CLUE
CYBER SECURE

Cyber Defense Hub

Die Schwachstelle

Wie lange würde es dauern, bis Sie einen Cyberangriff bemerken? In vielen Unternehmen fehlt nicht die Technik – sondern die Klarheit. Ohne Einblick in das, was wirklich passiert, werden Bedrohungen zu spät erkannt.Verzögerungen kosten Zeit, Geld und Vertrauen. Sicherheit beginnt dort, wo Entscheidungen auf verlässlichen Informationen basieren.

Die Kontrolle

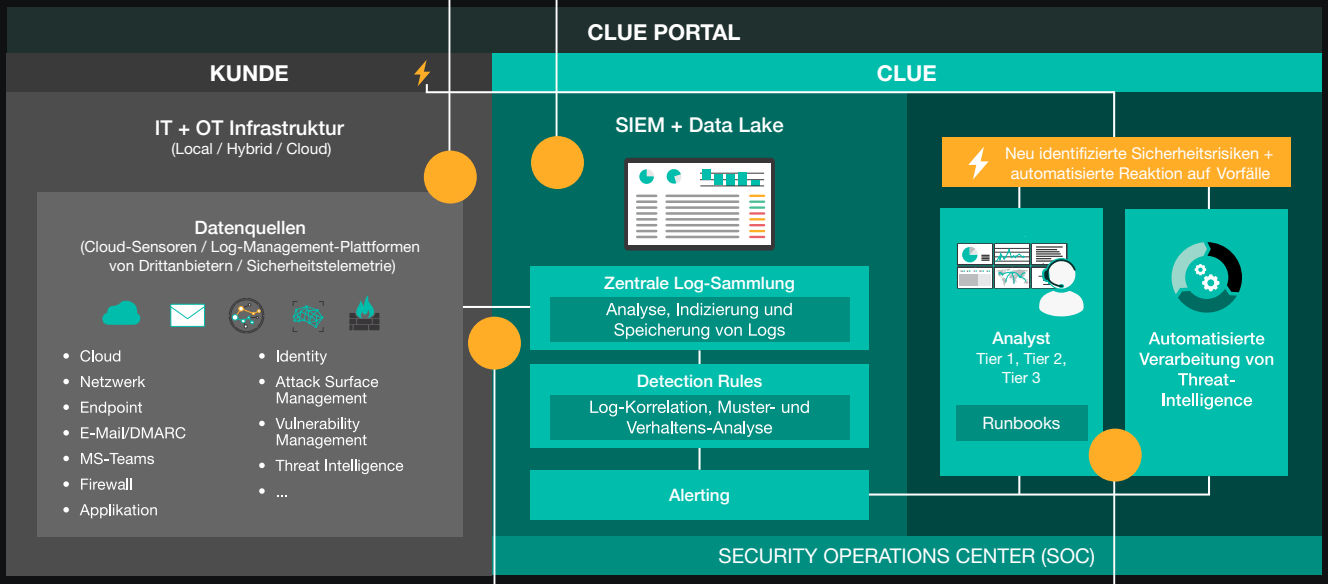
Der Cyber Defense Hub verwandelt Daten in Entscheidungsgrundlagen. Durch zentrale Analyse und 24/7-Überwachung entsteht Transparenz über Ihre gesamte IT- und OT-Landschaft. So werden Bedrohungen nicht nur erkannt, sondern verstanden – und Sie können gezielt handeln.
Decision Ready Security: Aus Daten werden Entscheidungen.

DATENINTEGRATION

Log- und Telemetriedaten aus unterschiedlichsten Quellen (Cloud, Netzwerk, Endpoints, E-Mail, Firewalls, etc.) laufen im Cyber Defense Hub zusammen.

ZENTRALE VERARBEITUNG

Die im SIEM und Data Lake gesammelten Daten werden analysiert, indiziert und gespeichert. Detection Rules korrelieren die Daten und erkennen Muster oder anomales Verhalten.



TRANSPARENZ

Die Bemessung des verarbeiteten Datenvolumens und der Verrechnung erfolgt dabei transparent nach Events per Second (EPS).

ANALYSE UND REAKTION

Alerts werden gemäss Runbooks durch Analysten in verschiedenen Stufen geprüft und verarbeitet. Bei verdächtigen Aktivitäten oder erkannten Angriffsversuchen wird der Kunde entsprechend informiert. Wo möglich werden über automatisierte Threat-Intelligence-Prozesse Bedrohungen autonom eliminiert

Benefits

Was uns als Security-Partner auszeichnet.

HUMAN EDGE

CLUE kombiniert Technologie mit direktem Expertenzugang. Statt Standardprozessen erhalten Kunden schnelle, fundierte Entscheidungen durch erfahrene Analysten.

- KI-gestützte Gefahren-erkennung für mehr Präzision
- Automatisierte Prozesse beschleunigen die Reaktion
- Flexible Einbindung verschiedenster Datenquellen
- Abrechnung nach Events per Second (EPS) für volle Kostentransparenz

OT-SPEZIALISIERUNG

OT-Umgebungen erfordern ein besonderes Sicherheitsverständnis: Produktionsprozesse und Steuerungssysteme dürfen nicht beeinträchtigt werden. CLUE bringt diese Erfahrung mit.

- Nachweisliche Expertise in Smart Building, Fertigung und kritischen Infrastrukturen
- Einheitliche Sensorik für IT und OT
- Zusammenarbeit mit führenden Branchenexperten
- Aktive Rolle in Fachgruppen von Industrieverbänden

EFFIZIENZ UND TRANSPARENZ

Statt unübersichtlicher Alarmfluten liefert CLUE nur Informationen, die wirklich relevant sind – klar aufbereitet und jederzeit nachvollziehbar.

- Reduktion von Fehlalarmen und unnötigen Meldungen
- Fokus auf tatsächliche Bedrohungen oder verdächtige Aktivitäten
- Solution Designs, die Effizienz und Kosten in Balance bringen
- Detaillierte Einblicke und Reports im CLUE Portal

Features

Die technischen Elemente unseres Ansatzes.

Proaktives Threat Hunting

Geht weit über klassische, reaktive Alarmierung hinaus und spürt auch neuartige Bedrohungen frühzeitig auf.

Technologie-Agnostisch

Integration sowohl von CLUE-Services als auch von Drittanbieter-Tools, um bestehende Investitionen optimal zu nutzen.

SOAR-Funktionalität

Ermöglicht granulare Eingriffe bis hin zur automatisierten Sperrung verdächtigen Traffics in Echtzeit.

Automatisiertes Reporting

Vereinfacht Compliance-Anforderungen und schafft gleichzeitig Transparenz für Management und Audits.

Erweiterte Data Retention

Individuell abgestimmt auf die regulatorischen Vorgaben der Kunden.

Standardkonform

Kombiniert mit weiteren CLUE-Diensten, erfüllt nahezu alle Anforderungen des IKT-Mindest-standards sowie des NIST CSF.

24/7 Business **braucht 24/7 Security.** **Erleben Sie 24/7 Schutz mit dem Cyber Defense Hub.**

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

11.2025