SecurityScorecard

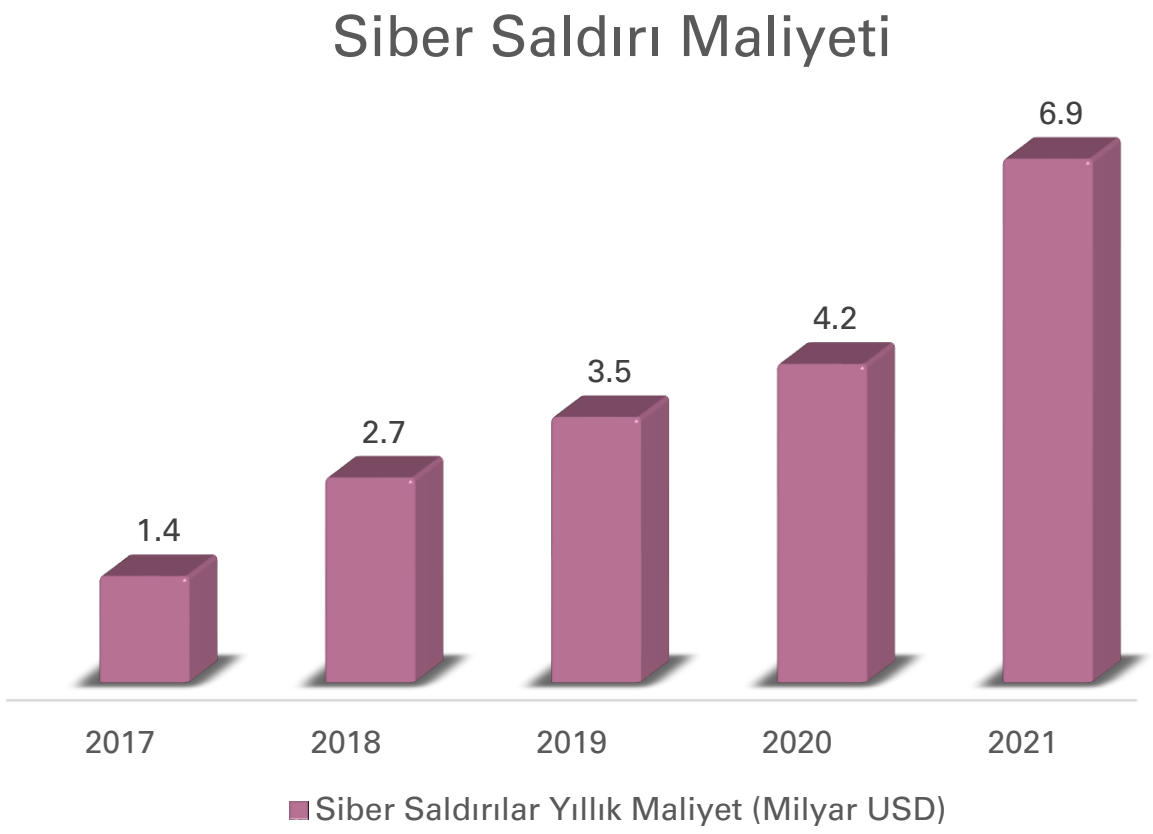
Forcerta
Advanced ICT Enabler & VAR

Türkiye Sektörel Siber Güvenlik Risk İncelemesi

28.09.2022

FORCERTA

Siber Suçlar Artıyor



Siber suçların global olarak artış göstermesi güvenlik önlemlerimizin hem daha yaygın ve etkin, hem de daha güncel dinamik olmasını gerektiriyor.

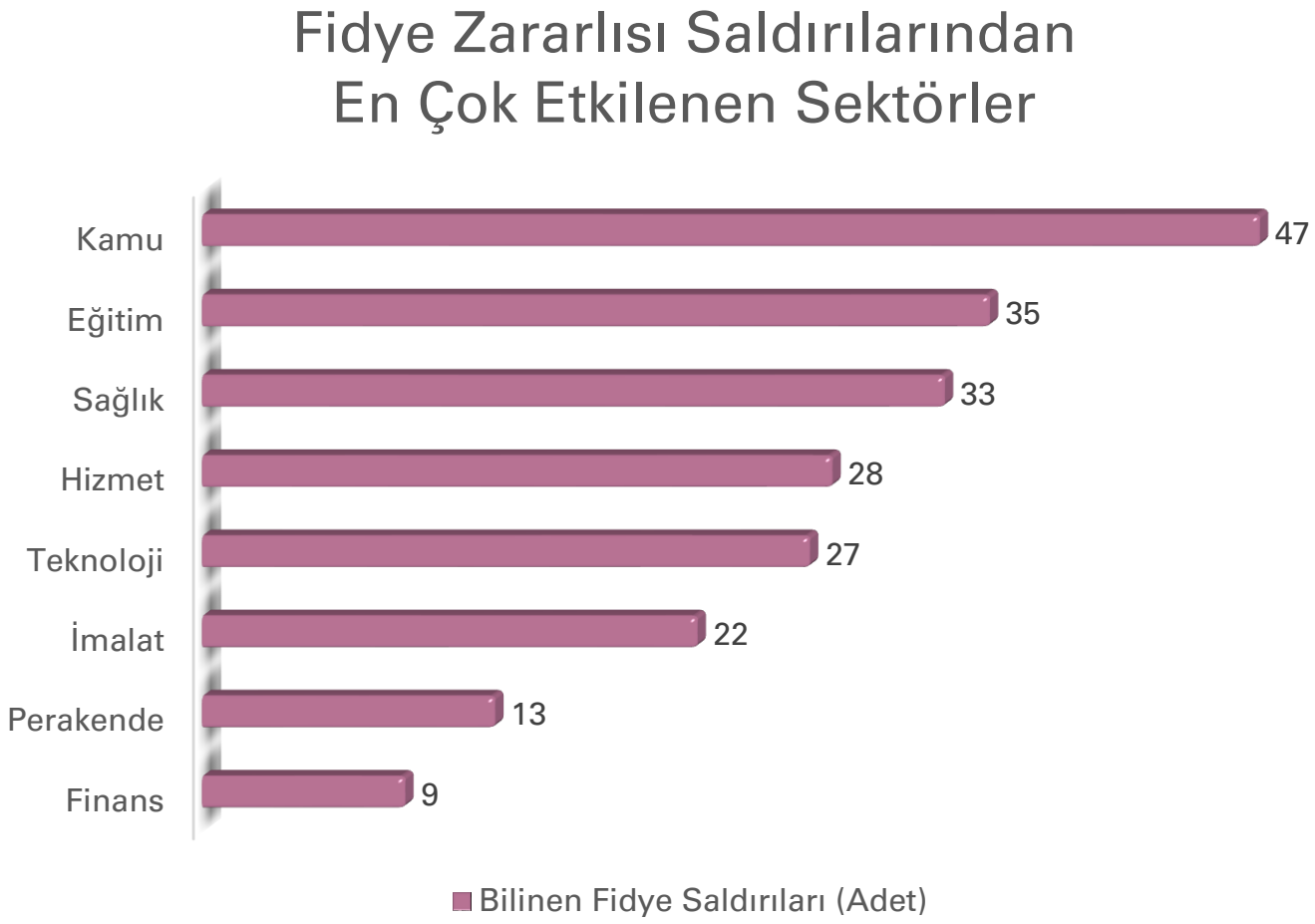
Riskleri izlemek ve hızlı önlem almak için yapılacak harcamaların, riskin gerçekleşmesinden çok daha uygun maliyetli olduğu görülüyor.

