Lenovo Services

Solutions & Services Group

Managed Detection & Response Service Powered by Critical Start

Description of Service

Service Overview

In today's cyber threat landscape, securing endpoint devices has become increasingly difficult. Cyber threats are more sophisticated and attackers' abilities to invent techniques, tactics and procedures have improved exponentially. If not handled properly, it will become more and more difficult for organizations to manage cyber security threats and security incidents. Threats like "fileless" malware (which writes nothing to disk) cannot be caught by anti-virus signatures, so traditional Anti-Virus tools are becoming less and less effective. Organizations need new ways to prevent the execution of malicious code on their endpoints. Critical Start's XDR Service redefines what endpoint protection can and should do for your organization by leveraging artificial intelligence to detect and prevent malware from executing on your endpoints, in real time.

Lenovo helps our customers navigate the security vendor noise and focuses on helping clients operationalize security and is committed to helping you simplify endpoint management and security in your environment. Critical Start's MxDR is an integrated threat prevention solution that combines the power of artificial intelligence and cyber analytics to operationalize your endpoint security strategy. Combining excellence in operations with state-of-the-art technology, Critical Start can protect, manage, and monitor your endpoints and ensure you get maximum value from your technology investment. This modern MxDR solution is available as a muti-tenant, cloud-based, endpoint management solution.

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 Exposure – Resolution of more than 99% of alerts.
- Decrease Complexity – Over 40% of Critical Start's customers rely on then to bring together conceptual insights across multiple security tools.
- Effectiveness – Prevents over 99% of malware before it can execute.

Offering

Critical Start is the only MDR 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, they focus on finding good. While others prioritize or suppress alerts, Critical Start resolves all alerts.

Supported technology: Microsoft Defender for Endpoint, Microsoft 365 Defender, Microsoft Sentinel, Cortex, Splunk, Trend Micro, VMWARE Carbon Black, BlackBerry Cylance, SentinelOne, Devo, CrowdStrike.

Critical Start brings the customer a team of skilled security experts who will deeply understand the customers' environment to adapt and scale with their organization's needs and partner with them to detect, investigate and respond to threats specific to the organization.

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

- 100% visibility to every action and every data point the Critical Start cybersecurity team has examined, what our detection engineers see, and a view of the detection coverage delivered by customer security tools.
- 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.

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

How It's Done

Detect the Right Threats

- Manage, maintain and curate out-of-the-box detections and IOCs released by the security tool manufacturer.
- Curate 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 develop and enrich new threat detections and Indicators of Compromise (IOCs) based on the evolving security landscape.
- Map threat detection content to the MITRE ATT&CK Framework to ensure the customer is protected against the latest attacker Techniques, Tactics and Procedures (TTPs)

Respond with the Right Actions

- Provide expert Security Operations Center (SOC) Analysts, to quickly investigate and respond to all escalated alerts through 24x7x365 monitoring, rapid investigation, and continuous threat hunting.
- MOBILESOC application allows the customer to communicate with the SOC and perform response actions on the go.

Provide Agility and Adaptability

- A dedicated project manager and implementation team dig in deep from the start to understand the customer environment, unique needs and business objectives.
- The Customer Success Team is the customer advocate, and they are with the customer on their journey, providing recommendations and support as needs change.

The service features consist of the following:

The Lenovo Managed XDR Service is an annual subscription service that is priced per monitored device or user. The Services are divided into two (2) phases, Implementation and On-going Operations, as described below.

Lenovo Services

Solutions & Services Group

The Onboarding Lifecycle

The key to a smooth onboarding launch is understanding. Critical Start has built a process to make customers completely comfortable including a comprehensive understanding of the resources they make available to enable success. Critical Start also wants to build understanding of the internal resource's customers need to leverage so that the customer is making the most of the resources provided. An effective onboarding and implementation process should take into the account an organization's unique environment and existing security tools and processes. Critical Start makes the effort and spends the time with the customer to learn this environment and build out a dedicated team to work effectively within it. One of the primary values that Critical Start provides, are resources that stay with the customer throughout the project. Critical Start wants to build a strong relationship with customer resources to work together daily, with a common purpose and understanding, to respond as a fluid, cohesive unit any time a threat presents itself.

Dedicated resources Critical Start provides during onboarding:

1.) Project Manager

- Point of contact for project plan, timeline, and milestones
- Will host cadence calls to ensure project is on track and on schedule.

2.) Customer Success Manager

- Will build relationship and ensure that all goals and primary business objectives are met.

3.) Endpoint Engineer(s)

- Will assist with event reduction, playbooking and technical integration into ZTAP.

4.) Support Analyst

- Provides additional support before moving into production monitoring and continues after launch.

The Customer will provide resources with the capabilities to perform the following tasks:

- Deploy/install endpoint/XDR/SIEM agents on hosts.
- Review security events as escalated by Critical Start
- Modify firewall rules to accommodate endpoint/XDR/SIEM connectivity.
- Knowledge of network environment to work with Critical Start on baselining security events. **Note:** if the customer is not able to provide the necessary resource, Lenovo can add in appropriate resources for an additional fee via time and material billing.

Lenovo Services

Solutions & Services Group

From start to finish, the **Onboarding Process** can be outlined through the following three stages:

Stage 1: Kick-off – During the initial kick-off call, the customer will meet the Critical Start team and review project milestones.

