MANAGED DETECTION AND RESPONSE

What is CPX MDR Offering?

Today, cyberattacks are sophisticated. They target endpoints, infrastructure, cloud platforms, servers, databases, identities, emails, etc. through multiple combined vectors.

CPX Managed Detection and Response (MDR) Service operates a 24/7/365 intelligence-driven package to defend against relentless attackers. With 24/7 treat monitoring, detection, investigation, hunting, and automated response capabilities powered by Microsoft security tools combined with CPX's advanced cybersecurity technologies for threat analytics, malware analysis, and machine learning, the result is a tailored service that identifies complex threats and removes attackers' abilities to exploit the desynchronized nature of extended digital environments.

Challenges addressed by the CPX MDR experience?

ATTACKERS NEVER REST, BUT YOUR EMPLOYEES NEED TO.

CPX MDR cybersecurity service is tailored to the current and emerging problems faced by organizations today. It plays an active role in protecting your data and assets and improves your organization's security posture. Below are some of the operational security challenges that CPX MDR addresses:

Talent Shortage

Staffing is a critical challenge across every IT department, with security resources being among the hardest to attract and retain. CPX MDR offers to bridge the skill gaps and ensure consistency for your organization's IT security.

Visibility Across Disparate Environments and Technologies

CPX MDR centralizes visibility across a distributed on-premises cloud environment into a single pane of glass, thereby decreasing the time to detect and effort to respond to cyberthreats.

Reduce False Positives

CPX MDR, supported by its backend-focused threat intelligence and machine learning SOAR as a Service platform, reduces the number of escalations that require attention from your organization's in-house IT teams and spares their time & effort to focus on initiatives that enable business growth.

24x7x365 Monitoring

Gartner's recommendation is to hire a team of at least eight dedicated resources to staff a 24/7 Security Operations Center (SOC). With the skills shortage, finding cybersecurity professionals with the right qualifications is difficult and most likely expensive. In addition to always-on detection and response, CPX MDR offers a consistent and cost-effective alternative to building your in-house team, and delivers turn-key SOC capabilities that monitor, detect, and respond to cyber threats across your organization.

Key features offered by CPX MDR

CPX MDR integrates with your organization's security stack to deliver 24/7 expert threat detection and automated incident response, based on the MITRE ATT&CK framework. CPX MDR gives you complete visibility into all cloud, network, and user activity, closing security blind spots, eliminating the false positive noise, and focusing your organization IT team to engage on incidents that negatively impact your business.
MDR services are only as good as the technology and people driving them. CPX provides a complete solution built on the most advanced SOAR platform, including threat hunting, alert triage, and automated incident response all customized to your environment.

Take a look at the following features of CPX MDR that can improve your organization's IT security posture and dramatically reduce your costs:

- SOAR platform, enriched by in-house developed automated response playbooks utilizing threat intelligence and contextual data to eliminate false positive alerts. Effective security automation, and orchestration aids the analysis, detection, triage and response to true positive threats found in your security events thereby reducing attacker dwell time and their ability to damage your business.
- Scalable, cloud-based, and managed SIEM to consolidate your log data and security events. Benefit from CPX's team of experts who will configure and manage it for you.
- Perpetual updates on security content by a team of experts that is constantly creating and updating detection & response playbooks, integrations, and dashboards to continuously protect you from the latest cyber threats.
- 24/7 monitoring, detection, analysis, and investigation for all security relevant events.
- Threat hunting by expert analysts investigating potential threats targeting your IT environment using the MITRE ATT&CK framework and threat hunting tools with automation capability.
- Dedicated cyber security team of experts serving as a 24/7 extension of your IT team, to learn your environment, needs, requirements, and processes.
- Reporting on activities status and the progress made on cases in investigation.

