SİBER TEHDİT İSTİHBARATI

HAFTA – 1

Dr. Burak Gülbay

Veri | Bilgi | İstihbarat

- Farkı nedir?

STİ Nedir?

- STİ, kuruluşların kendilerini savunmalarına yardımcı olan tehditler hakkındaki bilgidir.
- Önemli olan sadece veri toplamak değil; ham verileri, daha iyi güvenlik kararları almamızı sağlayacak bilgilere dönüştürmektir.
- Bunu bir dedektifin bir davayı çözmesi gibi düşünün; ham ipuçları, bağlam içinde birbirine bağlanmadığı, analiz edilmediği ve anlaşılmadığı sürece işe yaramaz.

Temeller

Veri	Ham
Bilgi	Yapısal
İstihbarat	Harekete Geçilebilir

Katma Değer

01/

Veri

Veriler yalnızca ham gerçeklerdir. Tek başına pek bir şey ifade etmeyebilir.

02/

Bilgi

Bilgi, söz konusu verilerin işlenip bir bağlam kazandırılmasıyla ortaya çıkar.

03/

İstihbarat

İstihbarat, bilginin analiz edilmesi, doğrulanması ve kararları desteklemek için kullanılmasıdır.

Değer Artar

Siber Güvenlikte Veri

- IP adresleri, alan adları, dosya özetleri (hash), günlük kayıtları (log) …
- Tek başlarına bize pek birşey anlatmazlar
- Gürültülüdür: Şüpheli görünen her IP gerçekten kötü niyetli değildir.

Siber Güvenlikte Bilgi

- Bir zararlı yazılım ailesine bağlı dosya özeti (hash)
- Bağlam eklenir ve veriler bilgiye dönüşür
- Veriden daha anlamlıdır ama yine de bulmacanın sadece bir parçasıdır.

Siber Güvenlikte İstihbarat

- İlişkilendirilmiş, analiz edilmiş, eyleme dönüştürülebilir: “APT28, kimlik avcılığının arkasındadır”
- İstihbarat noktaları birleştirir.
- “Birden fazla veri noktasını ve bilgiyi analiz ettikten sonra, APT28'in Türkiye'deki savunma sektörüne karşı bir kimlik avı kampanyası yürüttüğünü değerlendirebiliriz.”
- Eyleme dönüştürülebilirdir: Karar vericilere ve savunma tarafında çalışanlara rehberlik eder.

İstihbarat Yaşam Döngüsü

Veri -> Bilgi -> İstihbarat

- Ham veriler toplanarak başlanır,
- Kullanılabilir formatlara dönüştürülür,
- Anlam çıkarmak için analizler yapılır,
- Paydaşlara dağıtılır,
- Son olarak döngüyü iyileştirmek için geri bildirim verilir / toplanır,

Bu süreç tekrarlanır; yeni veriler devamlı güncellenmiş istihbarata aktarılır.

İstihbarat Türleri

Uzun Süreli

Kısa Süreli

Stratejik

Değişen riskler hakkında üst düzey bilgiler

Üst Düzey Yöneticiler ve Yönetim

Taktik

Saldırganların TTP'leri hakkında bilgi

BT Hizmet Yöneticileri ve SOC Yöneticileri

Operasyonel

Belirli bir gelen saldırı hakkında bilgi

Güvenlik Yöneticisi ve Ağ Güvenlikçileri

Teknik

Spesifik IoC

SOC Çalışanları

Yüksek Seviyeli

Düşük Seviyeli

STİ Ayrımı / Sınıflandırma Neden Önemli?

- Güvenlik Operasyon Merkezi (SOC), net bir anlamı olmayan ham verilerle dolup taşabilir.
- İstihbarat, doğru kişilerin doğru zamanda doğru içgörülere ulaşmasını sağlar.
- Veri, bilgi ve istihbarat arasında ayrım yapılmadığında, karar vericiler karar veremez hale gelir.
- Yapılan ayrım / sınıflandırma, istihbaratın ömrünü gösterir.

Vaka Çalışması

- Bir IP adresini log dosyasında gördünüz. — Veri
- Bu IP adresi oltalama saldırılarında komuta ve kontrol makinesi olarak kullanılıyor. — Bilgi
- Oltalama saldırıları Türkiye'de finans sektörünü hedef alan bir APT grubu ile ilişkilendiriliyor. — Intelligence

Her adım değer katar !

İstihbarat Toplama Disiplinleri

STİ genellikle bu kaynakları birleştirerek daha büyük bir resim oluşturur

- **OSINT:** sosyal medya, bloglar, forumlar
- **HUMINT:** muhbirler, içeriden gelen raporlar
- **SIGINT:** ağ trafiği, iletişimin izlenmesi
- **TECHINT:** Zararlı yazılım analizi, adli bilişim delilleri
- **GEOINT**
- **FININT**

MITRE ATT&CK ile İlişkilendirme

ATT&CK'da istihbarat, saldırganın Taktik, Teknik ve Prosedür'lerine (TTP'ler) eşlenebilir.

