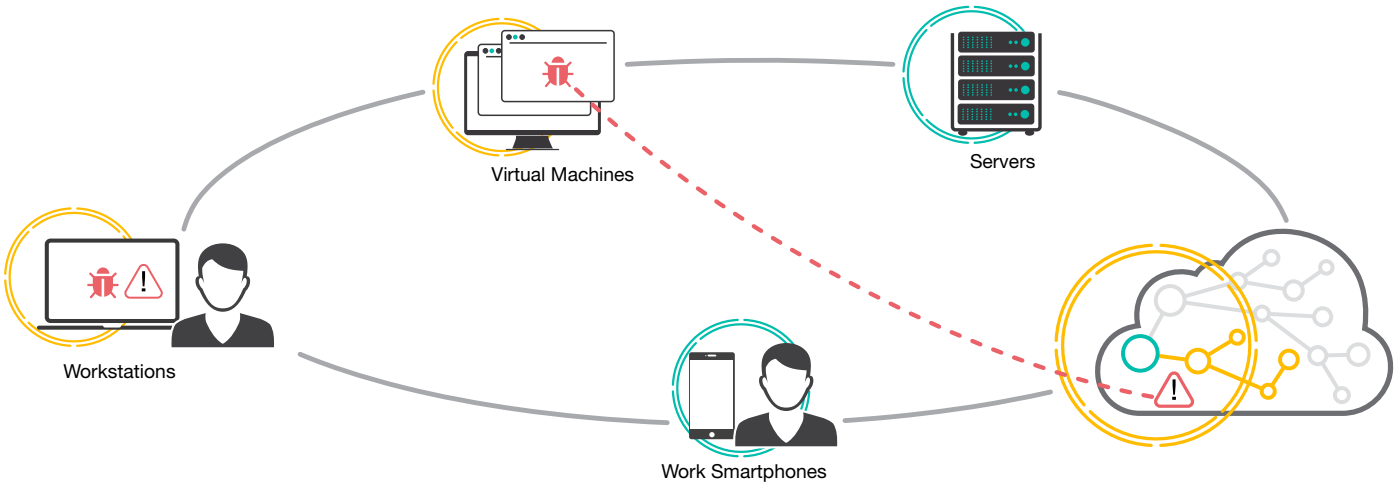
SECURITY SERVICES AG

CLUE

ADVANCED ENDPOINT PROTECTION

Die Bedrohung durch Cyberangriffe ist aktuell grösser als je zuvor und Angriffe werden automatisierter und komplexer. Neu entdeckte Schwachstellen, für die kein Patch existiert, auch Zero-Day Schwachstellen genannt, werden häufiger und die Reichweite dieser wird grösser. Die Aufwände zum Schutz von Endpunkten steigen dadurch weiter. Um dieser Problematik gerecht zu werden, reicht das Arbeiten mit klassischen, signaturbasierten Antivirenprogrammen nicht mehr aus, da diese nur auf bekannte Angriffe reagieren können. Mit Advanced Endpoint Protection von Clue kann die Sicherheit vor Cyber-Bedrohungen erfolgreich wiederhergestellt und eine optimale Verteidigung gegen die aktuelle Bedrohungslage aufgestellt werden.



AI BASED DETECTION ENGINE

Cyber-Attacken werden zunehmend schwieriger zu erkennen. Aus diesem Grund wird mit dem Advanced Endpoint Protection Service zusätzlich zur traditionellen Erkennung über Hashwerte künstliche Intelligenz (KI) eingesetzt, um Angriffe auf die IT-Systeme zu identifizieren. Die KI wird dabei einerseits lokal eingesetzt, damit ein Grundschutz garantiert ist, auch wenn sich der Endpunkt nicht mit der zentralen Konsole verbinden kann. Weiter läuft eine leistungsstarke zentrale KI, welche Daten über längere Zeiträume und über Geräte hinweg nutzen kann, um auch die kompliziertesten Angriffe zu erkennen.

STORYLINE

Cyber-Angriffe sind komplexe Abläufe, welche aus verschiedenen Prozessen bestehen, die einzelne schädliche Teilaufgaben erledigen. Mit Storyline erhält man den Überblick über alle Prozesse – wie diese Zusammenhängen und in welcher Reihenfolge einzelne Schritte ausgeführt wurden. Viele Teilprozesse von einem Angriff werden zu einer einzigen Benachrichtigung zusammengefasst und in einem zentralen Dashboard dargestellt. Diese strukturierte Übersicht ermöglicht eine schnelle und gezielte Reaktion.

