BARİKAT
Siber Güvenlik

barikat.com.tr
bilgi@barikat.com.tr
BARİKAT Siber Güvenlik

BARİKAT
Siber Güvenlik Operasyonları Merkezi

2023 Q4 Raporu

barikat.com.tr

BARİKAT
Siber Güvenlik

BARİKAT

Siber Güvenlik Operasyonları Rapor Özet

Bu rapor, ***BARİKAT Siber Güvenlik Operasyonları (SGOM)*** verileri baz alınarak SOC operasyonları metriklerinin detaylı bir ölçüm setiyle ve özellikle sektör kırılımlı olarak incelenmesi, müşteri-analist iletişiminin SOC operasyonlarındaki önemiyle ilgili kritik değerlendirmeler sunmaktadır.

Rapor standart metriklerine ek olarak; False/Positive (FP) trendleri, olay müdahaleye (OM) dönüşen olayların ölçümleri, olay kazıma bulguları, sektörel olay tipi dağılımları, sektör bazlı yanıt zaman dağılımları, veri sızıntısı (data exfiltration) özelinde dağılımlar gibi yeni metrikler eklenmiştir. Raporun sonunda tüm bu çıktıların belirli oranlarda yaptığı katkı bir Siber Güvenlik Operasyon Merkezi (SGOM) başarı puanı hesaplaması bulunmaktadır.

SOC operasyonlarının kalbi olan SOAR teknolojilerinin otomasyon ve orkestrasyon süreçlerine katkısı ile alarm inceleme ve aksiyon alma adımları hızlı bir şekilde icra edilmeye başlanmış olup BARİKAT SOAR Engineer takımı tarafından oluşturulan 3 katmanlı playbooklar sayesinde çoklu müşteri yapılarında hızlı ve verimli bir şekilde müşteriye özel çözümler sunulmaya başlanmıştır. Dinamik bir şekilde gelişen ve yıllar içinde olgunlaşan BARİKAT Tehdit Tespit Kural Seti (TDRF) Kütüphanesi kurallarıyla birlikte doğrulanmış, IOC'lerin dağıtımını otomatik yapan ve içeriği BARİKAT L2 mühendisleri tarafından doğrulanmış MISP servisi ile en güncel saldırı emareleri otomatik olarak alarma dönüşmektedir. EDR, NDR ve XDR teknolojilerinin SOAR üzerinden entegre edilmesi ve uçtan uca alan hakimiyetine olanak sağlaması otomatik aksiyon hızını ve doğruluğunu olgunlaştırmıştır. Analist ve müşterilerin hızlı etkileşimi üzerinden sağlanan düşük MTTR süreleri ve bu metriklerin sektörel bazda dağılımı rapor içeriğinde sunulmaktadır. Raporun sonunda tüm raporun anahtar çıktılarını içeren bir özete ulaşabilirsiniz.

41K

AYLIK ORTALAMA OLAY (INCIDENT) SAYISI

12 DK

MTTD - TESPİT SÜRESİ*

Severity bağımsız ölçülmüştür.

35 DK

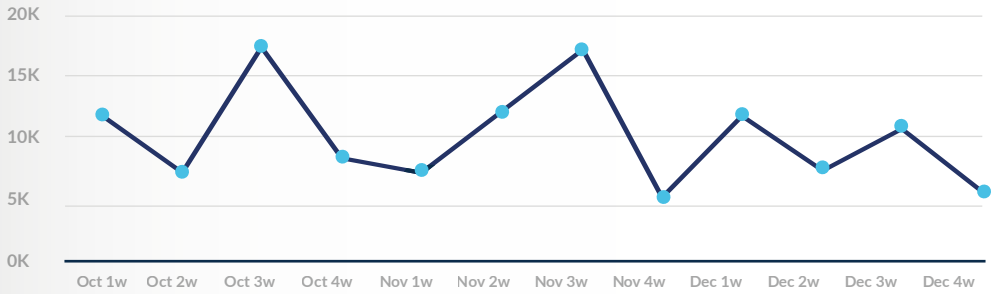
MTTR - ÇÖZÜM SÜRESİ*

Severity bağımsız ölçülmüştür.

