# EY Managed Extended Detection and Response (MXDR) for IT, OT and Cloud

**Helping improve your cyber resiliency**

Building a better working world

## Business drivers

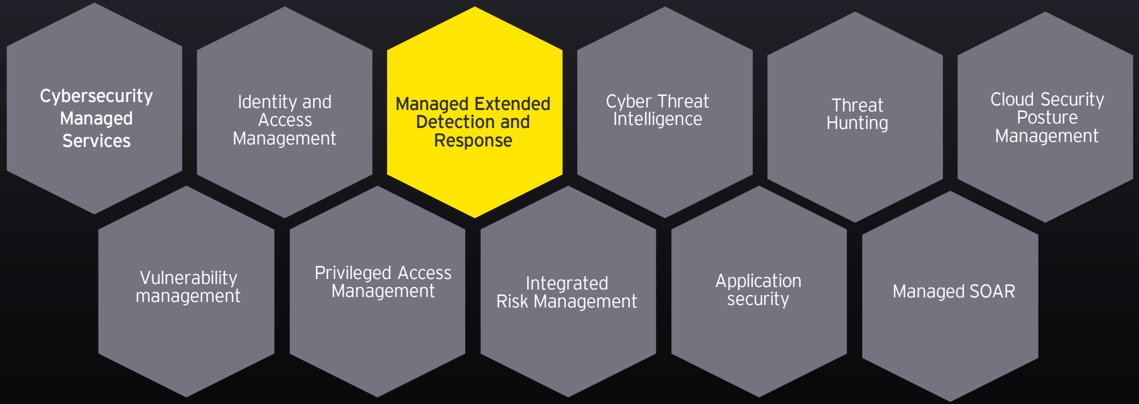
- More and more businesses are pressed to demonstrate appropriate due care to contain major cyber-attacks and protect your company's assets, reputation, and finances.
- The most overlooked indirect cybersecurity cost is directly related to crisis management in the event of an unexpected disruption and high incident remediation expenses.
- There is a growing need to increase visibility and gain insight and critical context into all industrial control systems (ICS) and operational technology (OT).
- The aftermath of the COVID-19 pandemic has triggered a chronic labor shortage across most developed countries, particularly in the cloud security space and has greatly impacted cybersecurity circles.
- Cyber insurers are increasing expectations in demonstrating attack detection and response capability. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.
- With threat actors increasingly looking to identify and exploit weaknesses in core security technologies, chief information security officers (CISOs) are under pressure to optimize current technology investments.

## Solution overview

- The EY MXDR offering for IT, OT and cloud can be deployed to focus on IT environments, OT environments, including hybrid environments. For clients with an existing, mature cybersecurity monitoring capability, a stand-alone IT or OT-focused MXDR solution may be preferred.
- Where feasible, an integrated, end-to-end EY MXDR capability provides economy of scale in 24x7x365 detect, disrupt, respond and escalate capabilities.
- EY MXDR focus areas are:
  - 24x7x365 monitoring for suspicious and malicious activity wherever your digital assets reside
  - Triaging alerts reporting suspicious activity to determine if is a cyber incident that needs to be contained and remediated
  - Communicating potential or actual incident to resources to take appropriate action
  - Managing and helping optimize enabling technologies to identify attack activity in your environment
  - Reporting on performance MXDR function effectiveness, which includes EY monitoring and triage of client custom rules or alerts
  - The EY MXDR offering for IT, OT and cloud is part of the EY Cybersecurity Managed Services (CMS) portfolio.
  - EY CMS accelerates and sustains transformative, leading practice cybersecurity operations to improve your cyber resiliency, reduce your digital risks and protect your business.

## Solution benefits

- Gain access to the named, assigned "core team" provides you subject matter resources who know your organization.
- Avail tailored reporting and actionable tickets that provide insights to help inform your cyber defense investments.
- Respond to threats via EY Security Orchestration, Automation and Response (SOAR) platform with playbooks tailored to your processes.
- Improve threat visibility and detection logic across the MITRE Adversarial Tactics, Techniques and Common Knowledge (MITRE ATT&CK®) life cycle.
- Identify malware and interactive attacker patterns and techniques using detection logic from the EY Attack Intelligence Lab (AIL).
- Gain access to US$1.5m investment in multiple commercial cyber threat intelligence feeds and work with an assigned intel analyst.
- Get transparent service and processes with client access to EY provided, commercial enabling technology.
- Extensive organizational integration leveraging your ticketing system and custom attack disruption actions.



