BT Sağlığı

BT hijyeni, kuruluşların ve bireylerin BT varlıklarının sağlığını ve güvenliğini korumak için aldıkları önlemleri ifade eder. BT hijyeni, ortaya çıkan siber güvenlik tehditlerine ve zorluklarına karşı koymak için uygulamaların ve süreçlerin sürekli olarak uyarlanmasını, güvenli ve dayanıklı bir BT ortamının teşvik edilmesini gerektirir. Kuruluşlar, veri kaybına, hizmet kesintisine, itibar kaybına veya finansal istikrarsızlığa yol açabilecek siber saldırıları, veri ihlallerini ve diğer güvenlik endişelerini önlemek için sağlam BT hijyeni uygulamaları uygular.

Sistem Envanteri

Güncel bir sistem envanteri, kuruluşların ortamlarındaki varlık görünürlüğünü optimize etmelerine yardımcı olur ve iyi bir BT hijyeni sağlamak için olmazsa olmazdır. Wazuh, donanım ve işletim sistemi bilgileri, yüklü yazılımlar, ağ arayüzleri, bağlantı noktaları ve çalışan süreçleri içeren sistem envanter verilerini toplar. Wazuh aracıları, izlenen uç noktalardan envanter verilerini toplamak ve bunları Wazuh sunucusuna göndermek için Syscollector modülünü kullanır.

Wazuh panosundaki Envanter veri modülünden sistem envanter raporları oluşturabilirsiniz . Raporda yer alan bilgiler istenmeyen uygulamaları, süreçleri, hizmetleri ve kötü amaçlı eserleri belirlemeye yardımcı olur.

Wazuh panosundaki envanter verileri

İzlenen bir uç nokta için özelliğe özgü raporlar da üretebilirsiniz. Örneğin, izlenen bir uç noktada yüklü yazılımların listesini veya çalışan işlemlerin listesini içeren bir rapor alabilirsiniz.

Envanter veri indirme

Toplanan envanter verileri, JSON biçiminde iç içe geçmiş verileri alan Wazuh API'si kullanılarak sorgulanabilir . Örneğin, Wazuh panosundaki **Sunucu yönetimi** > **Geliştirme Araçları** `wazuh-agent` modülünü kullanarak izlenen bir uç noktada paketi kontrol etmek için paket envanterini sorgulayabilirsiniz . cURL gibi komut satırı araçları da envanter veritabanını sorgulamak için kullanılabilir.

Dev Tools'u kullanarak paket envanterini sorgulama

Güvenlik Yapılandırma Değerlendirmesi

İyi BT hijyeni uygulamanın hedeflerinden biri, kuruluşunuzun saldırı yüzeyini azaltmaktır. Wazuh SCA modülü, güvenlik yanlış yapılandırmalarını ve kusurlarını belirlemek için izlenen uç noktaları İnternet Güvenliği Merkezi (CIS) kıyaslamalarına dayalı politikalara göre düzenli olarak tarar. CIS kıyaslamaları, kritik varlıklar için güvenli bir temel yapılandırma oluşturmak için temel yönergelerdir. Bu, yanlış yapılandırmalardan kaynaklanan güvenlik açıklarını en aza indirir ve güvenlik ihlalleri riskini azaltır.

Wazuh panosundaki Yapılandırma **Değerlendirme** modülü her bir aracının SCA tarama sonucunu sağlar. Sonuçlar uç noktada gerçekleştirilen kontrol sayısını, başarısız olanların sayısını ve geçen kontrollerin sayısını gösterir. Ayrıca, geçilen test sayısına göre hesaplanan bir puan gösterir ve size uyumluluk düzeyine ilişkin genel bir bakış sunar.

Wazuh panosundan geçen ve başarısız olan kontrolleri görüntülemek için daha fazla içgörü elde edebilirsiniz. Ayrıca, düzeltme faaliyetlerine yardımcı olmak için bir CSV raporu oluşturabilir ve böylece uç nokta güvenlik duruşunu iyileştirebilirsiniz.

SCA sonuçlarının ayrıntıları ve indirilmesi

Wazuh panosunda, gerekçe, düzeltme adımları ve uç noktada gerçekleştirilen kontrollerin açıklaması gibi bilgileri görebilirsiniz. Bu bilgiler Wazuh tarafından oluşturulan raporda yer almaktadır.

