

# Managed Extended Detection and Response (MXDR) by Deloitte

*24x7x365 attack prevention, detection, and response - implemented in 30 days\**

MXDR by Deloitte combines leading technology, with Chronicle SIEM (Security Information and Event Management) at the core, and service innovation to provide 24x7x365 prevention, detection, and response capabilities to help mitigate attacks on your critical networks, laptops, servers, and cloud assets. Delivered as a cloud-based, modular turnkey service, MXDR by Deloitte can typically be implemented in 30 days\*, helping you respond and recover with confidence in the event of a ransomware incident or security breach.



## Reality of the cyber world today



Cyber attacks are increasing, and every organization is a potential target



Cyber adversaries are constantly innovating



Cyber defense costs across people, process, and technology are growing



Cyber professionals are scarce and in high demand

**65%**

of C-suite execs cite ransomware as their greatest concern<sup>1</sup>

**73%**

of all successful attacks are identity system compromises<sup>2</sup>

**84  
minutes**

For adversaries to take action on objective after initial access<sup>3</sup>

<sup>1</sup> Deloitte, "Executives' ransomware concerns are high, but few are prepared for such attacks," press release, September 13, 2021.

<sup>2</sup> Verizon, Verizon data breach report, 2023.

<sup>3</sup> CrowdStrike, CrowdStrike global threat report, 2023.

We deliver  
outcomes  
that help your  
business



Lower Total Cost of Ownership (TCO)



Leading technology and services innovation to help you defeat cyber adversaries



Turnkey cyber security, maturity across prevention, detection, and response domains



Increase cyber operations maturity





Achieve cyber resiliency and defense from cyber attacks


# Making it real: Case study

A large healthcare organization and medical center experienced several challenges with their previous provider and legacy SIEM platform. Coupled with lack of integration and limited visibility, they suffered from bloated technology fees and fragmented threat detection capabilities.

With Chronicle and MXDR by Deloitte, the client was able to achieve:

**Predictable cost**  
versus client's previous SIEM solution

**Reduced client workload**  
by taking over containment, remediation

**Increased visibility,**  
fidelity, and detection capabilities

## Our capabilities

Native cloud SaaS delivery of unified, integrated modular services.

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

**OT Prevention Detection and Response**  
*Seamless integration of Information Technology (IT)/Operational Technology (OT) threat identification and monitoring. This platform merges XDR actions and alerts to efficiently handle and mitigate cybersecurity incidents related to OT.*

**Adversary Pursuit: Proactive Hunting**  
*Reduce risk with continuous hunting leveraging 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**  
*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.*

**Enterprise PDR**  
*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**  
*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.*

**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 and Entity Behavior Analytics (UEBA) capabilities.*

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

**Identity Prevention Detection and Response**  
*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 near real-time visibility into vulnerabilities, asset tracking, and rogue system detection.*

**Cyber Threat Intelligence**  
*Leverage predictive cyberthreat intelligence informed by adversary tactics, techniques and procedures, tailored analysis, and malware analysis.*



**FLEXIBLE DELIVERY APPROACHES**  
**FOR WHEN YOU NEED HELP WITH**  
**STRATEGY, EXECUTION, OR OPERATION**



Google Cloud Chronicle **DELIVERS**

**speed and scale** 

**&**

**MXDR by Deloitte** 

**DELIVERS** resilient security outcomes

**Start the conversation**



**Upen Sachdev**  
Principal  
Deloitte & Touche LLP  
[usachdev@deloitte.com](mailto:usachdev@deloitte.com)



**Chris Trollo**  
Senior Manager  
Deloitte Services LP  
[ctrollo@deloitte.com](mailto:ctrollo@deloitte.com)



**Jason Tarlton**  
GSI Strategic Partnerships  
Google Cloud Security  
[jtarlton@google.com](mailto:jtarlton@google.com)

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.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see <http://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.

Copyright © 2023 Deloitte Development LLC. All rights reserved.