Deloitte.

Detect & Respond solutions

Managed Extended Detection and Response (MXDR) by Deloitte

24x7x365 attack prevention, detection, and response implemented in 30 days[1]

MXDR by Deloitte combines leading technology and service innovation to provide 24x7x365 prevention, detection, and response to attacks on your critical networks, laptops, servers, operational technology (OT), and cloud assets. By identifying rogue systems and vulnerabilities (supported by actionable cyberthreat intelligence), it's possible to anticipate attacks before they happen. Delivered as a cloud-based, modular turnkey service, MXDR can typically be implemented in under 30 days, helping you respond and recover with confidence in the event of a ransomware incident or security breach.

Current trends

Adversaries continue to evolve, including these macro trends:

- **Speed of adversaries is increasing**—on average, 84 minutes after access to action on objectives[2]
- Malware forms 29% of attacks, while **non-malware attacks count for 71% of attacks**[3]
- **Identity system compromises are commonplace;** they're behind 73% of successful attacks[4]
- **59% of successful cloud compromises** are due to cloud misconfigurations[5]
- **Ransomware is the favored attack of choice,** accounting for 67% of interactive attacks[6]
- Supply chain **LOG4J-style attacks will likely continue**[7]
- **Insider threat** has the potential for **higher impact** as a ransomware delivery threat vector[8]
- As OT systems become more connected and accessible, the need for strong **cybersecurity measures around OT environments is growing**. Protecting critical infrastructures, from cyber threats has become a top priority

Desired outcomes

MXDR by Deloitte can help your business in several ways, including these:

- Broad, collaborative, and **scalable detection and response**
- **Improved maturity** across prevention, detection, and response domains **for increased resiliency and defense** from cyberattacks
- **Leading technology and service innovation** you can harness to **defeat cyber adversaries** and their evolving attack strategies
- **Reducing the need to continually recruit,** train, and retain large, specialized teams
- **Reducing your security infrastructure and lower total cost of ownership** (TCO) with a software-as-a-service (SaaS) solution
- **Enhanced detection** of malware, non-malware, and lateral movement attacks
- **Greater learning from internal and external intelligence** to better anticipate and prevent future attacks
- Create a **secure and resilient OT ecosystem** that can withstand cyber threats, protect critical infrastructure, and **maintain operational continuity**, even in the face of evolving cybersecurity challenges

Detect, respond, and recover with confidence

Building and maintaining a threat detection and response infrastructure is often a complex undertaking for organizations. With the turnkey services and technology of MXDR by Deloitte, you can gain confidence in your ability to achieve your organization's mission-critical detect-and-respond objectives without the worry of keeping pace with ever-changing cyberthreats—all while reducing your security infrastructure and TCO.

Solutions in action

Manufacturing
A client was building a new, state of the art facility and wanted to design and build the facility with leading OT cybersecurity. Deloitte assisted the client with designing the security architecture and developing a set of OT security policies and standards that can apply not only to the new facility but can be retrofitted into existing facilities.

Life sciences and health care
With current protection capabilities unable to keep pace with rapid growth, our client sought help from a security provider. Deloitte was selected because its MXDR platform met critical solution objectives, including leading practices, scalability, and efficiency of tools and actions. Fast deployment was an added benefit.

Footnotes

1. Timeline based on business days and depends on the modules selected and the complexity of the client's environment
2. Crowdstrike, "*CrowdStrike global threat report*", 2023.
3. Crowdstrike, "*Nowhere to hide: 2022 threat hunting report*", 2022.
4. Verizon, "*Verizon data breach report*", 2023.
5. Checkpoint, "*Cloud security report*", 2023.
6. Cyberint Ransomware Report 2023.
7. Cybersecurity and Infrastructure Security Agency (CISA), "Apache Log4j Vulnerability Guidance", update on April 8, 2022
8. Deloitte, "*Executives' ransomware concerns are high, but few are prepared for such attacks,*" press release, September 13, 2021.

Turn complex challenges into opportunities

Our industry-tailored approach enables us to apply solutions to help you protect your IT, Cloud, and OT network and devices.

When you want 24x7x365 prevention, detection, and response—in 30 days[1]

Deloitte continuously protects millions of client assets globally by processing and analyzing billions of cyber events daily to disrupt thousands of cyberattacks monthly. Better yet, services can typically be implemented in under 30 days.

When you need deep resources

With five security operations centers and 31 cyber intelligence centers, Deloitte offers access to 24,000 cyber professionals globally—3,000 of whom are dedicated detect and respond practitioners.