SCA kontrol sonucu ayrıntıları

Yukarıdaki SCA tarama sonucu, uç noktanın cramfs dosya sistemini bağlamanıza izin vermesi nedeniyle bir başarısızlığa işaret ediyor. Güvenlik duruşunu iyileştirmek için raporda önerilen düzeltmeyi uygulayabilirsiniz.

Güvenlik Açığı Yönetimi

Güvenlik açığı yönetimi, siber saldırıları önlemek için güvenlik açıklarını tespit edip gidermeyi amaçlar. Güvenlik açıklarını gidermek için proaktif adımlar atarak kuruluşunuz saldırı yüzeyini önemli ölçüde azaltabilir ve böylece BT hijyenini iyileştirebilir.

Wazuh güvenlik açığı tespit modülü, Wazuh CTI'mızda bulunan güvenlik açığı bilgilerini kullanarak güvenlik açığı bulunan uygulamaları belirler . Güvenlik açığı tespit modülü, izlenen uç noktalarda

keşfedilen güvenlik açıkları için uyarılar üretir. Bu, izlenen tüm uç noktalarda tanımlanan güvenlik açıklarının kapsamlı bir görünümünü sağlayarak güvenlik açıklarının düzeltilmesini görüntülemenize, analiz etmenize, düzeltmenize ve takip etmenize olanak tanır.

Keşfedilen güvenlik açıkları önem düzeylerine göre gruplandırılır ve Wazuh panosunda uygulama adı, CVE ve CVSS3 puanına göre bir özet sağlanır.

Güvenlik Açığı Tespiti envanter panosu
Image not found or type unknown

Wazuh panosundan izlenen bir uç noktada keşfedilen ve çözülen güvenlik açıklarıyla ilgili güvenlik olaylarını içeren bir rapor indirebilirsiniz. Bu özellik, çözülmemiş güvenlik açıkları olan uç noktaları belirlemenizi ve düzeltme etkinliklerini takip etmenizi sağlar.

Güvenlik açıkları veri indirme
Image not found or type unknown

Wazuh güvenlik açığı tespit modülü ayrıca, BT hijyenini iyileştirme veya sürdürme konusunda bir ilerleme raporu olarak hizmet edebilecek düzeltme faaliyetlerini izlemenizi sağlar. Örneğin, bir güvenlik açığı giderildiğinde, Wazuh panosunda bir uyarı oluşturulur. Bu özellik, bir yama veya yazılım yükseltmesinin daha önce tespit edilen bir güvenlik açığını çözdüğünü tespit eder.

Düzeltme uyarıları
Image not found or type unknown

Kötü amaçlı yazılım tespiti

Kötü amaçlı yazılım tespiti, bilgisayar sistemlerini ve ağlarını siber tehditlerden korumak için olmazsa olmazdır. Kuruluşlar, veri ihlallerine, sistem ihlallerine ve finansal kayıplara neden olabilecek kötü amaçlı yazılımları belirleyip azaltarak BT hijyenlerini iyileştirebilir.

Wazuh, kötü amaçlı yazılım modellerini tanımak ve hızlı yanıt için uyarıları tetiklemek üzere tasarlanmış, kullanıma hazır bir kurallar seti sunar. Wazuh ayrıca güvenlik analistlerinin ortamlarına göre uyarlanmış özel kurallar oluşturmalarına olanak tanır ve böylece kötü amaçlı yazılım algılama çabalarını optimize eder. Örneğin, Wazuh kullanarak Vidar bilgi hırsızı kötü amaçlı yazılımını algılamak için özel kurallar oluşturduk .

```
<group name="windows,sysmon,vidar_detection_rule,">
<!-- Vidar downloads malicious DLL files on victim endpoint -->
  <rule id="100084" level="10">
    <if_sid>61613</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)\\\\.+(exe|dll|bat|msi)</field>
    <field name="win.eventdata.targetFilename" type="pcre2">(?i)\\\\ProgramData\\\\(freebl3|mozglue|msvcp140|
    <description>Possible Vidar malware detected. $(win.eventdata.targetFilename) was downloaded on $(win.syst
    <mitre>
      <id>T1056.001</id>
    </mitre>
  </rule>
<!-- Vidar loads malicious DLL files -->
  <rule id="100085" level="12">
    <if_sid>61609</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)\\\\.+(exe|dll|bat|msi)</field>
    <field name="win.eventdata.imageLoaded" type="pcre2">(?i)\\\\programdata\\\\(freebl3|mozglue|msvcp140|ns
```

```
    <description>Possible Vidar malware detected. Malicious $(win.eventdata.imageLoaded) file loaded by $(win.ev
    <mitre>
      <id>T1574.002</id>
    </mitre>
  </rule>
<!-- Vidar deletes itself or a malicious process it creates -->
  <rule id="100086" level="7" frequency="5" timeframe="360">
    <if_sid>61603</if_sid>
    <if_matched_sid>100085</if_matched_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)\\\\cmd.exe</field>
    <match type="pcre2">cmd.exe\\" /c timeout /t \d{1,}.+del /f /q \\".+(exe|dll|bat|msi)</match>
    <description>Possible Vidar malware detected. Malware deletes $(win.eventdata.parentCommandLine)</descri
    <mitre>
      <id>T1070.004</id>
    </mitre>
  </rule>
</group>
```

