Komponentler

Wazuh platformu, bulutunuzu, konteynerinizi ve sunucu iş yüklerinizi korumak için XDR ve SIEM özellikleri sağlar. Bunlara günlük veri analizi, saldırı ve kötü amaçlı yazılım tespiti, dosya bütünlüğü izleme, yapılandırma değerlendirmesi, güvenlik açığı tespiti ve düzenleyici uyumluluk desteği dahildir. Wazuh çözümü, izlenen uç noktalara ve üç merkezi bileşene (Wazuh sunucusu, Wazuh dizinleyicisi ve Wazuh panosu) dağıtılan Wazuh aracısına dayanmaktadır. • Wazuh dizinleyicisi, son derece ölçeklenebilir, tam metin arama ve analiz motorudur. Bu merkezi bileşen, Wazuh sunucusu tarafından oluşturulan uyarıları dizinler ve depolar. • Wazuh sunucusu, ajanlardan alınan verileri analiz eder. Bunu kod çözücüler ve kurallar aracılığıyla işler ve bilinen tehlike göstergelerini (IOC'ler) aramak için tehdit istihbaratını kullanır. Tek bir sunucu, yüzlerce veya binlerce ajandan gelen verileri analiz edebilir ve bir küme olarak kurulduğunda yatay olarak ölçeklenebilir. Bu merkezi bileşen ayrıca ajanları yönetmek, gerektiğinde bunları uzaktan yapılandırmak ve yükseltmek için kullanılır. • Wazuh panosu , veri görselleştirme ve analizi için web kullanıcı arayüzüdür. Tehdit avcılığı, düzenleyici uyumluluk (örneğin, PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), tespit edilen güvenlik açığı uygulamaları, dosya bütünlüğü izleme verileri, yapılandırma değerlendirme sonuçları, bulut altyapısı izleme olayları ve diğerleri için kullanıma hazır panolar içerir. Ayrıca Wazuh yapılandırmasını yönetmek ve durumunu izlemek için kullanılır. • Wazuh ajanları dizüstü bilgisayarlar, masaüstü bilgisayarlar, sunucular, bulut örnekleri veya sanal makineler gibi uç noktalara yüklenir. Tehdit önleme, algılama ve yanıtlama yetenekleri sağlarlar. Linux, Windows, macOS, Solaris, AIX ve HP-UX gibi işletim sistemlerinde çalışırlar. Wazuh platformu, aracı tabanlı izleme yeteneklerine ek olarak, güvenlik duvarları, anahtarlar, yönlendiriciler veya ağ IDS'leri gibi aracı olmayan cihazları da izleyebilir. Örneğin, bir sistem günlük verisi Syslog aracılığıyla toplanabilir ve yapılandırması, verilerinin periyodik olarak incelenmesi, SSH veya bir API aracılığıyla izlenebilir.

- Wazuh Indexer
- Wazuh Server
- Wazuh Dashboard
- Wazuh Agent

Wazuh Indexer

Wazuh dizinleyicisi, son derece ölçeklenebilir, tam metin arama ve analiz motorudur. Bu Wazuh merkezi bileşeni, Wazuh sunucusu tarafından oluşturulan uyarıları dizinler ve depolar ve neredeyse gerçek zamanlı veri arama ve analiz yetenekleri sağlar. Wazuh dizinleyicisi, ölçeklenebilirlik ve yüksek kullanılabilirlik sağlayan tek düğümlü veya çok düğümlü bir küme olarak yapılandırılabilir.

Wazuh dizinleyicisi verileri JSON belgeleri olarak depolar. Her belge, bir dizi anahtar, alan adı veya özelliği, dizeler, sayılar, boole değerleri, tarihler, değer dizileri, coğrafi konumlar veya diğer veri türleri olabilen karşılık gelen değerleriyle ilişkilendirir.

