Güvenlik Yapılandırmaları (SCA)

Yapılandırma değerlendirmesi, uç noktaların yapılandırma ayarları ve onaylanmış uygulama kullanımıyla ilgili önceden tanımlanmış bir dizi kurala uyup uymadığını doğrulayan bir süreçtir. Mevcut yapılandırmayı, güvenlik açıklarını ve yanlış yapılandırmaları belirlemek için yerleşik endüstri standartları ve kurumsal politikalarla karşılaştırmayı içerir.

Düzenli yapılandırma değerlendirmeleri, kuruluşların güvenlik açıklarını proaktif bir şekilde belirlemesine ve yamalamasına yardımcı oldukları için güvenli ve uyumlu bir ortamın sürdürülmesinde önemlidir. Bu uygulama güvenlik kontrollerini güçlendirir ve güvenlik olayı riskini en aza indirir.

Wazuh SCA Modülü

Wazuh, güvenlik ekiplerinin ortamlarındaki yanlış yapılandırmaları tarayıp tespit etmelerine yardımcı olan bir Güvenlik Yapılandırma Değerlendirmesi (SCA) modülü sunar. Wazuh aracısı, izlediği uç noktaları taramak için politika dosyalarını kullanır. Bu dosyalar, izlenen her uç noktada gerçekleştirilecek önceden tanımlanmış kontrolleri içerir.

Wazuh, İnternet Güvenliği Merkezi (CIS) güvenlik ölçütlerine dayalı olarak SCA politikalarını kullanıma hazır olarak içerir. Bu ölçütler, BT sistemlerini ve verilerini siber saldırılardan korumak için en iyi uygulamalara ilişkin temel kılavuzlar olarak hizmet eder. Güvenli bir temel yapılandırma oluşturmak için net talimatlar sağlar ve kullanıcıların kritik varlıklarını korumak ve olası güvenlik açıklarını azaltmak için etkili önlemler uygulamasını sağlamak üzere rehberlik sunar. Bu standartlara uyarak, genel güvenlik duruşunuzu iyileştirebilir ve işletmenize yönelik siber tehdit riskini azaltabilirsiniz.

Wazuh Güvenlik Yapılandırma Değerlendirmesi (SCA) modülünün diğer bazı faydaları şunlardır:

- **Güvenlik duruşu yönetimi** : Wazuh SCA, kuruluşların uç noktalarının güvenli bir şekilde yapılandırılmasını sağlamalarına yardımcı olur. Bu, yanlış yapılandırmalardan kaynaklanan güvenlik açıklarını en aza indirir ve güvenlik ihlalleri riskini azaltır.
- **Uyumluluk izleme** : Kuruluşların düzenleyici standartlara, en iyi uygulamalara ve iç güvenlik politikalarına uyumu değerlendirmelerine ve uygulamalarına olanak tanır.
- **Sürekli izleme** : Wazuh SCA, uç noktaların yapılandırmasını sürekli olarak izler ve yanlış yapılandırmalar tespit ettiğinde uyarı verir.

Wazuh SCA Politikalarına Genel Bakış

Wazuh SCA modülü YAML formatında yazılmış politikaları kullanır. Her politika denetimlerden oluşur ve her denetim bir veya daha fazla kuraldan oluşur. Bu kurallar, dosyaların, dizinlerin, Windows kayıt defteri anahtarlarının, çalışan işlemlerin ve daha fazlasının varlığı gibi bir uç noktanın çeşitli yönlerini inceleyebilir.

Varsayılan olarak, Wazuh aracısı, kural kümesi dizininde bulunan her politika (`.yaml`veya `.yml`dosya) için taramalar çalıştırır. Bu dizin, Wazuh aracısını çalıştıran her işletim sisteminde aşağıdaki konumlarda bulunabilir:

- Linux ve Unix tabanlı ajanlar: `/var/ossec/ruleset/sca`.
- Windows aracıları: .`C:\Program Files (x86)\ossec-agent\ruleset\sca`
- macOS aracıları: `/Library/Ossec/ruleset/sca`.

Wazuh ayrıca uç noktaları tarayıp kuruluşunuzun politikalarına uyup uymadıklarını doğrulamak için kullanılabilecek özel politikalar oluşturmanıza da olanak tanır .