Kaynak: *Federal Bureau of Investigation Internet Crime Report 2021*

FORCERTA

Fidye Zararlısı Saldırılarının Sektörler Bazında Etkisi

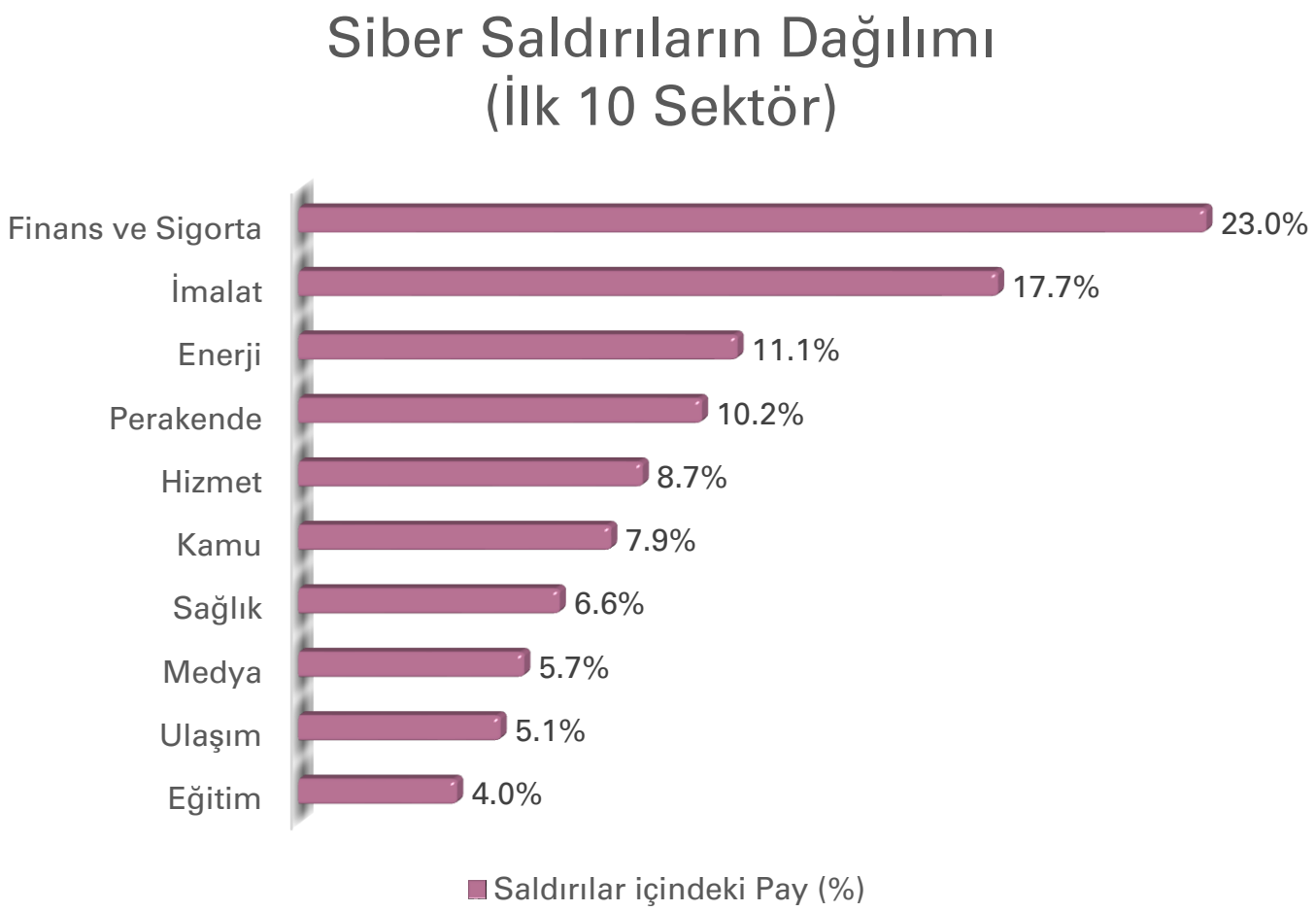
2021 yılında bildirilen vakalara dayanılarak oluşan istatistiklere göre, Finans sektörünün olgunluğunun iyi seviyede olduğu, kritiklik açısından bakılınca Kamu, Eğitim ve Sağlık sektörlerinde olgunluğunun iyileşme ihtiyacı olduğu görülmektedir.



