Olay Günlüğü Tutma

Günlükler, Wazuh aracılarından, harici API'lerden ve ağ cihazlarından alınan ham olaylardır. Wazuh sunucusu tüm günlükleri süresiz olarak depolar. Alan optimizasyonunu en üst düzeye çıkarmak için Wazuh yöneticisi günlük dosyalarını otomatik olarak sıkıştırır.

Wazuh, iki tür günlüğü yönetir, Wazuh sunucusundan gelen dahili günlükler ve izlenen uç noktalardan gelen harici günlükler. Bu günlükler `/var/ossec/logs/`Wazuh sunucusunun dizininde süresiz olarak saklanır.

Aşağıdaki tabloda Wazuh sunucusundaki günlük dosyaları ve bunların saklanma yerleri açıklanmaktadır.

Günlük depolama dosyası	Günlük kaynağı	Tanım
`/var/ossec/logs/ossec.log`	Dahili	Wazuh sunucusu tarafından oluşturulan tüm bilgi düzeyindeki günlükleri depolar.
`/var/ossec/logs/api.log`	Dahili	Wazuh uygulamasının Wazuh sunucu API'leriyle etkileşimi sırasında oluşturulan günlükleri depolar.
`/var/ossec/logs/cluster.log`	Dahili	Wazuh kümesinin faaliyetleri tarafından oluşturulan günlükleri depolar.
`/var/ossec/logs/integrations.log`	Dahili	Üçüncü taraf uygulamalar ve sistemlerle arayüz oluştururken Wazuh entegrasyon modülü tarafından oluşturulan günlükleri depolar.
`/var/ossec/logs/active-responses.log`	Dahili	Wazuh Active Response modülü tarafından oluşturulan günlükleri depolar.
`/var/ossec/logs/firewall/firewall.log`	Dahili	Güvenlik duvarı tarafından oluşturulan günlükleri depolar.
`/var/ossec/logs/archives/archives.log`	Harici	Üçüncü taraf uygulama ve sistemlerden alınan günlükleri düz metin olarak depolar.
`/var/ossec/logs/archives/archives.json`	Harici	Üçüncü taraf uygulamalardan ve sistemlerden alınan günlükleri JSON biçiminde depolar.

Günlük Sıkıştırma ve Döndürme

Günlük dosyaları bir sistemde önemli disk alanı biriktirebilir ve tüketebilir. Bunu önlemek için Wazuh yöneticisi, günlükleri döndürme işlemi sırasında sıkıştırarak disk kullanımını verimli bir şekilde yönetmeye ve sistem performansını korumaya yardımcı olur. Wazuh yöneticisi günlük dosyalarını günlük olarak veya belirli bir eşiğe (dosya boyutu, yaş, zaman ve daha fazlası)

ulaştıklarında sıkıştırır ve arşivler. Günlük döndürme işleminde Wazuh, sürekli olarak yeni olaylar yazmak için orijinal adla yeni bir günlük dosyası oluşturur.

`/var/ossec/logs/`Günlük dosyaları günlük olarak sıkıştırılır ve MD5, SHA1 ve SHA256 karma algoritmaları kullanılarak dijital olarak imzalanır. Sıkıştırılmış günlük dosyaları, aşağıdaki biçime göre isimler taşıyan iç içe dizinler içindeki dizinde saklanır :

- Orijinal günlük dosyasının adını belirten .`log file name`
- `year`İçinde bulunulan yılın adını belirten .
- `month`Yılın o anki ayının adını belirten .

