CyberCase
Record, Detect, Protect

WHITEPAPER
CYBERCASE
MONITORING

THE ULTIMATE SECURITY SOLUTION

Cybercase redefines security with cutting-edge technology designed to empower cybersecurity teams and network administrators

CODEVALUE

www.codevalue.com

CODEVALUE

The Problem CyberCase Solves

Organizations increasingly struggle with limited visibility, slow investigations, and operational constraints caused by complex security architectures.
CyberCase was built to address these challenges by offering instant deployment, full on-premise operation, and deep, unified visibility — regardless of network size or sensitivity.

- Common challenges include:
- Fragmented tools that provide only partial visibility
- Long deployment times during incidents
- Dependence on cloud-based systems where data cannot leave the environment
- Inability to monitor air-gapped, sensitive, or temporary networks
- Difficulty correlating network, endpoint, and physical security data during investigations

CyberCase was built to address these challenges by offering **instant deployment**, **full on-premise operation**, and **deep**, **unified visibility** — regardless of network size or sensitivity.

How is CyberCase Used?

CyberCase is designed to support two primary operational modes, using the same hardware and platform:

- **Continuous Monitoring** (SIEM-like)
- **Rapid Investigation** & **Temporary Monitoring**

Who Is CyberCase For?

- **Internal IT and security teams** requiring continuous network visibility
- **Incident response and forensic teams** performing rapid investigations
- **Enterprises and service providers** needing flexible, agentless monitoring
- **Critical infrastructure and operational environments** with strict security or air-gap requirements
- **Law enforcement and government organizations** conducting on-site digital investigations
- **High-security environments** where data must remain fully on-premise

A Suitcase for any Cyber Scenario

Comes with everything needed for monitoring the network:

CyberCase machine — A high-quality industrial level machine with 2 rj45 ports and 2 optical ports.

Lapdock — A portable device with a screen, keyboard, and trackpad for accessing CyberCase.

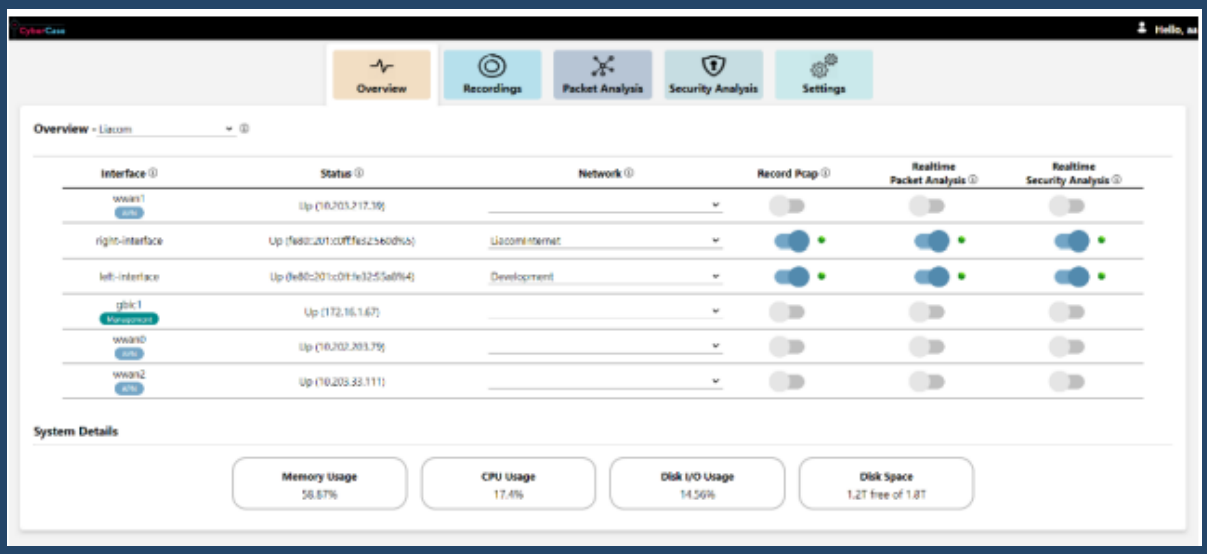
Network Tap — A high-quality network tap allows to mirror traffic from real networks to the CyberCase port without interfering within the traffic.

External Hard Drive — Certified hard drive for copying/moving the CyberCase gathered data.

Led USB stick — Lights indicator displaying the status of the CyberCase.

