Zararlı Tespiti

Kötü amaçlı yazılım, kötü amaçlı yazılım anlamına gelir ve bilgisayar sistemlerine, ağlara veya kullanıcılara zarar vermek veya bunları istismar etmek için özel olarak tasarlanmış herhangi bir yazılımı ifade eder. Yetkisiz erişim elde etmek, hasara yol açmak, hassas bilgileri çalmak veya hedef sistemde başka kötü amaçlı faaliyetler gerçekleştirmek amacıyla oluşturulur. Her biri belirli işlevlere ve enfeksiyon yöntemlerine sahip çeşitli kötü amaçlı yazılım türleri vardır. Bazı yaygın kötü amaçlı yazılım türleri arasında virüsler, solucanlar, fidye yazılımları, botnet'ler, casus yazılımlar, truva atları ve kök araç takımları bulunur.

Kötü amaçlı yazılım tespiti, bilgisayar sistemlerini ve ağlarını siber tehditlerden korumak için çok önemlidir. Veri ihlaline, sistem ihlaline ve mali kayba neden olabilecek kötü amaçlı yazılımları belirlemeye ve azaltmaya yardımcı olur.

Kötü Amaçlı Yazılım Tespiti İçin Wazuh

Yalnızca imza tabanlı tespitlere dayanan geleneksel yöntemlerin sınırlamaları vardır ve yeni tehditleri yakalamada başarısız olurlar. İmza tabanlı yaklaşımlar, sıfırıncı gün saldırılarını, polimorfik kötü amaçlı yazılımları ve tehdit aktörleri tarafından kullanılan diğer kaçınma tekniklerini tespit etmede zorluk çeker. Sonuç olarak, kuruluşlar tespit edilemeyen ihlaller ve veri sızdırma riski altındadır. Wazuh, kuruluşların karmaşık ve kaçamak tehditleri etkili bir şekilde tespit etmelerini ve bunlara yanıt vermelerini sağlar. Wazuh, kötü amaçlı yazılım özelliklerini, etkinlikleri, ağ bağlantılarını ve daha fazlasını tanımlayan farklı modülleri kapsar.

Tehdit Algılama Kurallarıyla Kötü Amaçlı Faaliyetlerin Tespiti

Wazuh, davranış tabanlı kötü amaçlı yazılım tespitini etkinleştiren tehdit tespit kurallarına sahiptir. Wazuh, yalnızca önceden tanımlanmış imzalara güvenmek yerine, kötü amaçlı yazılım tarafından sergilenen anormal davranışları izleme ve analiz etmeye odaklanır. Bu, Wazuh'un bilinen ve daha önce bilinmeyen tehditleri tespit etmesini sağlar. Bu şekilde, Wazuh siber tehditlere karşı proaktif ve uyarlanabilir bir savunma sağlar. Wazuh, tanınan kötü amaçlı yazılım kalıpları için uyarıları

tetiklemek üzere özel olarak tasarlanmış, kullanıma hazır kural setlerine sahiptir ve olası güvenlik olaylarına hızlı bir yanıt sağlar. Örneğin, aşağıdaki görüntü, `92213`kötü amaçlı yazılımlar tarafından yaygın olarak kullanılan bir klasöre bir yürütülebilir dosya bırakıldığında tetiklenen kural kimliğine sahip bir uyarıyı gösterir. Bu uyarı, güvenlik ekiplerini soruşturma ve düzeltme sürecini başlatmaya yönlendirir.



Yürütülebilir dosya kötü amaçlı yazılım uyarısı tarafından kullanılan klasöre bırakıldı

Wazuh, kullanıcıların algılamada daha fazla esneklik için özel kurallar oluşturmasına olanak tanır , ilgili etkinliklere odaklanmalarını ve kötü amaçlı yazılım algılamasını optimize etmelerini sağlar. Wazuh, izlenen uç noktalardan gelen günlükleri kod çözer ve alanlara düzenler, daha sonra kötü amaçlı etkinlik algılandığında uyarı vermek için özel kurallar oluşturmak üzere kullanılabilir.