Örneğin, `/var/ossec/logs/archives/archives.log`sıkıştırılmış bir dosya dizinde saklanır . Aşağıdaki komutu çalıştırarak dizinin içeriğini görebilirsiniz:`13th APR, 2024`.../archives/2024/Apr/

```
ls -la /var/ossec/logs/archives/2024/Apr/
```

Output

```
total 0
drwxr-x--- 2 wazuh wazuh 62 Apr 17 08:15 .
drwxr-x--- 4 wazuh wazuh 28 Apr 12 07:30 ..
-rw-r----- 1 wazuh wazuh  0 Apr 13 00:00 ossec-archive-13.log.gz
-rw-r----- 1 wazuh wazuh  0 Apr 13 00:00 ossec-archive-13.log.sum
```

Yukarıdaki çıktıda görüldüğü gibi, sıkıştırılmış dosyanın adına ve onun sağlama toplamına sırasıyla dize ve sonek eklenir.

Yukarıdaki çıktıda görüldüğü gibi, sıkıştırılmış dosyanın adının ve sağlama toplamının başına `ossec` dizesi ve `day of the current month` son eki sırasıyla eklenir ve eklenir.

İhtiyaçlarınıza bağlı olarak, sıkıştırılmış dosyaları belirli bir süre sonra kaldırılmak üzere yapılandırabilirsiniz. Ayrıca, daha uzun süreli saklama için günlük yönetim sistemlerine, yedekleme sunucularına veya bulut tabanlı depolama aygıtlarına taşıyabilirsiniz.

Olay Günlüklerinin Arşivlenmesi

Olaylar, uygulamalar, uç noktalar ve ağ cihazları tarafından oluşturulan günlüklerdir. Wazuh sunucusu, bir kuralı tetikleyip tetiklemediklerine bakılmaksızın aldığı tüm olayları depolar. Bu olaylar, `/var/ossec/logs/archives/archives.log`ve adresinde bulunan Wazuh arşivlerinde depolanır `/var/ossec/logs/archives/archives.json`. Güvenlik ekipleri, güvenlik olaylarının geçmiş verilerini incelemek, eğilimleri analiz etmek ve tehditleri avlamak için raporlar oluşturmak amacıyla arşivlenmiş günlükleri kullanır.

Varsayılan olarak, Wazuh arşivleri devre dışıdır çünkü günlükleri Wazuh sunucusunda süresiz olarak depolar. Etkinleştirildiğinde, Wazuh yöneticisi uyumluluk ve adli amaçlar için güvenlik verilerini

depolamak ve saklamak üzere arşivlenmiş dosyalar oluşturur.

Not

Wazuh arşivleri, izlenen tüm uç noktalardan toplanan günlükleri tutar, bu nedenle zamanla Wazuh sunucusunda önemli depolama kaynakları tüketir. Bu nedenle, bunları etkinleştirmeden önce disk alanı ve performans üzerindeki etkiyi göz önünde bulundurmak önemlidir.

Arşivlemeyi Etkinleştirme

Wazuh sunucunuzda arşivlemeyi etkinleştirmek için aşağıdaki adımları izleyin.

1. Wazuh yöneticisi yapılandırma dosyasını düzenleyin `/var/ossec/etc/ossec.conf`ve aşağıda vurgulanan alanların değerini şu şekilde ayarlayın `yes`:

   ```
   <ossec_config>
     <global>
       <jsonout_output>yes</jsonout_output>
       <alerts_log>yes</alerts_log>
       <logall>yes</logall>
       <logall_json>yes</logall_json>

       ...
   </ossec_config>
   ```

   Nerede:
   - `<logall>`tüm günlük iletilerinin arşivlenmesini etkinleştirir veya devre dışı bırakır. Etkinleştirildiğinde, Wazuh sunucusu günlükleri bir syslog biçiminde depolar. İzin verilen değerler `yes`ve ' dir `no`.
   - `<logall_json>`olayların günlüğe kaydedilmesini etkinleştirir veya devre dışı bırakır. Etkinleştirildiğinde, Wazuh sunucusu olayları bir JSON biçiminde depolar. İzin verilen değerler `yes`ve ' dir `no`.

   İstediğiniz biçime bağlı olarak, vurgulanan alanlardan bir veya her iki değeri de olarak ayarlayabilirsiniz `yes`. Ancak, yalnızca bu `<logall_json>yes</logall_json>`seçenek Wazuh panosundaki olayları görselleştirmek için kullanılabilecek bir dizin oluşturmanıza olanak tanır.

