**5651 Sayılı Kanun ve SIEM Ürünleri**

**-BOŞ BIRAKILMIŞTIR-**

## **İÇİNDEKİLER**

Kurum Üst Yazı

[**İÇİNDEKİLER** 3](#_Toc108968371)

[1. DOKÜMAN HAKKINDA 4](#_Toc108968372)

[2. 5651 SAYILI KANUN’UN AMACI 4](#_Toc108968373)

[3. KANUN VE YÖNETMELİK’TE GEÇEN TANIMLAMALAR 5](#_Toc108968374)

[4. “LOG TOPLAMA VE SAKLAMA” İLE İLGİLİ MADDELER 6](#_Toc108968375)

[5. KANUN, YÖNETMELİK VE SIEM ÜRÜNLERİ İLE İLGİLİ DEĞERLENDİRME 7](#_Toc108968376)

# DOKÜMAN HAKKINDA

Bu doküman, SIEM ürünlerinin kullanıldığı ortamlarda toplanan logların 5651 Sayılı Kanun’a (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) uyumluluğunu açıklamak amacıyla oluşturulmuştur.

Bahsi geçen Kanun ve Kanun’da atıf yapılan yönetmeliğin orijinal metinlerine aşağıdaki bağlantılardan ulaşılabilir.

**5651 Sayılı Kanun**

<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf?dil=tr-TR>

**İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik**

<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=23501&MevzuatTur=7&MevzuatTertip=5>

Dokümanda sırasıyla aşağıdaki konulardan bahsedilmektedir.

* 5651 Sayılı Kanun’un amacı
* Kanun ve yönetmelikte geçen tanımlamalar
* “Log Toplama ve Saklama” ile ilgili geçen maddeler
* Kanun, Yönetmelik ve SIEM ürünleri ile ilgili değerlendirme

# 5651 SAYILI KANUN’UN AMACI

5651 Sayılı Kanun’un, Kanun metninde yer alan amaç ve kapsamı aşağıdaki şekildedir:

*“Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.”*

# KANUN VE YÖNETMELİK’TE GEÇEN TANIMLAMALAR

Kanun’da Erişim Sağlayıcı, İçerik Sağlayıcı ve Yer Sağlayıcı için farklı yükümlülükler bulunmakta olup bu tanımlar Kanun’da aşağıdaki şekilde yapılmıştır.

**Erişim Sağlayıcı:** Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler.

**İçerik Sağlayıcı:**Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler.

**Yer sağlayıcı:** Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler.

Kanun’da, bu dokümana konu olan, SIEM tarafını ilgilendiren logların toplanması konularında “Trafik Bilgisi” ibareleri geçmektedir. Trafik bilgisi için yapılan tanım da aşağıdaki gibidir:

**Trafik Bilgisi:** Taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri.

Kanunun maddelerinin atıfta bulunduğu yönetmelikte bulunan erişim ve kullanım sağlayıcı tanımları aşağıdaki gibidir. Ayrıca Kanun’da bulunan Trafik Bilgisi tanımına benzer şekilde Erişim Kayıtları tanımı bulunmaktadır, tam tanım aşağıdaki gibidir.

**Erişim sağlayıcı:** İnternet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internet ortamına erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişiler.

**Erişim kayıtları:** Kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri, hedef IP adresi, bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgileri.

**Ticari amaçla internet toplu kullanım sağlayıcı:** İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zeka geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan gerçek ve tüzel kişiler.

**İnternet toplu kullanım sağlayıcı:** Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişiler.

# “LOG TOPLAMA VE SAKLAMA” İLE İLGİLİ MADDELER

Aşağıda bulunan metinler dokümanın başında bağlantıları ve isimleri verilen kanun ve yönetmeliklerden olduğu gibi kopyalanmıştır. Harf ve rakamlar da kanun ve yönetmelikteki madde, fıkra ve bentleri göstermektedir.

**(Kanun) Yer sağlayıcının trafik bilgilerini tutma ilgili yükümlülükleri:**

Madde 5 – 3:

Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

**(Kanun) Erişim sağlayıcının yükümlülükleri**

Madde 6 – 1:

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

**(Yönetmelik) İnternet toplu kullanım sağlayıcılarının yükümlülükleri**

Madde 4 – 1:

b) Erişim kayıtlarını elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamak.

