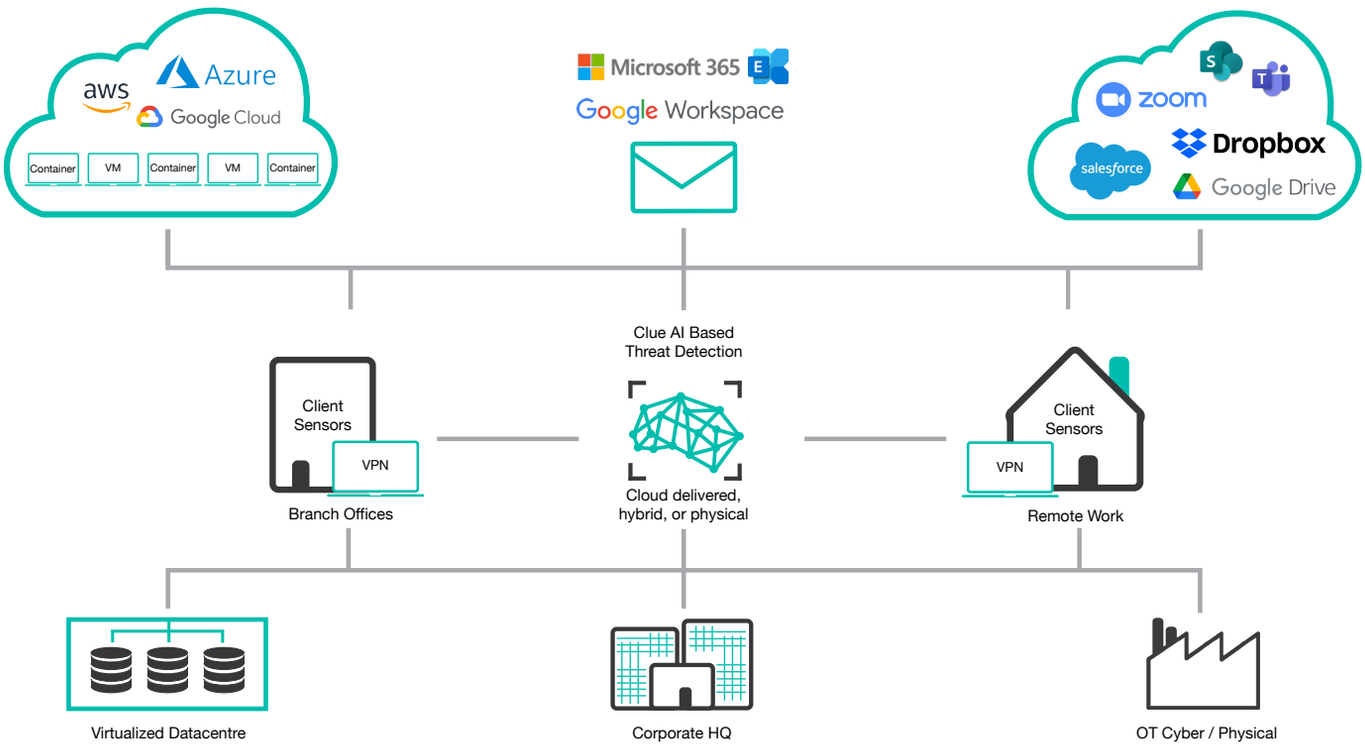
SECURITY SERVICES AG

CLUE

AI BASED THREAT DETECTION

Angriffe auf Unternehmen und Einrichtungen werden ständig adaptiert um neue Schwachstellen auszunutzen. Mit Hilfe von ausgereifter KI Technologie können Attacken gestoppt werden bevor sie Schaden anrichten. Mit dem AI Based Threat Detection Service ist dies möglich. Die Technologie lernt ständig selbständig und erkennt dadurch rasch abnormale und potentiell gefährliche Verhalten.