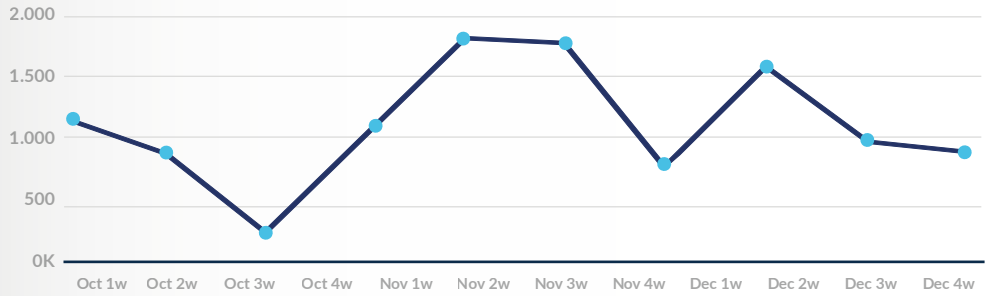
Alarm DAĞILIMI

68

ANALİST BAŞINA DÜŞEN GÜNLÜK ORTALAMA ALARM SAYISI



FP DAĞILIMI

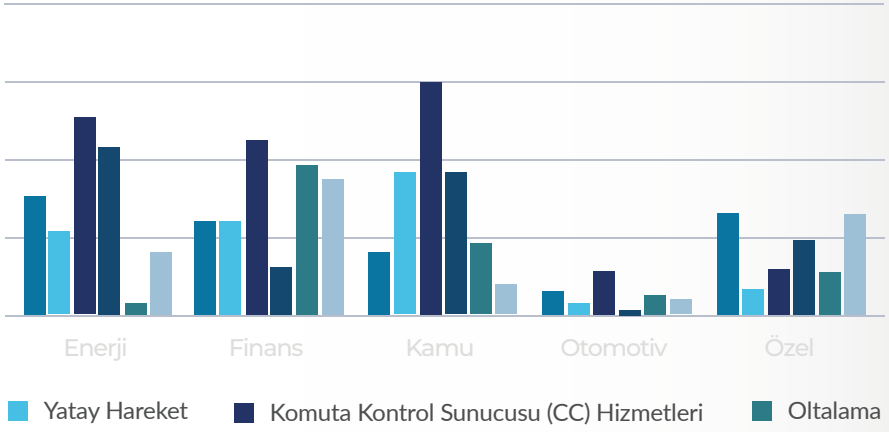


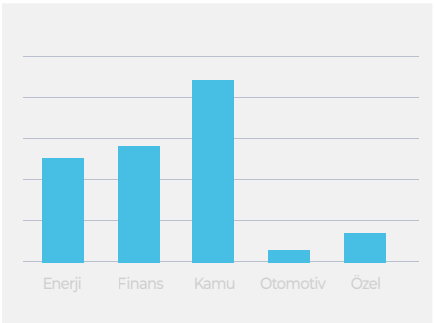
Oluşan FP alarmların dağılımında BARİKAT TDRF Kütüphanesi kullanılarak yazılan alarmlar **%7** etki ederken, TDRF harici yazılan alarmlar **%93** oranında FP etkisi sağlamıştır.

Yeni devreye alınan müşteriler ve TDRF harici yazılan kurallar nedeniyle Kasım'ın 2. haftasında FP değerlerinin yükseldiği görülmüştür.

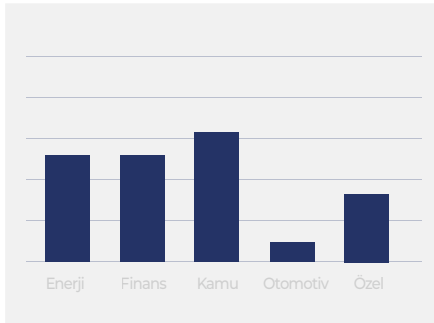
Sektör Bazında
Alarm Dağılımı

Sektörlere göre dağılan olay (incident) tiplerinde ***Komuta Kontrol Sunucusu (CC) Erişimleri, Oltalama (Phishing) ve Yatay Hareket (Lateral Movement)*** ilk 3 sırada yer almaktadır. DPA (Digital Process Automation) çalışmaları sayesinde MTTR değerleri otomasyona bağlı alarmlarda 4DK olarak ölçülmüştür. L3 katmanında tespit edilen alarmlar blacklist yöntemiyle engellenmiştir.





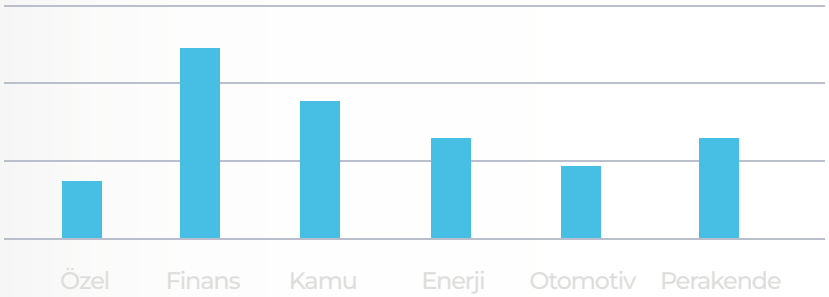
Sektörlere göre dağıtılan olay sayıları ***Kamu > Finans > Enerji ve Diğer özel sektörler*** olarak sıralanmaktadır.



