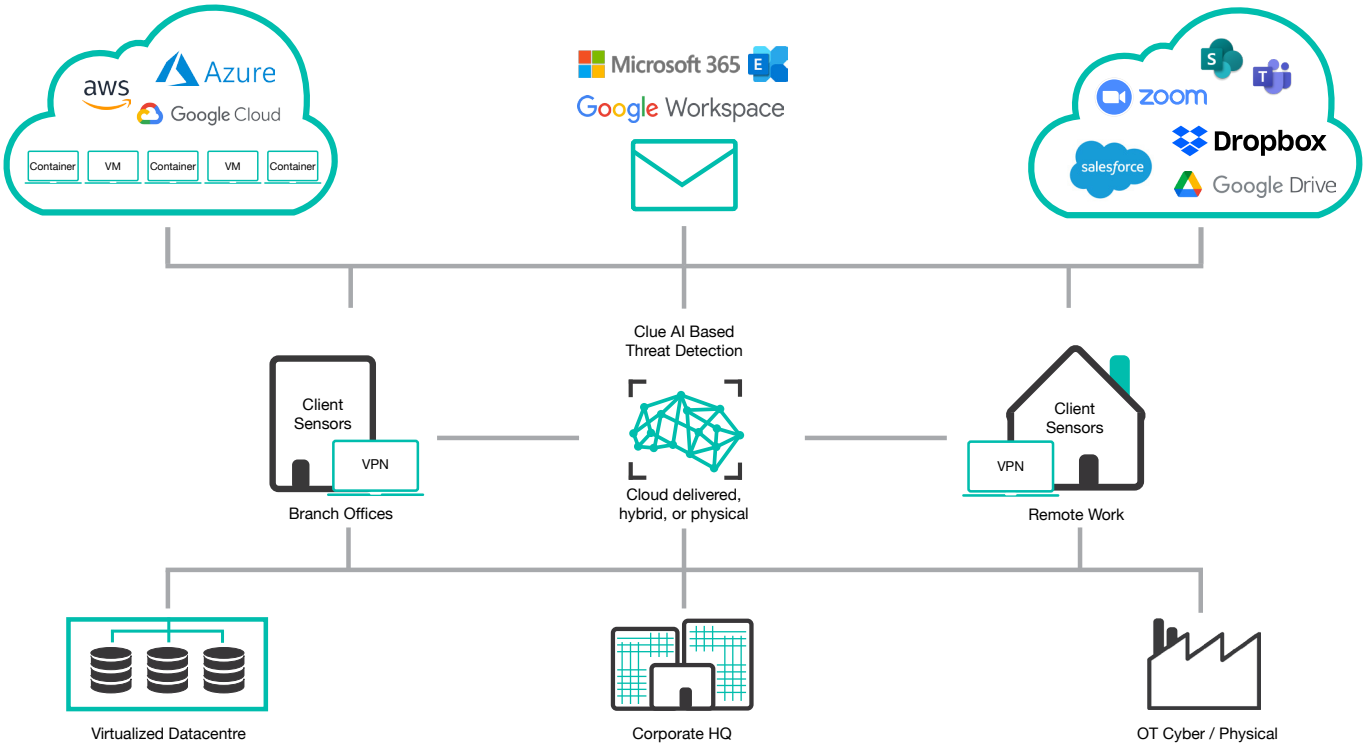
SECURITY SERVICES AG

CLUE

AI BASED THREAT DETECTION

Attacks on companies and institutions are constantly being adapted to exploit new vulnerabilities. With the help of sophisticated AI technology, threats can be caught before they do any damage. This is possible with the AI Based Threat Detection Service. The technology is constantly learning autonomously and thus quickly detects abnormal and potentially dangerous behaviour.



AI BASED DETECTION ENGINE

The AI-based detection of cyber threats analyzes and learns the “normal” behavior in the company’s own network and the cloud services used. It does not rely on pre-programmed patterns, but captures individual behavior. This behavior is constantly challenged by the AI and validated by Clue Security analysts. Attacks such as privilege escalation, ransomware, data exfiltration, lateral movement, C&C server communication and zero day exploits are detected and prevented.

INTEGRATION MICROSOFT

Remote and hybrid work environments have become an integral part of our everyday lives. With this development, the focus of cyber criminals has also shifted to these hybrid environments. AI Based Threat Detection therefore combines the monitoring of classic IT environments with SaaS such as Microsoft 365. User activity is aggregated across multiple products. As a result, an autonomous incident response can be performed by both Microsoft Azure Security and AI Based Threat Detection. Through integration with the Microsoft 365 API, contextual alerts can be generated. This also provides integration and support for Azure AD, Azure ADFS and other SAML 2.0 services.