Wazuh kuralları, yanlış pozitifleri azaltmak ve bilinen kötü amaçlı yazılımları belirli davranışlara göre tespit etmek için tehlike göstergelerini (IOC'ler) belirten birden fazla alan kullanır. Bu kurallar, kapsamlı tespit için saldırı, ayrıcalık yükseltme, yanal hareket, karartma ve sızdırma gibi ilgili kötü amaçlı yazılım etkinliklerini birbirine bağlayabilir.

Aşağıda, LimeRAT kötü amaçlı yazılımının kötü amaçlı faaliyetleri konusunda uyarı vermek için oluşturulmuş bazı Wazuh özel kurallarına bir örnek verilmiştir:

```
<group name="lime_rat,sysmon,">

  <!-- Rogue create netflix.exe creation -->
  <rule id="100024" level="12">
    <if_sid>61613</if_sid>
    <field name="win.eventdata.image" type="pcre2">\.exe</field>
    <field name="win.eventdata.targetFilename" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\che
    <description>Potential LimeRAT activity detected: checker netflix.exe created at $(win.eventdata.targetFilenam
    <mitre>
      <id>T1036</id>
    </mitre>
  </rule>

  <!-- Registry key creation for persistence -->
  <rule id="100025" level="12">
    <if_group>sysmon</if_group>
    <field name="win.eventdata.details" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\checker net
    <field name="win.eventdata.targetObject" type="pcre2" >HKU\\\\.+\\\\Software\\\\Microsoft\\\\Windows\\\\Curre
    <field name="win.eventdata.eventType" type="pcre2" >^SetValue$</field>
    <description>Potential LimeRAT activity detected:  $(win.eventdata.details) added itself to the Registry as a sta
    <mitre>
      <id>T1547.001</id>
    </mitre>
  </rule>

  <!-- Network activity detection -->
  <rule id="100026" level="12">
    <if_sid>61605</if_sid>
```

```
    <field name="win.eventdata.image" type="pcre2">(?i)[c-z]:\\\\Users\\\\.+\\\\AppData\\\\Roaming\\\\checker netf
    <description>Potential LimeRAT activity detected: Suspicious DNS query made by $(win.eventdata.image).</de
    <mitre>
      <id>T1572</id>
    </mitre>
  </rule>


  <!-- LimeRAT service creation -->
  <rule id="100028" level="12">
    <if_sid>61614</if_sid>
    <field name="win.eventdata.targetObject" type="pcre2" >HKLM\\\\System\\\\CurrentControlSet\\\\Services\\\\di
    <field name="win.eventdata.eventType" type="pcre2" >^CreateKey$</field>
    <description>Potential LimeRAT activity detected: LimeRAT service $(win.eventdata.targetObject) has been cre
      <mitre>
    <id>T1543.003</id>
      </mitre>
  </rule>

</group>
```

Bu kurallar , Wazuh panosundaki **Tehdit Avı** modülünde görülebilen uyarılar oluşturur .

LimeRAT özel uyarı örneği

Tam yapılandırma için Wazuh ile LimeRat tespiti ve tepkisi hakkındaki blog yazısına bakın .

Wazuh, kötü amaçlı yazılımlara işaret eden davranışları belirler, gerçek zamanlı uyarılar ve bildirimler üretir ve böylece güvenlik ekiplerinin hızlı bir şekilde yanıt vermesini ve potansiyel riskler tırmanmadan önce bunları azaltmasını sağlar.

