Tehdit Avcılığı

Tehdit avcılığı, geleneksel güvenlik önlemlerinden kaçan siber tehditleri belirlemek ve ortadan kaldırmak için günlükler, ağ trafiği ve uç nokta verileri gibi çok sayıda veri kaynağını analiz etmeyi içeren proaktif bir yaklaşımdır. Bir BT ortamında tespit edilememiş olabilecek potansiyel tehditleri ortaya çıkarmayı amaçlar. Tehdit avcılığı süreci genellikle birkaç adımı içerir: hipotez oluşturma, veri toplama, analiz ve yanıt.

Wazuh, güvenlik ekiplerinin bulundukları ortamdaki tehditleri tespit etmelerine yardımcı olan ve tehditleri kontrol altına almak ve daha fazla hasarı önlemek için hızlı aksiyon almalarını sağlayan çeşitli yetenekler sunuyor.

Günlük Veri Analizi

Etkili günlük veri toplama ve analizi, tehdit avı metodolojinizi geliştirmek için olmazsa olmazdır. Tehdit avı çabalarınızı optimize etmek için Wazuh'un sağlam yeteneklerinden yararlanabilirsiniz.

Birleşik bir XDR ve SIEM platformu olan Wazuh, uç noktalar, ağ cihazları ve uygulamalar gibi çeşitli kaynaklardan veri toplanmasına olanak tanıyan merkezi günlük veri toplama sunar. Bu merkezi yaklaşım, analizi basitleştirir ve birden fazla kaynağı izlemek için gereken çabayı azaltır.

Aşağıdaki görsel, izlenen bir uç noktadan denetim günlüklerini toplamak için Wazuh dashboard yapılandırma ayarlarını göstermektedir.

Günlük toplama ayarları

Wazuh, çeşitli kaynaklardan elde edilen günlük verilerinden anlamlı bilgiler çıkarmak için kod çözücüler kullanır. Ham günlük verilerini zaman damgası, kaynak IP adresi, hedef IP adresi, olay türü ve diğerleri gibi ayrı alanlara veya özniteliklere ayırır. Wazuh panosundaki Dizin desenleri sekmesi, dizin `wazuh-alerts-*` desenini ve alanlarını gösterir.

wazuh-alerts-* dizin deseni

Wazuh, verimli günlük verisi işleme için ajansız izleme ve syslog log toplama sunar . Çeşitli günlük formatları arasında tutarlılık ve uyumluluk sağlar. Wazuh dizinleme ve sorgulama yetenekleri, belirli günlük verilerine hızlı arama ve erişimi kolaylaştırır, analiz ve araştırmayı kolaylaştırır. Wazuh, gelişmiş ayrıştırma ve gerçek zamanlı analizini kullanarak riskleri proaktif olarak belirleyip azaltarak tehdit avını geliştirir ve böylece güvenliği artırır.

Wazuh Arşivleri

Wazuh, izlenen uç noktalardan toplanan tüm günlükleri arşivlemek için merkezi bir depolama konumu sağlar. Wazuh arşiv günlükleri, Wazuh panosunda uyarı tetiklemeyen günlükleri içerir. Wazuh arşivleri varsayılan olarak devre dışıdır ve kolayca etkinleştirilebilir. Ayrıntılı günlüklerin kullanılabilirliği, ortamınıza kapsamlı görünürlük sağlayarak etkili tehdit avcılığı için çok önemlidir.

Wazuh arşivleri, ortamınızdaki belirli izlenen uç noktalardaki olayları analiz etmek için somut görünürlük sağlayan günlük tutma, dizinleme ve sorgulama yetenekleri sağlar. Bu, olay nedenlerini, olay konumlarını, olay iletişimlerini, olay zaman damgalarını ve ilgili ebeveyn-çocuk süreçlerini ortaya çıkarmayı kolaylaştırır. Aşağıdaki görüntü, Wazuh panosundaki **Keşfet** bölümündeki arşivlenmiş günlükleri gösterir.

