Automated EDR

NGAV und EDR zum zuverlässigen Schutz Ihrer Daten, vor und nach der Infektion in Echtzeit

Herausforderung:

70% der Schadsoftware bleiben von Antiviren-Software unerkannt

Wussten Sie, dass laut einer Studie etwa 70% der modernen Schadsoftware durch herkömmlichen, aber auch durch Next Gen Antivirus-Lösungen unentdeckt bleiben? Die Folge: Den Service Desk erreichen nach und nach konkrete Störungsmeldungen und Sie erkennen erst jetzt, dass Malware ausgebrochen ist, dass Sie infiziert sind und alles daran setzen müssen, um mögliche Konsequenzen - von Datendiebstahl bis zur Verschlüsselung - einzudämmen?
Matrix42 Automated EDR (Endpoint Detection & Response) reduziert nicht nur die Anzahl der Alerts auf ein Minimum, es stoppt die Auswirkungen von Malware auch nach der Infektion und das automatisiert und in Echtzeit. So sind die wichtigsten Güter Ihres Unternehmens immer optimal geschützt - Ihre Daten und die Produktivität Ihrer Mitarbeiter.

Was ist Matrix42 Automated EDR?

Matrix42 Automated EDR erkennt und blockiert zum einen bereits vor der Infektion (Pre-Infection Prevention) moderne Schadsoftware dank der auf Machine Learning und Artifical Intelligence setzenden NGAV-Lösung. Zum anderen, und das stellt den wesentliche Mehrwert der Lösung dar, blockiert die Lösung selbst nach einer Infektion (Post-Infection Protection) die Konsequenzen eines Ausbruchs durch einen automatisierten EDR-Prozess in Echtzeit. Ihre Daten werden so vor dem Ausschleusen oder Manipulieren geschützt, ohne dass Sie manuell eingreifen müssen und ohne den Endanwender in seiner Produktivität einzuschränken. So können Sie in Ruhe und zum von Ihnen präferierten Zeitpunkt den Befall analysieren und Maßnahmen einleiten, ohne in der Zwischenzeit die Konsequenzen des Befalls fürchten zu müssen.

WELCHE VORTEILE BIETET DIE LÖSUNG?

Für IT-Abteilungen

- 17x höhere Erkennungsrate bei Zero-Day Attacken als andere Hersteller (NGAV)
- Erkennt den Versuch von Schadsoftware Daten zu manipulieren oder zu stehlen und blockiert diesen automatisiert im Moment der versuchten Ausführung.
- Reduziert nachhaltig die Anzahl an Alerts und verkürzt die Zeit bis zur Unschädlichmachung durch Automation.

Für Endanwender

- Die Produktivität der Mitarbeiter wird nicht durch die Sicherheitsmaßnahmen eingeschränkt, da diese ohne Einbezug des Endanwenders agieren.
- Selbst im Falle eines Ausbruchs bekommt der Anwender die Konsequenzen der Malware nicht zu spüren.

Für Unternehmen

- Niedrigere Ausgaben für IT-Security-Teams, da Alert-Fatique (Überfluss and Alerts) maximal reduziert und die Endpunkte ohne manuelles dazutun geschützt werden.
- Sicherung der beiden wichtigsten Güter des Unternehmens. Daten und Produktivität der Mitarbeiter.
- Kein Imageschaden durch Datenverlust oder Ransomware, da die Auswirkungen eines Angriffs in Echtzeit blockiert werden.

3 Gründe weshalb Sie diese Lösung nutzen sollten:

1. Weil ca. 70% der Malware-Angriffe von Antivirus & Co. unerkannt bleiben
   Automated EDR schützt vor Malware und Zero-Day-Exploits vor (Next Gen Antivirus) und nach (EDR) der Infektion. Selbst wenn Ihr System befallen ist, wird der Versuch der Manipulation oder Extraktion Ihrer Daten in Echtzeit verhindert ohne die Produktivität Ihrer Endanwender zu gefährden.

2. Weil etwa 70% aller Angriffe Ihren Ursprung auf Endgeräten haben
   Automated EDR verhindert dank ausgereifter Technologien das Ausführen schädlicher Aktivitäten dort wo sie auftreten - direkt am Endpunkt.

3. Weil Bedrohungen auch da erkannt werden, wo der Ursprung nicht eine Datei ist
   Automated EDR arbeitet systemzentrisch, während klassische Anbieter dateizentrisch arbeiten. So können auch Bedrohungen erkannt werden, wo der Ursprung nicht einer Datei zuzuordnen ist.