## 1. AMAÇ

Bu prosedürün amacı kurumun bilgi güvenliği tehditlerine ilişkin bilgileri toplamak, analiz etmek, değerlendirmek, ilgili taraflarla paylaşmak ve gerekli önlemleri almak için uygulanacak kuralları belirlemektir.

**Denetim Sebepleri:**

- Kurumun bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak,
- Güncel ve potansiyel tehditler hakkında farkındalık yaratmak,
- Tehditlere ilişkin bilgileri toplayarak riskleri azaltmak ve savunma mekanizmalarını güçlendirmek,
- Gerektiğinde kullanıcıların veya sistemlerin maruz kaldığı tehditleri tespit edip önleyici/düzeltici faaliyetler başlatmak.

## 2. KAPSAM

Bu prosedür, kurumun sahip olduğu veya kurum adına kullanılan tüm bilgi sistemleri, ağlar, sunucular, uç cihazlar ve uygulamalar için geçerlidir.

- Kurum bünyesinde bulunan ancak kurum mülkiyetinde olmayan (örneğin hizmet alınan üçüncü taraf sistemler) varlıklar da tehdit istihbaratı kapsamında değerlendirilebilir.
- Tehdit istihbaratı faaliyetleri sırasında hizmetlerin kesintiye uğramasına neden olacak saldırı simülasyonları (ör. DDoS testi) yapılmayacaktır.
- Tehdit istihbaratında elde edilen bilgiler yalnızca analiz ve savunma amaçlı kullanılacak, üçüncü taraflarla paylaşım gizlilik esaslarına uygun şekilde yapılacaktır.

## 3. SORUMLULAR

- **Bilgi İşlem Daire Başkanlığı:** Tehdit istihbaratı kaynaklarının takibi, kayıtların tutulması ve ilgili aksiyonların alınmasından sorumludur.
- **BGYS Komitesi:** Tehdit istihbaratının değerlendirilmesi, risk kayıtlarına işlenmesi ve gerekli önlemlerin alınmasına karar verir.

## 4. UYGULAMA

### 4.1. Tehdit Bilgisi Toplama

- Ulusal ve uluslararası CERT/USOM bültenleri,
- Siber güvenlik sağlayıcılarının raporları,
- SIEM, IDS/IPS gibi kurum içi güvenlik sistemleri,

- Sektör bazlı güvenlik toplulukları ve paylaşım platformları düzenli olarak takip edilir.

### 4.2. Analiz ve Sınıflandırma

- Toplanan tehdit bilgileri kritik, yüksek, orta ve düşük seviyelerde sınıflandırılır.
- Kritik ve yüksek seviyeli tehditler için acil önlemler planlanır.
- Yeni tespit edilen tehditler, yapılandırma standartlarına ve risk yönetim kayıtlarına işlenir.

### 4.3. Raporlama

- Tehdit istihbaratı raporları aylık periyotlarda veya önemli bir tehdit ortaya çıktığında hazırlanır.
- Raporlar BGYS Komitesine sunulur ve gerekli birimlerle paylaşılır.

### 4.4. Periyotlar

- Tehdit istihbaratı en az aylık olarak toplanır ve analiz edilir.
- Kritik olaylarda periyot beklenmeden raporlama yapılır.

### 4.5. Gizlilik

- Tehdit istihbaratı kapsamında elde edilen bilgiler, gizlilik esaslarına uygun şekilde saklanır.
- Üçüncü taraflarla paylaşım yapılacaksa karşılıklı gizlilik anlaşması imzalanır.

## 5. İLGİLİ DOKÜMANLAR

- PLT-020 Güvenlik Açıkları Tespit Etme Politikası
- PR-011 Risk Yönetimi Prosedürü
- RPR-011 Tehdit İstihbaratı Raporu

## 6. REVİZYON TAKİP TABLOSU

| REVİZYON NO | TARİH | AÇIKLAMA |
|---|---|---|
| 000 | 29.09.2025 | İlk yayın. |
| | | |