Keşfet bölümünde wazuh arşivleri
Image not found or type unknown

MITRE ATT&CK Haritalama

MITRE ATT&CK çerçevesi, siber saldırı taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) haritalamak ve anlamak için standart bir yaklaşım sunar. Wazuh MITRE ATT&CK modülünü kullanarak , tehdit aktörleri tarafından kullanılan TTP'lere ilişkin anlayışımızı geliştirebilir ve bunlara karşı proaktif bir şekilde savunma sağlayabiliriz.

Wazuh MITRE ATT&CK modülü, TTP'leri oluşturulan olaylara eşler ve saldırgan davranışındaki kalıpları hemen belirleyerek etkili tehdit avını kolaylaştırır. Örneğin, şüpheli bir oturum açma girişimi, MITRE ATT&CK çerçevesindeki "Kimlik Bilgisi Doldurma" tekniğiyle ilişkilendirilebilir. Bu, kullanıcıların bu tür saldırıların sıklığını değerlendirmesini ve çok faktörlü kimlik doğrulamayı etkinleştirme veya oturum açma girişimlerini hız sınırlama gibi riskleri azaltmak için gerekli önlemleri uygulamasını sağlar. Wazuh panosundaki **MITRE ATT&CK** modülü, izlenen bir ortamda bulunan çeşitli teknikleri görüntülemenizi sağlar.

MITRE ATT&CK modülü
Image not found or type unknown

Bu modül, Wazuh panosunda belirli TTP kullanan saldırıların sıklığını ve ciddiyetini gösteren raporlar ve görselleştirmeler üretir. Bu raporlar, güvenlik standartlarına ve yönetmeliklerine uyumu izlemeye yardımcı olurken, güvenlik önlemlerinin güçlendirilmesi gerekebilecek alanları vurgular. Wazuh panosundaki Wazuh **MITRE ATT&CK** modülü, aşağıda görüldüğü gibi izlenen bir ortamda bulunan TTP'lerin genel görünümünü gösteren özelleştirilebilir bir panoya sahiptir.

MITRE ATT&CK modülü kontrol paneli
Image not found or type unknown

MITRE ATT&CK çerçevesinden gelen içgörülerden yararlanarak sistemlerinizi ve verilerinizi proaktif olarak koruyabilirsiniz. MITRE ATT&CK'nin Wazuh ile entegrasyonu tehdit avını önemli ölçüde iyileştirir ve genel güvenliği iyileştirir.

Üçüncü Taraf Entegrasyonu

Wazuh, tehdit avlama yeteneklerini geliştiren üçüncü taraf çözümlerle entegre olur . Bu entegrasyonlar, kullanıcıların çeşitli kaynaklardan gelen verileri birleştirmesini ve tehdit algılama ve yanıtını otomatikleştirmesini sağlar. Wazuh, VirusTotal, AlienVault, URLHaus, MISP ve diğerleri gibi popüler açık kaynak platformlarıyla sorunsuz bir şekilde entegre olur. Bu entegrasyon, kullanıcıların tehdit istihbaratı beslemeleriyle telemetriyi çapraz referanslamasını sağlayarak tehdit algılama ve yanıtını iyileştirir.

Üçüncü taraf entegrasyonları, tehdit istihbaratını ve bir dizi iş birliği aracını kapsayan proaktif tehdit avında önemli bir rol oynar. Bu entegrasyonlar, hem yerleşik hem de ortaya çıkan tehditler hakkında temel içgörüler sunarak tehdit tespitine yönelik kapsamlı ve ileriye dönük bir yaklaşım sağlar. Bu entegrasyonlar, deneyimli güvenlik ekipleri arasında bilgi alışverişini teşvik ederek, genel tehdit avlama sürecinin etkinliğini artıran kolektif bir savunma stratejisini teşvik eder.

