MANAGED EXTENDED DETECTION & RESPONSE (MXDR) SERVICE

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

Member of
Microsoft Intelligent Security Association
Microsoft

Incident Response

Threat Intelligence

SOAR

Intelligent Onboarding

DynTek's Managed Extended Detection and Response (MXDR) Service Helps Organizations Improve Their Security Posture and Fight Advanced Cyber Threats

Today's organizations, at all levels, face an incredible number of security threats that evolve daily...and the stakes are high. One breach can have a significant negative impact on finances, trust, and reputation. The big challenge is to establish the ability to monitor, identify, respond to, and remediate multiple simultaneous security threats.

DynTek's MXDR service provides expert managed, 24x7x365 vigilance, providing you with comprehensive SIEM operations and threat detection coverage. Our fully managed service helps automate security detection and response to protect against internal and external threats to the IT infrastructure, systems, data, and more.

US-BASED SECURITY OPERATIONS CENTER

DynTek's Security Operations Center provides Advanced Threat Intelligence, Threat Hunting, Analytics, Monitoring and Alerting Services, Endpoint Protection and Management, and Proactive Threat Response DynTek actively monitors your environment to help you sort through the 'noise' of false positives in order to proactively hunt for threats and turn alerts into actionable intelligence. Through 24x7 'eyes on glass' coverage, we identify critical threats in near real-time and leverage analytics to gain granular detail and context for each security incident. All security events are correlated against millions of indicators of compromise in an automated manner to help detect threats that are not being identified by the security solutions in your environment. In the end, this leads to more accurate information and faster resolution time. You gain immediate insight so you can pinpoint the physical location of an incident and take appropriate action.

MANAGED XDR SOLUTION

DYNTEK'S MXDR SERVICE INCLUDES THE FOLLOWING COMPONENTS:

INCIDENT RESPONSE (IR)

DynTek's security experts leverage the extensive incident response capabilities available in our integrated platform to quickly identify, investigate, assess, contain, and remediate various threats.

THREAT INTELLIGENCE

Using native, first-party and third-party intelligence sources, DynTek's threat experts scan various sources and consider various scenarios for maximum detection and protection.

REPORTING

Timely and informative reporting is available to help with attack analysis and subsequent remediation efforts.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

Thousands of analytic rules, watchlists, playbooks, and automation scripts comprise an ever-expanding library to benefit our customers.

INTELLIGENT ONBOARDING

Logs are not created equal. DynTek will work with your team to identify and optimize log ingestion across a range of sources, including cloud and on-premises, to strike a balance between ample visibility into threats and cost.

KEY BENEFITS

ENHANCED SECURITY POSTURE

- Fast response times for security events with the ability to triage incidents
- Use of machine learning to increase efficacy of detection
- Shared knowledge gained from hundreds of projects across multiple industries
- Customer access and visibility into the same dashboard as the SOC analysts

PROACTIVE SECURITY CONSULTING

- Reviews with security experts to analyze metrics, incidents, recommended security enhancements to existing toolset, and security best practices

ENHANCED DATA PRIVACY & PROTECTION

- US-Based Security Operations Center staffed with W-2 employees with comprehensive background checks
- Analyst work done in a secure GovCloud environment
- Customers maintain full custodianship and control of their data

EXPERTISE BEYOND ALERTING

- Daily threat hunting and alert triage from experienced SOC analysts to rapidly contain and respond to threats
- Threat intelligence queries comprised of millions of Indicators of Compromise to detect current and emerging threats in data source logs

NEXT-LEVEL KNOWLEDGE & REPORTING

- Enhanced visibility into the security of users and systems including analysis of user and entity behavior analytics
- Executive dashboard and data visualizations to view data in real-time
- Performance reporting on existing cybersecurity toolset including metrics around each solution that provides data ingested into the system to justify expenditures

Microsoft Solutions Partner

Member of Microsoft Intelligent Security Association

Microsoft

CONTACT DYNTEK TODAY
FOR A COMPLIMENTARY CONSULTATION
For more details, visit us at dyntek.com/free-consultation

opscenter@dyntek.com | 877-297-3723 | www.dyntek.com