# Endpoint Detection and Response – Servers #23-103

The University of Texas at El Paso

**Office of Auditing and Consulting**

”Committed to Service, Independence and Quality”

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
www.utep.edu

January 13, 2023

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services has completed a limited-scope audit of *Endpoint Detection and Response–Servers*. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in a separate management letter. We intend the recommendations will assist the department in strengthening controls and help ensure that the University's mission, goals, and objectives are achieved.

We appreciate the cooperation and assistance provided by the Data Center Operations and Information Security Office staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

# EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of Endpoint Detection and Response (EDR)–Servers to determine adherence to State and University security controls and standards. Due to the confidential nature of the audit, we issued a separate management letter which details specific findings and recommendations. These confidential results are exempt from the Texas Public Information Act under Texas Government Code §552.139.

## Background

Data Center Operations (DCO) deployed SentinelOne's Endpoint Detection and Response (EDR) technology to approximately 600 University servers as part of its multi-layered security posture to better detect and respond to cyber threats in an automated manner. Using a three-month look back period (as of November 14, 2022), EDR detected and alerted the Information Security Office (ISO) to 275 threats. Of these, 272 were resolved as of this date, with the other three servers quarantined by EDR and awaiting action from ISO before bringing them online.

The audit was conducted by the Institute of Internal *Auditors' International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards.*

## Audit Objectives and Scope

Determine if (i) the EDR solution has been effectively deployed to current and new servers, (ii) proper administration and safeguards of the EDR solution are in place, and (iii) monitoring activities are in place to detect and respond to potential malicious activity. The scope of the audit is limited to (a) servers and (b) the test period from September 1, 2021, to November 4, 2022.

## Strengths

A leading third-party cyber security consultant has been engaged by the University to assist in various capacities, including EDR monitoring, triaged alerting, and escalation. An effective threat response and mitigation process has been established.

## Summary of Audit Results

| Endpoint Detection and Response Solution–Deployment Administration | Number of Findings |
|---|---|
| A. Completeness and Accuracy of Endpoint Detection Response Deployment for Servers | 3 |
| B. Administration and Safeguards of the Endpoint Detection Response Solution for Servers **(Resolved)** | 1 |
| C. Monitoring of the Endpoint Detection Response Solution for Servers | 0 |

## Conclusion

Based on the audit procedures performed, we conclude that DCO and the ISO can strengthen existing security controls by implementing the recommendations included in this memo.

We wish to thank the management and staff at DSO and the ISO for their assistance and cooperation throughout the audit.

## Report Distribution:

**University of Texas System (UT System):**
System Audit Office

**External:**
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office

**Auditor Assigned to the Audit:**
Ms. Victoria Morrison