Bir dizin, birbirleriyle ilişkili belgelerin bir koleksiyonudur. Wazuh dizinleyicisinde depolanan belgeler, parçalar olarak bilinen farklı kapsayıcılara dağıtılır. Belgeleri birden fazla parçaya ve bu parçaları birden fazla düğüme dağıtarak, Wazuh dizinleyici yedekliliği sağlayabilir. Bu, sisteminizi donanım arızalarına karşı korur ve düğümler bir kümeye eklendikçe sorgu kapasitesini artırır.

Wazuh farklı olay türlerini depolamak için dört farklı endeks kullanır:

Dizin	Tanım
wazuh - **uyarılar**	Wazuh sunucusu tarafından oluşturulan uyarıları depolar . Bunlar, bir olay yeterince yüksek önceliğe sahip bir kuralı tetiklediğinde her seferinde oluşturulur (bu eşik yapılandırılabilir).
wazuh - **arşivler**	Wazuh sunucusu tarafından alınan tüm olayları (arşiv verileri) , bir kuralı tetikleyip tetiklemediğine bakılmaksızın depolar.
wazuh - **izleme**	Wazuh aracı durumuyla ilgili verileri zaman içinde depolar. Web arayüzü tarafından bireysel aracıların ne zaman olduğunu veya olduğunu göstermek için kullanılır `Active`, `Disconnected`, veya . `Never connected`
wazuh - **istatistikler**	Wazuh sunucu performansıyla ilgili verileri depolar . Web arayüzü tarafından performans istatistiklerini temsil etmek için kullanılır.

Wazuh dizinleyici
Image not found or type unknown

Örnek Sorgu

Wazuh dizinleyici kümesiyle etkileşime girebilirsiniz, bu da çok fazla esneklik sunar. Aramalar yapabilir, belgeler ekleyebilir veya silebilir, dizinleri değiştirebilir ve daha fazlasını yapabilirsiniz.

İşte SSH tekniğini kullanarak son yanal hareket uyarısını döndüren Wazuh indeksleyicisine bir sorgu örneği:

```
GET /wazuh-alerts-4.x-*/_search
{
```

```
  "query": {
    "bool": {
      "must": [
        {"term": { "rule.mitre.tactic": "Lateral Movement" } },
        {"term": { "rule.mitre.technique": "SSH" } }
      ]
    }
  },
  "sort": [
    { "timestamp": { "order": "desc" } }
  ],
  "size": 1
}
```

Aşağıda, dizinlenmiş uyarı belgesinin bir parçası olan sorgu sonucunun bir özeti yer almaktadır:

Output


```
{
  "timestamp" : "2022-04-24T17:24:56.110+0000",
  "agent" : {
    "ip" : "10.0.1.52",
    "name" : "Amazon",
    "id" : "001"
  },
  "data" : {
    "srcip" : "68.183.216.91",
    "srcport" : "53820"
  },
  "rule" : {
    "description" : "sshd: insecure connection attempt (scan).",
    "id" : "5706",
    "level" : 6,
    "pci_dss" : ["11.4"],
    "mitre" : {
      "technique" : [
        "SSH"
      ],
      "id" : ["T1021.004"],
      "tactic" : [
        "Lateral Movement"
      ]
    }
  },
  "full_log" : "Apr 24 17:24:55 ip-10-0-1-52 sshd[32179]: Did not receive identification string from 68.183.216.91 p
  "location" : "/var/log/secure",
  "predecoder" : {
    "hostname" : "ip-10-0-1-52",
    "program_name" : "sshd",
    "timestamp" : "Apr 24 17:24:55"
  },
  "decoder" : {
```

```
    "parent" : "sshd",
    "name" : "sshd"
   },
   "GeoLocation" : {
    "city_name" : "Frankfurt am Main",
    "country_name" : "Germany",
    "region_name" : "Hesse"
   }
}
```


Wazuh dizinleyicisi, neredeyse gerçek zamanlı bir arama platformu olduğu için güvenlik analitiği ve altyapı izleme gibi zamana duyarlı kullanım durumları için oldukça uygundur. Bir belgenin dizine eklenmesinden aranabilir hale gelmesine kadar geçen gecikme süresi çok kısadır, genellikle bir saniyedir.

