CLUE
CYBER SECURE

AI Based Threat Detection

Der blinde Fleck

Herkömmliche Sicherheitstools stützen sich auf bekannte Angriffsmuster und vordefinierte Regeln. Heutige Angriffstechniken nutzen Social Engineering, gestohlene Identitäten und subtile Verhaltensänderungen, die signaturbasierte Erkennung umgehen. Dadurch entstehen blinde Flecken, in denen Bedrohungen unbemerkt bleiben, ehe sie Schaden anrichten.

Die Kontrolle

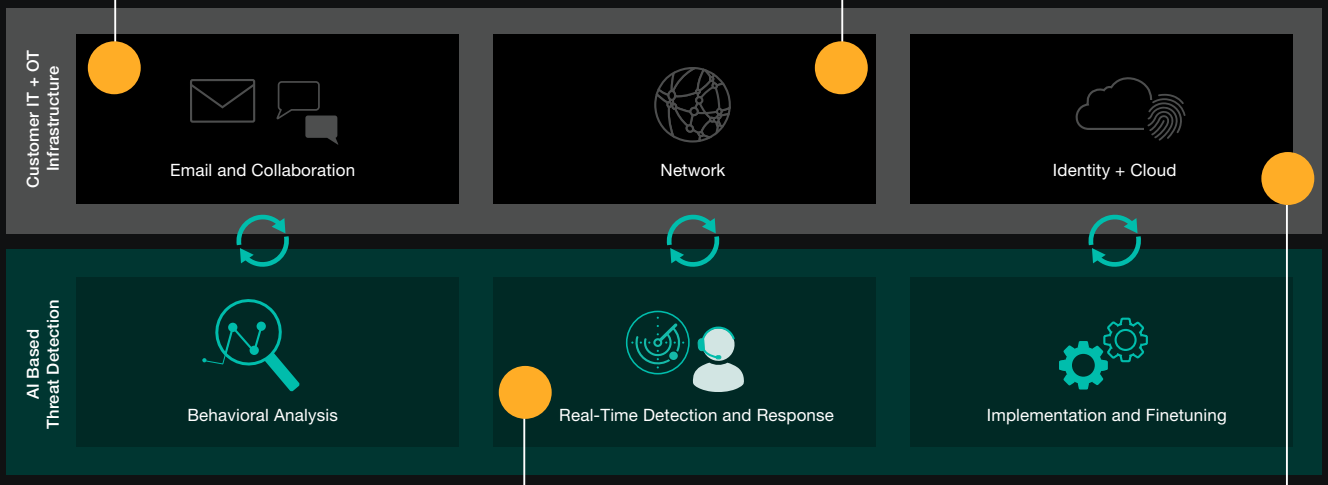
AI Based Threat Detection identifiziert auffälliges Verhalten in E-Mail-, Netzwerk- und Cloud-Umgebungen, indem sie das normale Verhalten von Benutzern, Geräten und Systemen analysiert. Dies ermöglicht die frühzeitige Erkennung bekannter und unbekannter Bedrohungen. So können gezielte Gegenmassnahmen ergriffen werden, um Angriffe zu stoppen, bevor sie eskalieren – ohne den Geschäftsbetrieb zu beeinträchtigen.

EMAIL SICHERHEIT

Schützt E-Mail- und Kollaborationsplattformen (z. B. Microsoft 365) vor Phishing, Betrug und böswilligen Kampagnen, ohne den Arbeitsablauf zu stören.

NETZWERKSICHERHEIT

Überwacht Netzwerkumgebungen in lokalen, hybriden und Remote-Infrastrukturen, um ungewöhnlichen Datenverkehr, laterale Bewegung und Command-and-Control-Aktivitäten aufzudecken.



AUTONOME ERKENNUNG UND REAKTION

Korreliert Aktivitäten über E-Mail-, Netzwerk- und Cloud-Domänen hinweg, um Bedrohungen frühzeitig zu erkennen und gezielte Eindämmungsmassnahmen einzuleiten, unterstützt durch die Überwachung durch Analysten.

