Unknown Cyber: Revolutionizing Digital Forensics and Incident Response with AI-Powered Genomic Analysis

www.unknowncyber.com

Digital Forensics and Incident Response (DFIR) teams face increasingly sophisticated cyber threats that traditional analysis tools struggle to address effectively. Unknown Cyber transforms this landscape by leveraging AI-driven cyber genomics—a DARPA-validated approach that dissects malware into its functional DNA at the bytecode level. This revolutionary platform automates what typically requires days or weeks of expert analysis, delivering instant malware triage, deep attribution, and genomic function comparison.

Core Technology: Cyber Genomics

At the heart of Unknown Cyber's innovation is its ability to scan and match functional components of code even when heavily obfuscated. By analyzing malware down to its genetic makeup, the platform can identify relationships between samples that share common code fragments—even when surface-level indicators have been altered. This approach proves particularly valuable against polymorphic threats that continuously change their appearance while maintaining core functionality.

Automated Reverse Engineering

Automatically unpacks, deobfuscates, and analyzes malware to the bytecode function level—eliminating hours of manual work even with polymorphic or packed threats.

Memory Dump Analysis

Extracts malware genomics directly from memory dumps, enabling detection of fileless malware—a critical capability for advanced threats.

Genomic YARA Rules

Generates high-precision detection rules based on function-level code patterns rather than superficial strings, creating durable signatures that catch future malware variants.

Operational Advantages

Instant Malware Triage

Upload any suspect file for immediate verification against known malware families without requiring sandboxing, dramatically accelerating initial assessment.

Variant and Campaign Correlation

Identifies malware across campaigns using shared functions—even when code is behaviorally dormant or deliberately obfuscated.

Forensic-Grade Evidence

Produces explainable findings with complete code provenance, providing defensible evidence suitable for litigation and expert witness testimony.

Versatile Deployment Options

Field-deployable toolkit with no cloud dependency for sensitive environments, including disconnected, classified, or critical infrastructure settings.

Advanced Capabilities

Unknown Cyber includes JUCY Sandbox, an interactive environment that combines real-time behavioral analysis with static genomic insights. This gives analysts hands-on control. Additionally suppported are hypervisor unpacking and URL queries. The platform is designed for collaboration, allowing teams to tag, comment, and share findings while preserving organizational knowledge. Previous investigations can be mapped through code down to the function level, eliminating duplicate work even when analyzing new, obfuscated binaries.

For organizations with operational technology (OT) concerns, Unknown Cyber offers specialized capabilities for analyzing firmware, embedded devices, and ICS/SCADA components without requiring source code or behavior replay. This makes it uniquely suited for critical infrastructure environments where attacker implants increasingly utilize fileless, persistent techniques.

By consolidating functionality that would typically require multiple specialized tools—VirusTotal, sandboxes, IDA, Ghidra—Unknown Cyber streamlines the entire investigation workflow from initial file upload to IOC generation, delivering unmatched speed, depth, and accuracy that provides confidence to DFIR teams and their customers.