AUTOMATED RESPONSE

With the “Automated Response” engine, countermeasures applied by the system can be carried out automatically. This stops ongoing attacks at an early stage, before they can cause any damage. On average, the system responds to threats within two seconds. It detects deviations from normal behavior of a user or device and takes steps to stop ongoing ransomware and insider attacks, compliance violations, malware, email attack campaigns and other threats. This gives the security team time to remediate the problem. Modules are available for network, email and cloud threats.

AI BASED THREAT DETECTION FEATURES

AI CYBER ANALYST

Once the AI Based Threat Detection System detects a model deviation or pattern of abnormal activity, the AI Analyst begins its analysis. Like a human security analyst, the system asks qualified questions to identify and assess a potential threat.

CLOUD RISKS

The shift of IT systems and applications to the cloud has dramatically increased the attack surface on enterprises. For enterprises, this often increases complexity and makes it more difficult to keep track of access points. AI Based Threat Detection's self-learning AI routinely detects and defends against threats in this space.

ACTIVE INTEGRATIONS

The system uses an open and extensible architecture to seamlessly integrate with the existing security architecture. In addition, active integrations can prevent and block threats detected by the AI in other ways. It also enables threats on firewalls and NACL systems to be blocked by the AI..

WORKFLOW INTEGRATIONS

To harness tailored AI-powered insights between established workflows, AI Based Threat Detection integrates a wide range of technologies, security mechanisms and collaboration platforms. Interfaces for ingesting and delivering relevant threat intelligence include, for example, EDR, VPN, and Zero Trust Network Access (ZTNA) systems.

ZERO DAYS, MALWARE AND RANSOMWARE.

Threats towards enterprises via zero-day exploits, malware and ransomware have reached escalating levels. Companies across all industries, and especially critical infrastructure, are being affected severely. The consequences of ransomware attacks are not only financial, but also have an impact on public life and patient care, for example. The AI engine can detect and prevent ransomware in seconds.

INSIDER THREAT AND ACCOUNT TAKEOVER

Deliberate attacks by employees or unknowingly infected systems can be difficult to detect because employees have authorized access and deeper knowledge of corporate resources. When AI detects insider threats, it will stop the threatening activity and alert SOC analysts.

TELEMETRY DATA

In addition to the asset and workflow integrations, the AI-based system provides a powerful API that provides access to the system's intelligence, such as alerts, model violations, security incidents detected by the Cyber AI Analyst, and advanced search results for integration with SIEM, SOAR, and other systems.

ADVANCED PHISHING

The AI Based Threat Detection Engine for Email detects targeted and complex phishing attacks on enterprises - regardless of whether Microsoft 365, Microsoft Exchange or Google Workspace is used. The engine does not rely on the language of email, as it relies purely on mathematical formulas to learn the "normal" of the organization's communications. This allows it to efficiently detect and neutralize anomalous emails.

OT/ICS SECURITY

Security breaches in OT and ICS can have far-reaching consequences. In addition to the damage caused by operational interruptions and production stops, the interface of technology to the environment can also put people and lives at risk. With the prolonged use of technology and the reactive approach in OT components, versatile vulnerable systems become a convenient target. AI also understands these OT/ICS protocols and detects anomalies immediately.

AI BASED THREAT DETECTION SERVICES

Clue AI Based Threat Detection combines the high quality of service provided by our security engineers with the benefits of artificial intelligence to ensure that your IT infrastructure is protected with the highest level of security. This enables attacks to be stopped quickly and reliably. Our security experts will be happy to work with you to develop a concept that fits your needs.

CLUE-LESS?

Bolster your team with Clue Managed Services. Our security experts are a welcome addition to your business. Proven products, tailor-made features and your very own personal support - we meet your requirements at a low TCO. The monthly service fee eliminates high investments and training costs, enabling you to use our services in a modular way.

WHAT'S NEXT?

Do you operate a critical infrastructure? Would you like to increase the security of your IT environment with the help of AI? We would be happy to show you the advantages of an AI-based security concept in a personal meeting.

CLUE SECURITY SERVICES AG | NEUHOFSTRASSE 5A | CH-6340 BAAR | +41 44 667 77 66 | INFO@CLUE.CH | WWW.CLUE.CH