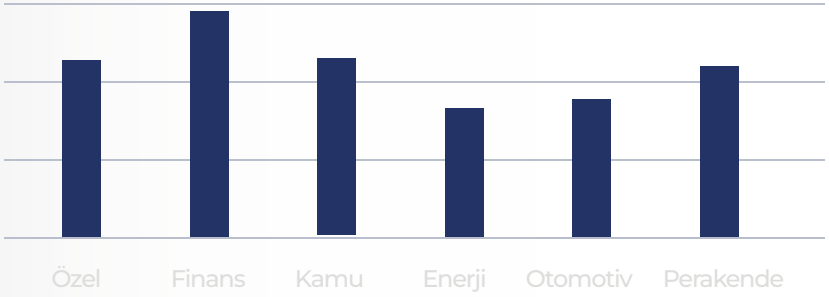
Sektörlere göre dağıtılan olay sayılarında ***Kamu, Finans, Enerji sektörleri*** birbirine çok yakın bir dağılıma sahiptir.

Sektör Bazında
SLA Dağılımı

Sektör bazında MTTD değerleri ***Finans-Kamu-Enerji*** olarak sunulmaktadır. Tespit süreleri açısından büyük farklar bulunmamaktadır.



Sektör bazında MTTR değerleri birbirine çok yakın dağılım göstermektedir.



MTTD - ORTALAMA TESPİT SÜRESİ

12 DK

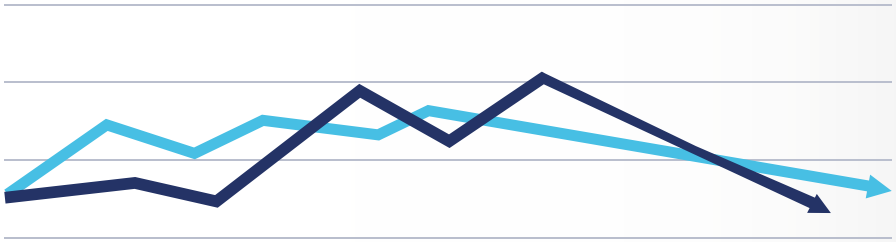
(*) Severity bağımsız ölçülmüştür.

MTTR - ORTALAMA ÇÖZÜM SÜRESİ

35 DK

(*) Severity bağımsız ölçülmüştür.

SLA Sürecinde
Müşteri Etkisi



AWAITING CUSTOMER MTTD

+33 DK

*Müşteri **Onayı Alınan Olayların,** Ortalama **Awaiting Customer** Süreleri*

Ortalama bekleme süresi üzerinde kalan olaylar ***müşteri tarafından onayı geciken veya otomasyona bağlı olmayan alarmlar*** olarak ölçülmüştür. Alarm bildirimlerinde izleme ekibiyle entegre olan müşterilerin daha kısa zamanda olay çözülmesine katkı sağladıkları, MTTR ölçümlerinde doğrudan azaltıcı yönde etki ettikleri görülmüştür.

OM Sonrası Bulgulara göre 1 yıllık süre için geçmişe yönelik olay sorgusu yapılarak tespit edilen farklı bir ize rastlanmamıştır.

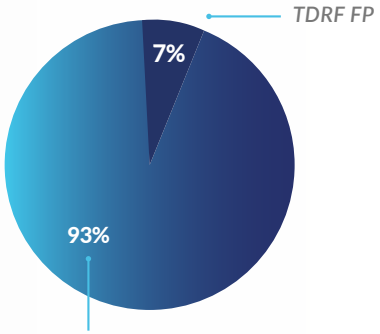
Son 3 Ay içinde yapılan OM çalışmalarından ***6 adeti*** şirketimizden hizmet almayan organizasyonlardan oluşmaktadır.

NDR - XDR Servisleri üzerinden gelen ***3 adet*** tespit, OM sürecini tetiklemiştir.