Cybersecurity Managed Services
Identity and Access Management
Managed Extended Detection and Response
Cyber Threat Intelligence
Threat Hunting
Cloud Security Posture Management
Vulnerability management
Privileged Access Management
Integrated Risk Management
Application security
Managed SOAR

## Joint value proposition

- Recognized worldwide by analysts as leaders in market share in both information security consulting and managed services
- Delivered by a trusted advisor, combining global reach with local knowledge, and regulatory rigor with the latest technology
- Flexible, scalable and transparent services with a risk-based approach to security delivery
- Extensive global delivery capability using global service centers all supported by leading-class technology
- Business transformation supported by technology through robotic process automation (RPA), artificial intelligence (AI) or machine learning (ML) and alliance ecosystems
- End-to-end services and solution scope that is fit for purpose
- Viewed as a bridge between business and the security organization

## Solution differentiators

### Threat detection

- EY threat detection logic
- 24x7x365 threat monitoring
- Threat identification and alert triage
- Incident validation analysis
- Threat notification and escalation

### Threat hunting

- Analyst-driven (daily to weekly)
- Structured analysis or threat intelligence-driven (daily to weekly)
- Tactic-and-technique driven
- Scenario-based (monthly to quarterly)
- Scenario-based with Red Team or pen testing (quarterly)

### Threat response

- Incident scope and severity determination
- Containment, eradication and recovery recommendations
- Attack disruption of pre-approved activities
- Automated attack containment via the EY SOAR platform

### Incident response

- Investigation management and coordination
- Malware analysis
- Eradication event planning and execution assistance
- Computer forensics
- Executive communications

## Case study

The client is a financial holding company, and the main operating segments are personal banking and lending, business banking and lending, and wealth management. The client engaged EY teams to provide managed security operations support to help identify, analyze and triage alerts reported by EY threat detection tools. The client had Microsoft E5 licenses and engaged EY teams to assist with activating security components migrating from another security technology.

### Client challenge

- The client's incident response team was understaffed and underbudgeted and consisted of personnel who were not fully dedicated to cybersecurity tasks.
- The client wanted to partner with a vendor that could provide managed extended detection and response in addition to a cyber threat intelligence (CTI) program that could provide a holistic program designed to inform information security risk mitigation at multiple levels.
- The client also needed assistance on their M365 E5 journey.

### Engagement summary

- EY teams are currently providing managed security operations support, which includes:
- Identifying, analyzing and triaging alerts reported by EY threat detection tools
- Performing specialist review of specific events by offshore global SOC team and US EY resources
- Providing incident investigation, malware analysis and advising the client on remediation actions
- Providing reports on threat indicators as discovered by the EY Cyber Threat Intelligence team and third-party providers
- Continuing to support client with tactical and strategic intelligence support, including event assistance and technical analysis, incident bridge support, advice and handoff for IR retainer activation, and formal RFI (requests for intelligence) responses
- Building and providing monthly briefings on significant cyber threat and risk trends to the CISO

### Value delivered

- Provided assistance in managed extended detection & response, 24x7 security operations, including EY CTI report on assessing future threats
- Supported ongoing protection of on-prem and Azure Cloud infrastructure with a broad security operations center (SOC) program
- Operationalized the Azure Cloud security monitoring program
- Helped prioritize, integrate and enhance Microsoft technology
- Helped operationalize ASR rules, Defender for O365 and Endpoint
- Enhanced Purview Insider Risk Management
- Facilitated activation of Microsoft technology that is out of scope

## Contacts

### EY

**John J Senn**
Executive Director
Technology Consulting
Ernst & Young LLP United States
john.senn@ey.com

### Microsoft

**Jodi Lustgarten**
Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.com

### EY and Microsoft: Work Better. Achieve More.

Every day, throughout the world, businesses, governments and capital markets rely on EY business ingenuity and the power of Microsoft technology to solve the most challenging global issues.

EY and Microsoft bring a compelling formula to spark the potential of the cloud and unlock the power of data. We solve our clients' most challenging issues by blending trusted industry expertise with innovative cloud technology.

