BARİKAT
Siber Güvenlik

BARİKAT SİBER GÜVENLİK
OPERASYONLARI MERKEZİ

2024
Q2 Raporu

bilgi@barikat.com.tr

BARİKAT Siber Güvenlik Operasyonları Q2 Rapor Özeti

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), yayınlanmış güncel zafiyetler özelinde dağılımlar gibi yeni metrikler eklenmiştir. Tüm bu çıktıların katkı oranları hesaplanarak, ***Siber Güvenlik Operasyon Merkezi (SGOM) başarı puanı*** oluşturulmuştur. Başarı Puanlarına raporun sonunda yer verilmiştir.

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 Mühendisleri 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 ve Müdahale 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.

32 K

Aylık Ortalama *(Incident)* **Sayısı**

14 DK

MTTD - Tespit Süresi (*)

Severity bağımsız ölçülmüştür.

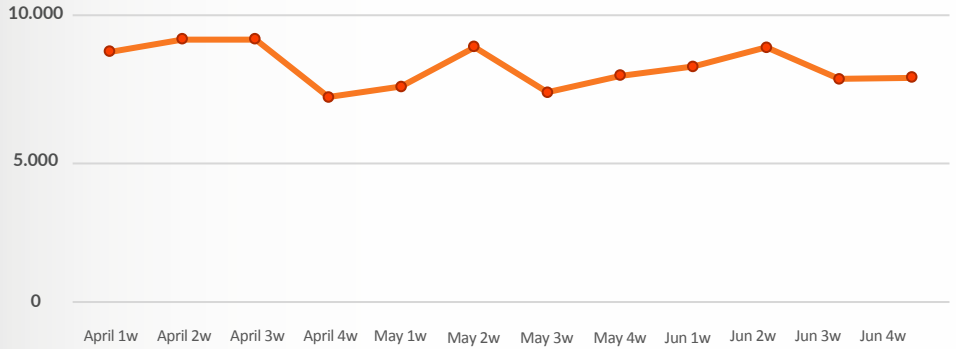
36 DK

MTTR - Çözüm Süresi (*)

Severity bağımsız ölçülmüştür.

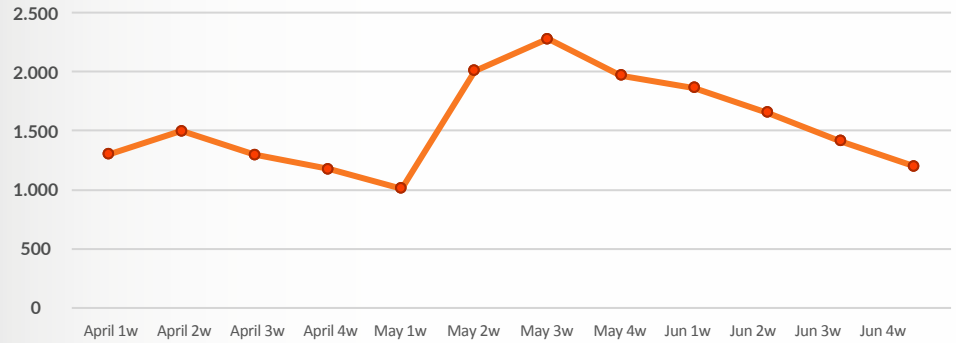
Alarm Dağılımı

ANALİST BAŞINA DÜŞEN GÜNLÜK ORTALAMA ALARM SAYISI **82**



3 aylık dilimde haftalık olarak oluşan **Analist Başına Düşen Olay Sayısı** grafikte gösterildiği gibidir. Her vardiyada birden fazla analistin görevlendirildiği ve günlük bazda analist başına düşen alarm sayısının kontrolü bu grafikle gerçekleşmektedir.