Wazuh'un tehdit avına yardımcı olmak için entegre olduğu bazı üçüncü taraf çözümleri şunlardır:

- **VirusTotal** : VirusTotal'ı entegre etmek, doğru tanımlama ve daha hızlı olay müdahalesi için VirusTotal kötü amaçlı yazılım veritabanından yararlanarak tehdit tespitini geliştirir. Aşağıdaki görüntü, VirusTotal entegrasyonu aracılığıyla kötü amaçlı yazılım tespitini gösterir.

  > Image not found or type unknown
  > VirusTotal entegrasyonu aracılığıyla kötü amaçlı yazılım tespiti

- **URLHaus** : URLHaus by abuse.ch'nin Wazuh ile entegre edilmesi, tehdit istihbarat yeteneklerini artırarak kullanıcıların kötü amaçlı URL'leri gerçek zamanlı olarak proaktif bir şekilde tespit edip engellemesini sağlıyor.
- **osquery** : Wazuh, osquery aracını Wazuh ajanlarından yönetmek için bir modül sağlar. osquery modülü, güvenlik analistlerinin osquery tarafından oluşturulan bilgileri yapılandırmasına ve toplamasına olanak tanır. Yapılandırma yönetimi, veri toplama, osquery sorgu sonuçlarına dayalı özel uyarılar ve SQL benzeri sözdizimi sorguları gibi tehdit avlama yetenekleri için ekstra bir katman sağlar.
- **MISP** : IOC'lerin tanımlanmasını otomatikleştirerek ve MISP'yi Wazuh ile entegre ederek Wazuh uyarılarını zenginleştirebiliriz.

Wazuh, yukarıda belirtilenlerin ötesinde tehdit avına yardımcı olan diğer araçlarla entegre olur. API'ler ve diğer entegrasyon yöntemlerini kullanarak tehdit istihbarat platformları, SIEM'ler ve mesajlaşma platformları için üçüncü taraf entegrasyonlarını destekler.

Kurallar ve kod çözücüler

Wazuh, çeşitli saldırı vektörleri ve siber faaliyetler için sağlam kurallar, kod çözücüler ve önceden yapılandırılmış kurallarla tehdit avcılığını geliştirir.

Wazuh panosundaki **Kurallar** modülü , aşağıda görülen sistem anormallikleri, kötü amaçlı yazılım tespiti, kimlik doğrulama hataları ve diğer potansiyel tehditler de dahil olmak üzere çok çeşitli güvenlik olaylarını kapsayan hem varsayılan hem de özel kuralları sunar.

Wazuh panosu kuralları görünümü

Wazuh, kendi kurallarınızı ve kod çözücülerinizi özelleştirmenize ve oluşturmanıza olanak tanır , bunlar belirli ortamınıza ve tehdit manzaranıza göre uyarlanmıştır. Bu, algılamayı ince ayarlamanıza, benzersiz gereksinimleri ele almanıza ve kör noktaları en aza indirmenize olanak tanır.

Wazuh kod çözücüler, çeşitli günlük formatlarını ve veri kaynaklarını normalleştirme ve ayrıştırmada hayati bir rol oynar. Toplanan bilgilerin standart bir şekilde sunulmasını sağlayarak çeşitli kaynaklardan gelen verilerin etkili bir şekilde analiz edilmesini ve ilişkilendirilmesini kolaylaştırır.

Wazuh panosundaki Decoders modülü varsayılan ve özel decoder'ları görüntülemenizi sağlar. Aşağıdaki görüntü varsayılan decoder'ın ayrıntılarını gösterir `agent-upgrade`.

Varsayılan araç yükseltme kod çözücüsünün ayrıntıları

Güvenlik ekipleri, Wazuh kuralları ve kod çözücülerinden yararlanarak eyleme dönüştürülebilir içgörüler elde ediyor ve bu sayede IOC'leri, anormal davranışları ve potansiyel ihlalleri hızla tespit edebiliyor.

Özel kuralları ve kod çözücüleri yapılandırmaya ilişkin ayrıntılı kılavuz için Wazuh kuralları seti belgelerine bakın .

Revision #6
Created 6 December 2023 17:39:29 by LastGuard
Updated 30 December 2024 16:13:14 by Ayşegül Sarıkaya