Our strategic relationship draws on decades of success in developing visionary solutions that provide lasting value.

Together, we empower organizations to create exceptional experiences that help the world work better and achieve more.

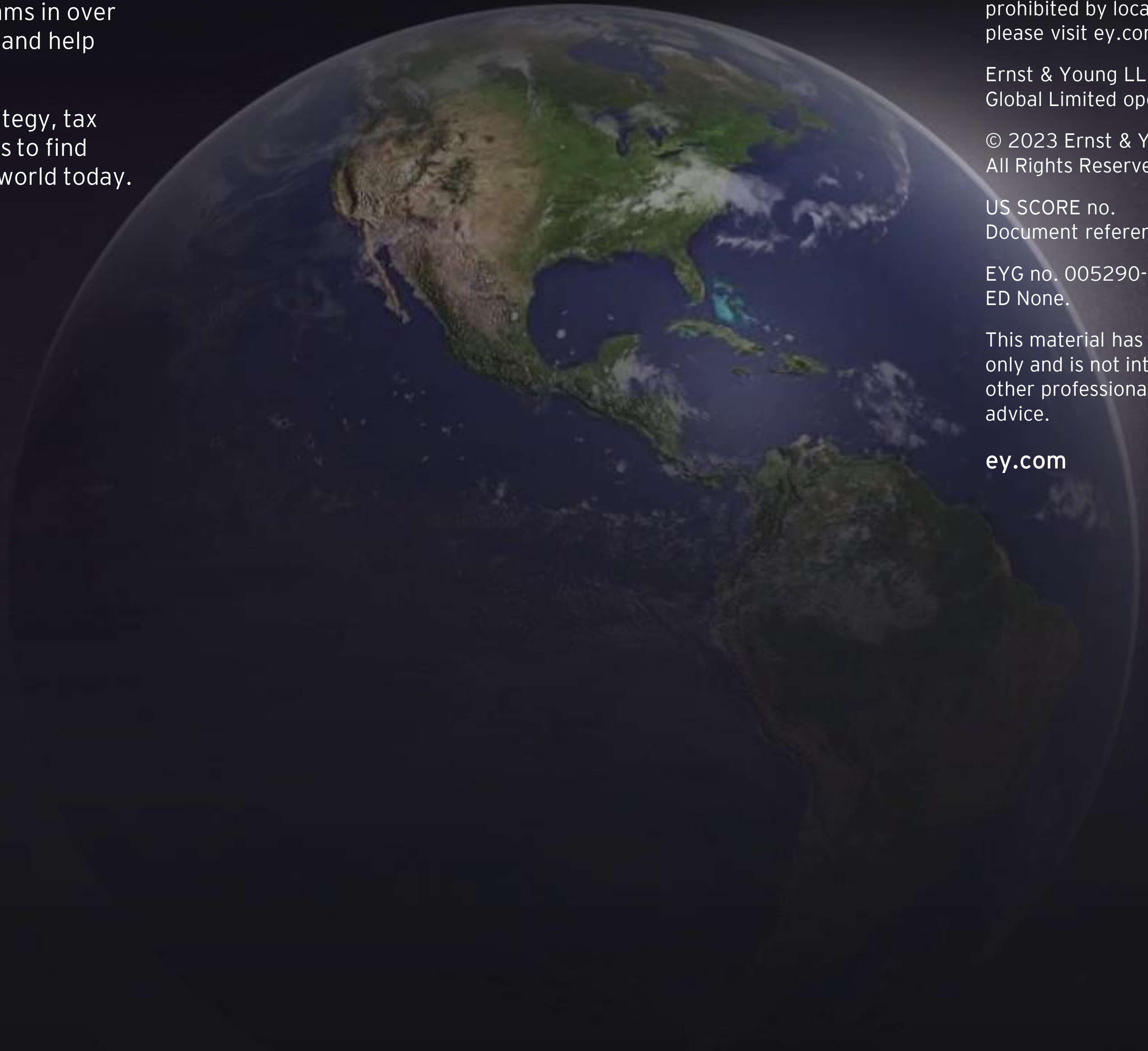
For more information, visit: ey.com/Microsoft.

## EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society, and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



US SCORE no.
Document reference no.

EYG no. 005290-23Gbl
ED None.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com