be designed to efficiently manage the costs of the MXDR Platform.

Validation

Once the Implementation phase is complete, it is crucial that everything works properly. To this end, an adversary simulation exercise will be carried out where each use case will be tested and its correct operation will be confirmed.



Kick Off

Design Approved

MXDR Deployed

Week 1

Week 2

Analyze Assets and Network

Analyze Processes

Review MDE and MDO

Design MXDR

Adjust MDE and MDO

Deploy Sentinel

Int. Sources MDE/MDO

Use Cases & Automations

Threat Hunting

Reporting

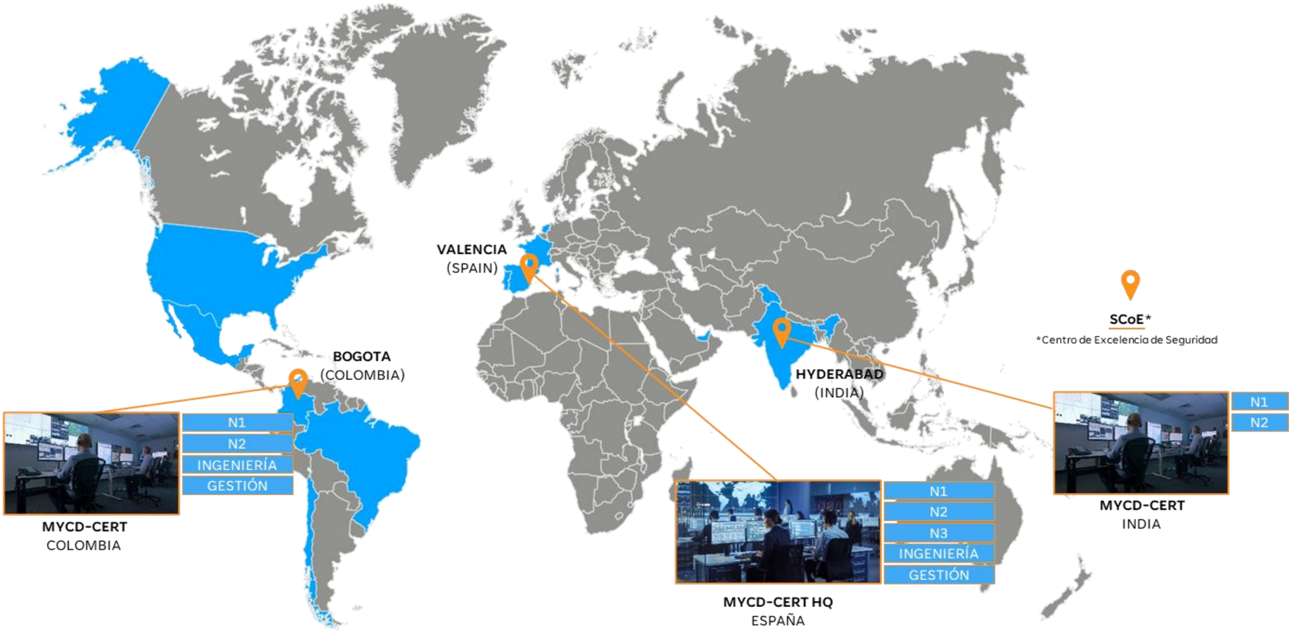
Battery of Tests

Transfer

Closing

**Microsoft Defender for Endpoint P1/P2 and Defender for Office 365 P1/P2 must already be deployed and working on the client.*

Discover our MXDR service in detail



Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Gold Microsoft Partner | Azure Expert MSP
Managed Service Provider
This award recognizes the competences of myCloudDoor in helping its clients during their Cloud Journey: planning, designing, operating and optimizing solutions on Azure.

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Categoría ALTA RD 3/2010

AENOR GESTIÓN SERVICIOS TI ISO/IEC 20000-1

FIRST Improving Security Together

AENOR SEGURIDAD INFORMACIÓN ISO/IEC 27001

AENOR GESTIÓN CONTINUIDAD NEGOCIO ISO 22301

Red Nacional de SOC

Learn why Microsoft is a leader in cybersecurity solutions

- ✓ **Microsoft Defender XDR demonstrates 100% detection coverage across all cyberattack stages in the 2024 MITRE ATT&CK® Evaluations: Enterprise**
- ✓ **Microsoft is named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms**
- ✓ **Microsoft is again named a Leader in the 2024 Gartner® Magic Quadrant™ for Security Information and Event Management**

Visit us at

https://myclouddoor.com

Telephone: (+34) 678 08 26 44
Email: info@myclouddoor.com