Kaynak: *Statista Blackfog – 1 Kasım 2021*

FORCERTA

Siber Saldırıların Sektörler Bazında Dağılımı



Finans sektörünün siber saldırı karşılamada en önde olması ve siber saldırıdan zarar gören sektörler içinde de en güçlü görünmesi, etkin çözümler kullanıldığını gösteriyor.

Bazı sektörlerin göreceli olarak daha az atak almasına rağmen daha büyük zararlarla karşılaştığı görülmektedir. Bu da izleme ve önleme alanında yatırım yapması gerektiğini göstermektedir.

Kaynak: *IBM Security X-Force 2021*

FORCERTA

Çalışma Hakkında

Bu çalışmada, SecurityScorecard platformunu kullanarak; **Türkiye'nin en önemli 6 sektöründeki 50 kurumu inceledik** ve elde ettiğimiz detaylı bilgilerden sektörler siber güvenlik olgunluk durumlarını ortaya koyan özet bir analiz hazırladık.

Forcerta olarak iş ortağı olduğumuz SecurityScorecard hakkında daha fazla bilgi edinmek için
https://www.forcerta.com/urunler/security-scorecard/
https://securityscorecard.com

Özetle, bir hacker gözüyle kurumun ve tedarikçilerinin dijital ayak izlerinden siber güvenlik risklerini tespit eder, ölçer ve iyileştirme önerileri sunar.

Çalışmaya konu sektörler için seçilmiş olan şirketler, finansal ve dijital altyapıları birbirine yakın, sektörlerinin öncü kuruluşlarıdır.

FORCERTA

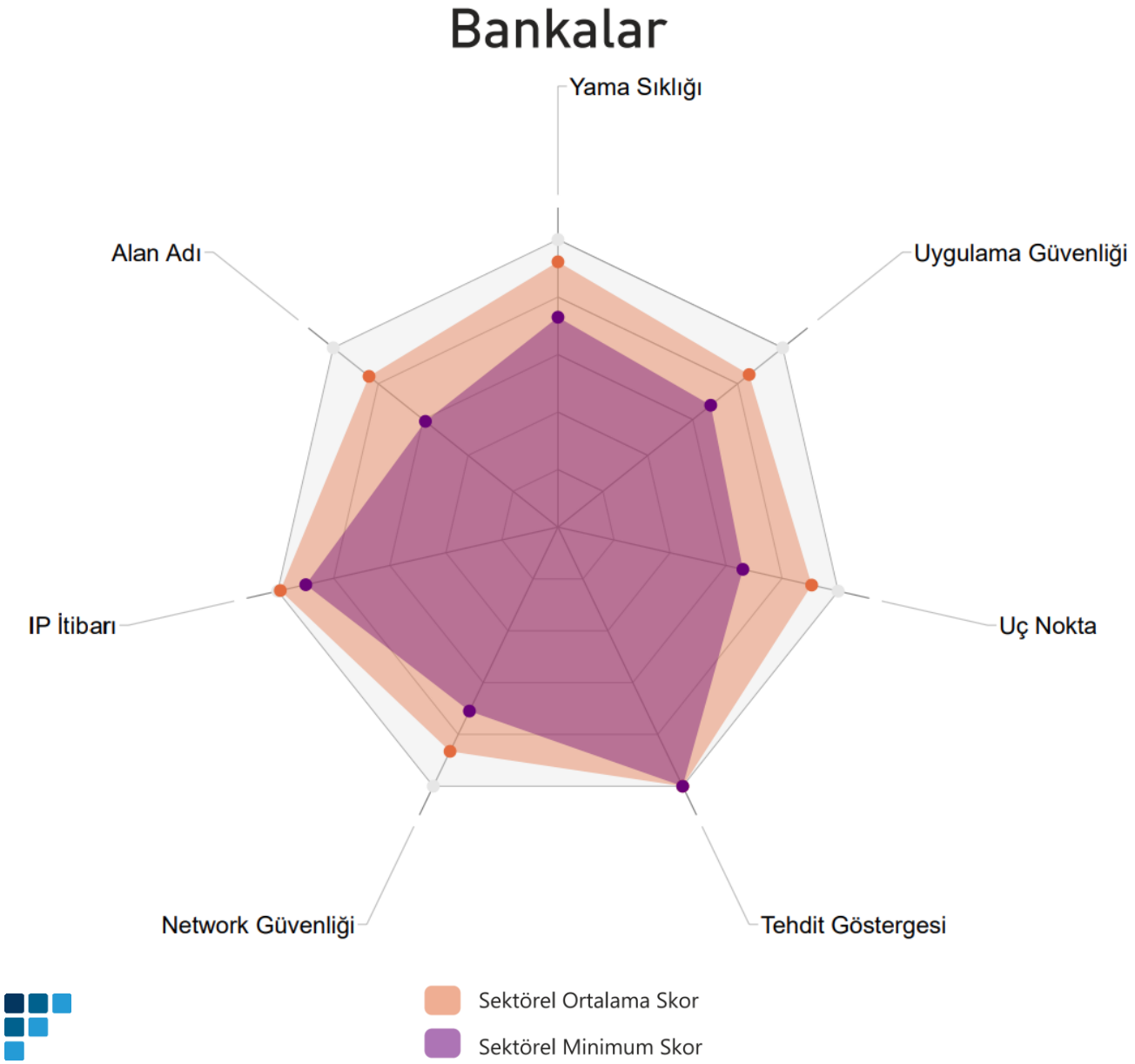
İnceleme Alanları

Security Scorecard

Çalışmamızda her bir kurum için tespit edilen bulgular sektör incelemesinde aşağıdaki kategorilerde konsolide edilmiştir:

