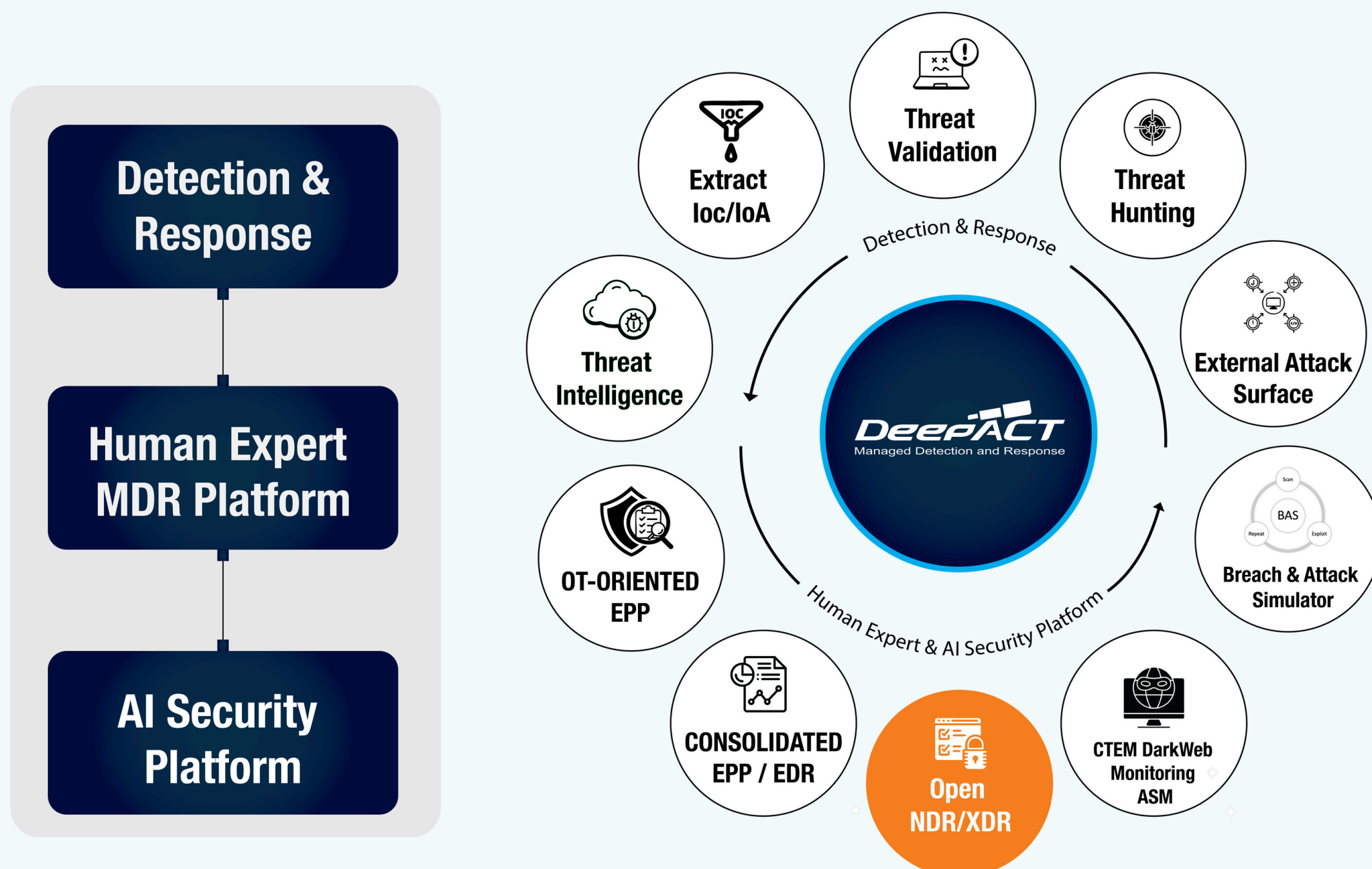


# AI-Based Open XDR Integrated Security Operations and Analysis

NDR (Network Traffic), AD/FW Event Integration, and Intelligent Threat Detection and Response

By combining PAGO MDR (Managed Detection and Response) platform, DeepAct, with Stellar Cyber's Open XDR/NDR, enterprises can enhance their advanced threat detection and response capabilities. This integration enables effective management of multiple security tools through a single dashboard, facilitating rapid and accurate threat detection and response even in complex security environments.



