CLUE
CYBER SECURE

Cyber Defense Hub

The Blind Spot

How long would it take you to notice a cyberattack? In many organizations, the problem isn’t a lack of technology—it’s a lack of clarity. Without real visibility into what is actually happening, threats are detected too late. Delays cost time, money, and trust. Effective security requires decisions built on reliable information.

The Control

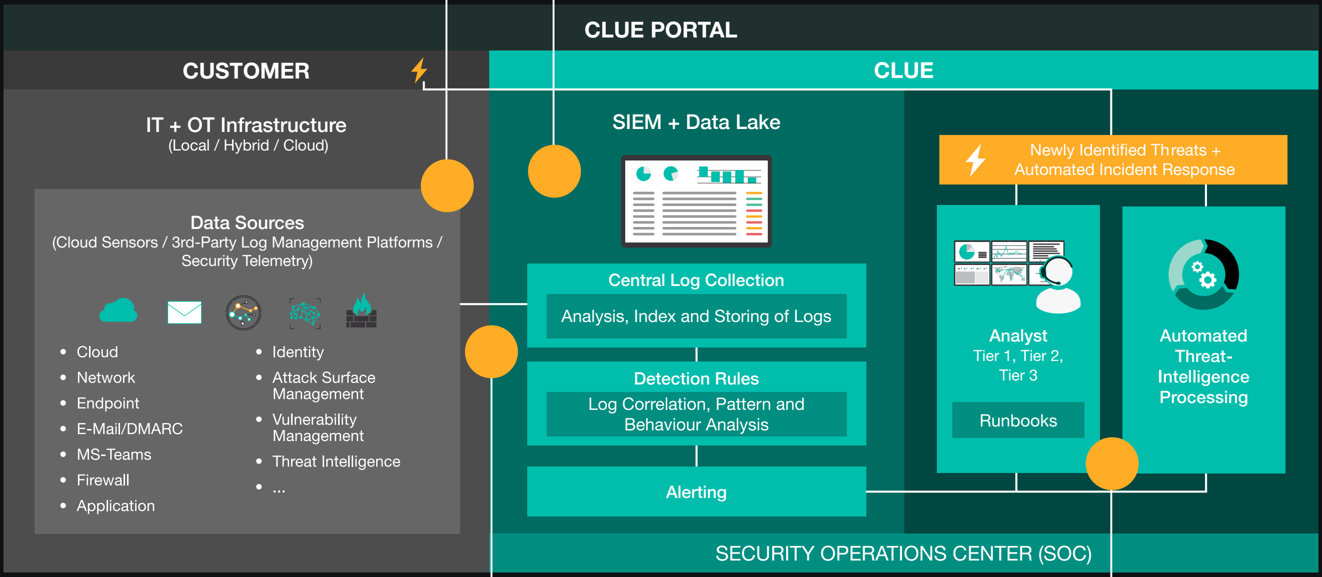
The Cyber Defense Hub turns data into actionable insight. Through centralized analysis and 24/7 monitoring, it provides full visibility across your IT and OT environments. Threats are not just detected, but understood—so you can respond with precision. Decision-Ready Security: Turning data into decisions.

DATA INTEGRATION

Log and telemetry data from a wide variety of sources (cloud, network, endpoints, email, firewalls, etc.) converge in the Cyber Defense Hub.

CENTRALIZED PROCESSING

Data collected in the SIEM and data lake is analyzed, indexed, and stored. Detection rules correlate events to identify patterns and anomalous behavior.



CLUE PORTAL

CUSTOMER

IT + OT Infrastructure
(Local / Hybrid / Cloud)

Data Sources
(Cloud Sensors / 3rd-Party Log Management Platforms / Security Telemetry)

- Cloud
- Network
- Endpoint
- E-Mail/DMARC
- MS-Teams
- Firewall
- Application

- Identity
- Attack Surface Management
- Vulnerability Management
- Threat Intelligence
- ...

CLUE

SIEM + Data Lake

Central Log Collection
Analysis, Index and Storing of Logs

Detection Rules
Log Correlation, Pattern and Behaviour Analysis

Alerting

Newly Identified Threats + Automated Incident Response

Analyst
Tier 1, Tier 2, Tier 3

Runbooks

Automated Threat-Intelligence Processing

SECURITY OPERATIONS CENTER (SOC)

TRANSPARENCY

The volume of processed data and its billing are calculated transparently based on events per second (EPS).

ANALYSIS AND RESPONSE

Alerts are reviewed and handled by analysts across multiple tiers in accordance with defined runbooks. When suspicious activity or attack attempts are identified, the customer is informed accordingly. Where possible, threats are neutralized automatically through threat intelligence–driven processes.

CLUE
CYBER SECURE

Benefits

What sets us apart as a security partner.

HUMAN EDGE

CLUE combines technology with direct access to experts, enabling fast, well-informed decisions by experienced analysts.

- AI-driven threat detection for greater precision
- Automated processes to accelerate response times
- Flexible integration of a wide range of data sources
- Billing based on events per second (EPS) for full cost transparency

OT-SPECIALIZATION

OT environments require a distinct security mindset: production processes and control systems must not be disrupted. CLUE brings this experience to the table.

- Proven expertise in smart buildings, manufacturing, and critical infrastructure
- Unified sensor technology for IT and OT
- Collaboration with leading industry experts
- Active involvement in specialist groups within industry associations

EFFICIENCY AND TRANSPARENCY

Instead of overwhelming alert noise, CLUE delivers only information that truly matters—clearly structured and fully traceable at any time.

- Reduction of false positives and unnecessary alerts
- Focus on real threats and suspicious activity
- Solution designs that balance efficiency and cost
- Detailed insights and reports in the CLUE portal

Features

The technical elements of our approach.

Proactive Threat Hunting

Goes far beyond traditional, reactive alerting and also detects new types of threats at an early stage.

Technology-Agnostic

Integration of both CLUE services and third-party tools to make the most of existing investments.

SOAR-Functionality

Enables granular interventions, including automated blocking of suspicious traffic in real time.

Automated Reporting

Simplifies compliance requirements while creating transparency for management and audits.

Extended Data Retention

Strengthen endpoint defenses with centrally managed firewall rules, restricting unwanted connections effectively.

Standard-Compliant

Combined with other CLUE services, almost all requirements of the ICT minimum standard and the NIST CSF are met.

24/7 Business **needs 24/7 Security.**

Experience 24/7 protection with the Cyber Defense Hub.

+41 44 667 77 66 | info@clue.ch | clue.ch