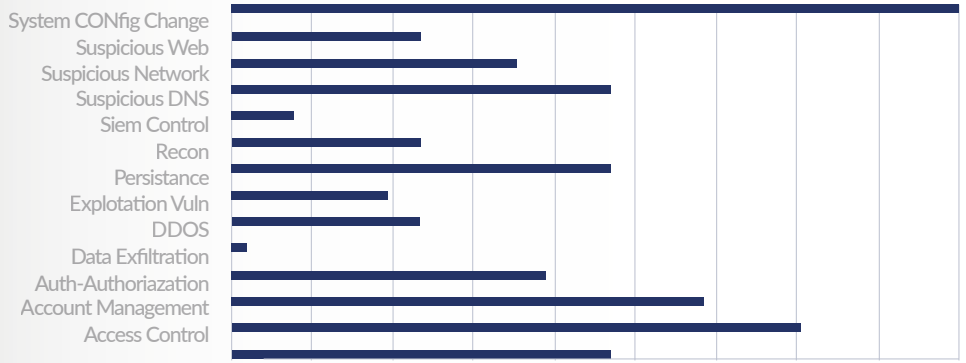
OM İstatistikleri ve
TDRF FP Etkisi

BARİKAT danışmanları tarafından ***BARİKAT (TDRF)*** kütüphanesi içerisinde bulunan ve harici kuralların (FP) alarm sayılarına etkileri aşağıda yer alan grafikler üzerinden gözlemlenebilir.

Üretilen FP Alarmların TDRF/Harici Kural Oranı



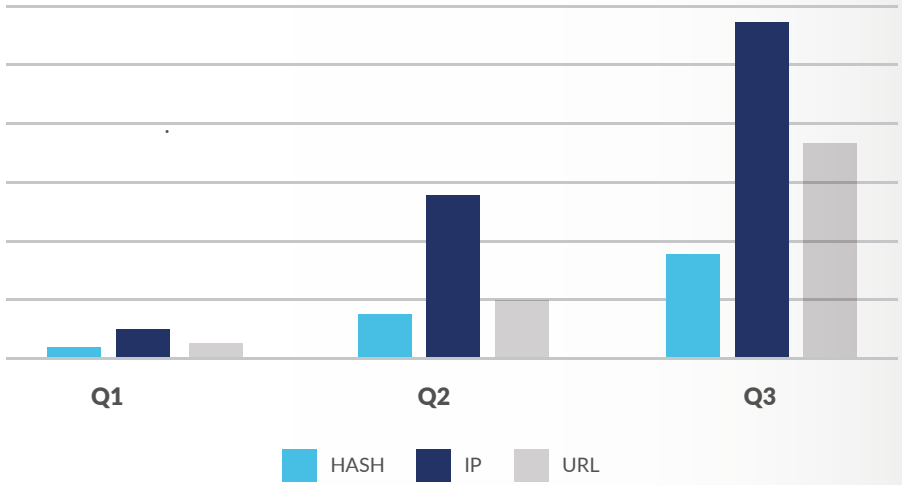
TDRF Kütüphanesi Kural Dağılımları



BARİKAT İstihbarat Paylaşım Platformu
Dağıtılan IOC Tespitleri

BARİKAT SGOM L2 Mühendisleri tarafından doğrulanarak hazırlanan ve tespit aşamasında FP oranı düşük olan MISP IOC girdi dağılım trendi aşağıda yer alan grafik üzerinden gözlemlenebilir.

BARİKAT MISP SERVER IOC SAYILARI



445/500

Aylık olay sayıları, FP değişim oranları, OM ile sonuçlanan alarmlar, MISP üzerinden gelen yüksek önem (severity) değerine sahip olaylar, otomasyon/analist performansı gibi konuların ağırlıklı olarak katkıda bulunduğu 3 aylık "SGOM BAŞARIM ORANI 445/500" olarak hesaplanmıştır.

350/5000

41K toplam alarm içerisinde 5K alarm, Siber Tehdit İstihbarat Paylaşım Platformu (MISP) kuralları üzerinden tespit edilmiştir. Bu alarmların 350 tanesi FP olarak ölçülmüştür. Çoğunluk olarak şüpheli IP ve URL erişimi kuralları hit almıştır.

5000/41000

BARİKAT SGOM L2 Mühendisleri tarafından hazırlanan/doğrulanmış en güncel bilgileri içeren ve müşteri SIEM ürünlerine otomatik olarak gönderilen (push) IOC bilgisi üzerinden yapılan tespitlerin sayısıdır.

Rapor
Sonuçları

1 syf. SOC metriklerinin detaylı bir ölçüm setiyle ve özellikle sektör kırılımlı olarak incelenmesi müşteri-analist iletişiminin SOC operasyonlarındaki önemiyle ilgili kritik değerlendirmeler sunmaktadır.

2 syf. Analist iş yükünü azaltmak ve inceleme kalitesini düşürmemek için TDRF gibi bir disipline bağlı tespit kuralı yazımı SOC başarım yolculuğundaki ilk parça olmaktadır.