2. Yapılandırma değişikliklerini uygulamak için Wazuh yöneticisini yeniden başlatın:

   ```
   systemctl restart wazuh-manager
   ```

Seçtiğiniz formata bağlı olarak, dosya `archives.log`, , veya her ikisi de Wazuh sunucusundaki dizinde `archives.json`oluşturulacaktır .`/var/ossec/logs/archives/`

Wazuh varsayılan bir günlük döndürme politikası kullanır. Günlükleri günlük, aylık ve yıllık bazda döndürerek ve sıkıştırarak kullanılabilir disk alanının korunmasını sağlar.

Dashboard'daki Olayların Görselleştirilmesi

1. Filebeat yapılandırma dosyasını düzenleyin ve from `/etc/filebeat/filebeat.yml`değerini şu şekilde değiştirin :`archives: enabledfalsetrue`

   ```
   archives:
    enabled: true
   ```

2. Yapılandırma değişikliklerini uygulamak için Filebeat'i yeniden başlatın:

   ```
   systemctl restart filebeat
   ```

Wazuh Dashboard

1. Ana menüyü açmak için sol üst menü simgesine tıklayın. **Pano yönetimi'ni genişletin ve Pano yönetimi** > **Dizin desenleri'ne** gidin . Sonra, **Dizin deseni oluştur'a** tıklayın . Dizin deseni adı olarak kullanın `wazuh-archives-*`ve **Zaman alanı** açılır listesinde `timestamp` ayarlayın .
   Aşağıdaki GIF, endeks deseninin nasıl oluşturulacağını göstermektedir.

   wazuh-archives-* dizin deseninin oluşturulması
   Image not found or type unknown
2. Gösterge tablosundaki etkinlikleri görüntülemek için sol üst menü simgesine tıklayın ve **Keşfet'e** gidin . Dizin desenini olarak değiştirin `wazuh-archives-*`.

   Gösterge tablosunda etkinlikleri görüntüleyin
   Image not found or type unknown

Use Case: İmzalanmış İkili Proxy Yürütmeyi Algılama

`T1218.010`İmzalanmış ikili proxy yürütme, tehdit aktörlerinin kötü amaçlı kod çalıştırmak için güvenilir ikili dosyaları kullanarak uygulama beyaz listesini atlatmak için kullandıkları bir tekniktir. Bu teknik , MITRE ATT&CK çerçevesine dayalı olarak tanımlanmıştır .

Bu kullanım örneğinde, `regsvr32.exe`uygulama denetimlerini atlatmak için Windows yardımcı programı 'nın nasıl kötüye kullanılacağını gösteriyoruz. Daha sonra bu teknikle ilgili şüpheli etkinliği

tespit etmek için Wazuh arşivlerindeki olayları analiz ediyoruz.

Windows 11 Yapılandırması

Windows 11 uç noktasına Sysmon ve Atomic Red Team'i (ART) yüklemek ve imzalanmış ikili proxy yürütme tekniğini taklit etmek için aşağıdaki adımları uygulayın.

Sysmon Entegrasyonu

Windows 11 uç noktasına Sysmon'ı yüklemek ve yapılandırmak için aşağıdaki adımları uygulayın.

1. Sysmon'ı Microsoft Sysinternals sayfasından indirin .
2. Sysmon yapılandırma dosyasını indirin: sysmonconfig.xml .
3. İndirilen yapılandırma dosyasıyla PowerShell'i yönetici olarak kullanarak Sysmon'u yükleyin:

```
> .\sysmon64.exe -accepteula -i .\sysmonconfig.xml
```

4. Sysmon günlüklerinin toplanacağı konumu belirtmek için `<ossec_config>`Wazuh aracı dosyasına blok içinde aşağıdaki yapılandırmayı ekleyin :`C:\Program Files (x86)\ossec-agent\ossec.conf`

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

5. Değişiklikleri uygulamak için Wazuh aracısını yeniden başlatın ve aşağıdaki PowerShell komutunu yönetici olarak çalıştırın:

```
> Restart-Service -Name Wazuh
```

Atomic Red Team Kurulumu

PowerShell'i yönetici olarak kullanarak Windows 11 uç noktasına Atomic Red Team PowerShell modülünü yüklemek için aşağıdaki adımları uygulayın.