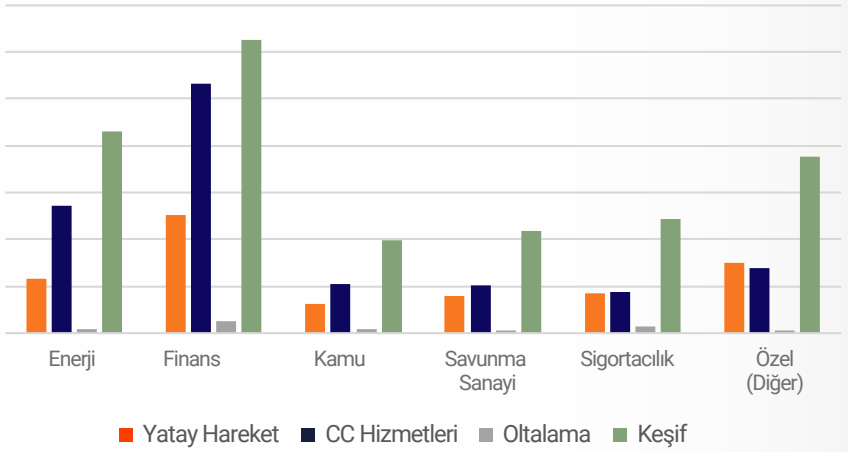
FP Dağılımı

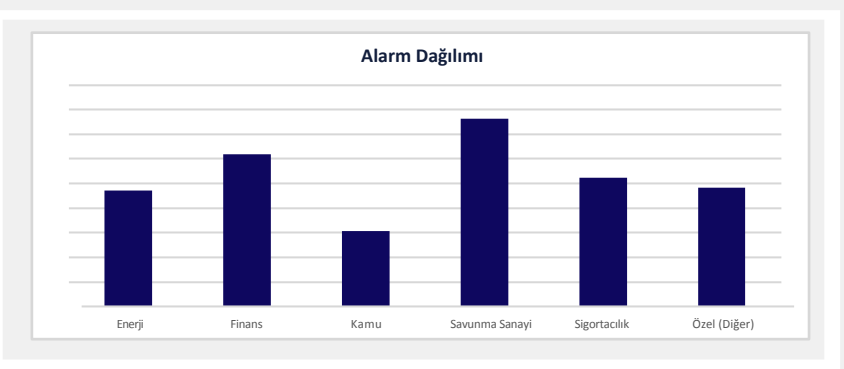


Oluşan FP alarmların dağılımında BARİKAT TDRF Kütüphanesi kullanılarak yazılan alarmlar **%11** etki ederken, TDRF harici yazılan alarmlar **%89** oranında FP etkisi sağlamıştır. Yeni devreye alınan müşteriler ve TDRF harici yazılan kurallar nedeniyle ve yeni gelen müşterilerde yazılan kuralların çok sayıda False Positive üretmesi nedeniyle Mayıs'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 3 DK olarak ölçülmüştür.

