DATASHEET

CRITICALSTART®

Guide to Managed eXtended Detection & Response (MxDR) Services

Breach prevention simplified.

Critical Start is the only MxDR provider on the market today who dared to approach simplifying the cybersecurity problem by first embracing the complex. While others are focused on finding bad, we focus on finding good. While others prioritize or suppress alerts, we resolve all alerts.

Critical Start bring you a team of skilled security experts who will deeply understand your environment to adapt and scale with your organization's needs and partner with you to detect, investigate and respond to threats specific to your organization.

Critical Start delivers something priceless – the peace of mind that comes from:.

- ✓ Available on-site and remote incident response and digital forensics capabilities, for situations requiring trained incident responders
- ✓ 100% visibility to every action and every datapoint our team has examined, what our detection engineers see, and a view of the detection coverage delivered by your security tools and MDR service
- ✓ Service Level Agreements for Time to Detect (TTD) and Median Time to Resolution (MTTR) for all alerts, regardless of severity level – guaranteed in one hour or less – with no fine print

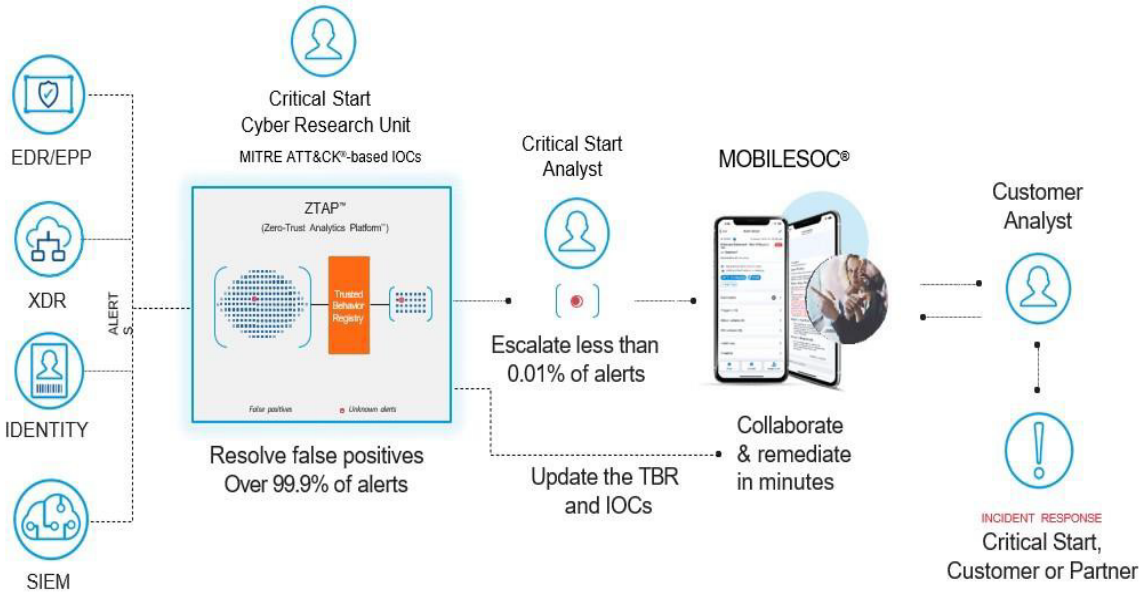
Smarter technology for all

Lenovo

MxDR service is purpose-built as the industry's only Trusted Behavior Registry™ (TBR) within our Zero-Trust Analytics Platform™(ZTAP™) to resolve all alerts. It integrates with multiple security tools, including endpoint, SIEM, XDR, and identity, to reduce the volume of alerts by morethan 99%, escalate less than 0.01% of alerts, and never sends the same alert twice.

Key Benefits

- ✓ Optimize security investments
  90% reduction in false positives on the first day of production monitoring and escalation of less than 0.01% of alerts
- ✓ Reduce risk exposureresolution of more than 99% of alerts
- ✓ Decrease complexity Over 40% of customers rely on us to bring together conceptual insights acrossmultiple security tools.



How This Is Done

Detect the right threats. MxDR Services:

- ✓ Manages, maintains and curates out-of-the-box detections and IOCs released by the security tool manufacturer.
- ✓ Curates original and third-party threat intelligence, combined with real-time threat analysis, to create a high- fidelity, actionable view of existing and emerging threats.
- ✓ Continuously develops and enriches new threat detections and Indicators of Compromise (IOCs) based on the evolving security landscape.
- ✓ Maps threat detection content to the MITRE ATT&CK®Framework to ensure you are protected against the latest attacker Techniques, Tactics, and Procedures (TTPs).

Respond with the right actions.

- ✓ Critical Start provides expert Security Operations Center (SOC) Analysts, to quickly investigate and respond to all escalated alerts through 24x7x365 monitoring, rapid investigation, and continuous threat hunting.
- ✓ The MOBILESOC® application allows you to communicate with the SOC and performresponse actions on the go.

Provide agility and adaptability.

- ✓ A dedicated project manager and implementation team dig in deep fromthe start to understand your environment, unique needs and business objectives.
- ✓ The Customer Success Team is your advocate and there with you on the journey, providing recommendations and support as your needs change.

Critical Start only works with the **best.**

Critical Start MxDR services integrate with leading security technologies to detect every alert, resolve every alert and respond to breaches.

Microsoft Defender for Endpoint · Microsoft 365 Defender · Microsoft Sentinel

CORTEX · splunk> · TREND MICRO · vmware Carbon Black

BlackBerry CYLANCE · SentinelOne · DEVO · CROWDSTRIKE