1. **Network Security / Ağ Güvenliği:** Güvenli olmayan ağ ayarlarının algılanmasını,
2. **DNS Health / Alan Adı Servisi Sağlığı:** Güvenli olmayan DNS yapılandırmaları ve güvenlik açıklarının algılanmasını,
3. **Patching Cadence / Yamalama Sıklığı:** Güvenlik açıklıkları ve riskler içerebilecek, güncelliğini yitirmiş şirket varlıklarını,
4. **Endpoint Security / Uç Nokta Güvenliği:** Uç noktaların güvenlik seviyesinin ölçülmesini,
5. **IP Reputation / IP İtibarı:** Şirket ağınızdaki kötü amaçlı yazılım veya spam gibi şüpheli etkinliklerin algılanmasını,
6. **Application Security / Uygulama Güvenliği:** Yaygın web sitesi uygulama açıklarının algılanmasını,
7. **Cubit Score / Tehdit Göstergesi:** Yönetim portalleri ile ilgili kritik güvenlik ve konfigürasyon sorunlarını ölçmeyi sağlayan tehdit göstergelerini,

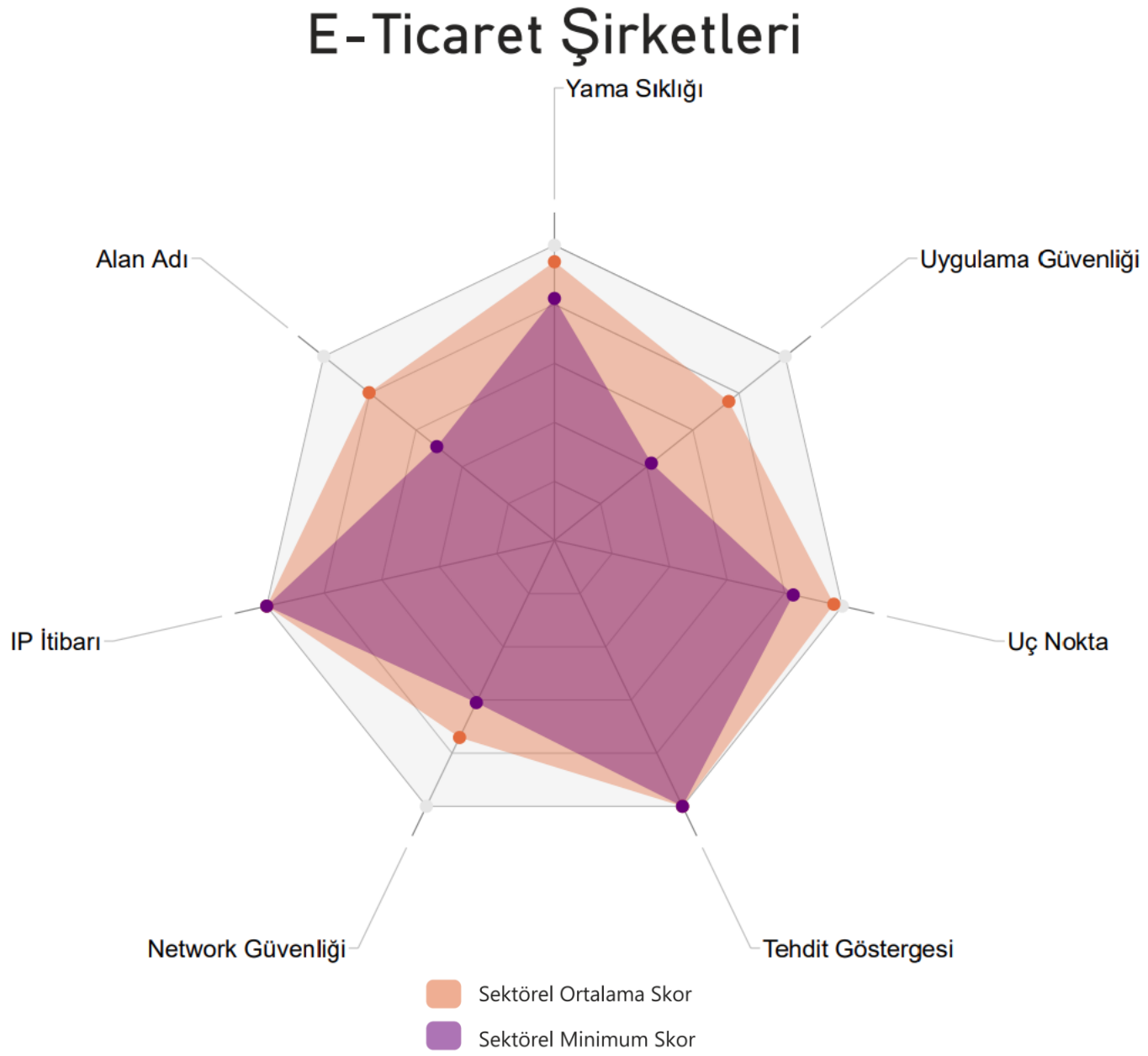
FORCERTA



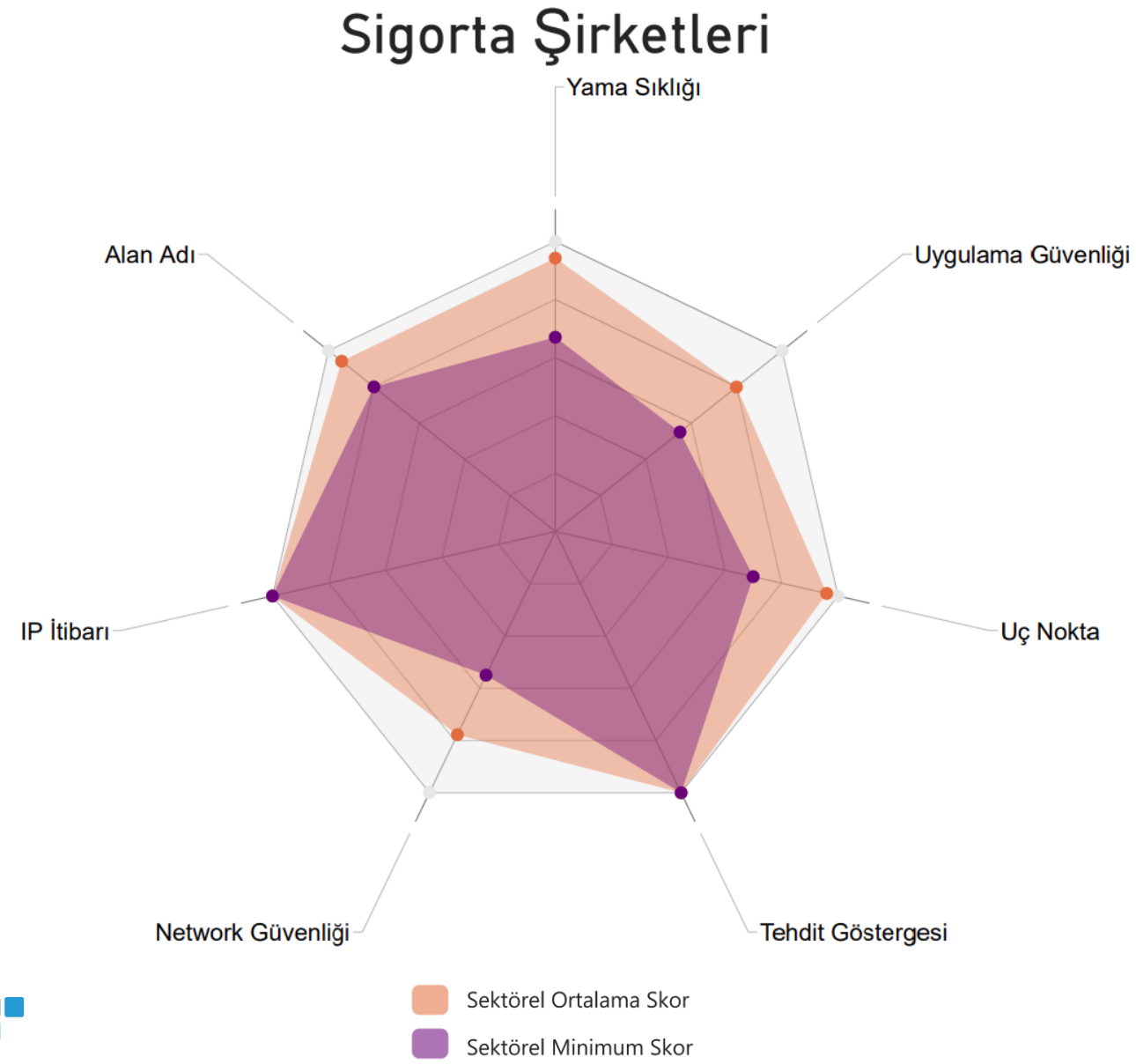
- Bankacılık sektörünü incelemek için benzer ölçekte 11 banka incelenmiştir.
- Regülasyonun çok sıkı olduğu bankacılık sektörü ortalama skor ve min. skor verilerinden de görüleceği gibi, siber güvenlik olgunluğunda diğer sektörlerin çok ilerisindedir.
- Çalışmaya konu bankaların her bir alan için hazırlık ve olgunluk durumları birbirlerine yakındır.
- Tüm sektör ortalamalarına göre, “Alan Adı”, “Network Güvenliği” ve Uygulama güvenliği” gelişim fırsatının olduğu alanlardır.

FORCERTA

- E-Ticaret sektörünü incelemek için öncü 9 şirket incelenmiştir.
- Büyük ticari hacim olmasına karşın bu sektörde “Web Uygulama Güvenliği”, “Network Güvenliği” ve “Alan Adı” özelinde ciddi eksikleri olan firmalar bulunmaktadır.



