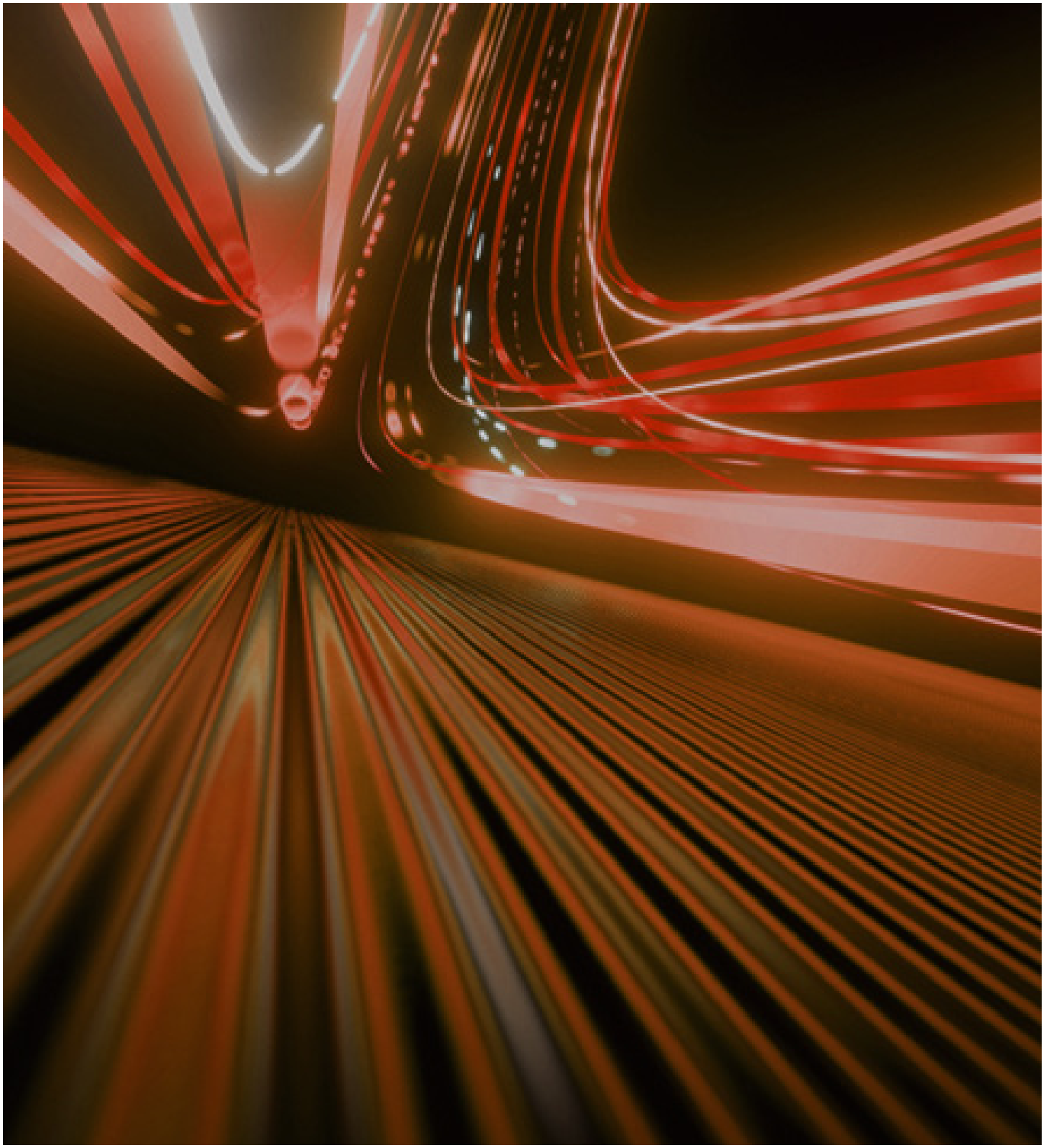
EVIDEN

Digital Security Magazine - 11th edition
July 2023

The Future of MDR: The CTO Vision

By Vinod Vasudevan



Managed detection and response (MDR) is at an inflection point.

Detection and response remain at the core of the offering, but the evolution of threat landscape in combination with rapid digital transformation is expanding the scope of detection and response.

The following are the seven key changes that are transforming this space.

1

Chat GPT has shown us all that AI works.

There is a positive impact across all industries, and MDR is no exception. One use case that is strongly aligned with the use of Generative AI is the automation of response and threat hunting. Generative AI bots assist security analysts in hunting through large datasets, investigating incidents and automating rapid responses.

It's a strong use case that is now receiving significant R&D investment.

This will address the widespread shortage of security staff and reduce the burden on overworked security professionals in the security operations center.

2

Cybersecurity remains fragmented in terms of best-of-breed,

niche technologies that address specific aspects of the threat landscape.

Security information and event management (SIEM), MDR, and extended detection and response (XDR) platforms have attempted to solve the problem of leveraging an organization's various security technologies to achieve security outcomes.

There is still much that can be done to achieve deep integration. But it has been difficult due to the lack of a standard but dynamic architecture in the industry. The emergence of cybersecurity mesh architecture (CSMA) [1] will lead the way to an industry framework for integrating the mess of disparate security products into a mesh of security outcomes.

The AWS Open Cybersecurity Schema Framework (OCSF) initiative is an industry accelerator toward mesh.

3

Security has gained traction at boardroom level.

However, there is still a communication gap between how the board consumes security information and how it is reported by security teams. The need to report security metrics in the context of the business is gaining traction in the industry.

The industry is moving toward a unified real-time business risk visualization approach. For example, if there are operational technology (OT) or Industrial Internet of Things devices in factories that have been affected by a cyberbreach, the board would like to visualize the business impact of production delays and associated financial impacts.

This is a major shift from security dashboards to unified real-time business risk visualization.

[1] Hevesi, P. and Ruddy M. (2022). Gartner Research: The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA).

4

Exposure management complements detection.

Understanding the exposures that cybercrime syndicates can exploit has become important for high fidelity detection.

Exposure could be through unmanaged assets, vulnerabilities in externally exposed assets, exposed code on GitHub or customer/card data on the dark web.

5

Recovery is emerging as a key component of the MDR offering.

To date, the focus has been on response to contain and manage an attack. After response, organizations still need to perform a number of recovery actions to restore business operations.

Therefore, automating common recovery actions such as patching, reimaging and restoring workloads with required data is an integral part of the MDR roadmap.

6

MDR is also shifting left with preventive features.

Policy management and posture management are two areas that work hand-in-hand to proactively improve the security controls.

This is very important in a hybrid, multicloud environment. Take, for example, the ability to centrally push security best-practice policy settings for workloads, containers and storage tiers. It's important to be able to do this without having to worry about the nuances of implementation across different hyperscalers or datacenters with different flavors of OS and application platforms.

The same capability can be used to centrally push security policies to improve the posture of affected devices in a breach scenario.

7

MDR becomes vertical with industry-specific use cases.

Attacks are no longer generic, they are industry-specific. We need to secure each industry with its own set of devices, applications and use cases.

Some examples to illustrate are manufacturing with OT, healthcare with Internet of Medical Things, and financial services with financial transaction applications.

Eviden is innovating in all of the above areas and working toward the next-generation MDR offering.

The evolution of our MDR offering with our platform AIsaac and markitecture view of the future is captured below.