Harmonia Incident Response

Threat Intelligence Report - Executive

Executive Summary

This report provides a comprehensive analysis of threat intelligence data collected over the past 7 days. The analysis covers 13 threat indicators from multiple sources including MITRE ATT&CK; and CISA KEV catalog.

Key Metrics

Metric	*Value*
Total Indicators	13
Average Severity	5.69
High Severity Indicators	3
Most Common Type	MITRE Technique
Most Active Source	MITRE ATT&CK;

Threat Analysis

Threat Analysis Summary: Total Indicators Analyzed: 13 Average Severity Score: 5.69/10 High Severity Threats (≥7): 3 (23.1%) Most Common Threat Type: MITRE Technique (10 instances) Key Findings: • 3 high-severity threats require immediate attention • Average threat severity of 5.69 indicates moderate overall risk • MITRE Technique threats are the most prevalent, suggesting focused defense needed Recommendations: • Prioritize response to high-severity threats • Implement specific defenses against MITRE Technique threats • Consider threat hunting for related indicators • Review and update security controls based on threat patterns

Top Threats by Severity

Name	*Type*	*Severity*	*Source*
FortiOS	CVE Vulnerability	8.0	CISA KEV Catalog

DIR-859 Router	CVE Vulnerability	8.0	CISA KEV Catalog
MegaRAC SPx	CVE Vulnerability	8.0	CISA KEV Catalog
Data Obfuscation	MITRE Technique	5.0	MITRE ATT&CK;
Data Compressed	MITRE Technique	5.0	MITRE ATT&CK;
OS Credential Dumping	MITRE Technique	5.0	MITRE ATT&CK;
Winlogon Helper DLL	MITRE Technique	5.0	MITRE ATT&CK;
Data from Local System	MITRE Technique	5.0	MITRE ATT&CK;
File System Logical Offsets	MITRE Technique	5.0	MITRE ATT&CK;
System Service Discovery	MITRE Technique	5.0	MITRE ATT&CK;

Recommendations

Security Recommendations: 1. Immediate Actions: • Review and respond to all high-severity threats • Update threat detection rules based on observed patterns • Conduct threat hunting for related indicators 2. Strategic Improvements: • Enhance monitoring for most common threat types • Implement additional security controls where gaps exist • Develop incident response playbooks for observed threats 3. Long-term Planning: • Regular threat intelligence updates and analysis • Continuous improvement of security posture • Staff training on emerging threats and response procedures