Malware (Kötü Amaçlı Yazılım) Tespiti

Kötü amaçlı yazılım tespiti, kötü amaçlı yazılım ve dosyaların varlığı açısından bir bilgisayar sistemini veya ağını analiz etme sürecini ifade eder. Güvenlik ürünleri, bilinen kötü amaçlı yazılımların imzalarını kontrol ederek kötü amaçlı yazılımları tespit edebilir. Güvenlik araçları ayrıca yazılım etkinliğinden şüpheli davranışları tespit ederek kötü amaçlı etkinliği tespit edebilir. Kötü amaçlı yazılım bir sistemi enfekte ettiğinde, tespitten kaçınmak için çeşitli teknikler kullanarak sistemi değiştirebilir. Wazuh, kötü amaçlı dosyaları ve kötü amaçlı yazılımın varlığını gösteren anormal kalıpları tespit etmek için bu tekniklere karşı koymak amacıyla geniş spektrumlu bir yaklaşım kullanır.

Wazuh dosya bütünlüğü izleme (FIM) modülü, izlenen uç noktalardaki kötü amaçlı dosyaları tespit etmeye yardımcı olur. FIM modülü kendi başına kötü amaçlı dosyaları tespit edemez. Ancak, FIM modülünü tehdit tespit kuralları ve tehdit istihbarat kaynaklarıyla birleştirerek kötü amaçlı yazılımları tespit edebilirsiniz. Wazuh'u, dosya karmaları içeren VirusTotal ve CDB listeleri ve kötü amaçlı yazılımları tespit etmek için YARA taramaları gibi tehdit istihbarat kaynaklarıyla FIM olaylarını kullanacak şekilde yapılandırabilirsiniz.

Wazuh, Rootcheck modülünü kullanarak izlenen uç noktalardaki rootkit davranışını algılar . Rootcheck, uç noktaları sürekli olarak izler ve herhangi bir anormallik algıladığında uyarılar üretir. Anormallik izleme, Wazuh'un imza tabanlı tekniklerin kaçırmış olabileceği kötü amaçlı yazılımları algılamasını sağlar. Rootcheck ayrıca izlenen uç noktalardaki varlıklarını algılamak için bilinen rootkit ve truva atı imzalarını kullanır. Wazuh'un esnekliği, kullanıcıların bu rootkit imzalarını kendilerinin güncelleyebilmesini sağlar.

Wazuh günlük toplama yeteneği, üçüncü taraf kötü amaçlı yazılım tespit yazılımlarından günlükleri toplamanıza olanak tanır. Bu yeteneği kullanarak Wazuh, Windows Defender ve ClamAV gibi çeşitli kötü amaçlı yazılım tespit yazılımlarından günlükleri toplar ve analiz eder.

Revision #3
Created 23 December 2024 18:06:20 by Ayşegül Sarıkaya
Updated 31 December 2024 17:56:20 by Ayşegül Sarıkaya