**(Yönetmelik) Ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri**

Madde 5 – 1:

d) Erişim kayıtlarını elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamak,

e) (d) bendi gereğince kaydedilen bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri iki yıl süre ile saklamak,

# KANUN, YÖNETMELİK VE SIEM ÜRÜNLERİ İLE İLGİLİ DEĞERLENDİRME

Kanun ve yönetmelikte belirtildiği üzere hizmet sağlayıcıların sağladığı hizmet türüne göre erişim ve/veya trafik kayıtlarını 6 aydan 2 yıla kadar (ilgili maddenin belirttiği kadar) saklaması gerekmektedir.

İlgili maddelerde trafik bilgisi ve erişim kayıtlarının doğruluk, bütünlük ve gizliliğini koruyarak saklanması gerektiği belirtilmektedir. Sadece yönetmeliğin 5-1-e maddesinde (Ticari amaçla internet toplu kullanım sağlayıcıların yükümlülükleri) kayıtların bütünlüğünü, doğruluğunu teyit eden değerin günlük olarak kaydedilmesi ve bu değerin iki yıl kaydedilmesi istenmektedir. Burada bahsedilen değer bütünlük (integrity) kontrolünde kullanılan hash değeridir.

Kullanılan SIEM ürünlerinde (IBM Qradar, Microfocus ArcSight, Mcafee SIEM) toplanan logların değişmediğini göstermek için kullanılan hashing/integrity check özellikleri bulunmaktadır. Ön tanımlı olarak kapalı durumda gelen bu özellikler açıldığında logun SIEM’e kaydedildiği andaki hash’ini almakta ve her log için bir hash’i kaydetmektedir. Logun saklandığı süre boyunca da bu değer saklanmaktadır.

Kanun ve yönetmeliğin her hangi bir maddesinde KAMUSM ve/veya TÜBİTAK gibi kurumlardan alınacak olan kontör ile zaman damgası oluşturulmasından bahsetmediğinden ve bahsi geçen SIEM ürünlerinin (IBM Qradar, Microfocus ArcSight, Mcafee SIEM) logun değişmediğini ispatlamak için geçerli yöntemleri olduğundan ötürü bahsi geçen SIEM ürünleri gerekli ayarlar yapıldıktan sonra 5651 sayılı kanunun gereklerini teknik olarak karşılamaktadır. Buna ek olarak kanun ve yönetmelikte geçen trafik bilgileri ve erişim kayıtlarını oluşturabilecek tüm sunucu, güvenlik cihazı ve ağ ürünlerinin gerekli loglarının da SIEM’de toplanması gerekmektedir.

SIEM ürününe sahip kurum, ikinci bir önlem olarak SIEM’de toplanan logları, KAMUSM veya TÜBİTAK’tan kendi satın alacağı kontör ile damgalayarak, kendi sağlayacağı bir depolama alanında saklamak isterse BARİKAT tarafından sağlanacak bir script ile ilgili logları SIEM dışına aktarıp, kontör ile damgalayarak gösterilen depolama alanına kopyalama yöntemini tercih edebilir.

SIEM ürünlerinde yapılan bütünlükte kontrolü işlemleri ile ilgili bilgilere aşağıdaki linklerden ulaşılabilir.

* IBM QRadar
	+ Enabling log hashing

<https://www.ibm.com/docs/en/qsip/7.4?topic=logs-enabling-log-hashing>

* + Checking the integrity of event and flow logs

<https://www.ibm.com/docs/vi/qsip/7.3.2?topic=qradar-checking-integrity-event-flow-logs>

* Microfocus ArcSight
	+ ArcSight Smart Connector Installation and User Guide
	(Sayfa 94, Check Event Integrity Method bölümü)
	<https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/pdfdoc/SmartConnInstallandUserGuide/SmartConnInstallandUserGuide.pdf>
* Mcafee SIEM
	+ Enterprise Log Manager integrity check information
	<https://kcm.trellix.com/corporate/index?page=content&id=KB74301&locale=en_US>