## What's the Problem with Security Operations and Analysis?

MDR Center have deployed a wide range of detection and analysis tools to detect and defend against rapidly evolving attacks. However, this has resulted in a highly complex security detection environment. Consequently, numerous security events are generated across various solutions, yet pinpointing the events that actually require action remains a significant challenge.

In addition, today's IT infrastructure spans not only on-premises environments but also public/private virtualization, cloud environments, container workloads, and countless applications, all of which produce an overwhelming number of security-related events. Security teams are finding it increasingly difficult to keep up, and the need for a "faster, more accurate, and efficient integrated security operations and analysis platform" is now more critical than ever.



- **Integrated Threat Detection and Response:** Integrates various security tools and systems for broader and more sophisticated threat detection.
- **Advanced Analytics and Visibility:** Provides real-time analysis of threats across diverse environments, ensuring comprehensive visibility even in complex security landscapes.
- **Automated Response:** Quickly blocks and isolates advanced attacks in real time.
- **Scalability and Flexibility:** Easily scalable and adaptable to environments and organizations of different sizes.
- **Ease of Management:** Centralized dashboard simplifies management and monitoring.



- **24/7 Expert Monitoring and Automated Threat Response:** Managing potential threats that could be missed through round-the-clock expert monitoring and automation.
- **Advanced Threat Analysis and Response:** Providing advanced analysis services tailored to specific environments and threat models.
- **Customized Reports and Insights:** Delivering client-specific reports and insights.
- **Real-Time Threat Response and Incident Management:** Offering real-time alerts and optimized response strategies during incidents.
- **Threat Intelligence and Trend Analysis:** Analyzing threat intelligence and trends to stay ahead of emerging threats.
- **Scalable and Flexible Security Solutions:** Providing security solutions tailored to customer requirements, scalable to different environments and needs.
- **Efficient Security Operations and Cost Reduction:** Simplifying security infrastructure to reduce management and operational costs.

**Stella Cyber's Open XDR/NDR platform is equipped with an advanced security architecture that provides various features to strengthen enterprise cybersecurity environments. Its key features and advantages include:**

- **Integrated Security Data Collection:** The Open XDR/NDR platform provides centralized management by integrating various security data sources, including networks, endpoints, clouds, and emails. It collects data from multiple security tools in real time and extracts critical security insights without redundancy, significantly improving the efficiency of security operations.
- **Advanced Threat Detection Capabilities:** Stella Cyber leverages AI and machine learning to implement unique algorithms for detecting advanced cyber threats in real time. The platform effectively identifies a wide range of sophisticated threats, including unknown attacks and zero-day vulnerabilities, maximizing threat accuracy and minimizing false positives.
- **Automated Response and Action Features:** Open XDR/NDR offers automated threat detection and real-time response capabilities. When an attack occurs, the system automatically classifies the threat and executes appropriate response procedures. This automated process reduces the burden on security teams and shortens response times to security incidents.
- **AI-Based Correlation Analysis:** The Open XDR/NDR platform utilizes AI-driven advanced correlation analysis to process and correlate events occurring in various security data sources in real time, identifying threats. This allows for quick tracking of the cause and path of an attack, providing more refined security insights.
- **Scalability and Flexibility:** This platform supports both cloud and on-premise environments and can be flexibly expanded to meet enterprise security requirements through seamless integration with various security tools. Additionally, the platform offers high scalability, allowing it to adapt to changes in company size and security environments, supporting gradual security improvements.
- **User-Friendly Dashboard and Management Interface:** StellaCyber's Open XDR/NDR offers an intuitive, user-friendly dashboard and management interface. This enables security teams to monitor threats in real time and quickly respond to incidents by providing the necessary information. The dashboard effectively presents various security data visually, helping operators take timely actions.
- **Open Architecture:** The Open XDR/NDR platform adopts an open architecture, facilitating integration with existing security infrastructures and offering high flexibility when adding new security tools or technologies. This enables companies to respond to ever-evolving security threats and, if necessary, expand or improve their security environment.

*Thanks to these features, Stella Cyber's Open XDR/NDR platform delivers the ability to quickly and accurately detect and respond to advanced cyber threats, significantly enhancing the efficiency and effectiveness of enterprise security management.*