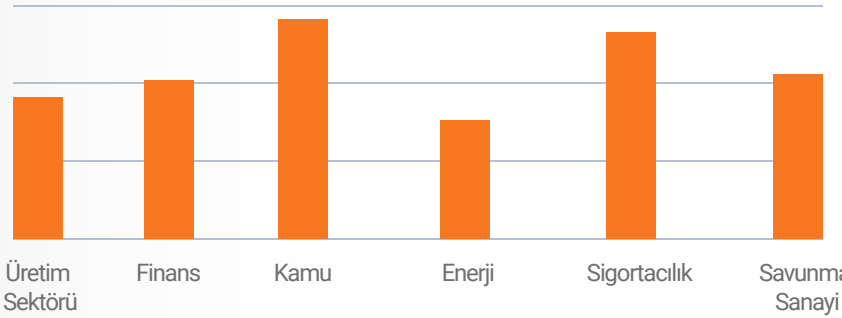




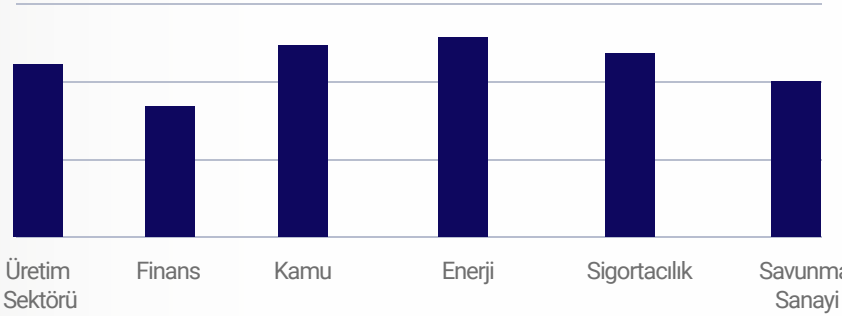
Sektörlere göre dağıtılan olay sayıları ***Savunma > Finans > Sigortacılık > Özel > Enerji > Kamu*** olarak sıralanmaktadır.

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

11 DK

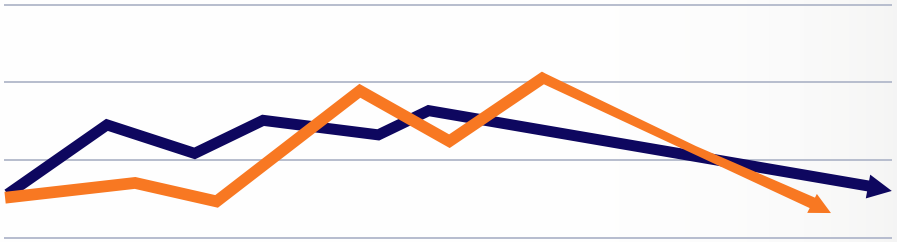
(*) Severity bağımsız ölçülmüştür.

MTTR - ORTALAMA ÇÖZÜM SÜRESİ

32 DK

(*) Severity bağımsız ölçülmüştür.

SLA Sürecinde
Müşteri Etkisi



AWAITING CUSTOMER MTTD

+36 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.

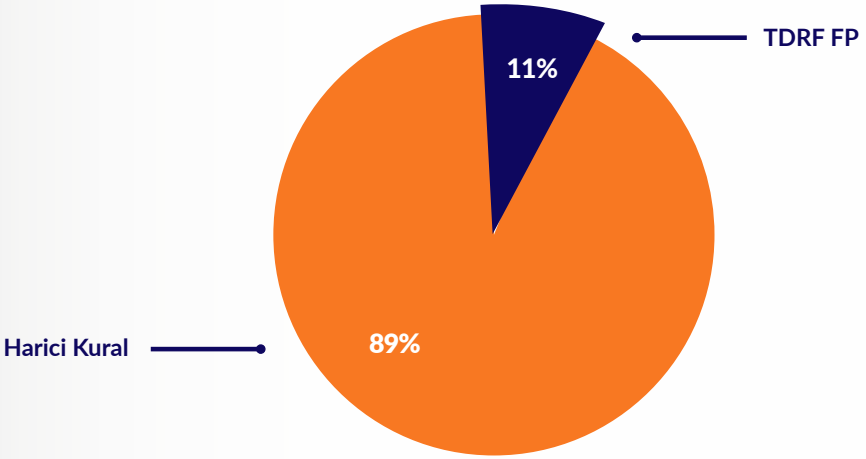
Son 3 Ayda OM çalışmalarından ***4 Adeti*** şirketimizden hizmet almayan organizasyonlardır.

NDR - XDR servisleri üzerinden gelen ***1 Adet*** tespit, OM sürecini tetiklemiştir. Bunun yanı sıra L1 tarafından yapılan incelemenin ardından L2 incelemesinin de akabinde OM süreci tetiklenen ***1 Olay*** bulunmaktadır.

