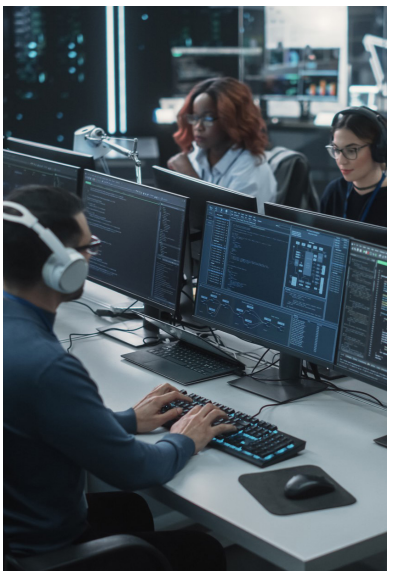
Managed Extended Detection & Response



Address blind spots from siloed security solutions and benefit from the most effective means of identifying and mitigating security incidents with Avalon's managed extended detection and response (MXDR) service, KnightVision MXDR.

KnightVision MXDR includes our world class 24/7/365 security operations center (SOC), staffed by expert security analysts, who tune, monitor, triage, and respond to security incidents in your environment. The SOC utilizes our state-of-the-industry SIEM platform (a software tool that helps increase the efficiency and timeliness of incident response activities) to perform advanced analytics and investigate indicators of compromise (IOCs), including malicious entities probing your infrastructure, compromised systems, and potentially unsecured user behaviors.

KnightVision MXDR's combination of **people, processes, and technologies** delivers **round-the-clock threat hunting, monitoring,** and **analysis...** protecting your organization from **the most sophisticated online threats.**

This combination of people, processes, and technologies delivers round-the-clock threat hunting, monitoring, and analysis across your organization's entire environment, protecting it from the most sophisticated online threats.

Why You Need KnightVision MXDR

- **Improved operational efficiency:** With the ever-increasing number of threats, there's an ever-increasing number of alerts – and your IT team doesn't have the time to address every one of them. By outsourcing this massive task to Avalon, your IT team can focus on their core duties. Our world-class XDR technology automates many aspects of detection and response, so our battle-tested team is armed and ready to protect your organization, 24/7.
- **The latest and greatest:** MXDR is the best option for stopping threats in their tracks, as you have a team of experts utilizing the most comprehensive range of security telemetry data, including endpoint data, network traffic, and cloud-based environments.
- **Save time and money:** Outsourcing this service to Avalon means you don't have to take on the expense of adding full-time, highly paid security professionals to your payroll. Instead, we become a seamless extension of your IT and security team at a predictable price – minus the costs of recruiting and expensive employee benefits.

AVALON Managed Extended Detection & Response

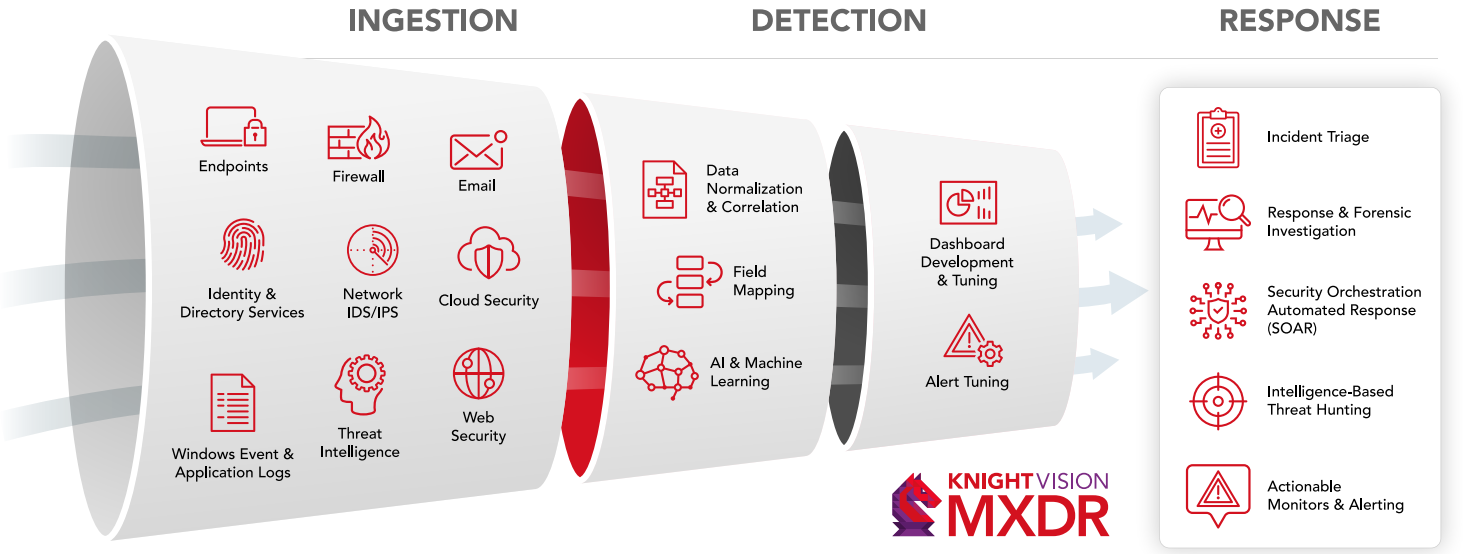
How Does MXDR Work?

XDR technology collects and correlates the data that identifies threats occurring at different layers of your security stack. Our team (who add the "M" to MXDR) can properly configure the XDR to conduct forensic investigation and threat hunting activities across numerous security solutions, all from a single console.

Step 1. Ingest: Data from security log sources such as endpoints, cloud infrastructure, identity solutions, network traffic, and more is brought into the system.

Step 2. Detect: Log data is parsed, normalized, and correlated to automatically detect threats using cutting-edge artificial intelligence and machine learning.

Step 3. Respond: Through human and machine analysis, alerts are prioritized, so our highly trained security analysts and threat hunters can quickly analyze new events and automate investigation and response activities.



Whether conducting a vulnerability assessment, providing security advisory services, or responding to a cyber incident, the Avalon team delivers a five-star experience and unwavering support throughout the engagement.

AVALON

QUESTIONS?

To learn more about our MXDR service, contact:

Rebecca Rudell, Marketing Manager
rebecca.rudell@teamavalon.com