3 syf. Komuta kontrol erişimleri, oltalama ve yatay yayılım olaylarının otomasyonla çözülmesi tüm sektörlerde ortalama çözüm sürelerini dramatik şekilde düşürmektedir. Ülkemizde alarm tipi ve FP sayıları sektörler arasında dengeli bir dağılıma sahiptir. Kullanıcı farkındalığı ve tespit adımından başlayan SOC süreçlerinin tek elden ve dünya standartlarında kurgulanması bu homojen dağılımda rol oynamaktadır.

4 syf. Olayların kritiklik derecesi göz önününe alınmadan tüm alarm tipleri için hesaplanan ortalama tespit süresi ve ortalama çözüm süresi ve bu dağılımların analist seviseyine göre değişmemesi SOC süreçlerinde SOAR kullanımının önemini göstermektedir.

5 syf. Analist-Müşteri iletişiminde bir olayın müşteride beklediği zamanı tanımlayan Awaiting Customer değeri ne kadar düşük olursa MTTR değerleri de o kadar düşük olmaktadır , zaman kritik operasyonlarda işbirliği her şeydir.

6 syf. Bir kurala bağlı kalmadan günlük olarak on-demand yazılan tespit kurallarının FP oluşturma oranının aylara göre dağılımı ve analist başına düşen ortalama olay sayısı göstermektedir ki; analist iş yükü ve inceleme kalitesini düşürmemek için tespit kuralı yazımı SOC başarım yolculuğundaki ilk parça olmaktadır.

6 syf. Log oluşumu-tespit-analiz-eskalasyon ve olay müdahale ile sonuçlanan ihlal olaylarında NDR, XDR gibi AI bazlı yeni güvenlik yaklaşımlarının kullanımı FP oranını azaltarak, ciddi durumlarda insan etkileşimine ihtiyaç duymadan yüksek kritik seviyede Red Flag kaldırabilmektedir. BARİKAT SGOM olarak müşterilerimize verdiğimiz geleneksel SIEM tespit hizmetlerinin yanında NG olarak tanımlanan teknolojilerle etkin ve hızlı sonuçlar almaktayız.

7 syf. BARİKAT tarafından yönetilen MISP çözümü L2 Mühendislerinin On-Demand olarak zaman içerisinde kanıtladıkları IOC'ler üzerinden çalışır ve mevcut TI tespit kurallarına ek olarak yüksek kritiklik seviyesinde alarm üretir.

7 syf. Tehdit istihbaratı çözümlerindeki IOC gürültüsünü engellemek için BARİKAT SGOM L2 Mühendisleri tarafından kanıtlanılmış ve güncel IOC bilgilerini içeren listeler BARİKAT MISP Server üzerinden otomasyonla müşteri SIEM tespit sistemlerine senkron edilir ve güncel tehditlerin tespit mekanizmalarında tanımlanması hızlı ve doğru bir şekilde gerçekleştirilir.

BARİKAT SGOM ekibi tarafından şeffaf bir şekilde paylaşılan bu rapor, Türkiye'deki SOC operasyonlarını daha verimli bir hale getirmeyi ve sektörde ortak bir ölçüm dili geliştirmeyi amaçlamaktadır.

Gelecek raporlarda ölçülmesi istenilen değerleri iletişim bilgilerimiz üzerinden paylaşarak gelecek raporlara katkı sağlayabilirsiniz.

barikat.com.tr
bilgi@barikat.com.tr
BARİKAT Siber Güvenlik

Kısaltmalar

AI	**Artificial Intelligence** (Yapay Zeka)
CC	**Command Control** (Komuta Kontrol Sunucu Erişimleri)
DPA	**Digital Process Automatiozn** (Dijital Süreç Otomasyonu)
IOC	**Indicator Of Compormise** (İstila Emaresi)
MISP	**Malware Information Sharing Platform** Tehdit İstihbaratı Paylaşım Platformu)
MTTD	**Mean Time to Detect** (Ortalama Tespit Süresi)
MTTR	**Mean Time to Resolve** (Ortalama Çözüm Süresi)
FP	**False/Positive** (Yanlış /Pozitif)
OM	**Incident Response** (Olay Müdahale)
TDRF	**Threat Detection Response Framework** (Tehdit Tespit Müdahele Kural Seti)
TI	**Threat Intelligence** (Tehdit İstihbaratı)
NDR	**Network Detection Response** (Ağ Algılama ve Yanıt Sistemleri)
SOC	**Security Operations Center** (Güvenlik Operasyonları Merkezi)
NG	**Next Generation** (Gelecek Nesil)