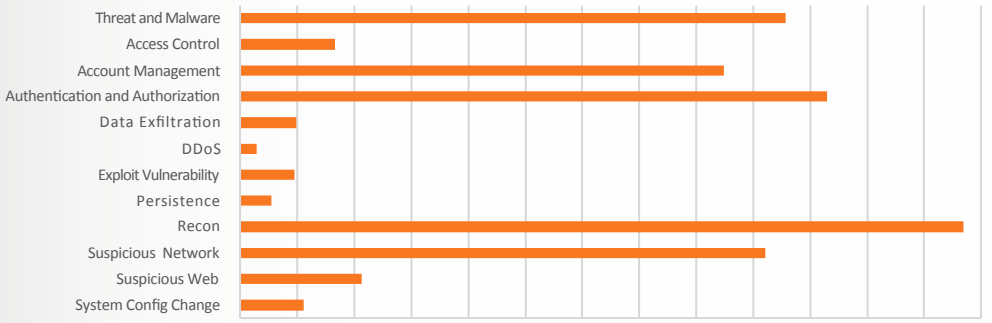
OM İstatistikleri ve
TDRF FP Etkisi

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

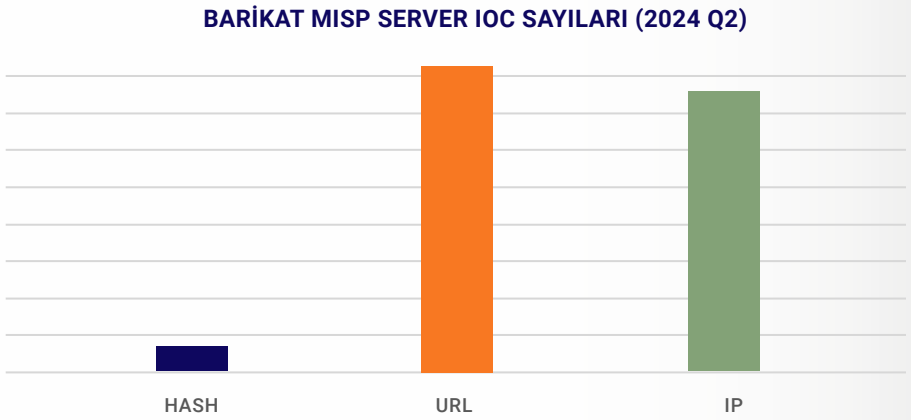
ÜRETİLEN FP ALARMLARIN TDRF/HARICI KURAL ORANI



TDRF KÜTÜPHANESI KURAL DAĞILIMLARI



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.

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 455/500" olarak hesaplanmıştır.

32K toplam alarm içerisinde 7K alarm, Siber Tehdit İstihbarat Paylaşım Platformu (MISP) kuralları üzerinden tespit edilmiştir. Bu alarmların 450 tanesi FP olarak ölçülmüştür. Çoğunluk olarak şüpheli IP ve URL erişimi kuralları hit almıştır.

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.

1) Linux Dağıtımlarında XZ Utils'deki CVE-2024-3094 Güvenlik Açığının Giderilmesi Oluşturuldu.

Çeşitli Linux dağıtımlarında yaygın olarak kullanılan XZ Utils sıkıştırma araçlarında CVE-2024-3094 olarak adlandırılan kritik bir güvenlik açığı tespit edilmiştir. Bu güvenlik açığı, xz kütüphanelerinin 5.6.0 ve 5.6.1 sürümlerine gömülü olan ve sshd kimlik doğrulama mekanizmalarını atlayarak yetkisiz uzaktan erişime izin veren kötü amaçlı koddan kaynaklanmaktadır. Bu güvenlik açığı, diğer dağıtımların yanı sıra özellikle **Fedora 41 ve Fedora Rawhide'ı etkilemektedir. Debian, openSUSE ve Kali Linux da potansiyel maruziyeti kabul etmiş ve hafifletmeye yönelik adımlar başlatmıştır.**

CVE-2024-3094'ün keşfi, açık kaynaklı yazılım tedarik zincirinde devam eden zorlukların altını çizmekte ve dikkatli güvenlik uygulamalarının önemini vurgulamaktadır. **Kuruluşların ve bireysel kullanıcıların sistemlerini etkilenen sürümler açısından gözden geçirmeleri ve ortamlarını bu önemli güvenlik tehdidine karşı korumak için derhal düzeltici önlemler almaları gerekmektedir.**

Etkilenen Sistemler:

XZ Utils 5.6.0 ve 5.6.1 sürümleri etkilenmiştir.