AI BASED DETECTION ENGINE

Die auf KI basierte Erkennung von Cybergefahren analysiert und erlernt das „normale“ Verhalten im eigenen Netzwerk und der eingesetzten Cloud Services. Dabei wird nicht auf vorprogrammierte Muster gesetzt, sondern das individuelle Verhalten erfasst. Dieses Verhalten wird ständig von der KI hinterfragt und durch Clue Security Analysten validiert. Dabei werden Angriffe wie Privilege Escalation, Ransomware, Datenexfiltration, Lateral Movement, C&C Server Kommunikation und Zero Day Exploits erkannt und verhindert.

INTEGRATION MICROSOFT 365

Remote- und Hybride Arbeitsumgebungen sind aus unserem Alltag nicht mehr weg zu denken. Mit dieser Entwicklung hat sich auch der Fokus von Cyber-Kriminellen auf diese hybriden Umgebungen verlagert. Die AI Based Threat Detection kombiniert daher die Überwachung von Klassischen IT Umgebungen mit SaaS wie Microsoft 365. Dabei wird die User Aktivität über mehrere Produkte zusammengefasst. Dies bringt den Vorteil, dass eine autonome Reaktion auf Vorfälle sowohl durch die Microsoft Azure Security sowie auch die AI Based Threat Detection durchgeführt werden kann. Durch die Integration in die Microsoft 365 API können kontextabhängige Alarme erzeugt werden. Dadurch ist ebenfalls die Integration und Unterstützung von Azure AD, Azure ADFS und anderer SAML 2.0 Services gegeben.

AUTOMATED RESPONSE

Durch die «Automated Response» Engine können durch das System angebrachte Gegenmassnahmen automatisch durchgeführt werden. Hiermit werden laufende Angriffe frühzeitig gestoppt, bevor diese Schaden anrichten können. Im Durchschnitt reagiert das System innerhalb von zwei Sekunden auf Bedrohungen. Es erkennt Abweichungen vom normalen Verhalten eines Benutzers oder Geräts und unternimmt Schritte, um laufende Ransomware- und Insider-Angriffe, Compliance-Verstösse, Malware, E-Mail-Angriffskampagnen und andere Bedrohungen zu stoppen. Dies verschafft dem Sicherheitsteam Zeit, das Problem zu beheben. Es sind Module für Netzwerk-, Email- und Cloud Bedrohungen verfügbar.

AI BASED THREAT DETECTION FEATURES

AI CYBER ANALYST
Sobald das AI based Threat Detection System eine Modellabweichung oder ein Muster anormaler Aktivität feststellt, beginnt der AI Analyst mit seiner Analyse. Das System stellt, wie auch ein menschlicher Security Analyst qualifizierte Fragen, um eine potenzielle Bedrohung zu erkennen und zu bewerten.

CLOUD GEFAHREN
Die Verlagerung der IT Systeme und Applikationen in die Cloud hat die Angriffsfläche auf Unternehmen drastisch vergrössert. Für Unternehmen erhöht sich damit häufig die Komplexität und es wird schwieriger, die Übersicht über Zugangspunkte zu behalten. Die selbstlernende KI von AI Based Threat Detection entdeckt in diesem Bereich routinemässig Bedrohungen und wehrt diese ab.

ACTIVE INTEGRATIONS
Neben einer RADIUS Schnittstelle für Remote Access Systeme stehen Module für die Betriebssysteme Windows, MacOS und Linux zur Verfügung. Auch SAML für moderne Authentifizierungslösungen und eine API Schnittstelle für die direkte Integration in Applikationen sind verfügbar.

WORKFLOW INTEGRATIONS
Um massgeschneiderte, KI gestützte Einblicke zwischen etablierten Arbeitsabläufen nutzen zu können, integriert AI Based Threat Detection eine grosse Bandbreite von Technologien, Security Mechanismen und Kollaborations-Plattformen. Die Schnittstellen für die Aufnahme und Abgabe von relevanten Informationen zur Abwehr von Bedrohungen umfassen z.B. EDR, VPN und Zero Trust Network Access (ZTNA) Systeme.