MITRE ATT&CK 'ın Amacı:

- Tehdit Davranışlarının Standartlaştırılmış Bilgi Tabanı
- Tehdit Modelleme ve Simülasyon
- Boşluk Analizi ve Savunma Önceliklendirmesi
- Olay Müdahalesi ve Tehdit Avcılığı
- Sektör İşbirliği ve Bilgi Paylaşımı

YAYGIN HATALAR

DİKKAT !

01/

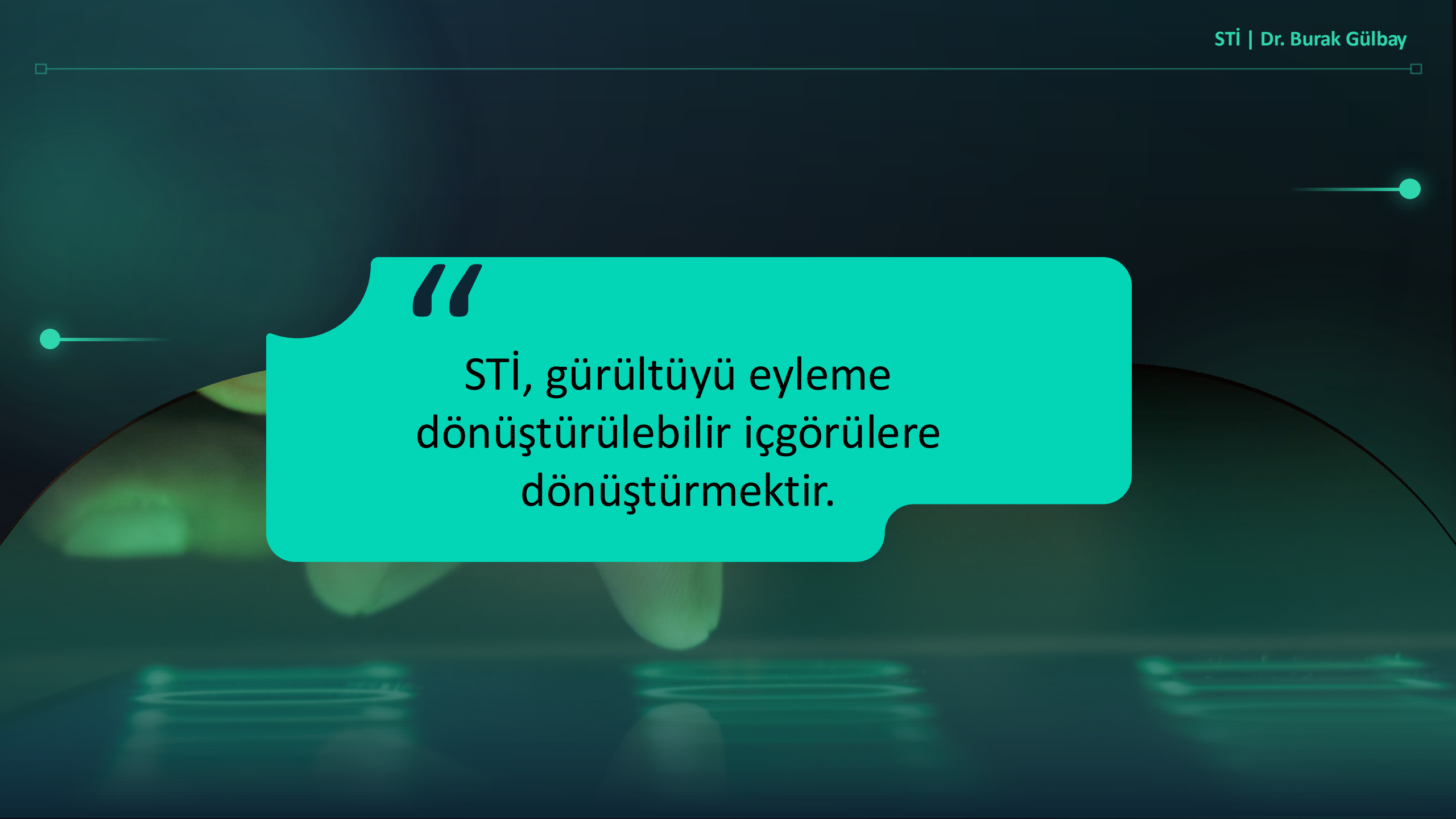
Yaygın bir hata, ham verileri istihbarat olarak ele almaktır.

02/

Uzman görüşü olmadan otomatik gelen tehdit haberlerine (feed) aşırı güvenmektir.

03/

Doğrulanmadığı ve bağlam kazandırılmadığı takdirde istihbaratın hiçbir faydası yoktur.



> STİ, gürültüyü eyleme dönüştürülebilir içgörülere dönüştürmektir.