Cables

- **User Manual**

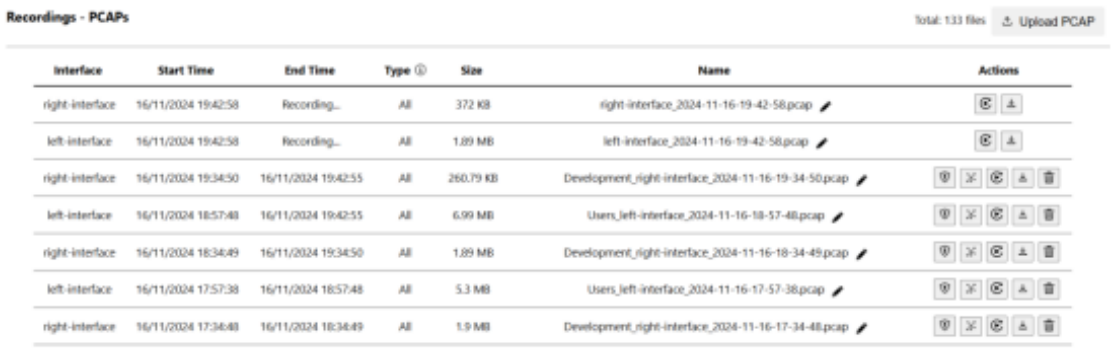


Recording Traffic

Three Recording Modes offers flexibility to choose from three recording modes:

- **All Traffic:** Capture all the data on your network
- **Only Headers:** Capturing only header information
- **Smart Recording:** Record all traffic for unencrypted protocols and headers only for encrypted.

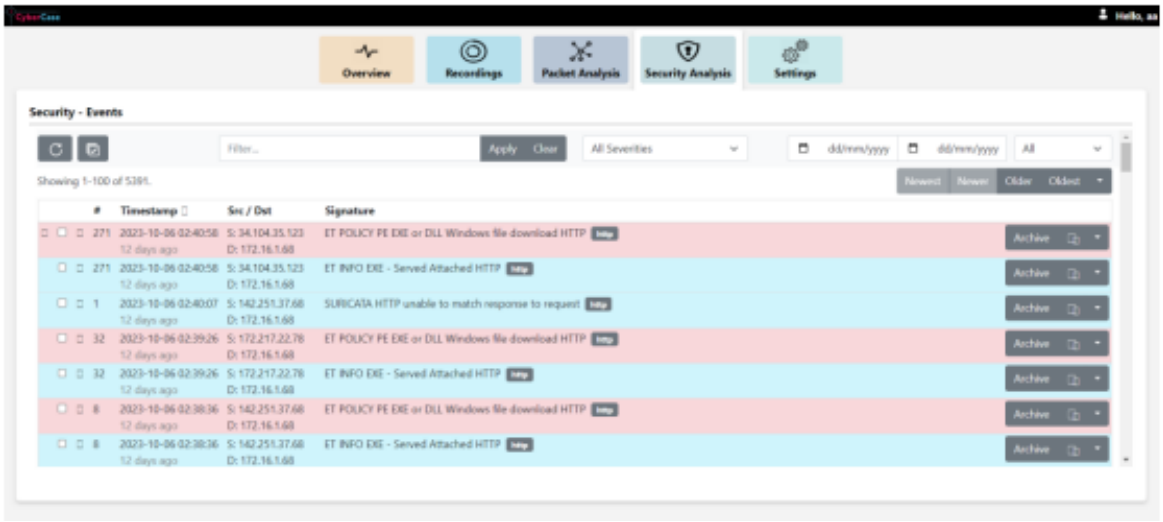
A de-duplicate feature is available to remove duplicate packets.



The recorded traffic can be downloaded, sent for analysis or replayed.

Analysis & Visibility

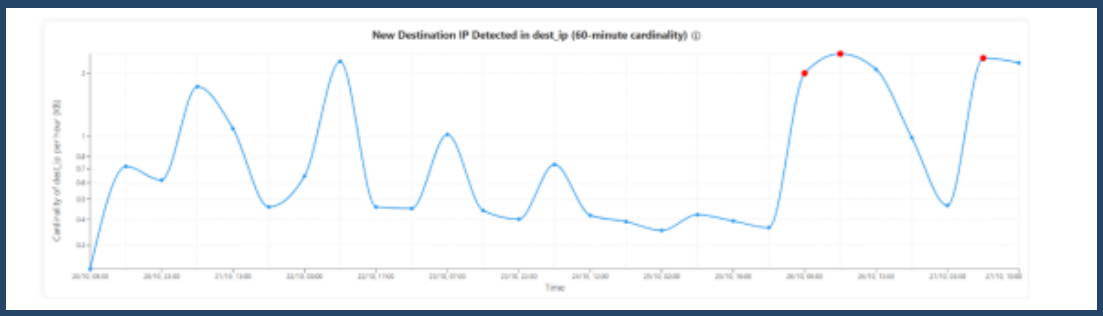
Packet Analysis: Dive deep into packet-level details and obtain in-depth insights.
Security Analysis: Enhance your network's security with advanced analysis tools