ZERO DAYS, MALWARE UND RANSOMWARE
Die Bedrohungen für Unternehmen durch Zero-Day Exploits, Malware und Ransomware haben ein eskalierendes Level erreicht. Unternehmen aller Branchen und vor allem kritische Infrastrukturen sind stark betroffen. Die Konsequenzen von Ransomware Angriffen sind nicht nur finanzieller Natur, sondern haben z.B. auch einen Einfluss auf das öffentliche Leben und die Versorgung von Patienten. Die KI Engine kann Ransomware in Sekunden erkennen und verhindern.

INSIDER THREAT UND ACCOUNT TAKEOVER
Bewusste Übergriffe durch Mitarbeiter oder unbewusst infizierte Systeme können nur schwer erkannt werden, da Mitarbeiter über berechtigten Zugriff verfügen und tieferes Wissen über die Unternehmensressourcen haben. Wenn die KI Insider Threats erkennt, wird diese die bedrohlichen Aktivitäten unterbinden und die SOC Analysten alarmieren.

TELEMETRIE DATEN
Durch einen API-First Ansatz erhalten Sie unlimitierte Möglichkeiten im Einsatz von Multi Factor Authentication. Die Integration in ihre Management Tools, User Self Service Portale, Produkte und Applikationen bringen volle Flexibilität und niedrige Kosten in der Implementation und Entwicklung.

ADVANCED PHISHING
Die AI Based Threat Detection Engine für Email erkennt gezielte und komplexe Phishing Angriffe auf Unternehmen – unabhängig davon, ob Microsoft 365, Microsoft Exchange oder Google Workspace eingesetzt wird. Die Engine ist nicht auf die Sprache der Email angewiesen, denn sie basiert rein auf mathematischen Formeln, um das «Normal» der Kommunikation des Unternehmens zu erlernen. Dies erlaubt ihr, anomale Emails zu erkennen und zu neutralisieren.

OT/ICS SECURITY
Sicherheitsverletzungen in OT und ICS können weitreichende Folgen haben. Zusätzlich zum Schaden durch Betriebsunterbrüche und Produktionsstopps kann durch die Schnittstelle von Technologie auf die Umwelt auch Mensch und Leben in Gefahr sein. Durch den längeren Einsatz von Technologien und dem reaktiven Ansatz in OT Komponenten, bieten sich vielseitig angreifbare Systeme gerade zu an. Die KI versteht ebenso diese OT/ICS Protokolle und erkennt Anomalien unmittelbar.

AI BASED THREAT DETECTION SERVICE

Clue AI Based Threat Detection kombiniert die hohe Service Qualität von unseren Security Engineers mit den Vorteilen der künstlichen Intelligenz, damit Ihre IT Infrastruktur das höchste Mass an Sicherheit geniesst. So können Angriffe schnell und zuverlässig gestoppt werden. Unsere Security Experten erarbeiten gerne zusammen mit Ihnen ein Konzept, das zu Ihren Bedürfnissen passt.

CLUE-LESS?

Clue Managed Services erweitert Ihr Team mit Security Experten zur Stärkung der Sicherheit Ihres Unternehmens. Bewährte Produkte, massgeschneiderte Features und Ihr ganz persönlicher Support – wir erfüllen Ihre Anforderungen bei einem niedrigen TCO. Durch die monatlichen Servicegebühren entfallen hohe Investitionen sowie Trainingskosten, was Ihnen einen modularen Einsatz unserer Services ermöglicht.

NÄCHSTE SCHRITTE
Betreiben Sie eine kritische Infrastruktur? Möchten Sie die Sicherheit Ihrer IT-Umgebung mit der Hilfe von KI erhöhen? Gerne zeigen wir Ihnen in einem persönlichen Gespräch die Vorteile eines KI basierten Security-Konzepts auf.

CLUE SECURITY SERVICES AG | GRABENSTRASSE 17 | CH-6340 BAAR | +41 44 667 77 66 | INFO@CLUE.CH | WWW.CLUE.CH