Kötü Amaçlı Yazılım Etkinliğini Tespit Etmek İçin Dosya Bütünlüğü İzleme Özelliğinden Yararlanma

Dosya Bütünlüğü İzleme (FIM), kötü amaçlı yazılım tespitinde değerli bir bileşendir. Wazuh, izlenen uç noktalardaki dosya ve dizinlerdeki değişiklikleri izlemek ve tespit etmek için FIM yetenekleri sağlar. Bu değişiklikler oluşturma, değiştirme veya silmeyi içerir. FIM temel içgörüler sağlarken, onu diğer yetenekler ve entegrasyonlarla birleştirmek kötü amaçlı yazılım tespiti için etkinliğini daha da artırır. Wazuh, güvenlik ekiplerinin FIM olaylarına dayalı özel kurallar oluşturmasına olanak tanır ve hedefli kötü amaçlı yazılım tespitini mümkün kılar. Bu özelleştirilebilir kurallar, FIM olaylarını şüpheli dosya uzantıları, kod parçacıkları veya bilinen kötü amaçlı yazılım imzaları gibi

belirli tehlike göstergeleriyle ilişkilendirir.

Aşağıdaki görüntü, bir web kabuğunun web sunucusunda bir dosya oluşturduğunda veya değiştirdiğinde oluşan uyarıyı göstermektedir.

Web kabuğu FIM uyarısı

Kötü amaçlı yazılımlar, kalıcılık oluşturma ve diğer kötü amaçlı eylemleri gerçekleştirme gibi kötü amaçlı hedeflere ulaşmak için sıklıkla Windows Kayıt Defterini hedef alır. Wazuh Dosya Bütünlüğü İzleme (FIM) modülü, değişiklikleri tespit etmek için yaygın olarak hedeflenen kayıt defteri yollarını izleyen Windows Kayıt Defteri izlemesini içerir . Değişiklikler meydana geldiğinde, FIM modülü gerçek zamanlı uyarıları tetikleyerek güvenlik ekiplerinin şüpheli kayıt defteri anahtarı manipülasyonunu hızla belirlemesini ve bunlara yanıt vermesini sağlar.

Aşağıdaki görseller Wazuh FIM modülünün panosunu ve Windows Kayıt Defteri değişikliklerinin olaylarını göstermektedir.

FIM modül panosundaki Windows kayıt defteri değişiklikleri

Windows kayıt defteri değişiklikleri olaylarıyla FIM modülü

Tehdit İstihbaratı Entegrasyonuyla Kötü Amaçlı Yazılım Algılamayı Geliştirme

Kullanıcılar, tehdit istihbarat kaynaklarıyla entegre olarak kötü amaçlı yazılım tespit yeteneklerini artırabilirler . Bu istihbarat beslemeleri, bilinen kötü amaçlı IP adresleri, etki alanları, URL'ler ve diğer tehlike göstergeleri hakkında ek güncel bilgilerle Wazuh bilgi tabanını zenginleştirir. Wazuh'un entegre olabileceği tehdit istihbarat kaynaklarına örnek olarak VirusTotal, MISP ve daha fazlası verilebilir.

VirusTotal entegrasyon örneği uyarısı

Wazuh, tanımlanan IOC'leri CDB listelerinde (sabit veritabanları) depolanan bilgilerle karşılaştırarak kötü amaçlı dosyaları proaktif bir şekilde belirler . Bu listeler, dosya karmaları, IP adresleri ve etki alanı adları dahil olmak üzere bilinen kötü amaçlı yazılım tehlike göstergelerini (IOC'ler) depolayabilir.

`key:value`Girişleri, özelleştirilmiş algılama için her iki biçimde de özelleştirebilirsiniz `key:`, bunun bir örneği aşağıda görülmektedir. Mirai ve Xbash kötü amaçlı yazılımlarının bilinen MD5 kötü amaçlı yazılım karmalarını içeren bir CBD listesi algılama için kullanılır:

```
e0ec2cd43f71c80d42cd7b0f17802c73:mirai
55142f1d393c5ba7405239f232a6c059:Xbash
```

Tespit edildiğinde bu uyarılar, aşağıda görüldüğü gibi Wazuh kontrol panelinin **Tehdit Avı** modülünde gözlemlenir .

