SightGain.ai

AI-Powered Cybersecurity Solution Performance Report: EDR-X

(Healthcare Industry)

Executive Summary

This assessment provides an evaluation of EDR-X, an AI-powered Endpoint Detection and Response (EDR) solution. The testing focused specifically on prevalent cybersecurity threats facing the healthcare industry, such as ransomware, targeted phishing, unauthorized access to sensitive health records, insider threats, and Advanced Persistent Threats (APTs). EDR-X demonstrated significant strengths in threat detection and prevention but also revealed areas needing improvement, particularly in persistence detection and lateral movement prevention. Overall, EDR-X exhibited strong capabilities suited to the healthcare sector, showing above-average performance in critical threat mitigation.

Overall Performance: Slightly Better Than Industry Average

Assessment Scope

The assessment simulated cybersecurity threats specifically relevant to the healthcare industry, evaluating EDR-X's AI-driven threat detection, prediction, and response capabilities against a benchmark representing category averages.

Threat Profile: Healthcare Industry

Key cybersecurity threats evaluated include:

- **Ransomware:** LockBit, Hive
- **Credential Theft:** Unauthorized access to Electronic Health Records (EHR)
- **Insider Threats:** Intentional and accidental disclosures
- **Advanced Persistent Threats (APTs):** Targeting patient data and research
- **Third-Party/Vendor Risk:** Exploiting vendor system vulnerabilities

Threat scenarios were prioritized based on frequency, impact, and likelihood in healthcare environments.

EDR-X Solution Overview

- **Vendor:** EDR-X

- **Key AI-driven Capabilities:**
  - Behavioral analytics
  - Predictive threat detection
  - Real-time anomaly detection

Assessment Methodology

Testing was conducted in a controlled environment emulating healthcare-specific cyber threats aligned with the MITRE ATT&CK framework. Results were scored by the percentage of threats blocked, detected, and an overall success ratio, comparing EDR-X performance to category averages.

Performance Summary

EDR-X's performance was compared against the industry category average across prioritized MITRE ATT&CK tactics:

Tactic	EDR-X Success Ratio	Category Avg.
INITIAL ACCESS	**85%**	79%
EXECUTION	**89%**	84%
PERSISTENCE	62%	**72%**
PRIVILEGE ESCALATION	**83%**	78%
DEFENSE EVASION	**75%**	70%
CREDENTIAL ACCESS	**90%**	86%
DISCOVERY	**77%**	75%
LATERAL MOVEMENT	58%	**67%**
COLLECTION	**80%**	76%
EXFILTRATION	**82%**	78%
COMMAND AND CONTROL	**88%**	83%
IMPACT	**87%**	81%

Top Strengths:

- Credential Access
- Command and Control
- Execution

Areas for Improvement:

- Persistence
- Lateral Movement

MITRE ATT&CK Tactic Detailed Results

Initial Access

- **Description:** Threat actors gain initial foothold in systems.
- **Blocked:** 60% | **Detected:** 77% | **Overall:** 85%
- EDR-X slightly outperformed category average, demonstrating robust entry-point protection relevant to phishing and malware delivery methods.

Execution

- **Description:** Execution of malicious code on systems.
- **Blocked:** 65% | **Detected:** 81% | **Overall:** 89%
- Strong AI analytics enhanced detection rates.

Persistence

- **Description:** Threat actors maintain presence in compromised systems.
- **Blocked:** 45% | **Detected:** 58% | **Overall:** 62%
- Underperformed against category average; requires improved model training for persistence methods.

Privilege Escalation

- **Description:** Attackers escalate their system privileges.
- **Blocked:** 58% | **Detected:** 75% | **Overall:** 83%
- Strong AI capabilities effectively identified unauthorized privilege escalations, outperforming the category average.

Defense Evasion

- **Description:** Techniques used to evade detection or defenses.
- **Blocked:** 50% | **Detected:** 71% | **Overall:** 75%
- Slightly above average, showing reliable AI-driven detection but opportunities remain for improvement in evasion tactic identification.

Credential Access

- **Description:** Techniques to steal credentials.
- **Blocked:** 70% | **Detected:** 81% | **Overall:** 90%
- Significantly exceeded category performance, indicating strong prevention and detection capabilities critical to healthcare data security.

Discovery

- **Description:** Techniques to gain knowledge about the system.
- **Blocked:** 52% | **Detected:** 70% | **Overall:** 77%
- Adequate performance, aligning closely with the category average, effectively identifying common discovery techniques.

Lateral Movement

- **Description:** Techniques to move through compromised networks.
- **Blocked:** 40% | **Detected:** 48% | **Overall:** 58%
- Notably below average; recommendations include enhancing integration with network monitoring to improve detection.

Collection

- **Description:** Techniques to gather data of interest.
- **Blocked:** 55% | **Detected:** 67% | **Overall:** 80%
- EDR-X effectively detected common data collection techniques, outperforming industry benchmarks.

Command and Control

- **Description:** Techniques attackers use to communicate with compromised systems.
- **Blocked:** 63% | **Detected:** 75% | **Overall:** 88%
- Very strong performance, highly effective AI analytics in detecting communication with external threats.

Exfiltration

- **Description:** Techniques to remove stolen data from systems.
- **Blocked:** 57% | **Detected:** 65% | **Overall:** 82%
- Exceeded average performance, crucial for healthcare data protection.

Impact

- **Description:** Techniques disrupting systems or data.
- **Blocked:** 65% | **Detected:** 72% | **Overall:** 87%
- Significantly above average, providing effective protection against high-impact threats like ransomware.

Key Security Strengths

EDR-X excels in preventing and detecting credential theft, command and control operations, and malicious code execution—crucial for healthcare data protection.

Key Areas for Improvement

EDR-X demonstrated vulnerability in detecting persistence and lateral movement tactics. Enhanced machine learning algorithms and enriched datasets focusing on these tactics are recommended.

General Recommendations and Observations

- Enhance AI training datasets specific to persistence and lateral movement.
- Strengthen integration with network security controls to bolster lateral movement prevention.
- Continuous model updates recommended to handle evolving ransomware behaviors.

Glossary of Key Terms

- **Overall:** Threat action was blocked or detected.
- **Blocked:** Threat action was actively prevented.
- **Detected:** Threat action was identified but not necessarily prevented.
- **AI Model Efficacy:** Effectiveness of predictive models.
- **Mean Time to Detect (MTTD):** Average time taken to identify threats.
- **Mean Time to Respond (MTTR):** Average time taken to respond effectively to threats.
- **Electronic Health Records (EHR):** Digital versions of patients' paper charts.
- **Protected Health Information (PHI):** Individually identifiable health information.

Details of specific threat simulations and methodologies available upon request.