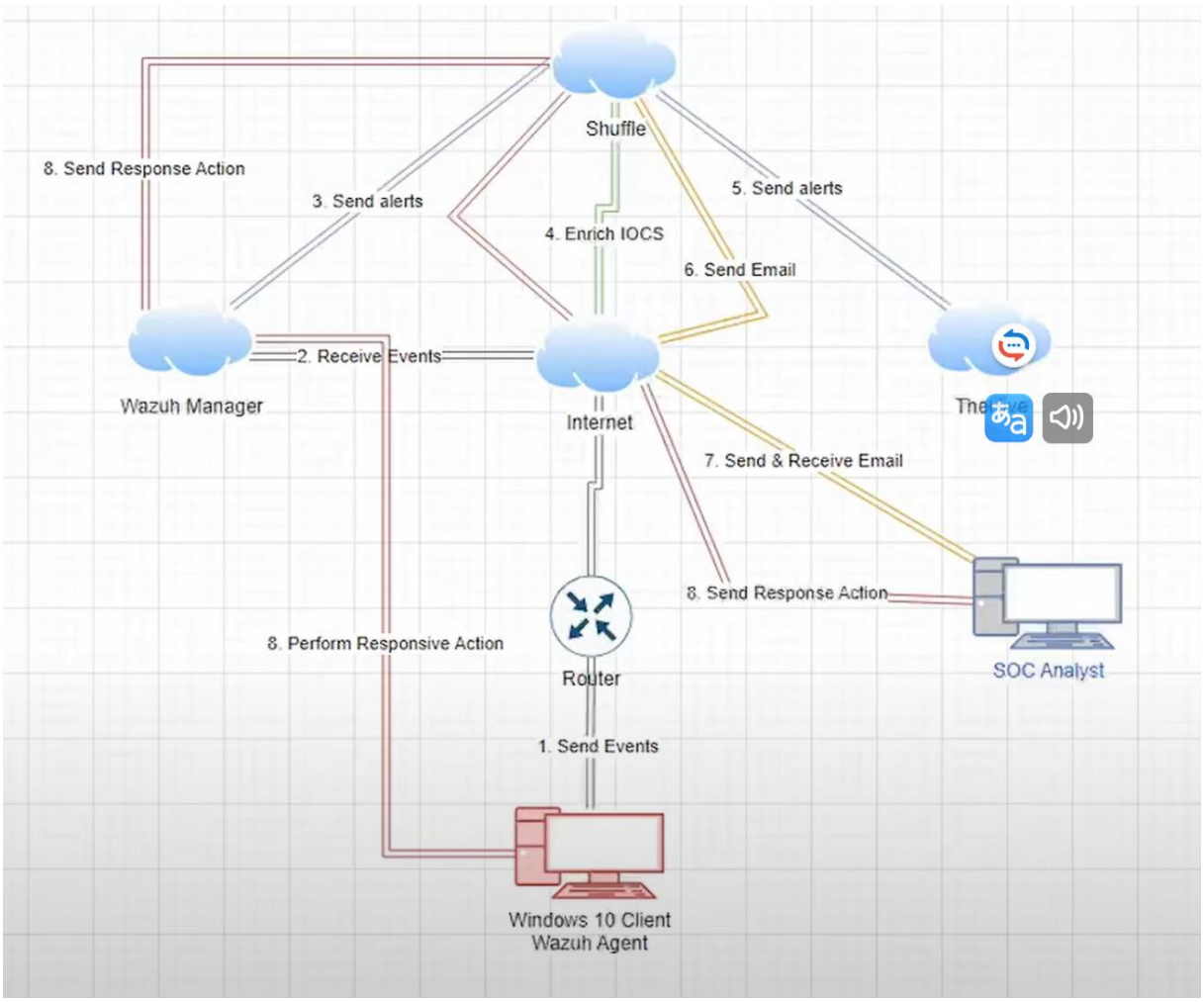


Yapı ve Akış Detayları:

1. Windows 10 Client (Wazuh Agent) → Wazuh Manager:

- **Gönderilen olaylar:** Windows 10 istemcisine yüklenmiş olan Wazuh Agent, istemci üzerindeki güvenlik olaylarını toplar ve bu olayları merkezi yönetim sunucusu olan **Wazuh Manager**'a iletir. Wazuh Agent, sistemdeki her türlü şüpheli aktiviteyi izler ve Wazuh Manager'a düzenli olarak raporlar.
- **Droplet ortamı:** Wazuh Manager, **Droplet** adlı bulut tabanlı bir sunucuda çalışır. Bu sunucu üzerinde, **Networking > Firewall** kısmında Wazuh için yapılandırılmış bir güvenlik duvarı kullanılarak trafiğin güvenli bir şekilde yönetilmesi sağlanır. Yalnızca belirli portlar (örneğin, Wazuh Agent ile iletişim için kullanılan portlar) açık bırakılarak istenmeyen erişim engellenmiştir.

2. Wazuh Manager → Shuffle:

- **Olayların alınması:** Wazuh Manager, istemciden aldığı olayları işler ve **Shuffle** isimli olay yönlendirme ve zenginleştirme sistemine gönderir. Bu adımda olaylar analiz edilmek üzere toplanır ve diğer sistemlerle entegre edilmesi sağlanır.
- **Güvenlik duvarı:** Shuffle sistemi, Wazuh Manager ile aynı **Droplet** ortamında çalışıyor olabilir. Bu nedenle Shuffle'ın iletişim kurduğu portlar da güvenlik duvarı tarafından koruma altına alınmıştır.

3. Shuffle → TheHive / Diğer Sistemler:

- **Uyarıların gönderilmesi:** Shuffle, olayları tehdit göstergeleri (IOC) ile zenginleştirdikten sonra, analiz edilmiş uyarıları **TheHive** gibi olay yönetim sistemlerine veya başka güvenlik sistemlerine gönderir. Bu uyarılar, saldırı göstergeleri içerebilir ve potansiyel tehditlerin belirlenmesine yardımcı olur.

4. Shuffle → IOC Zenginleştirme:

- **IOC'lerin zenginleştirilmesi:** Olay verileri, tehdit istihbarat sistemleriyle kıyaslanarak zenginleştirilir. Bu aşamada, saldırı göstergeleri (IP adresleri, hash değerleri, domain isimleri gibi) mevcut tehdit istihbaratı veritabanlarıyla karşılaştırılır ve anlamlandırılır. Bu süreç, olayların ne kadar ciddi olduğu ve nasıl aksiyon alınması gerektiği konusunda önemli veriler sağlar.

5. Shuffle → SOC Analisti / TheHive:

- **Uyarı gönderimi:** Shuffle, elde ettiği analiz sonuçlarını SOC (Security Operations Center) analistlerine veya **TheHive** olay yönetim platformuna iletir. TheHive, güvenlik olaylarının yönetimi için kullanılır ve SOC analistleri burada olayları inceleyip gerekli aksiyonları belirlerler.

6. Shuffle → E-posta ile bilgilendirme:

- **E-posta gönderimi:** Önemli güvenlik uyarıları ve olaylarla ilgili raporlar, ilgili kişilere veya sistemlere e-posta yoluyla iletilir. Bu süreç, kritik güvenlik olaylarının zamanında fark edilmesi ve aksiyon alınması açısından oldukça önemlidir.

7. TheHive → SOC Analisti:

- **E-posta gönderme/alma: TheHive**, SOC analistine güvenlik olayları hakkında e-posta gönderir ve analistten geri bildirim alır. Analist, bu e-posta üzerinden olayı değerlendirir ve alınması gereken aksiyonları belirler. TheHive platformu üzerinden, olaylar üzerinde detaylı incelemeler yapılabilir ve olaya dair aksiyonlar belirlenebilir.

