

# PREDICTPATH AI

## Cyber Security Strategic Audit Report

*Generated: February 20, 2026 16:18:41 UTC*

CONFIDENTIAL - SOC AUDIT DOCUMENTATION

## 1. EXECUTIVE SUMMARY

This report summarizes a comprehensive cyber defense lifecycle conducted by the PredictPath AI suite. The analysis covers threat identification (Tool 2/3), strategic response planning (Tool 4), automated remediation generation (Tool 5), and governance oversight (Tool 6). All identified high-probability threats have been processed through the mitigation engine.

## 2. THREAT ANALYSIS & FORECASTING

### **Analysis Target: Activity on <https://learning-digitech.vercel.app/>**

Captured Weaknesses: CWE-1021, CWE-20, CWE-525, CWE-284, CWE-287, CWE-693, CWE-615, CWE-264, CWE-78, CWE-200

### **Analysis Target: Activity on <https://learning-digitech.vercel.app/assets/index-bkkz15b8.css>**

Captured Weaknesses: CWE-525, CWE-284, CWE-287, CWE-693, CWE-264, CWE-200

### **Analysis Target: Activity on <https://learning-digitech.vercel.app/assets/index-d1dhjboy.js>**

Captured Weaknesses: CWE-284, CWE-287, CWE-693, CWE-615, CWE-264

### **Analysis Target: Activity on <https://learning-digitech.vercel.app/robots.txt>**

Captured Weaknesses: CWE-525, CWE-284, CWE-287, CWE-693, CWE-264, CWE-200

### **Analysis Target: Activity on <https://learning-digitech.vercel.app/sitemap.xml>**

Captured Weaknesses: CWE-20, CWE-525, CWE-284, CWE-287, CWE-693, CWE-615, CWE-264, CWE-78, CWE-89, CWE-200

## 3. RECOMMENDED MITIGATION STRATEGIES

### **ACTION: Isolate Host on learning-digitech.vercel.app**

*Tactical Steps: Disconnect host from all internal and external networks. | Retain network for forensic connection to management console only. | Scan all other hosts in the same segment for persistence.*

## 4. REMEDIATION IMPLEMENTATION

## Generated Remediation Package:

Final Artifact: PredictPath\_Remediation\_20260220\_120200.ps1

Status: Context-Aware PowerShell Script & Tactical Guideline Generated.

## 5. GOVERNANCE POSTURE & TAKEAWAYS

### System Trust State:

*Active Model Version: v4a566c39*

*Containment Threshold: 54.0%*

### Key Security Takeaways:

1. Attack Surface: The system successfully identified critical vulnerabilities (CWE-based) on public-facing assets.
2. Defense Response: Pre-emptive host isolation and process auditing were recommended to neutralize execution threats.
3. Operational Status: All critical remediation steps are now documented in the deployments folder for SOC review.
4. Continuous Monitoring: Post-remediation trust levels have been adjusted to account for current threat density.