- **Customer Action Items**
  - Fill out and return questionnaire prior to kick-off.
  - Download the MobileSOC app and sig-up for ZTAP training.
  - Approve the project plan after review.

Stage 2: Implementation – Rolling out the MxDR service offering.

- **Access and Integration** During this phase we will perform a health check of your current cybersecurity policies to uncover and address any gaps in coverage. Detections and indicators of compromise are infused directly into the tools used by our MDR team. Through this approach, we can create a high-fidelity threat detection and validation platform that uses specific detection logic customized to your environment. At this stage, we will need access to your security product in order to build and connect the ZTAP environment.
- **Event Reduction** We will develop playbooks to reduce the volume of alerts and security events. Additionally, threat intelligence includes a curation of original and third-party data to derive new detections with everything mapped to the MITRE ATT&CK® framework to reduce complexity and improve SOC effectiveness.
- **ZTAP Training** Your team will have multiple options for self-paced training through video instruction, or through online instruction for both console-based ZTAP and our MobileSOC application.

- **Customer Action Items**
  - Provide security product tenant access.
  - Assist in event reduction through handling of escalated alerts.
  - Work with the Critical Start team to develop alert exclusions in security product.

Stage 3: Production – Testing and monitoring environment for potential changes.

- **Final Health Check -** We work with you to ensure the technology, processes and people are in place to resolve alerts and mitigate threats to your enterprise.
- **Move to Production Monitoring** - Managed Detection and Response goes live, and monitoring and response are transitioned to our customer success team. This is another dedicated team to provide you with a consistent point of contact to ensure dynamic and adaptive protection.

- **Customer Action Items**

- Approve move to production monitoring.

Steady-state Operations – Critical Start MxDR Business As Usual includes the following functions:

- Endpoint Monitoring and Investigation - Vendor will provide continuous endpoint monitoring for client's device(s) 24 hours a day, 7 days a week, across the year. More specifically, tasks include monitoring Agent endpoint deployment to ensure:
  1. Installed agents are online and up-to-date.
  2. Agent licenses are current and operational.
  3. Security events are managed, and remediation has occurred.
  4. Detect, evaluate, classify and prioritize security events to ensure threats are mitigated.
  5. User Policy Violations are managed.
  6. 24 x 7 event monitoring, investigation and response
  7. Access to Vendor v-SOC security analysts to assist in:
     - Identifying threats
     - Rapid response to security events
     - Delivery of timely security event notifications
     - Providing detailed mitigation steps and actionable counter measure recommendations for handling the security event based on information collected from client endpoint devices.
     - Actionable alerts will be prioritized and worked to resolution. Alerts will be delivered to the client in a timely manner notifying customer of potential issues and action responses required when necessary.
- Reporting - The reports to be provided under this service are listed below. Reporting is primarily done via an online report portal. Custom report generation and frequency of report delivery would be decided upon mutual discussion between client & Lenovo during project kickoff meeting.

  Tasks include:
  - Providing online access to current endpoint system reports
  - Online reports are available 24 x 7

  Types of reports available:
  - Threat Summary Reports
  - Threat Detection Reports
  - Device Summary Reports

Move, Add, Changes

What if Something Changes?

Change happens, and that's ok. Critical Start processes and technology are built to scale with customer growth. They have a formal change management process to ensure full visibility and alignment into expectations, capabilities, timelines and performance. Just notify Critical Start regarding the change, and they will advise the customer on the best course of action to keep the cyber protection moving forward. For inquiries, please contact information@criticalstart.com

Cost Components

Unit Definition

The Unit of Definition for Critical Start MxDR Service is per Endpoint or users monitored unless otherwise stated.

Delivery Options

Delivery Model: The Service is delivered remotely from a Critical Start v-SOC depending on the customer region.

Service Level Objectives

Upon the Transition Completion Date Critical Start will perform the Services and begin measuring the performance of the Services in accordance with the below service level objectives.

Service Level Name	Description	Metric	Expected Threshold	Minimum Threshold
Time to Detection & Median Time to Resolution	"TTD & MTTR" are guaranteed in 1-hour or less – no fine print, no extra charge.	Monthly average per incident	60 minutes	60 minutes

Ordering and Billing

- **How to Order** - To order service, New Accounts typically follow an RFP cycle. Existing Accounts can contact their Account Executive or Delivery Manager to create a customer quote. Typical lead time for activation is generally 90 business days.
- **Billing** – Lenovo Managed XDR Service is billed yearly, per device monitored via a Standard Business Rate (SBR) for Business as Usual (BAU) portions of the service.
- **Change and Termination** - Service rates are modified to reflect the new level of service. There is no charge for service termination if it is within the contractual boundaries. Normal service termination requires 60 days advanced notice. Should there be an abnormal contractual termination, only the actual costs incurred will be billed to the account.

- **Transition and Project Costs** - Transition time and labor costs are estimated for each customer IF the customer is unable to provide the required resources for implementation. Actual startup and service transition costs are billed to the customer.

Dependencies and Assumptions

- Services may be performed remotely and using a mix of on and off shore resources as deemed appropriate by Critical Start.
- Critical Start team will be allowed access to the necessary Client facilities during non-business hours.
- Use of Critical Start ticketing and incident management, change management and remediation processes and systems.
- Use of Critical Start's Customer Portal for technical support.

Third Party Partners and Suppliers

Lenovo utilizes Critical Start, Inc. as the Managed Detection and Response Service provider.