1. Varsayılan olarak, PowerShell çalışan betiklerin yürütülmesini kısıtlar. Varsayılan yürütme politikasını şu şekilde değiştirmek için aşağıdaki komutu çalıştırın `RemoteSigned`:

```
> Set-ExecutionPolicy RemoteSigned
```

2. ART yürütme çerçevesini yükleyin:

```
> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredt
> Install-AtomicRedTeam -getAtomics
```

3. Fonksiyonu kullanmak için ART modülünü içe aktarın `Invoke-AtomicTest`:

```
> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
```

4. `Invoke-AtomicTest`Tekniğin ayrıntılarını göstermek için fonksiyonu kullanın `T1218.010`:

```
> Invoke-AtomicTest T1218.010 -ShowDetailsBrief
```

Output

```
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1218.010-1 Regsvr32 local COM scriptlet execution
T1218.010-2 Regsvr32 remote COM scriptlet execution
T1218.010-3 Regsvr32 local DLL execution
T1218.010-4 Regsvr32 Registering Non DLL
T1218.010-5 Regsvr32 Silent DLL Install Call DllRegisterServer
```

Saldırı Emülasyonu

Windows 11 uç noktasında imzalı ikili proxy yürütme tekniğini taklit edin.

1. Testi gerçekleştirmek için aşağıdaki komutu Powershell'i yönetici olarak çalıştırın `T1218.010`:

```
> Invoke-AtomicTest T1218.010
```

Output

```
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Done executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Executing test: T1218.010-2 Regsvr32 remote COM scriptlet execution
Done executing test: T1218.010-2 Regsvr32 remote COM scriptlet execution
Executing test: T1218.010-3 Regsvr32 local DLL execution
Done executing test: T1218.010-3 Regsvr32 local DLL execution
Executing test: T1218.010-4 Regsvr32 Registering Non DLL
Done executing test: T1218.010-4 Regsvr32 Registering Non DLL
Executing test: T1218.010-5 Regsvr32 Silent DLL Install Call DllRegisterServer
Done executing test: T1218.010-5 Regsvr32 Silent DLL Install Call DllRegisterServer
```

Exploitin başarılı bir şekilde yürütülmesinin ardından birkaç hesap makinesi örneği açılacaktır.

Wazuh Dashboard

Wazuh arşivlerini, avlanan teknikle ilgili olayları sorgulamak ve görüntülemek için kullanın. Arşivlere danışırken bazı olayların Wazuh panosunda uyarı olarak yakalanmış olabileceğini unutmamak önemlidir. Algılama yapılmayan uyarılar ve olaylar dahil olmak üzere Wazuh arşivlerinden gelen bilgileri kullanarak özel gereksinimlerinize göre özel kurallar oluşturabilirsiniz.

1. Testin gerçekleştirildiği son beş dakika içinde meydana gelen olayları görüntülemek için bir zaman aralığı filtresi uygulayın. `agent.id`, `agent.ip`veya kullanarak belirli Windows uç noktasından günlükleri görüntülemek için filtre uygulayın `agent.name`.

   

   Daha önceki saldırı emülasyonuyla bir korelasyon belirlemek için inceleyebileceğiniz birden fazla isabet vardır. Örneğin, test sırasında Windows uç noktasında gözlemlenene benzer bir hesap makinesi oluşturma olayı fark edebilirsiniz.