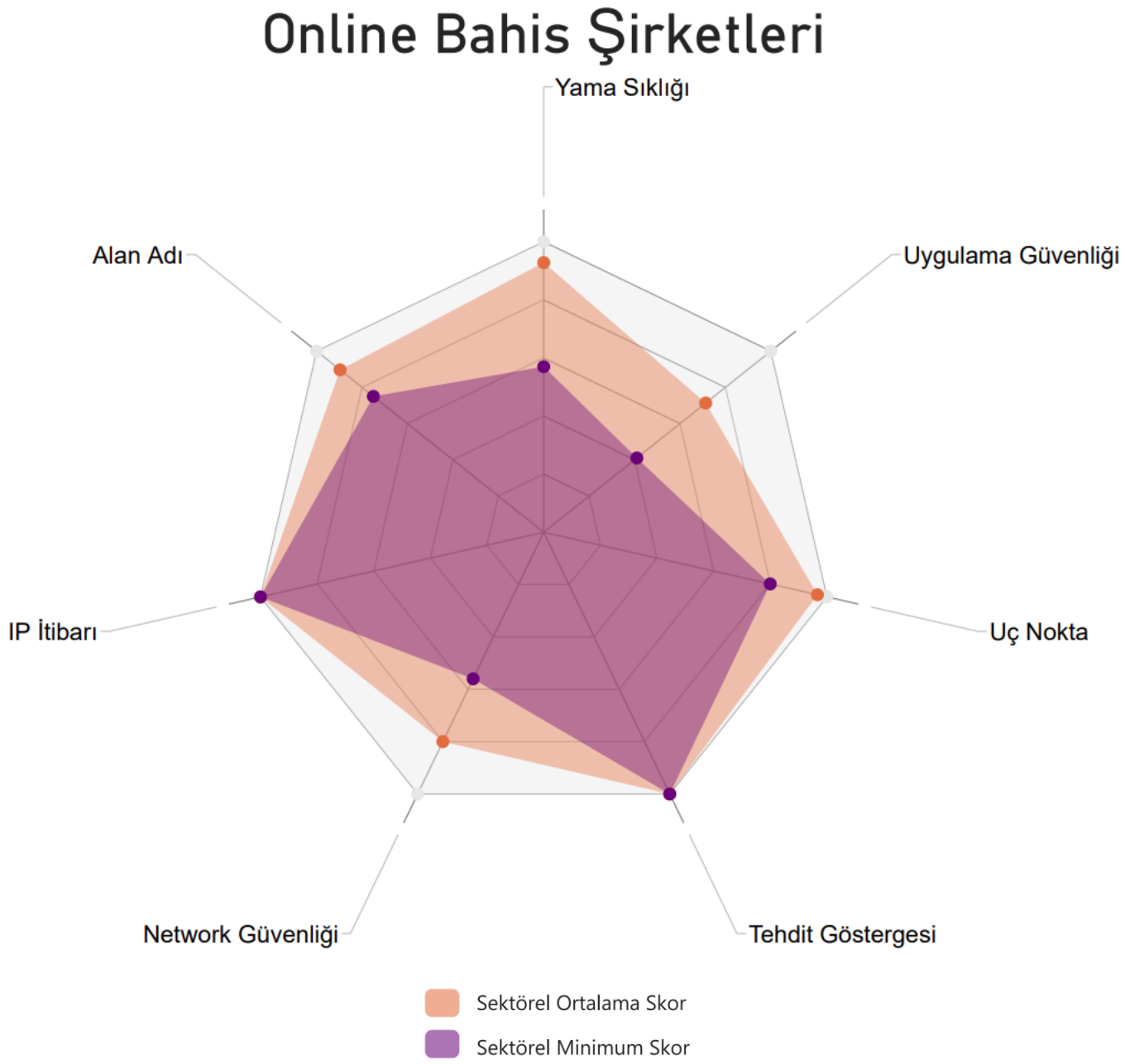
FORCERTA



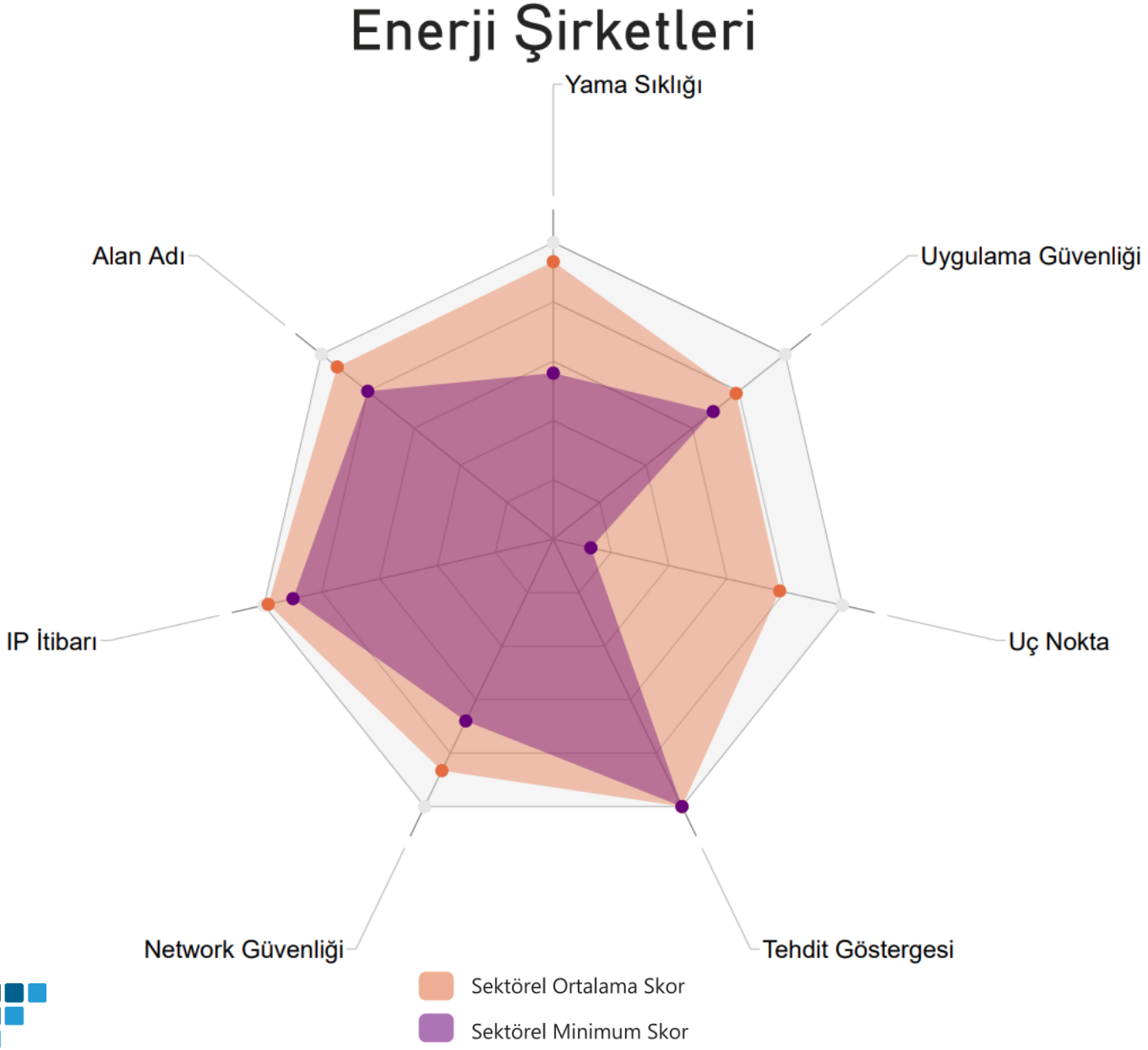
- Sektörü temsil eden 10 firmadan oluşan Sigorta Şirketi Analiz sonuçları, bankacılık sonrası diğer tüm sektörlerden daha iyi sonuçlar göstermiştir.
- Kişisel veriler ve özel nitelikli kişisel verilerin yoğun işlendiği bir sigorta şirketleri, bağlı bulundukları regülasyonlar sebebiyle siber güvenlik yatırımına önem veriyor gözükmektedir.
- Bu sektörde “Uygulama Güvenliği”, “Uç Nokta” ve “Network Güvenliği” gelişim alanları olarak gözükmektedir.