Wazuh indeksleyicisinin hızı, ölçeklenebilirliği ve dayanıklılığının yanı sıra, veri toplama, uyarı, anormallik tespiti ve indeks yaşam döngüsü yönetimi gibi verileri depolamayı ve aramayı daha da verimli hale getiren çeşitli yerleşik özellikleri vardır.

Wazuh Server

Wazuh sunucu bileşeni, ajanlardan alınan verileri analiz ederek tehditler veya anormallikler algılandığında uyarıları tetikler. Ayrıca, ajan yapılandırmasını uzaktan yönetmek ve durumlarını izlemek için kullanılır.

Wazuh sunucusu, algılama yeteneklerini geliştirmek için tehdit istihbarat kaynaklarını kullanır. Ayrıca, MITRE ATT&CK çerçevesini ve PCI DSS, GDPR, HIPAA, CIS ve NIST 800-53 gibi düzenleyici uyumluluk gereksinimlerini kullanarak uyarı verilerini zenginleştirir ve güvenlik analitiği için yararlı bir bağlam sağlar.

Ek olarak, Wazuh sunucusu ServiceNow , Jira ve PagerDuty gibi bilet sistemleri ve Slack gibi anlık mesajlaşma platformları dahil olmak üzere harici yazılımlarla entegre edilebilir . Bu entegrasyonlar güvenlik operasyonlarını kolaylaştırmak için uygundur.

Sunucu Mimarisi

Wazuh sunucusu analiz motorunu, Wazuh RESTful API'sini, aracı kayıt hizmetini, aracı bağlantı hizmetini, Wazuh küme arka plan programını ve Filebeat'i çalıştırır. Sunucu bir Linux işletim sistemine kurulur ve genellikle bağımsız bir fiziksel makinede, sanal makinede, docker konteynerinde veya bulut örneğinde çalışır.

Aşağıdaki diyagram sunucu mimarisini ve bileşenlerini göstermektedir:

Wazuh sunucu mimarisi
Image not found or type unknown

Sunucu Bileşenleri

Wazuh sunucusu, yeni aracıları kaydetme, her bir aracının kimliğini doğrulama ve Wazuh aracısı ile Wazuh sunucusu arasındaki iletişimi şifreleme gibi farklı işlevlere sahip aşağıda listelenen birkaç bileşenden oluşur.

- **Aracı kayıt hizmeti:** Yeni aracıları kaydetmek için kullanılır. Bu hizmet her aracıya benzersiz kimlik doğrulama anahtarları sağlar ve dağıtır. İşlem bir ağ hizmeti olarak çalışır ve TLS/SSL sertifikaları aracılığıyla veya sabit bir parola sağlayarak kimlik doğrulamayı destekler.
- **Aracı bağlantı hizmeti:** Bu hizmet aracılardan veri alır. Her aracı kimliğini doğrulamak ve Wazuh aracısı ile Wazuh sunucusu arasındaki iletişimleri şifrelemek için kayıt hizmeti tarafından paylaşılan anahtarları kullanır. Ayrıca, bu hizmet merkezi yapılandırma yönetimi sağlayarak yeni aracı ayarlarını uzaktan göndermenize olanak tanır.

