

# PREDICTPATH AI

## Cyber Security Strategic Audit Report

Generated: February 23, 2026 15:32:11 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 172.20.192.1

Captured Weaknesses: None Identified

#### Analysis Target: Activity on System

Captured Weaknesses: CWE-89, CWE-285, CWE-78, CWE-20, CWE-77, CWE-306, CWE-94, CWE-434, CWE-284, CWE-200

### 3. RECOMMENDED MITIGATION STRATEGIES

#### ACTION: Isolate Host on Unknown

*Tactical Steps: Disconnect host from all internal and external networks. | For Cloud/Web assets: Suspend deployment or enable 'Maintenance Mode' in console. | Scan all other hosts in the same segment for persistence.*

#### ACTION: Enable Process Auditing on Activity on 172.20.192.1

*Tactical Steps: Activate Sysmon or similar tool to track process creation. | Review command-line arguments for suspicious encoded strings. | Monitor for unauthorized use of living-off-the-land (LotL) binaries.*

### 4. REMEDIATION IMPLEMENTATION

#### Generated Remediation Package:

Final Artifact: PredictPath\_Remediation\_20260223\_123202.ps1

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

### 5. GOVERNANCE POSTURE & TAKEAWAYS

#### System Trust State:

Active Model Version: vd4cf1991

Containment Threshold: 40.0%

#### Key Security Takeaways:

1. Attack Surface: Identified 10 distinct vulnerability matches across the analysis targets.
2. Defense Response: Generated 2 validated remediation actions covering Enable Process Auditing, Isolate Host.
3. Operational Status: Remediation package 'PredictPath\_Remediation\_20260223\_123202.ps1' is staged for SOC deployment.
4. Continuous Monitoring: System trust is relaxing based on a success streak of 6 sessions.