servicenow

Deloitte.

Managed Extended Detection and Response (MXDR) by Deloitte

MXDR by Deloitte combines leading technology with rigorously trained Deloitte teams to deliver a modular set of military-grade threat hunting, detection, response and remediation capabilities to organizations as a managed security service.

Common challenges

- Your organization's digital infrastructure is expanding, but **visibility into potential threats and vulnerabilities** is not.
- Keeping up with the speed, sophistication, and ever-changing tactics of persistent and **well-resourced adversaries**.[1]
- **Legacy security tools** don't provide the protection your organization requires
- **Security technology complexity** drives up costs and inhibits rapid detection and response.
- Difficulty finding, training and retaining **cybersecurity talent**.
- Ongoing cybersecurity **budget pressure.**
- **Reporting** meaningful cyber risk metrics to the executive team and board.

Solution

An integrated, modular platform that helps drive measurable cybersecurity outcomes - all enabled by industry-leading cyber security technology

Powered by ServiceNow Security Incident Response, MXDR by Deloitte provides continuous intelligence, threat visibility, and telemetry across IT and operational technology (OT) assets—from the cloud to the ground to the edge—so clients can see where threats lie and can gain sophisticated defensive capabilities. Deloitte's teams deliver this platform globally via a composable, modular set of cloud-native and software-as-a-service (SaaS)-based services available 24x7x365 using FedRamp-authorized and commercially-available technology.

Potential Benefits

- Accelerated time to value through SaaS delivery model
- Ability to prioritize alerts, automate workflows, and accelerate security processes
- Enhanced visibility into >99 percent of their organization's assets and identities
- Faster time to resolution of critical incidents and vulnerabilities
- Improved reporting capabilities to provide a full view of incidents and threats across your organization

This offering is designed to give your organization access to the advanced threat detection and response capabilities so urgently needed, while unburdening you of the cost and complexity of having to build and maintain this infrastructure on your own.

[1] CrowdStrike. "2021 CrowdStrike Global Threat Report," July 12, 2021.

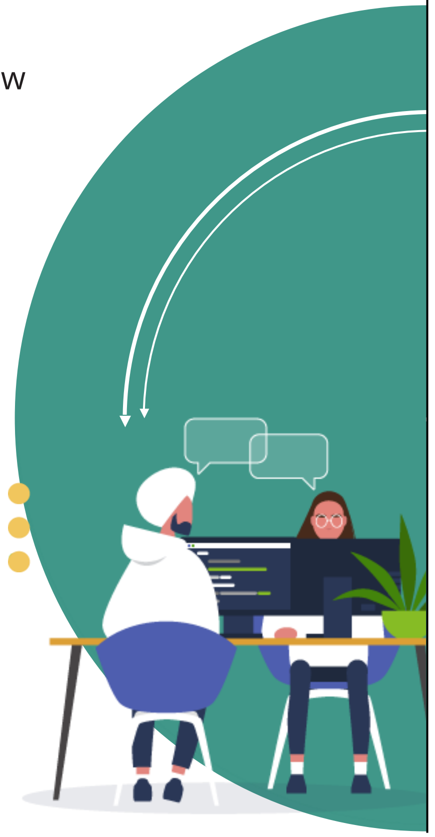
Contacts

Curt Aubley
Managing Director
Detect & Respond Leader
Deloitte & Touche LLP
caubley@deloitte.com

Mike Morris
Managing Director
Technology & Solutions Leader
Deloitte & Touche LLP
micmorris@deloitte.com

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

Learn how we can help:
deloitte.com/us/ServiceNow



Client assets

Identity Management (IDM)

Enterprise
Private cloud, containers, servers, laptops, desktops, mobile

Cloud
Software-platform-infrastructure-as-a-service, virtual machines (VMs), services, configuration

Networks
Cloud, on premises, secure access services edge (SASE)

Health care/IoT
Agent and non-agent,

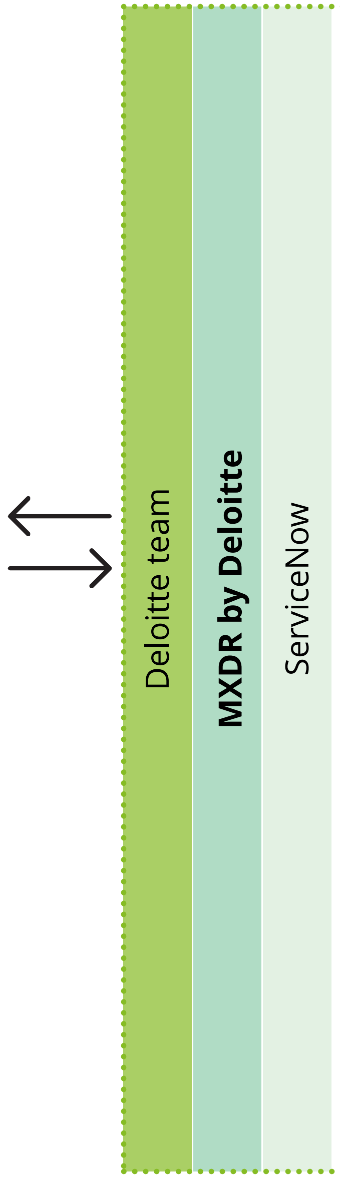
Operational Technology (OT)/ Industrial Control Systems (ICS) Agent and non-agent

Suppliers
Certifications, guard, firmware, versions

Edge/5G

Auto/Futures

People IT, HR, mobile, travel



MXDR by Deloitte platform modules

Client unified user interface (UI): Transparency and self-service alerts and reporting

Unified Detection and Response: Central security information and event management (SIEM)/logging/analytics management

Cybersecurity Intelligence: Insider; outsider; adversary; tactics, techniques and procedures (TTPs); malware; dark web; tailored analysis

Deloitte Insider Threat: Instrumentation, detection and response; advise on and implement an insider program

Adversary Pursuit: Hunting and remediation: Continuous hunting using intelligence, artificial intelligence/machine learning (AI/ML) and hypothesis approach

Cloud SaaS Prevention, Detection, and Response: Leveraging cloud access security broker (CASB) and data loss prevention (DLP) technology for our SaaS managed detection and response (MDR) services

Cloud Security Prevention, Detection and Response: Visibility and MDR into cloud workloads, containers, VMs; cloud security posture management; cloud workload protection platform; serverless

Zero Trust Identity Prevention, Detection and Response: Visibility and MDR into active directory and identity management systems

Enterprise Prevention, Detection and Response: Visibility and MDR for laptops, desktops, mobile, server, and private clouds

Attack Surface Management (ASM) and Vulnerability Management: Continuous identification of hardware, software, firmware, rogue and vulnerabilities

Incident Response (IR): Broad emergency management, sensor deployment and response

Master Hunter/Operator Training: Advanced training to bring security teams to the next level

Why Deloitte & ServiceNow?

Deloitte helps our clients enhance business outcomes by leveraging ServiceNow as an end-to-end digital workflow platform. We don't just leverage ServiceNow to help you automate your current processes; we can help you reimagine how work gets done, delivering material improvements in revenue and cost reduction with higher job satisfaction.

As a leading Global Systems Integrator and ServiceNow's Global Transformation Partner of the Year, Deloitte applies its breadth of industry and technology experience to help clients extract value from this powerful technology to create a united workflow with one platform.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.