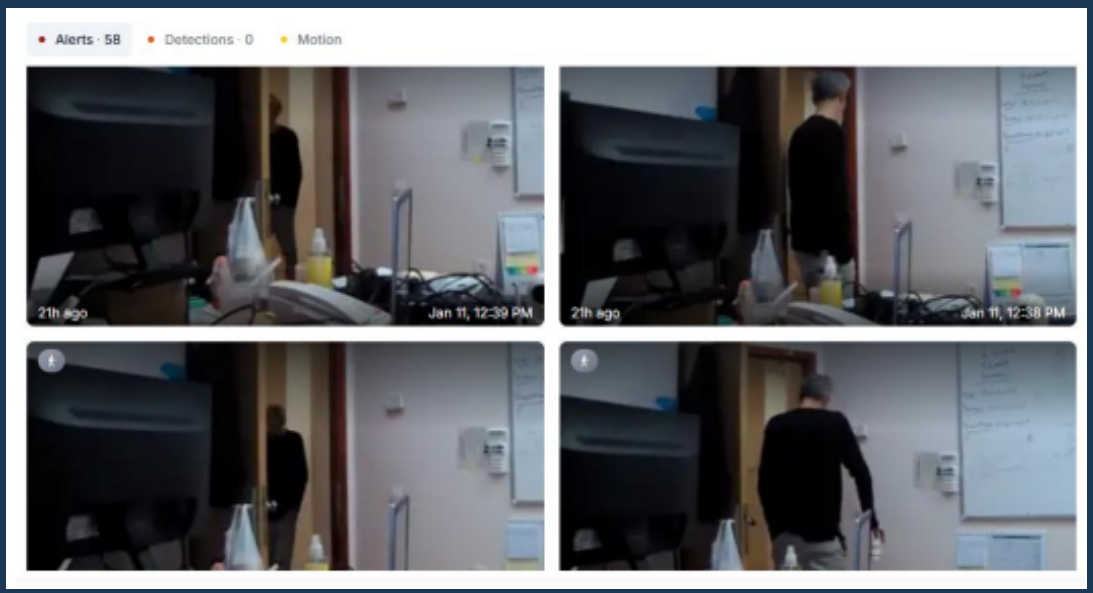
Logs & Endpoint Monitoring: Collect and analyze logs from various sources (endpoints and network equipment via syslog). File integrity monitoring, vulnerability detection, security configuration assessment, and real-time threat detection.

Network Mapping: Visualize connections, dependencies and traffic flow

Rule Management: Prioritize key issues by filtering or ignoring irrelevant alerts.
Anomaly Detection: It trains based on your organization's real data and then detects anomalies.



Camera Integration: Connect and analyze existing security cameras with AI-powered object detection and alert detection. Search and filter footages by keywords (people, gestures, etc).

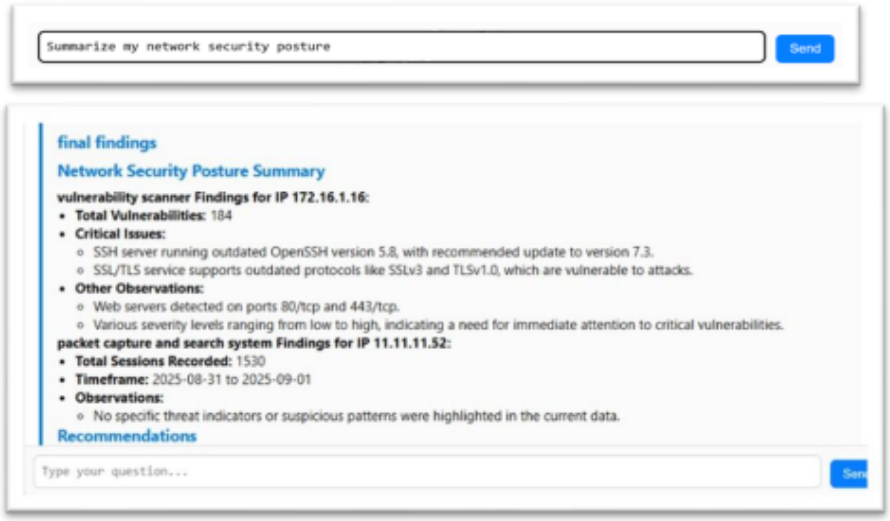


Offline PCAP Upload and Analysis: Easily upload PCAP data from external sources for comprehensive packet analysis and security insights