- **Analiz motoru:** Bu, veri analizini gerçekleştiren sunucu bileşenidir. İşlenen bilgi türünü (Windows olayları, SSH günlükleri, web sunucusu günlükleri ve diğerleri) belirlemek için kod çözücüleri kullanır. Bu kod çözücüler ayrıca günlük iletilerinden kaynak IP adresi, olay kimliği veya kullanıcı adı gibi ilgili veri öğelerini çıkarır. Daha sonra, motor kuralları kullanarak, uyarıları tetikleyebilecek ve hatta otomatik karşı önlemler (örneğin, bir IP adresini yasaklama, çalışan bir işlemi durdurma veya kötü amaçlı yazılım eserini kaldırma) gerektirebilecek kod çözülmüş olaylardaki belirli kalıpları belirler.
- **Wazuh RESTful API:** Bu hizmet, Wazuh altyapısıyla etkileşim kurmak için bir arayüz sağlar. Aracıların ve sunucuların yapılandırma ayarlarını yönetmek, altyapı durumunu ve genel sağlığı izlemek, Wazuh kod çözücülerini ve kurallarını yönetmek ve düzenlemek ve izlenen uç noktaların durumu hakkında sorgulama yapmak için kullanılır. Wazuh panosu da bunu kullanır.
- **Wazuh küme arka planı:** Bu hizmet, Wazuh sunucularını yatay olarak ölçeklendirmek ve bunları bir küme olarak dağıtmak için kullanılır. Bu tür bir yapılandırma, bir ağ yük dengeleyicisiyle birleştirildiğinde yüksek kullanılabilirlik ve yük dengeleme sağlar. Wazuh küme arka planı, Wazuh sunucularının birbirleriyle iletişim kurmak ve senkronize kalmak için kullandıkları şeydir.
- **Filebeat:** Wazuh dizinleyicisine olayları ve uyarıları göndermek için kullanılır. Wazuh analiz motorunun çıktısını okur ve olayları gerçek zamanlı olarak gönderir. Ayrıca, çok düğümlü bir Wazuh dizinleyici kümesine bağlandığında yük dengelemesi sağlar.

Wazuh Dashboard

Wazuh panosu, güvenlik olaylarını ve uyarı verilerini çıkarmak, analiz etmek ve görselleştirmek için esnek ve sezgisel bir web kullanıcı arayüzüdür. Ayrıca Wazuh platformunun yönetimi ve izlenmesi için de kullanılır. Ek olarak, rol tabanlı erişim kontrolü (RBAC) ve tek oturum açma (SSO) için özellikler sağlar.

Veri Görselleştirme ve Analizi

Web arayüzü, kullanıcıların Wazuh aracısı tarafından toplanan farklı veri türleri ve Wazuh sunucusu tarafından oluşturulan güvenlik uyarıları arasında gezinmesine yardımcı olur. Kullanıcılar ayrıca raporlar oluşturabilir ve özel görselleştirmeler ve panolar oluşturabilir.

Örneğin Wazuh, PCI DSS, GDPR, HIPAA ve NIST 800-53 gibi düzenleyici uyumluluk için kullanıma hazır panolar sağlar. Ayrıca MITRE ATT&CK çerçevesi ve ilgili uyarılar arasında gezinmek için bir arayüz sağlar.

• Uç nokta güvenliği • Güvenlik operasyonları	• Tehdit istihbaratı • Bulut güvenliği

Aracıların İzlenmesi ve Yapılandırılması

Wazuh panosu kullanıcıların aracı yapılandırmasını yönetmelerine ve durumlarını izlemelerine olanak tanır. Örneğin, izlenen her uç nokta için kullanıcılar hangi aracı modüllerinin etkinleştirileceğini, hangi günlük dosyalarının okunacağını, hangi dosyaların bütünlük değişiklikleri için izleneceğini veya hangi yapılandırma kontrollerinin gerçekleştirileceğini tanımlayabilir.

Ajanların izlenmesi

Platform Yönetimi

Wazuh dashboard (panosu), Wazuh dağıtımınızı yönetmeye adanmış bir kullanıcı arayüzü sağlar. Bu, farklı Wazuh bileşenlerinin durumunu, günlüklerini ve istatistiklerini izlemeyi içerir. Ayrıca Wazuh sunucusunu yapılandırmayı ve günlük analizi ve tehdit tespiti için özel kurallar ve kod çözücüler oluşturmayı içerir.

