BlockChain Security

chainsecurity.asia

eDetector

Real-time,Efficient,Automatic

eDetector is a cutting-edge endpoint digital forensic and evidence collection system designed for cybersecurity investigations, honored with multiple awards, including the Ministry of Economic Affairs Innovation Award.

Automated Forensic Analysis

1.Malware Detection

2.Dynamic Behavior Analysis

AI-Powered Report Generation

1.Integration of Various AI Technologies

2.Support for Large-Scale Malware Databases

YARA Scanning Technology

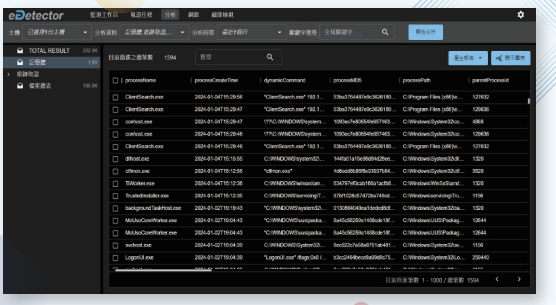
1.YARA Support Implementation

2.Rapid Malware Identification

Cloud Scalable Architecture

1.High Availability and Scalability

2.Multi-Endpoint Forensic Collection and Correlation Monitoring



"By combining memory detection and behavioral artifact analysis, eDetector quickly identifies malicious activities such as code injection, hidden programs, core interception, and connection history. It detects suspicious actions and provides root cause analysis of attacks. The system also generates process correlation maps and marks source IPs, helping users gain a comprehensive view of incidents."

BCS dedicate ourselves to create client-focus solutions based on innovation, integrity, and sustainability

eDetector

A More Comprehensive Digital Forensic Solution

Multi-Mode and Easy Deployment

The cloud version supports cross-machine management and forensic analysis, while the local version is designed for on-premises security needs. Agent deployment is fast and supports large-scale simultaneous installation for up to 500 devices.

Efficient Forensic Collection and Threat Analysis

Supports the collection of over 40 types of digital evidence and detection of unknown threats. Dynamic behavior tracking quickly identifies potential risks and generates analysis reports.

Forensic Collection and Analysis

- Supports the collection of over 40 types of digital evidence, including browser history, USB device information, program network traffic, DNS information, and Windows activities.
- High-speed search capabilities allow scanning of millions of records within seconds, providing real-time file listings and dynamic data retrieval.
- Integrates AI technology and the VirusTotal database to generate rapid analysis reports, capturing malware characteristics and source information.

Threat Detection and Protection

- Supports dynamic detection of unknown malware, identifying potential threats through memory analysis and behavior tracking.
- Provides process tree diagrams, loaded module and DLL lists, and marks program connections and source IPs for quick identification of malicious activities.
- Integrates Yara scanning technology to efficiently filter malware characteristics and pinpoint potential risks.

Cloud Scalability and Management

- Provides stable cloud services with flexible storage expansion, ensuring data confidentiality, integrity, and availability.
- Security personnel can monitor cross-machine operations and manage task progress via a web interface, enhancing operational convenience.
- The visualized timeline feature allows for quick review and analysis of data insights.

About BlockChain Security

Founded in 2018, by industry experts with over 17 years in digital forensics, evidence preservation and information security. We noticed the gap of blockchain adaptations and began our mission to combine two core technologies; blockchain and information security.

chainsecurity.asia service@chainsecurity.asia +886 2 2515-2533