   

2. `regsvr32`Olaylarla ilgili işlemleri kolaylaştırmak ve araştırmak için arama çubuğuna yazın `regsvr32`.

   

3. İlgili alanları görüntülemek için herhangi bir olayı genişletin.

   

4. Arşivlenmiş günlüklerin JSON formatını görüntülemek için JSON sekmesine tıklayın.

   

   Komutlar, hizmetler, yollar ve daha fazlası gibi etkinliklere ilişkin belirli ayrıntıları JSON günlüğünden çıkarabilir ve doğrulayabilirsiniz. Aşağıda, ilk işlem oluşturmayı ve yürütülen komutla ilgili öznitelikleri tanımlayabilirsiniz:


```
"data": {
    "win": {
      "eventdata": {
        "originalFileName": "REGSVR32.EXE",
        "image": "C:\\\\Windows\\\\SysWOW64\\\\regsvr32.exe",
        "product": "Microsoft® Windows® Operating System",
        "parentProcessGuid": "{45cd4aff-35fc-6463-6903-000000001300}",
        "description": "Microsoft(C) Register Server",
```

```
        "logonGuid": "{45cd4aff-2ce5-6463-2543-290000000000}",

        "parentCommandLine": "C:\\\\Windows\\\\system32\\\\regsvr32.exe  /s /i C:\\\\AtomicRedTeam\\\\atomics

        "processGuid": "{45cd4aff-35fc-6463-6a03-000000001300}",
        "logonId": "0x294325",
        "parentProcessId": "7652",
        "processId": "4064",
        "currentDirectory": "C:\\\\Users\\\\THECOT~1\\\\AppData\\\\Local\\\\Temp\\\\",
        "utcTime": "2023-05-16 07:51:24.512",
        "hashes": "SHA1=8E2C6B7F92A560E0E856F8533D62A1B10797828F,MD5=5F7264BD237FAEA46FB24
        "parentImage": "C:\\\\Windows\\\\System32\\\\regsvr32.exe",
        "ruleName": "technique_id=T1117,technique_name=Regsvr32",
        "company": "Microsoft Corporation",
        "commandLine": "  /s /i C:\\\\AtomicRedTeam\\\\atomics\\\\T1218.010\\\\bin\\\\AllTheThingsx86.dll",
        "integrityLevel": "High",
        "fileVersion": "10.0.22621.1 (WinBuild.160101.0800)",
        "user": "Windows11\\\\Testuser",
        "terminalSessionId": "2",
        "parentUser": "Windows11\\\\Testuser"
      },
      "system": {
        "eventID": "1",
        "keywords": "0x8000000000000000",
        "providerGuid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
        "level": "4",
        "channel": "Microsoft-Windows-Sysmon/Operational",
        "opcode": "0",

        "message": "\"Process Create:\r\nRuleName: technique_id=T1117,technique_name=Regsvr32\r\nUtcTir

        "version": "5",
        "systemTime": "2023-05-16T07:51:24.5131006Z",
        "eventRecordID": "88509",
        "threadID": "3960",
        "computer": "Windows11",
        "task": "1",
        "processID": "3156",
        "severityValue": "INFORMATION",
        "providerName": "Microsoft-Windows-Sysmon"
      }
    }
  },
```