Yukarıdaki kurallar, Vidar infostealer zararlı yazılımının belirli davranışlarını tespit eder ve kontrol panelinde uyarıları tetikler.

Vidar kötü amaçlı yazılım uyarıları

Wazuh , VirusTotal, MISP ve daha fazlası gibi tehdit istihbarat kaynaklarıyla entegre olarak kötü amaçlı yazılım tespit yeteneklerini artırır . Wazuh ayrıca ClamAV ve Windows Defender gibi üçüncü taraf kötü amaçlı yazılım tespit araçlarının entegre edilmesi için destek sunar . Wazuh, üçüncü taraf kötü amaçlı yazılım tespit araçlarından günlükleri toplayarak ve analiz ederek güvenlik analistlerine merkezi bir izleme platformu sağlar. Wazuh, üçüncü taraf araçlardan gelen çeşitli tehdit istihbaratlarını birleştirerek kötü amaçlı yazılım tespitinde verimliliği artırır ve böylece kuruluşun BT hijyenini iyileştirir.

Aşağıdaki görüntü, Wazuh sunucusu tarafından işlenen VirusTotal olayına ait uyarıyı göstermektedir.

VirusTotal bulgu uyarısı

Wazuh, kötü amaçlı yazılımları tespit etmek için tehlike göstergeleri (IOC'ler) içeren CDB listelerini (sabit veritabanları) kullanır . Bu listeler, dosya karmaları, IP adresleri ve etki alanı adları gibi bilinen kötü amaçlı yazılım IOC'lerini içerir. Wazuh, tanımlanan IOC'leri CDB listelerinde depolanan bilgilerle karşılaştırarak kötü amaçlı dosyaları proaktif olarak belirler.

Kötü amaçlı yazılım algılandı uyarısı

Mevzuata Uygunluk

Düzenleyici standartlar, müşteri güvenini ve işletme itibarını iyileştirmeye yardımcı olmak için en iyi iş uygulamaları için küresel bir ölçüt sağlar. Düzenleyici standartlara uyum, kuruluşların BT hijyenlerini geliştirmelerine de yardımcı olur.

Wazuh , PCI DSS, HIPAA, GDPR ve diğerleri gibi endüstri standartlarının gereksinimlerini karşılayan sağlam bir çözüm sunarak düzenleyici uyumluluk yükümlülüklerini karşılama sürecini kolaylaştırır .

Güvenlik operasyonları modülü

Wazuh, uyumluluk ihlallerini belirlemek ve raporlamak için SCA , güvenlik açığı tespiti , FIM ve daha fazlası gibi yeteneklerini kullanır . Ayrıca uyumluluk durumunu izlemeye, iyileştirme alanlarını belirlemeye ve uygun düzeltme eylemlerini gerçekleştirmeye yardımcı olmak için özel uyumluluk panoları sağlar.

Örneğin, Wazuh panosunda izlenen bir uç noktanın PCI DSS gereksinimine ilişkin genel bir bakış elde edebilirsiniz.

PCI DSS panosu

Denetimler sekmesinden, politika ihlallerinin nerede meydana geldiğini bulmak için bireysel PCI DSS gereksinimlerine ayrıntılı olarak bakabilirsiniz .

PCI DSS gereklilik ihlalleri

Aşağıdaki görselde *PCI DSS Gereksinimi 11.2.1'i* ihlal eden güvenlik açıkları için oluşturulan uyarılar gösterilmektedir .

PCI DSS gereklilik ihlali ayrıntıları

Bu özellik GDPR, TSC, HIPAA ve NIST-800-53 gibi diğer uyumluluk standartları için de mevcuttur.

Revision #4
Created 6 December 2023 18:03:44 by LastGuard
Updated 11 December 2024 20:51:51 by Ayşegül Sarıkaya