8. Wazuh Manager / Shuffle / TheHive → Yanıt Aksiyonları:

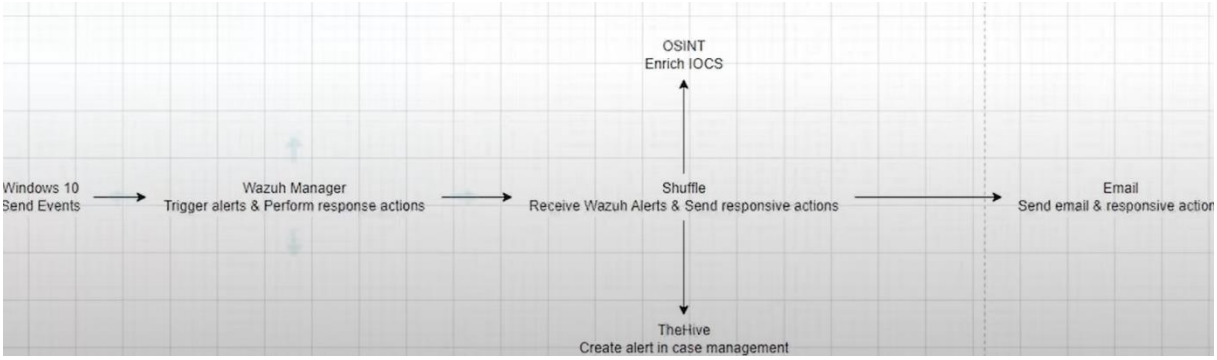
- **Yanıt aksiyonları ve savunma mekanizmaları:** Wazuh Manager, Shuffle ve TheHive sistemleri, belirli güvenlik olaylarına yanıt olarak otomatik veya manuel olarak aksiyonlar gönderebilir. Örneğin, bir saldırı tespit edildiğinde ilgili istemcideki işlemleri durdurmak veya istemciyi karantinaya almak gibi savunma mekanizmaları devreye sokulabilir.

9. Wazuh Manager → Windows 10 Client:

- **Yanıt aksiyonlarının uygulanması:** Wazuh Manager, Windows 10 istemcisine geri bildirim göndererek belirli yanıt aksiyonlarını uygular. Örneğin, bir zararlı yazılım tespiti durumunda, sistemdeki zararlı işlemler durdurulabilir veya istemci karantinaya alınabilir.

Genel Sistem Bileşenleri:

- **Wazuh Manager:** Windows 10 istemcisinden gelen güvenlik olaylarını toplar, analiz eder ve merkezi yönetim sağlar. **Droplet** sunucusunda yapılandırılmış olup güvenlik duvarı ile korunur.
- **Shuffle:** Gelen olayların analizini yapar, IOC zenginleştirmesi gerçekleştirir ve olayları diğer sistemlerle entegre eder.
- **TheHive:** Olay yönetim platformu olarak, SOC analistlerinin güvenlik olaylarını incelemesi ve gerekli aksiyonları belirlemesi için kullanılır.
- **SOC Analisti:** Güvenlik olaylarını inceleyip gerekli aksiyonları belirleyen uzman kişidir. Analistler, TheHive üzerinden olayları yönetebilir ve e-posta yoluyla bilgilendirilir.
- **Router/İnternet:** Sistemler arası veri trafiğini yönlendirir. Wazuh Manager ve Shuffle gibi sistemlerin dış dünyayla güvenli iletişimini sağlamak için gerekli ağ yapılandırması yapılmıştır.
- **Droplet: Wazuh Manager** ve **TheHive** sunucularının çalıştığı bulut platformudur. **Firewall** yapılandırması ile sunucuların sadece yetkili bağlantılara izin verilerek korunması sağlanmıştır.