IDENTITÄTS- UND CLOUD-SICHERHEIT

Schützt Identitätsanbieter und Cloud-Dienste (z. B. Microsoft 365, Dropbox, SaaS-Anwendungen) vor Kontoübernahmen, dem Missbrauch von Berechtigungen und verdächtigem Zugriffsverhalten.

CLUE
CYBER SECURE

Benefits

Was uns als Security-Partner auszeichnet.

HUMAN EDGE

KI erkennt Muster – Menschen sorgen für die Relevanz. Die Sicherheitsanalysten von CLUE überwachen die Erkennung, überprüfen die Ergebnisse und verfeinern die Modelle kontinuierlich auf der Grundlage des tatsächlichen Verhaltens.

- Implementierung, Feinabstimmung und Anpassung
- Warnmeldungen und Reaktionsmassnahmen
- Integrationen, die auf die betrieblichen Gegebenheiten zugeschnitten sind – keine generischen Standardeinstellungen

OT-SPEZIALISIERUNG

OT-Umgebungen erfordern eine andere Sichtweise auf Sicherheit: Schutz ohne Ausfälle. Der Service wurde entwickelt, um Anomalien in industriellen und betrieblichen Netzwerken zu erkennen, bevor sie den Betrieb beeinträchtigen.

- Verfügbarkeit, Sicherheit und Prozessstabilität bleiben erhalten.
- Sicherheitsmassnahmen die in zuverlässig Produktionsumgebungen funktionieren.
- Gestützt auf bewährte Erfahrung aus den Bereichen OT und kritische Infrastruktur.

TRANSPARENZ

Sicherheitsentscheidungen erfordern Vertrauen. Warnmeldungen, Erkennungen und Reaktionsmassnahmen sind jederzeit lückenlos nachvollziehbar und erklärbar. So wird sichergestellt, dass jede Entscheidung verstanden, überprüft und begründet werden kann.

- Was erkannt wird und warum Massnahmen ergriffen werden
- Wie sich der Dienst im Laufe der Zeit weiterentwickelt
- Transparenz für Betrieb, Management und Audits

Features

Die technischen Elemente unseres Ansatzes.

Cloud Bedrohungen

Analysiert die Angriffsfläche, die durch die Einführung von Cloud-Lösungen und verteilte Workloads entsteht. Hilft Transparenz und Kontrolle zu wahren, wenn Nutzer, Daten und Dienste über die traditionellen Netzwerkgrenzen hinausgehen.

Workflow Integrationen

Lässt sich in Sicherheitstools, Identitätsplattformen und Kollaborationssysteme integrieren, um die Erkennung und Reaktion zu erweitern. Unterstützt automatisierte Arbeitsabläufe, die Untersuchungen beschleunigen und die Effizienz steigern.

Zero Days, Malware und Ransomware

Erkennt neue Angriffstechniken, Ransomware-Kampagnen und Malware-Aktivitäten frühzeitig. Ermöglicht eine schnelle Eindämmung, um Betriebsunterbrechungen und finanzielle Auswirkungen zu minimieren.

Insider Threat und Account Takeover

Erkennt kompromittierte Zugangsdaten, böswillige Insider-Aktivitäten und ungewöhnliches Nutzerverhalten. Trägt dazu bei, unbefugten Zugriff, Datenverlust und den Missbrauch vertrauenswürdiger Konten zu verhindern.

Telemetrie Daten

Liefert Erkenntnisse zur Sicherheit durch konsolidierte Telemetrie- und Alarmdaten. Ermöglicht Transparenz, schnellere Untersuchungen und die Integration in bestehende Überwachungs- und Berichtsplattformen.

Fortgeschrittenes Phishing

Schützt Unternehmen vor gezielten Social-Engineering-Kampagnen, die auf Lieferketten abzielen und herkömmliche Filtermechanismen umgehen.

Moderne Bedrohungen **erfordern eine intelligente Abwehr** **Bleiben sie mit AI-Based Threat Detection einen Schritt im voraus.**

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

04.2026