The CPX MDR difference

- Locally hosted in the UAE leveraging Microsoft Azure Cloud and supported by Microsoft security's market leading toolset.
- Built, managed, and supported by CPX Operations Center experts based in the UAE.
- Powered by CPX SOC Advanced Technologies: Security Automation, Orchestration and Response (SOAR) platform, and machine learning complex algorithms developed and managed by a sovereign data science team based in the UAE.
- In-house generated 1st party threat intelligence feeds tailored to the GCC region that provide information on attacks, including zero-day attacks, malware, botnets, and other security threats that enable faster, more informed, data-backed security decisions with a proactive approach in the fight against threat actors.
- Access to cybersecurity talent through MDR and 24/7 security operations center that complement your organization's internal security teams with domain experts to achieve the Promise of Elevated Security posture.

How does the CPX MDR offering work?

The CPX MDR offering is powered by Microsoft and delivered by CPX advanced SOC technologies. Incorporated within it are security logs from the entire Microsoft security toolset as well as many third-party technologies that activate 24/7 monitoring, proactive threat hunting, threat analysis, alert triage, and response and remediation working alongside your IT security stack and personnel. MDR typically involves planning that is followed by applying technology and expertise to the core network and endpoint security responsibilities, including:

Deployment

Cover an organization's entire deployment of endpoints to minimize the vulnerability to threats soon and as thoroughly as possible including Azure cloud.

Proactive Threat Hunting

Continuous 24/7 monitoring of an organization's networks and endpoints, using Microsoft endpoint detection and response tool (Defender) combined with CPX's threat intelligence that is tailored to the region's up-to-date intel to identify security incidents and instantly notify the respective people and systems for investigation, triage and response & remediation.

Threat Context

Investigate an alert and determine whether it is a true incident or a false positive. This is accomplished through a combination of data analytics, machine learning, and human investigate.

Triage

Quickly validate and prioritize detected threats based on the context of each event and its most likely impact.

Respond Remediate

Notify your organization security team to take recommended actions and (or) trigger automatic responses to terminate each high-priority threat and return the system to its unthreatened status.

Report

Create a detailed report for each incident. It will identify the threat, how (and when) it was detected, steps taken, and how the incident was resolved.

Microsoft Sentinel

A cloud based security information and event management (SIEM) tool.

Microsoft 365 XDR Platform

An extended detection and response (XDR) platform, designed to natively integrate with Microsoft Sentinel and provides: Exchange Online Protection, Defender for Office 365, Defender for Endpoint, Defender for Identity and Defender for Cloud Apps

Microsoft Defender for Endpoint

A platform that provides XD Capabilities for infrastructure and cloud platforms including virtual machines, databases and containers.

Proactive Threat Hunting

Proactive search on your organization network and systems for indications of compromise

Alert Triage

Organise the received security events in order to enable the analysts to address the most critical as priority

Remediation

Take the necessary best practice actions for solving the root issue and implementing a solution

Incident Investigation

Investigate received alerts to determine whether it is an actual incident or a false positive report

What are the key benefits of CPX MDR cybersecurity service?

24x7 Monitoring

CPX MDR offers 24/7/365 monitoring and protection for your organization networks. Constant protection is essential for rapid response to threats since cyberattacks can happen at any time.

Vulnerability Assessment

Vulnerability management can be complex and time-consuming, and many companies rapidly fall behind. CPX MDR can help to identify vulnerable systems, perform virtual patching, and support the installation of required updates.

Proactive Approach

CPX MDR offers proactive cyber protection as threat hunting and vulnerability assessments. By identifying and closing security holes before they are exploited by an attacker, MDR helps to reduce cyber risk and the likelihood of a successful cyber security incident.

Improved Compliance

CPX has the expertise in regulatory compliance, and its MDR is designed to meet the requirements of applicable laws and regulations. Additionally, with the deep visibility of CPX MDR to your organization, it can simplify and streamline compliance reporting and audits.

Skilled & Experienced Analysts

CPX MDR helps to close the cybersecurity skills gap by providing you with access to skilled and experienced cybersecurity professionals. This both helps to meets headcount and ensures you have access to specialized skill sets when you need them.

Leverage Microsoft Licenses

Benefit from utilizing Microsoft E3 or E5 licenses and avoid duplication and double investment into endpoint protection such as Microsoft Defender and SEIM licenses