`/var/ossec/ruleset/sca/cis_ubuntu22-04.yml`Ubuntu 22.04 uç noktalarında kutudan çıktığı haliyle dahil edilen bir CIS politika dosyasının bir kesitini görün . CIS kıyaslamalarına dayanan SCA politikası, sistem güçlendirme için en iyi uygulamalara uyup uymadığını belirlemek için uç noktada kontroller çalıştırır. Kimlikli SCA politikası, dizinin ayrı bir bölümde olup `28500`olmadığını kontrol eder .`/tmp`

```
- id: 28500
  title: "Ensure /tmp is a separate partition."
  description: "The /tmp directory is a world-writable directory used for temporary storage by all users and some ap
  rationale: "Making /tmp its own file system allows an administrator to set additional mount options such as the no
  impact: "Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not
  remediation: "First ensure that systemd is correctly configured to ensure that /tmp will be mounted at boot time.
  references:
    - https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/
    - https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html
  compliance:
    - cis: ["1.1.2.1"]
    - cis_csc_v7: ["14.6"]
    - cis_csc_v8: ["3.3"]
    - mitre_techniques: ["T1499", "T1499.001"]
    - mitre_tactics: ["TA0005"]
    - mitre_mitigations: ["M1022"]
    - cmmc_v2.0: ["AC.L1-3.1.1", "AC.L1-3.1.2", "AC.L2-3.1.5", "AC.L2-3.1.3", "MP.L2-3.8.2"]
    - hipaa: ["164.308(a)(3)(i)", "164.308(a)(3)(ii)(A)", "164.312(a)(1)"]
    - pci_dss_v3.2.1: ["7.1", "7.1.1", "7.1.2", "7.1.3"]
```

```
    - pci_dss_v4.0: ["1.3.1", "7.1"]
    - nist_sp_800-53: ["AC-5", "AC-6"]
    - soc_2: ["CC5.2", "CC6.1"]
  condition: all
  rules:
    - 'c:findmnt --kernel /tmp -> r:\s*/tmp\s'
    - "c:systemctl is-enabled tmp.mount -> r:generated|enabled"
```

Dizin `/tmp`, sistem ve kullanıcı uygulamaları tarafından kısa bir süre için ihtiyaç duyulan verileri depolamak için kullanılır. `/tmp`Ayrı bir bölüme bağlanma, bir yöneticinin `noexec`, `nodev`, ve gibi ek bağlama seçenekleri ayarlamasına olanak tanır `nosuid`. Bu nedenle, dizini bir saldırganın yürütülebilir kod yüklemesi için işe yaramaz hale getirir. SCA ilke dosyası ayrıca bu sorunun nasıl düzeltileceğine dair öneriler sunar.

SCA Sonuçlarını Görüntüleme

Wazuh kontrol panelinde, her bir acente için SCA tarama sonuçlarını görüntülemenize olanak tanıyan bir **Yapılandırma Değerlendirme modülü bulunur.**

Yapılandırma Değerlendirme modülü

SCA Sonuçlarının Yorumlanması

Aşağıdaki görüntü, Ubuntu Linux 22.04 LTS için CIS kıyaslamasına dayalı politikayı göstermektedir. Ubuntu 22.04 uç noktasına karşı 191 denetimin yürütüldüğünü görebilirsiniz. Bunlardan 56'sı geçti, 87'si başarısız oldu ve 48'i uç noktaya uygulanamaz. Ayrıca, geçilen test sayısına göre hesaplanan %39'luk bir puan da göstermektedir.

Ubuntu 22.04 kontrolleri için CIS kıyaslama politikası

Daha fazla bilgi edinmek için çeklere tıklayabilirsiniz. Aşağıdaki resimde gerekçe, düzeltme ve kimliği olan çekin açıklaması gibi bilgileri görebilirsiniz `3003`.

Ubuntu 22.04 için CIS kıyaslama sonuçları kontrol kimliği 3003

Yukarıdaki SCA tarama sonucu, `failed`ssh için genel anahtar kimlik doğrulamasının etkinleştirilmediğini gösteriyor. Düzeltme uygulanırsa, sonuç `passed`uç noktanın güvenliğini artıracak şekilde değişecektir.

SCA İyileştirme Adımlarının Uygulanması

Önceki bölümdeki örnekte, Wazuh SCA tarafından sağlanan düzeltmenin uygulanması uç noktanın güvenliğini artırır. Bu, `PubkeyAuthentication`dosyadaki seçenek değerinin değiştirilmesini içerir `sshd_config`. Aşağıdaki görüntüde, kontrolün durumunun . `3003`olarak değiştiğini görebilirsiniz `passed`.

Wazuh SCA modülünü kullanarak yanlış yapılandırmaları tespit edebilir, bunları düzeltebilir ve uç noktalarınızın sektördeki en iyi uygulamalara uyduğunu doğrulayabilirsiniz. Bu proaktif yaklaşım, ortamınızdaki güvenlik ihlallerinin olasılığını önemli ölçüde azaltır.

Revision #3
Created 6 December 2023 17:37:58 by LastGuard
Updated 23 December 2024 19:23:23 by Ayşegül Sarıkaya