Diğer ilgili olaylar üzerinde daha fazla araştırma yaparak, regsvr32 yardımcı programı tarafından oluşturulan bir işlem enjeksiyon olayını ve yüklenen görüntüyü görebilirsiniz:


```
"data": {
    "win": {
      "eventdata": {
        "originalFileName": "mscoree.dll",
```

```
        "image": "C:\\\\Windows\\\\SysWOW64\\\\regsvr32.exe",
        "product": "Microsoft® Windows® Operating System",
        "signature": "Microsoft Windows",

       "imageLoaded": "C:\\\\Windows\\\\SysWOW64\\\\mscoree.dll",

       "description": "Microsoft .NET Runtime Execution Engine",
        "signed": "true",
        "signatureStatus": "Valid",
        "processGuid": "{45cd4aff-35fc-6463-6a03-000000001300}",
        "processId": "4064",
        "utcTime": "2023-05-16 07:51:24.774",
        "hashes": "SHA1=52A6AB3E468C4956C00707DF80C7609EEE74D9AD,MD5=BEE4D173DA78E4D3AC9E
        "ruleName": "technique_id=T1055,technique_name=Process Injection",
        "company": "Microsoft Corporation",
        "fileVersion": "10.0.22621.1 (WinBuild.160101.0800)",
        "user": "Windows11\\\\Testuser"
      },
      "system": {
        "eventID": "7",
        "keywords": "0x8000000000000000",
        "providerGuid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
        "level": "4",
        "channel": "Microsoft-Windows-Sysmon/Operational",
        "opcode": "0",

       "message": "\"Image loaded:\r\nRuleName: technique_id=T1055,technique_name=Process Injection\r\n

       "version": "3",
        "systemTime": "2023-05-16T07:51:24.7768916Z",
        "eventRecordID": "88510",
        "threadID": "3960",
        "computer": "Windows11",
        "task": "7",
        "processID": "3156",
        "severityValue": "INFORMATION",
        "providerName": "Microsoft-Windows-Sysmon"
      }
     }
    },
```


5. `data.win.eventdata.ruleName:technique_id=T1218.010,technique_name=Regsvr32` Teknik kimliğini görmek için aşağıda gösterilen filtreyi uygulayın.

Filtre T1218.010 tekniği

Image not found or type unknown

6. İlgili alanları görüntülemek için olayı genişletin.

Filtre T1218.010 tekniği

Image not found or type unknown

7. Arşivlenmiş günlüklerin JSON formatını görüntülemek için JSON sekmesine tıklayın.

JSON sekmesi

Image not found or type unknown

Aşağıdaki kayıttan, olayı analiz etmeyi kolaylaştıran daha yapılandırılmış ayrıntılar çıkarabilirsiniz:


```
"data": {
    "win": {
      "eventdata": {
        "destinationPort": "443",
        "image": "C:\\\\Windows\\\\System32\\\\regsvr32.exe",
        "sourcePort": "63754",
        "initiated": "true",
        "destinationIp": "1.1.123.23",
        "protocol": "tcp",
        "processGuid": "{45cd4aff-36b5-645a-9e07-000000000e00}",
        "sourceIp": "192.168.43.16",
        "processId": "4704",
        "utcTime": "2023-05-09 21:19:25.361",

       "ruleName": "technique_id=T1218.010,technique_name=Regsvr32",

       "destinationIsIpv6": "false",
        "user": "Windows11\\\\Testuser",
        "sourceIsIpv6": "false"
       },
       "system": {
        "eventID": "3",
        "keywords": "0x8000000000000000",
        "providerGuid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
        "level": "4",
        "channel": "Microsoft-Windows-Sysmon/Operational",
        "opcode": "0",

       "message": "\"Network connection detected:\r\nRuleName: technique_id=T1218.010,technique_name=

       "version": "5",
        "systemTime": "2023-05-09T12:04:07.0231156Z",
        "eventRecordID": "63350",
        "threadID": "3096",
        "computer": "Windows11",
        "task": "3",
        "processID": "3156",
        "severityValue": "INFORMATION",
        "providerName": "Microsoft-Windows-Sysmon"
       }
     }
    },
```


Algılama mantığını geliştirmek ve özel kod çözücüler ve kurallar yazmak için Wazuh arşivlerinden gelen olayları kullanabilirsiniz. Ayrıca `wazuh-logtest`, kuralları sağlanan günlüklere göre test etmek ve doğrulamak için hazır aracı da kullanabilirsiniz.

Revision #7
Created 11 December 2024 16:27:00 by Ayşegül Sarıkaya
Updated 31 December 2024 13:26:28 by Ayşegül Sarıkaya