AI Investigator

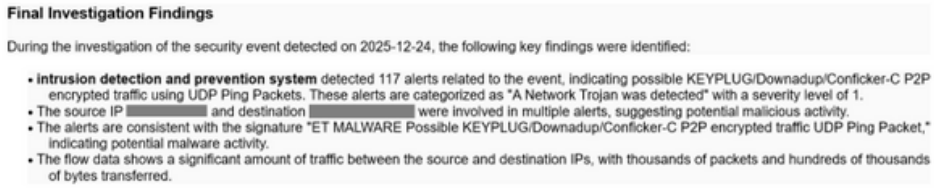
Your Built-In Cybersecurity Assistant – Connecting physical and digital security

Chatbot and auto-event researcher using a smart AI Agent. Ready to perform any investigation for you while correlating between multiple data sources:



Actions on Security Alerts

Notifications: Sending security alerts or anomalies by syslog or by email (can include AI analysis):



Auto-record: Start recording traffic right away after a security alert is detected.

External Management

Syslog & Web API Support – Seamlessly transfer data to remote servers or SIEMs.
External Device Management – Export analysis results or logs directly to external devices.

System Health Monitoring

Ensure Your Machine's Well-Being in the long term with health monitoring

Comprehensive Monitoring: CyberCase now provides more accurate and consistent monitoring and automatic troubleshooting of all its services, storage and machine's status**. Error Notifications:** In case of a health issue – the user will be notified by email.

Flexible Hardware

Fit any client needs:

Rack Server Option – A constant option to fit in the server room.
High Bandwidth – Multiple ports with high bandwidth.
Cellular Modems – Up to 3 cellular modems for monitoring APN or for remote alerts.
GPIO – Monitoring digital/analog Inputs or using it for custom alerts.
On-Premise LLM – Empowering Ollama for local AI Agent.

Real-World Use Cases

Policy Violation Detection

In one deployment, CyberCase was connected to a client's network and immediately identified unauthorized IPv6 traffic that violated organizational policy. The issue had gone undetected by existing tools due to partial visibility and configuration blind spots.

infected Endpoint Discovery

IUsing CyberCase built-in AI analysis capabilities, another organization discovered malicious domain communication originating from within the network.

The AI Investigator:
• Flagged abnormal DNS and traffic patterns
• Identified a malicious external domain in use
• Correlated network traffic with endpoint logs
• Pinpointed the infected endpoint responsible for the communication

This enabled the security team to isolate the endpoint quickly and prevent further compromise.

Root Cause Analysis of Network Failures

An organization that deployed CyberCase as a permanent monitoring solution used it to investigate recurring network instability issues that traditional monitoring tools failed to explain. Through long-term traffic recording, anomaly detection, and network mapping, CyberCase:

- **Revealed abnormal traffic flows and configuration inconsistencies**
- **Correlated events across network devices and logs**
- **Identified the root cause of the organization's recurring networking failures**

This allowed the organization to permanently resolve the issue and improve overall network reliability

Why CyberCase Is Different

Plug & Play
CyberCase can be deployed in minutes without installing agents, modifying network architecture, or relying on existing infrastructure**.**

Fully On-Premise & Offline-Capable
All data collection, analysis, and AI-driven investigation can run entirely on-premise. This makes CyberCase suitable for air-gapped, classified, or high-sensitivity environments.

Digital to Physical Unified Security CyberCase correlates network traffic, logs, endpoints, and camera data within a single investigation platform — enabling analysts to connect cyber events with physical-world activity**.**

Built-In AI Investigator
An on-prem AI agent assists analysts by correlating events, identifying anomalies, and accelerating investigations — without exporting data to the cloud**.**

Non-Intrusive Monitoring
Passive traffic capture via network taps ensures zero impact on production traffic and eliminates deployment risk**.**

One Platform for Incidents and Continuous Monitoring
CyberCase supports short-term investigations, breach response, and long-term monitoring with the same platform and hardware.

👉 **Request a Demo or Discovery Call**

info@codevalue.com
www.codevalue.com