



## TEHDİT İSTİHBARATI PROSEDÜRÜ

|                     |            |
|---------------------|------------|
| Doküman No          | PR.021     |
| Yayın Tarihi        | 01.07.2024 |
| Revizyon No         | 00         |
| Revizyon Tarihi     |            |
| Toplam Sayfa Sayısı | 16         |

- Giriş :** ISO 27001:2022 standardı, Kurumların bilgi güvenliğini yönetmelerine yardımcı olan bir çerçeve sunar. Tehdit istihbaratı prosedürü, bu standardın önemli bir bileşenidir ve Kurumların potansiyel tehditleri belirleyerek önleyici tedbirler almalarını sağlar.
- Amaç :** Bu prosedürün amacı, Kurumun bilgi varlıklarına yönelik potansiyel tehditleri sistematik olarak tanımlamak, analiz etmek ve bu bilgiler doğrultusunda uygun güvenlik önlemlerini belirlemektir.
- Kapsam :** Bu prosedür, Kurum Bilgi İşlem birimlerini ve bilgi varlıklarını kapsar. Tehdit istihbaratı toplama, analiz etme, değerlendirme ve raporlama süreçlerini tanımlar.
- Sorumluluklar :** Bilgi Güvenliği Yöneticisi: Prosedürün uygulanmasından genel olarak sorumludur. Tehdit İstihbaratı Ekibi: Tehdit istihbaratı toplama, analiz etme ve raporlama görevlerini yürütür. İlgili Birimler: Kendi alanlarına özgü tehditleri belirlemek ve gerekli önlemleri almakla görevlidir.

### 5. Uygulama :

#### 5.1.Tehdit Kaynaklarının Belirlenmesi

İç tehditler (çalışan hataları, kasıtlı saldırılar)

Dış tehditler (siber saldırılar, doğal afetler)

Tedarikçiler ve iş ortakları

Yasal ve düzenleyici gereksinimler

#### 5.2.Tehdit İstihbaratı Toplama

|                   |                    |
|-------------------|--------------------|
| <b>HAZIRLAYAN</b> | <b>ONAYLAYAN</b>   |
| Şube Müdürü       | B.İ. Daire Başkanı |

“Bu doküman elektronik kopyasının basılması durumunda **kontROLSÜZ kopya** olarak işlem görür”

|   |                                     |                     |            |
|---|-------------------------------------|---------------------|------------|
|  | <b>TEHDİT İSTİHBARATI PROSEDÜRÜ</b> | Doküman No          | PR.021     |
|   |                                     | Yayın Tarihi        | 01.07.2024 |
|   |                                     | Revizyon No         | 00         |
|   |                                     | Revizyon Tarihi     |            |
|   |                                     | Toplam Sayfa Sayısı | 16         |

Açık kaynaklar (haberler, sosyal medya, güvenlik forumları)

Ticari istihbarat hizmetleri

Güvenlik yazılımları (intrusion detection systems, SIEM)

Sektör raporları ve analizleri

İç raporlar ve olay kayıtları

### 5.3.Tehdit Analizi

Toplanan bilgilerin değerlendirilmesi

Tehditlerin olasılığı ve etkisi

Benzer saldırıların incelenmesi

Mevcut güvenlik kontrollerinin etkinliği

### 5.4.Risk Değerlendirmesi

Tehditlerin Kurum üzerindeki potansiyel etkisi

Varlıkların değerlendirilmesi

Risklerin önceliklendirilmesi

### 5.5.Raporlama

|                   |                    |
|-------------------|--------------------|
| <b>HAZIRLAYAN</b> | <b>ONAYLAYAN</b>   |
| Şube Müdürü       | B.İ. Daire Başkanı |

“Bu doküman elektronik kopyasının basılması durumunda **kontROLSÜZ kopya** olarak işlem görür”

|   |                                     |                     |            |
|---|-------------------------------------|---------------------|------------|
|  | <b>TEHDİT İSTİHBARATI PROSEDÜRÜ</b> | Doküman No          | PR.021     |
|   |                                     | Yayın Tarihi        | 01.07.2024 |
|   |                                     | Revizyon No         | 00         |
|   |                                     | Revizyon Tarihi     |            |
|   |                                     | Toplam Sayfa Sayısı | 16         |

Yönetime düzenli raporlama  
İlgili birimlere bilgi paylaşımı  
Tehdit istihbaratı raporlarının arşivlenmesi

### 5.6.Tedbirlerin Alınması

Riskleri azaltmak için uygun güvenlik kontrollerinin belirlenmesi ve uygulanması  
Güvenlik farkındalığı eğitimleri  
Acil durum planlarının güncellenmesi  
Sürekli iyileştirme

### 5.7.Ölçüm ve İzleme

Prosedürün etkinliğinin düzenli olarak değerlendirilmesi  
Tehdit istihbaratı süreçlerinin sürekli iyileştirilmesi

|                   |                    |
|-------------------|--------------------|
| <b>HAZIRLAYAN</b> | <b>ONAYLAYAN</b>   |
| Şube Müdürü       | B.İ. Daire Başkanı |

“Bu doküman elektronik kopyasının basılması durumunda **kontROLSÜZ kopya** olarak işlem görür”