Platform yönetimi

Geliştirici Araçları

Wazuh panosu, günlük mesajlarını nasıl çözüldüğünü ve bir tehdit algılama kuralıyla eşleşip eşleşmediğini kontrol etmek için işleyebilen bir Kural Seti Test aracı içerir. Bu özellik, özel kod çözücüler ve kurallar oluşturulduğunda ve kullanıcı bunları test etmek istediğinde özellikle yararlıdır.

Kural seti testi

Wazuh panosu ayrıca kullanıcıların Wazuh API'siyle etkileşim kurması için bir API konsolu içerir. Bu, Wazuh dağıtımını yönetmek için kullanılabilir (örneğin, sunucu veya aracı yapılandırmalarını yönetmek, durumu ve günlük mesajlarını izlemek, aracıları eklemek veya kaldırmak vb.).

Sunucu yönetimi > Geliştirme Araçları	Güvenlik kuralları oluşturma

Wazuh Agent

Wazuh aracısı Linux, Windows, macOS, Solaris, AIX ve diğer işletim sistemlerinde çalışır. Dizüstü bilgisayarlara, masaüstü bilgisayarlara, sunuculara, bulut örneklerine, kapsayıcılara veya sanal makinelere dağıtılabilir. Aracı, tehdit önleme, algılama ve yanıt yetenekleri sağlayarak sisteminizi korumaya yardımcı olur. Ayrıca, şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla Wazuh sunucusuna ilettiği farklı türdeki sistem ve uygulama verilerini toplamak için kullanılır .

Aracı Mimarisi

Wazuh aracısı modüler bir mimariye sahiptir. Her bileşen, dosya sistemini izleme, günlük mesajlarını okuma, envanter verilerini toplama, sistem yapılandırmasını tarama ve kötü amaçlı yazılım arama gibi kendi görevlerinden sorumludur. Kullanıcılar, aracı modüllerini yapılandırma ayarları aracılığıyla yönetebilir ve çözümü kendi özel kullanım durumlarına uyarlayabilir.

Aşağıdaki diyagram, aracı mimarisini ve bileşenlerini göstermektedir:

Aracı mimarisi
Image not found or type unknown

Ajan Modülleri

Tüm aracı modülleri yapılandırılabilir ve farklı güvenlik görevleri gerçekleştirir. Bu modüler mimari, her bileşeni güvenlik ihtiyaçlarınıza göre etkinleştirmenize veya devre dışı bırakmanıza olanak tanır. Aşağıda tüm aracı modüllerinin farklı amaçları hakkında bilgi edinebilirsiniz.

- **Günlük toplayıcı:** Bu aracı bileşeni, işletim sistemi ve uygulama günlük mesajlarını toplayarak düz günlük dosyalarını ve Windows olaylarını okuyabilir. Windows olayları için XPath filtrelerini destekler ve Linux Denetim günlükleri gibi çok satırlı biçimleri tanır. Ayrıca JSON olaylarını ek meta verilerle zenginleştirebilir.
- **Komut yürütme:** Aracılar, yetkili komutları periyodik olarak çalıştırır, çıktılarını toplar ve daha fazla analiz için Wazuh sunucusuna geri bildirir. Bu modülü, kalan sabit disk alanını izlemek veya son oturum açan kullanıcıların listesini almak gibi farklı amaçlar için kullanabilirsiniz.
- **Dosya bütünlüğü izleme (FIM):** Bu modül, dosyalar oluşturulduğunda, silindiğinde veya değiştirildiğinde raporlama yaparak dosya sistemini izler. Dosya özniteliklerindeki, izinlerdeki, sahiplikteki ve içerikteki değişiklikleri takip eder. Bir olay meydana geldiğinde, gerçek zamanlı olarak kim, ne ve ne zaman ayrıntılarını yakalar. Ayrıca, FIM modülü izlenen dosyaların durumuyla bir veritabanı oluşturur ve korur ve sorguların uzaktan çalıştırılmasına olanak tanır.
- **Güvenlik yapılandırması değerlendirmesi (SCA):** Bu bileşen, İnternet Güvenliği Merkezi (CIS) kıyaslamalarına dayalı olarak kullanıma hazır kontrolleri kullanarak sürekli yapılandırma değerlendirmesi sağlar. Kullanıcılar ayrıca güvenlik politikalarını izlemek ve

uygulamak için kendi SCA kontrollerini oluşturabilirler.