AUTOMATIC RESPONSE

Advanced Endpoint Protection bietet nicht nur eine schnelle Angriffserkennung, sondern kann auch sofort reagieren. So wird bei einem Angriff automatisch der Prozess und betroffene Dateien in Quarantäne verschoben, sodass diese keine Auswirkungen mehr auf die Endpunkte haben können. Darüber hinaus können Änderungen an den Systemeinstellungen und Registry automatisch oder mit einem Klick auf den Stand vor dem Angriff gebracht werden.

ADVANCED ENDPOINT PROTECTION FEATURES

ONE-CLICK ATTACK ROLLBACK
Wenn durch einen schädlichen Prozess Dateien verschlüsselt oder zerstört wurden, gibt es die Möglichkeit den Zustand vor dem Angriff herzustellen. So können Ransomware-Angriffe mit einem simplen Klick bereinigt werden.

CUSTOM DETECTION RULES
Neben der automatischen Erkennung ist es zusätzlich möglich eigene Erkennungsregeln zu schreiben. Mit diesen kann man schnell auf neue Angriffsarten reagieren und diese werden explizit als solche markiert.

DEEP VISIBILITY
Die gesammelten Daten aller Endpunkte werden nachträglich untersucht, damit komplexe Anfragen gestellt und auch nötige Erkennungsausnahmen abgeschätzt werden können.

FILE FETCH
Falls ein Vorfall vorliegt, ist es oft entscheidend, die potenziell schädliche Datei zu untersuchen. Dafür gibt es die Möglichkeit, direkt aus dem Dashboard die Dateien nachzuladen und dann zu untersuchen. Damit erübrigt sich der Umweg zum Endpunkt.

SECURE REMOTE SHELL
Nach einem Vorfall kann ein Endpunkt durch die Shell des Betriebssystems problemlos fernuntersucht werden. Das Versenden und Abholen eines Gerätes ist nicht mehr nötig. Dies spart Zeit und Kosten.

HOST-BASED FIREWALL RULES
Um den Schutz vom Endpunkt weiter zu erhöhen kann die Firewall des Endpunktes genutzt werden um ungewünschte Verbindungen (z.B. Netzwerkverbindungen, Internetverbindungen, etc.) weiter einzuschränken. Damit können die Host Firewall Regeln zentral verwaltet und eingerichtet werden.

AUTONOMOUS HOST ISOLATION
Damit die Ausbreitung von Angriffen weiter eingedämmt wird, können Endpunkte bei Erkennung von Angriffen automatisch vom Netzwerk getrennt werden. Lediglich die Verbindung zur zentralen Plattform bleibt bestehen, womit der Angriff analysiert und behoben werden kann.

OPERATING SYSTEM SUPPORT
Neben einem guten Schutz ist auch eine breite Abdeckung der Betriebssysteme nötig, um den Schutz für Geräte verschiedener Hersteller gewährleisten zu können. Der Endpunktschutz von Clue deckt alle aktuell gängigen Betriebssysteme ab (MacOS, Windows Clients und Server, Linux Distributionen, virtuelle Maschinen).

AUTONMOUS INCIDENT ANALYSIS
Bei einem Angriff ist es wichtig schnellmöglich diesen zu verstehen. Dafür werden die einzelnen Abläufe und Prozesse bei einem Angriff mit zusätzlichen Informationen angereichert. So werden die Schritte mit Referenzen vom MITRE ATT&CK Framework angereichert, um die Angriffe besser zu verstehen.

UNSER SERVICE

Der Schutz, der unser Advanced Endpoint Protection bietet, zeichnet sich durch eine Vielzahl an Erkennungsmechanismen aus. Endpunkte können auf diese Weise auch gegen sehr komplexe Angriffe optimal geschützt werden. Mit einem auf Ihr Unternehmen abgestimmten Design stellen wir sicher, dass Sie rund um die Uhr ein gleich hohes Niveau an Sicherheit profitieren können.

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.

NEXT STEPS

Sind Sie daran interessiert, die Sicherheit in Ihrem Unternehmen auf den aktuellsten Stand zu bringen? Möchten Sie mehr über die Vorteile von Managed Advanced Endpoint Protection erfahren? Kontaktieren Sie uns und wir nehmen uns gerne Zeit, um diese und weitere Fragen mit Ihnen zu besprechen.