We're well-positioned to help you achieve your objectives

Wherever you are in your journey, we have the experience, knowledge, and tools to help your organization move forward.

Outcomes-driven

In the face of growing complexity, we make finding a cyber and strategic risk provider easy. Our breadth and depth enable us to provide the outcomes (and value) you seek in a trusted adviser, a technology-savvy pioneer, a visionary integrator, and a dependable operator. We connect the dots, so you don't have to—helping you to improve security, trust, and resilience.

Quality-oriented

We bring together a powerful combination of proprietary technology, domain experience, leading alliances, and industry knowledge. Our focus on quality means we consistently work to help you realize your vision because addressing cyber and strategic risks are mission critical.

Value-focused

We act as a leader in times of crisis, a teammate to help you navigate change, and a force to have your back when you are on the front lines. We create value for our clients beyond the deal, pioneering cutting-edge resources and innovation, paving the way for forward-leaning collaboration, and leading bold thinking on tomorrow's emerging technologies so you can turn risks into opportunities.

Our capabilities

Native cloud SaaS delivery of unified, integrated modular services.

Extended Detection and Response (XDR)
Achieve faster cyberattack prevention, detection, and response with central XDR security information and event management/logging/analytics management capabilities.

OT Prevention, Detection, and Response (OTPDR)
Smooth integration of IT/OT threat identification and monitoring. This platform merges XDR actions and alerts to efficiently handle and mitigate cybersecurity incidents related to OT.

Adversary Threat Hunting
Reduce risk with continuous hunting that leverages intelligence, artificial intelligence/machine learning, and a hypothesis-driven approach with the Deloitte Threat Hunting Platform and master hunter operator trained teams.

Cloud Security PDR (CSPDR)
Initiate service discovery to learn what is and is not secured, along with supporting instances, containers, cloud services, serverless, various cloud platforms, and operating systems.

Endpoint Prevention, Detection, and Response (EPDR)
Support assets both on and off network to prevent both malware and ransomware attacks using next-generation antivirus and endpoint detection and response.

Incident Response (IR)
Identify incident management gaps in current processes and procedures and streamline response to adversary techniques to provide containment, eradication, and remediation actions to remove threats.

Flexible delivery approaches for when you need help with strategy, execution, or operation

Digital Risk Protection (DRP)
Identify and decrease the impact of exposed data with continuous digital asset monitoring that is operationalized with analytics and actionable intelligence.

Insider Threat Detection
Evaluate the environment to observe behavioral anomalies, identify risky user actions and detect possible insider threats utilizing User Entity and Behavior Analytics (UEBA) capabilities.

SaaS Prevention, Detection, and Response (SPDR)
Use cloud access security broker and data loss prevention technology to detect and respond to SaaS-targeted attacks.

Identity Prevention, Detection, and Response (IPDR)
Provide visibility into identity, anomalous behavior, detection of lateral movement, and advanced threats to detect compromised identities.

Attack Surface and Vulnerability Management
Bolster host and network endpoints as well as virtual and private clouds across multiple technology environments, providing real-time visibility into vulnerabilities, asset tracking, and rogue system detection.

Cybersecurity Intelligence (CSI)
Leverage broad predictive cyberthreat intelligence informed by adversary tactics, techniques and procedures; tailored analysis; and malware analysis.

Analyst and industry recognition

Deloitte ranked #1 in Market Share for Security Consulting Services based on revenue for 12th consecutive year in Gartner® Market Share report[9]

Deloitte named a worldwide leader in Incident Readiness Services by IDC MarketScape[10]

MSSP Alert Top 250 2022 - Deloitte #1 MSSP[11]

Deloitte named a worldwide leader in Managed Cloud Security Services by IDC MarketScape[12]

Meet the team

Adnan Amjad
Partner
US Cyber & Strategic Risk Offering Portfolio Leader
Deloitte & Touche LLP
aamjad@deloitte.com

Jon Korol
Partner
US Detect & Respond Leader
Deloitte & Touche LLP
jkorol@deloitte.com

Steve Mahar
Managing Director
Sales Leader, Detect & Respond
Deloitte Services LP
smahar@deloitte.com

Footnotes

9. Gartner®, Market Share Analysis: Security Consulting Services, Worldwide, 2022, Rustam Malik, 14 July 2023. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
10. IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment, by Craig Robinson and Christina Richmond, November 2021, IDC # US46741420
11. Top 250 MSSPs List: Managed Security Services Provider Company Research 2022 - MSSP Alert
12. IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment, by Cathy Huang, September 2022, IDC # US48761022