- **Sistem envanteri:** Bu aracı modülü, işletim sistemi sürümü, ağ arayüzleri, çalışan işlemler, yüklü uygulamalar ve açık portların listesi gibi envanter verilerini toplayarak periyodik olarak taramalar çalıştırır. Tarama sonuçları, uzaktan sorgulanabilen yerel SQLite veritabanlarında saklanır.
- **Kötü amaçlı yazılım tespiti:** İmza tabanlı olmayan bir yaklaşım kullanarak, bu bileşen anormallikleri ve olası kök araç takımlarının varlığını tespit edebilir. Ayrıca, sistem çağrılarını izlerken gizli süreçleri, gizli dosyaları ve gizli bağlantı noktalarını arar.
- **Active Response:** Bu modül, tehditler algılandığında otomatik eylemler çalıştırır ve bir ağ bağlantısını engellemek, çalışan bir işlemi durdurmak veya kötü amaçlı bir dosyayı silmek için yanıtları tetikler. Kullanıcılar ayrıca gerektiğinde özel yanıtlar oluşturabilir ve örneğin bir ikili dosyayı bir sanal alanda çalıştırmak, ağ trafiğini yakalamak ve bir dosyayı bir antivirüsle taramak için yanıtları özelleştirebilir.
- **Konteyner güvenlik izleme:** Bu aracı modülü, konteynerleştirilmiş bir ortamda değişiklikleri izlemek için Docker Engine API ile entegre edilmiştir. Örneğin, konteyner görüntülerinde, ağ yapılandırmasında veya veri birimlerinde değişiklikleri algılar. Ayrıca, ayrıcalıklı modda çalışan konteynerler ve çalışan bir konteynerde komutları yürüten kullanıcılar hakkında uyarılar verir.
- **Bulut güvenliği izleme:** Bu bileşen, Amazon Web Services, Microsoft Azure veya Google GCP gibi bulut sağlayıcılarını izler. API'leriyle yerel olarak iletişim kurar. Bulut altyapısındaki değişiklikleri (örneğin, yeni bir kullanıcı oluşturulur, bir güvenlik grubu değiştirilir, bir bulut örneği durdurulur, vb.) tespit edebilir ve bulut hizmetleri günlük verilerini (örneğin, AWS Cloudtrail, AWS Macie, AWS GuardDuty, Azure Active Directory, vb.) toplayabilir.

Wazuh Sunucusuyla İletişim

Wazuh aracısı, toplanan verileri ve güvenlikle ilgili olayları iletmek için Wazuh sunucusuyla iletişim kurar . Ayrıca, aracı operasyonel verileri göndererek yapılandırmasını ve durumunu bildirir. Bağlandıktan sonra, aracı Wazuh sunucusundan uzaktan yükseltilebilir, izlenebilir ve yapılandırılabilir.

Aracının sunucuyla iletişimi güvenli bir kanal (TCP veya UDP) üzerinden gerçekleşir ve gerçek zamanlı olarak veri şifrelemesi ve sıkıştırması sağlar. Ek olarak, taşmayı önlemek, gerektiğinde olayları sıraya koymak ve ağ bant genişliğini korumak için akış kontrol mekanizmaları içerir.

Aracı ilk kez sunucuya bağlamadan önce kaydetmeniz gerekir. Bu işlem, aracıya kimlik doğrulama ve veri şifrelemesi için kullanılan benzersiz bir anahtar sağlar.