Genel Akış ve Bileşenler:

1. **Windows 10 Client (Wazuh Agent)**:
    - Windows 10 istemcisine kurulu olan Wazuh Agent, cihazda gerçekleşen olayları tespit eder ve bu olayları merkezi yönetim sistemine (Wazuh Manager) iletir. Bu olaylar güvenlik tehditleri, sistem hataları veya anormallikler olabilir.
2. **Wazuh Manager**:

- **Olayları alma** ve **tetikleme**: Windows 10 istemcisinden gelen olaylar burada toplanır. Wazuh Manager, bu olayları değerlendirir ve tehdit oluşturabilecek durumlar için uyarılar oluşturur. Aynı zamanda, belirli olaylara karşı önceden tanımlanmış yanıt aksiyonlarını tetikler.
- **Yanıt aksiyonlarının uygulanması**: Wazuh Manager, belirlenen güvenlik olaylarına karşı yanıt aksiyonlarını uygulayabilir. Bu aksiyonlar, istemcide (Windows 10) belirli işlemleri durdurma, erişim kısıtlamaları veya karantinaya alma gibi işlemleri içerebilir.

3. **Shuffle**:
   - **Wazuh Uyarıları Alma ve Yanıt Aksiyonlarını Gönderme**: Wazuh Manager'dan gelen uyarılar, Shuffle aracılığıyla alınıp yönetilir. Aynı zamanda, bu sistem diğer aksiyonları koordine etmek ve olayları zenginleştirmek için kullanılır.
   - **IOC'lerin (Tehdit Göstergeleri) Zenginleştirilmesi**: Shuffle, Open Source Intelligence (OSINT) kaynaklarını kullanarak olaylardaki IOC'leri zenginleştirir. Bu işlem, olaylardaki tehdit göstergelerini daha anlamlı hale getirir ve tehdit düzeylerini analiz eder.
   - **Yanıt aksiyonlarının dağıtımı**: Shuffle, Wazuh Manager'dan gelen yanıt aksiyonlarını diğer sistemlere iletir ve gerektiğinde SOC analistlerine veya olay yönetim sistemlerine gönderir.
4. **TheHive**:
   - **Olayların yönetimi**: Shuffle'dan gelen uyarılar TheHive üzerinde bir olay yönetimi sürecine dönüşür. TheHive, SOC analistlerinin olayları incelemesine, kategorize etmesine ve çözüme ulaştırmasına olanak sağlar.
   - **Vaka yönetimi**: TheHive, her bir olayı incelemek ve olayla ilgili aksiyonları belirlemek için kullanılır. Ayrıca, SOC ekibiyle daha iyi iletişim sağlamak amacıyla entegre bir sistem olarak çalışır.
5. **Email**:
   - **E-posta ile bilgilendirme**: Olay yönetim süreçlerinin kritik anlarında e-posta uyarıları ile ilgili kişilere bilgilendirme yapılır. Bu, olaylar veya aksiyonlar hakkında hızlı bilgi akışını sağlar.
   - **Yanıt aksiyonlarının bildirilmesi**: Aynı zamanda, olaylara verilen yanıt aksiyonları e-posta aracılığıyla ilgili sistemlere veya personele iletilebilir.

Sürecin Özeti:

- **Olayların toplanması**: Windows 10 istemcisinde gerçekleşen olaylar Wazuh Agent aracılığıyla Wazuh Manager'a iletilir.
- **Uyarıların tetiklenmesi ve aksiyonlar**: Wazuh Manager, olayları değerlendirir ve tehdit oluşturan durumlar için uyarı tetikler. Yanıt aksiyonlarını belirleyip istemciye uygular.
- **Shuffle ve IOC Zenginleştirme**: Shuffle, olayları alıp OSINT kullanarak tehdit göstergelerini zenginleştirir ve yanıt aksiyonlarını koordine eder.

- **TheHive Olay Yönetimi**: Uyarılar TheHive'da vaka yönetimi sürecine dönüştürülür ve SOC analistleri tarafından incelenir.
- **E-posta Bildirimleri**: E-posta aracılığıyla uyarılar ve yanıt aksiyonları ilgili taraflara iletilir.

Bu iki şema, olayların nasıl toplanıp işlendiğini ve sonrasında nasıl aksiyon alındığını detaylıca gösteriyor. Olay yönetimi, tehdit istihbaratı zenginleştirme ve SOC analistlerinin süreçteki rolü net bir şekilde çizelgede açıklanmış durumda.