FORCERTA

- Yasal bahis sektörü analizini seçtiğimiz 6 farklı şirket üzerinden gerçekleştirdik.
- Faaliyet için özel lisans gerektiren “Online Bahis”, kullanıcılarının yoğun ve zaman kritik olarak ödeme işlemlerinin yaptığı bir sektör.
- Uygulama Güvenliği sektör ortalaması çok düşük.
- Potansiyel riskleri işaret eden, Uygulama Güvenliği, Network Güvenliği ve Yama Sıklığı alanlarında çok düşük puanlı şirketler var.



FORCERTA

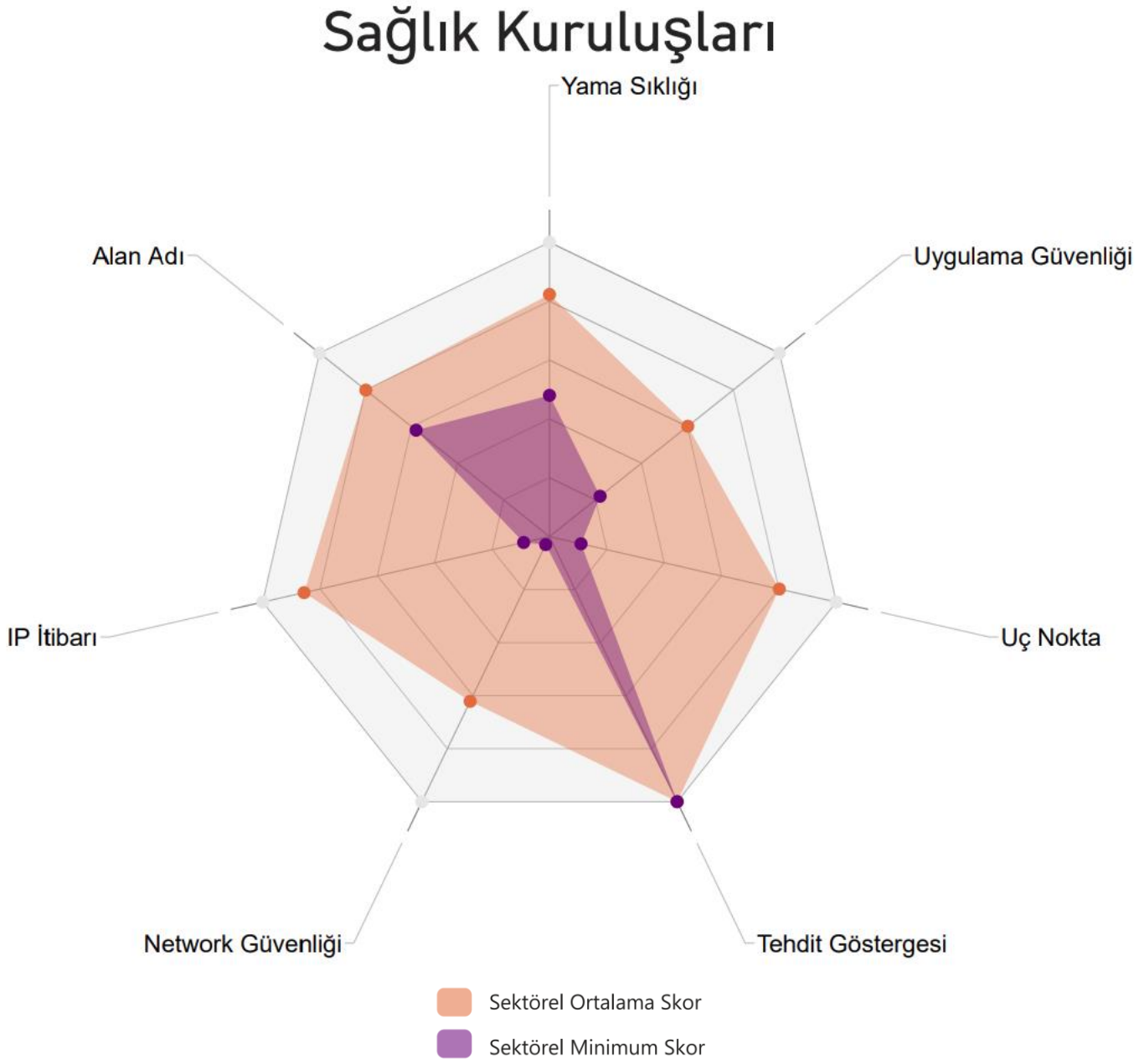


- Kritik altyapı olan Enerji sektörü incelemesini, sektörün öncü 7 kuruluşu üzerinden gerçekleştirdik.
- Günümüzde uluslararası rekabetlerde hedef haline gelen kritik altapılar siber güvenlik riskleri açısından önemli bir yere sahiptir.
- Ülkemizdeki riskler değerlendirildiğinde özellikle Uç Nokta ve Yama Sıklığı konularında ciddi riskleri olan enerji şirketlerinin olduğu görülmektedir.