Bilinen kötü amaçlı yazılım karmasıyla dosya uyarısı

Tam yapılandırmalar için Kullanım örneğine bakın : CDB listesindeki dosya karma değerlerini kullanarak kötü amaçlı yazılımları tespit etme .

Rootkit Tespiti ile Gizli Tehditleri Açığa Çıkarma

Rootkit'ler, sistem çağrılarını değiştirmek veya çekirdek veri yapılarını değiştirmek gibi işletim sistemi işlevlerini manipüle ederek bir uç noktadaki kötü amaçlı yazılımların varlığını gizlemek için tasarlanmış kötü amaçlı yazılımlardır. Wazuh, izlenen uç noktayı periyodik olarak tarayarak hem çekirdek hem de kullanıcı alanı düzeyinde rootkit'leri tespit eden bir Rootcheck modülüne sahiptir . Rootcheck, olası rootkit etkinliğini belirler ve uyarır. Wazuh, sistem davranışını analiz ederek ve bunu bilinen rootkit kalıplarıyla karşılaştırarak rootkit ile ilgili kalıpları derhal tespit eder ve daha fazla araştırma için uyarılar verir.

Aşağıda, Wazuh Rootcheck modülünün dosya sisteminde bir anormallik tespit ettiğinde oluşturduğu bir uyarının örneğini gösteriyoruz:

```
** Alert 1668497750.1838326: - ossec,rootcheck,pci_dss_10.6.1,gdpr_IV_35.7.d,
2022 Nov 15 09:35:50 (Ubuntu) any->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 't0rn' detected by the presence of file '/usr/bin/.t0rn'.
title: Rootkit 't0rn' detected by the presence of file '/usr/bin/.t0rn'.
```

Wazuh, rootkit davranış algılama yeteneklerini geliştirmeye devam ederken , Komut izleme modülü ayrıca uç noktalardaki komut satırı etkinliklerini izlemek üzere yapılandırılabilir ve bu da kötü amaçlı komutların ve kötü amaçlı yazılım etkinliklerinin algılanmasını sağlar. Bu modül, kuruluşlara gizli tehditleri ortaya çıkarmak ve sistemlerini etkili bir şekilde korumak için kapsamlı bir yaklaşım sağlar.

İzleme Sistemi Kötü Amaçlı Yazılım ve Anormallik Algılamayı Gerektirir

Wazuh, kötü amaçlı yazılım tespitini güçlendirmek ve anormallik tespitine yardımcı olmak için Linux uç noktalarındaki sistem çağrılarını izler . Wazuh, sistem çağrılarını izlemek için Linux Denetim sistemini kullanır.

Wazuh Dosya Bütünlüğü İzleme (FIM) ve tehdit istihbaratı entegrasyonuyla birlikte sistem çağrısı izleme, kötü amaçlı yazılım tespitini geliştirir. Dosya erişimi, komut yürütme ve ayrıcalık yükseltme gibi güvenlikle ilgili olayları yakalayarak olası güvenlik olaylarına ilişkin gerçek zamanlı içgörüler sağlar. Bu kapsamlı yaklaşım, kuruluşların siber güvenlik dayanıklılığını güçlendirir. Aşağıdaki görüntüde, Ubuntu Linux 22.04 için Wazuh panosundaki ayrıcalık kötüye kullanımı uyarılarını görselleştirebilirsiniz.

Ayrıcalık kötüye kullanımı uyarıları

Wazuh, güvenlik ekiplerinin Auditd tarafından sağlanan denetim kurallarını kullanmasını sağlar. Sistem çağrı olaylarına dayalı özel kurallar oluşturmak kötü amaçlı yazılım tespit çabalarını geliştirir ve genel siber güvenlik dayanıklılığını güçlendirir.

Revision #6
Created 6 December 2023 17:38:45 by LastGuard
Updated 23 December 2024 19:25:45 by Ayşegül Sarıkaya