CLUE
CYBER SECURE

AI Based Threat Detection

The Blind Spot

Traditional security tools rely on known attack patterns and predefined rules. Modern attackers continuously adapt, using social engineering, compromised identities, and subtle behavioral changes that by pass signature-based detection. This creates blind spots where threats remain unnoticed until damage has already occurred.

The Control

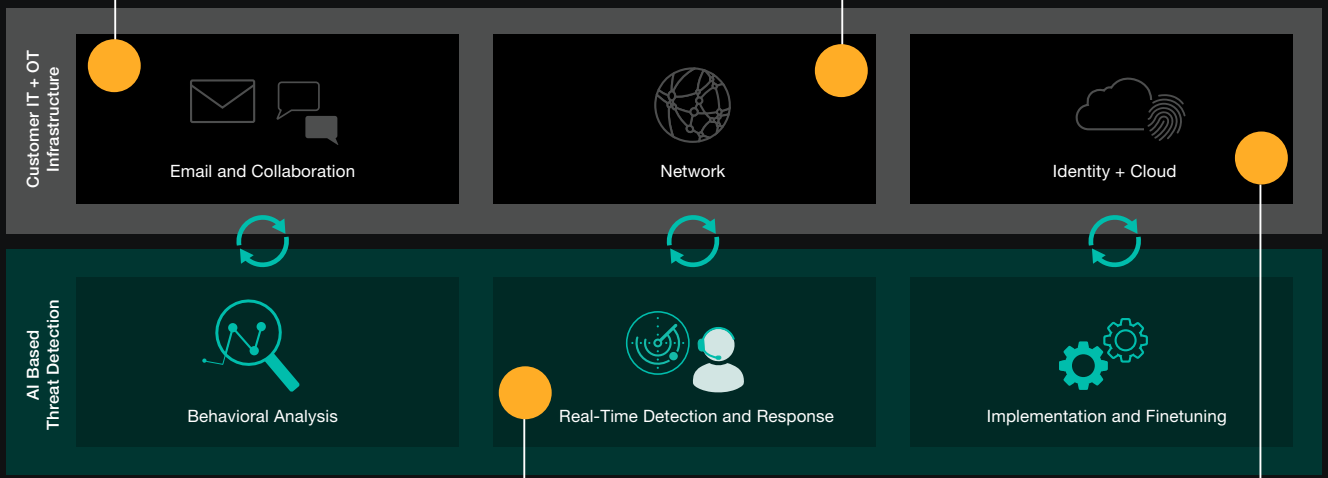
AI-Based Threat Detection identifies abnormal behavior across email, network, and cloud environments by understanding what is normal for users, devices, and systems. This enables early detection of known and previously unseen threats, allowing targeted response actions that stop attacks before they escalate — without disrupting business operations.

EMAIL SECURITY

Protects email and collaboration platforms (e.g. Microsoft 365, Teams) from phishing, business email compromise, and malicious communication campaigns. Suspicious content can be contained without disrupting daily workflows.

NETWORK SECURITY

Monitors network environments across on-premise, hybrid, and remote infrastructure to uncover abnormal traffic, lateral movement, and command-and-control activity.



AUTONOMOUS DETECTION AND RESPONSE

Correlates activity across email, network, and cloud domains to identify threats early and initiate targeted containment actions, supported by analyst oversight.

IDENTITY AND CLOUD SECURITY

Secures identity providers and cloud services (e.g. Microsoft 365, Dropbox, SaaS applications) against account takeover, privilege abuse, and suspicious access behavior.

Benefits

What sets us apart as a security partner.

HUMAN EDGE

AI detects patterns — people ensure relevance. CLUE security analysts oversee detection, validate findings, and continuously refine models based on real-world behavior.

- Implementation, tuning, and customization
- Alerts and response actions
- Integrations that fit operational reality — not generic defaults

OT-SPECIALISATION

OT environments require a different security mindset: protection without disruption. The service is designed to detect anomalies in industrial and operational networks before they impact operations.

- Availability, safety, and process stability are preserved
- Security measures are built to work reliably in production environments
- Backed by proven experience from OT and critical infrastructure

TRANSPARENCY

Security decisions require trust. Alerts, detections, and response actions are fully traceable and explainable at any time — ensuring every decision can be understood, reviewed, and justified.

- What is detected and why actions are taken
- How the service evolves over time
- Clarity for operations, management, and audits

Features

The technical aspects of our approach.

Cloud Threats

Addresses the attack surface created by cloud adoption and distributed workloads. Helps organizations maintain visibility and control as users, data, and services move beyond traditional network boundaries.

Workflow Integrations

Integrates with security tools, identity platforms, and collaboration systems to extend detection and response. Supports automated workflows that accelerate investigations and improve efficiency.

Zero Days, Malware and Ransomware

Identifies emerging attack techniques, ransomware campaigns, and malware activity at an early stage. Enables rapid containment to minimize operational disruption and financial impact.

Insider Threat and Account Takeover

Detects compromised credentials, malicious insider activity, and unusual user behavior. Helps prevent unauthorized access, data loss, and misuse of trusted accounts.

Telemetry Data

Provides security insights through consolidated telemetry and alert data. Enables visibility, faster investigations, and integration with existing monitoring and reporting platforms.

Advanced Phishing

Protects organizations from targeted social engineering campaigns that attack supply chains and bypass traditional filtering.

Modern Threats **Need Intelligent Defense** **Stay ahead with AI-Based Threat Detection.**

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

04.2026