FORCERTA

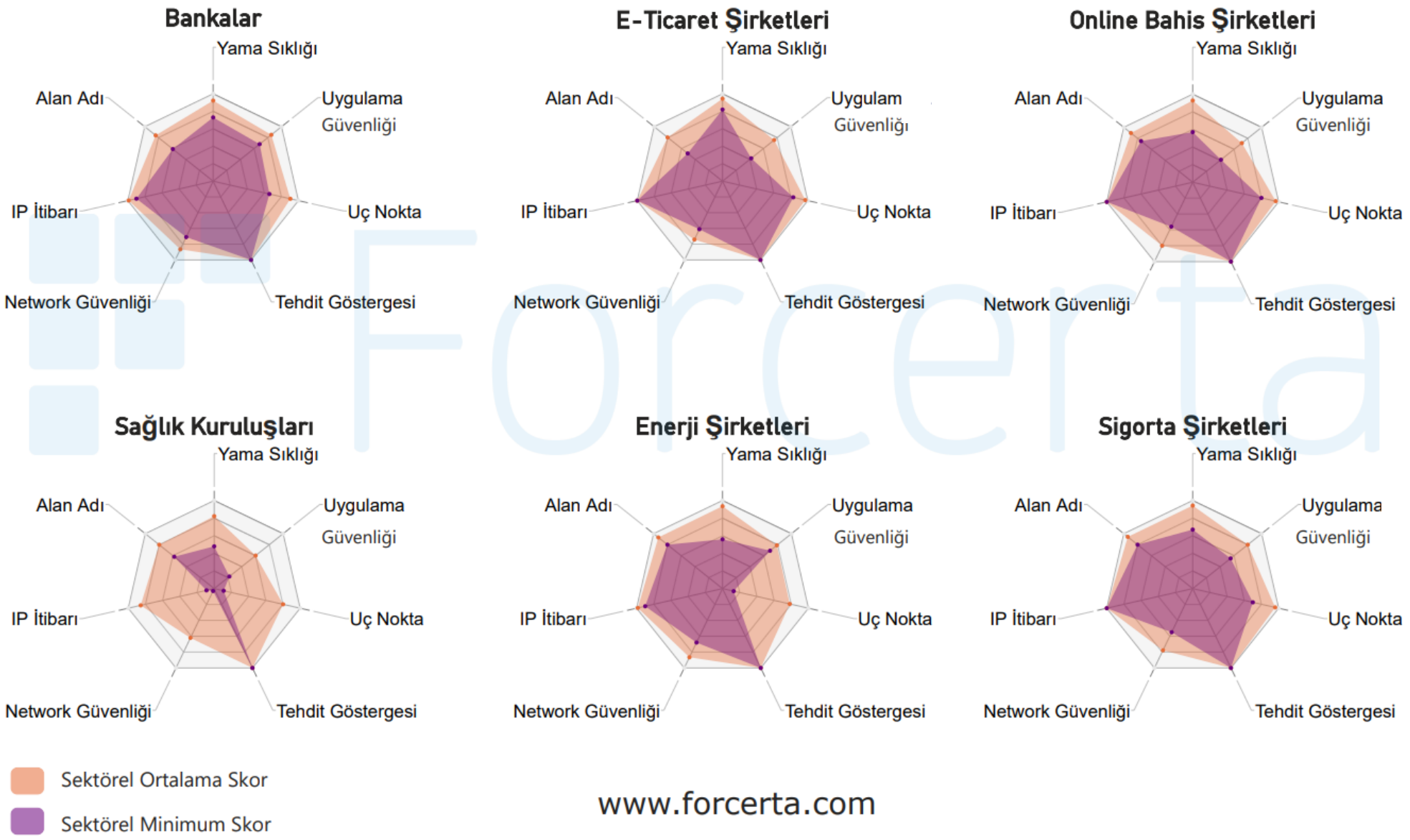
- Öncü 7 kuruluş üzerinden incelediğimiz Sağlık Sektörü, Siber Güvenlik Olgunluğu bakımından incelenen tüm sektörler içinde en geride olandır.

- Kişisel veriler ve özel nitelikli kişisel verilerin bulunduğu bu sektördeki bazı kuruluşların geçmiş dönemde büyük riskler barındırdıkları görülmektedir.



FORCERTA

Türkiye Sektörel Siber Güvenlik Risk Haritası



www.forcerta.com

FORCERTA

Özet

Yapılan araştırmada sadece internet üzerinden erişilebilen veriler toplanmış olmasına karşın önemli zafiyetlerin bulunduğu şirketlerin varlığı tespit edilmiştir.

Günümüzde siber güvenlik riskleri, kurumlara sadece itibar kaybı değil, ticari kayıp ve bilgi sızıntısı riskleri de getirmektedir.

Çalışmanın detaylarını öğrenmek, şirketiniz ve tedarikçilerinizin risklerini izleyip yönetmek isterseniz bize ulaşabilirsiniz

iletisim@forcerta.com

Forcerta

www.forcerta.com


Teşekkürler...
Forcerta
Advanced ICT Enabler & VAR