Çözüm Önerileri:

Etkilenen dağıtımların kullanıcılarına, tehlikeye atılmış sürümlerin kullanımını derhal durdurmaları tavsiye edilir. Olası güvenlik ihlallerini önlemek için XZ Utils'in 5.4.6 sürümü gibi bu güvenlik açığından etkilenmeyen bir sürümüne geçilmesi önerilir.

Tedbirler:

Güvenlik Ekibi Eylemleri: Güvenlik ekipleri, her Linux dağıtımı için sağlanan özel kılavuzlara uymalıdır. CISA'nın XZ Utils'in tehlikesiz bir sürümüne (ör. 5.4.6 sürümü) düşürülmesi ve etkilenen sürümlerin yüklü olduğu sistemlerde herhangi bir kötü niyetli veya şüpheli faaliyetin araştırılması tavsiyesine uyulması çok önemlidir.

2) Linux Dağıtımlarında XZ Utils'deki CVE-2024-3094 Güvenlik Açığının Giderilmesi Oluşturuldu.

Palo Alto Networks, güvenlik duvarı yazılımı PAN-OS'u etkileyen ciddi bir sıfır gün güvenlik açığını (CVE-2024-3400) açıkladı. Bu güvenlik açığı, kritik önemini gösteren **10.0 CVSS puanı** taşımaktadır.

Başarılı sömürü, kimlik doğrulanmamış saldırganların etkilenen güvenlik duvarlarında kök ayrıcalıklarıyla rastgele kod yürütmesine izin verebilir.

Şirket yayınladığı bir duyuruda **"Palo Alto Networks PAN-OS yazılımının GlobalProtect özelliğinde belirli PAN-OS sürümleri ve farklı özellik yapılandırmaları için bir komut enjeksiyonu güvenlik açığı, kimliği doğrulanmamış bir saldırganın güvenlik duvarında kök ayrıcalıklarıyla rastgele kod çalıştırmasına olanak tanıyabilir"** dedi.

Etkilenen Sürümler	Fixlenen Sürümler
✓ PAN-OS 10.2	✓ PAN-OS 10.2.9-h1
✓ PAN-OS 11.0	✓ PAN-OS 11.0.4-h1
✓ PAN-OS 11.1	✓ PAN-OS 11.1.2-h3

Çözüm Önerileri:

GlobalProtect arayüzünüze güvenlik açığı koruması uyguladığınızdan emin olun.

Cihaz Telemetrisini Devre Dışı Bırakın (Tehdit Önleme'yi uygulayamıyorsanız): Web arayüzü aracılığıyla cihaz telemetrisini geçici olarak **devre dışı bırakın** ve **güvenlik duvarınız güncellendikten sonra yeniden etkinleştirin.**

PuTTY SSH İstemcisi Anahtar Kurtarma Saldırısına Karşı Savunmasız Bulundu.

Yaygın olarak kullanılan bir SSH istemcisi olan PuTTY'nin, NIST P-521 özel anahtarlarının kurtarılmasına yol açabilecek kritik bir kusura karşı savunmasız olduğu tespit edildi.

Bochum Ruhr Üniversitesi'nden araştırmacılar tarafından keşfedilen açık, **saldırganların taraflı ECDSA şifreleme nonce'larından yararlanarak özel anahtarı ele geçirmelerine** olanak tanıyor. Saldırganlar sadece birkaç imzalı mesaj ve genel anahtarla **imzaları taklit edebilir** ve ele geçirilen anahtarla doğrulanan **sunuculara yetkisiz erişim** sağlayabilirler.

Etkilenen Sistemler:

CVE-2024-31497 olarak atanan bu güvenlik açığı, PuTTY'nin 0.68 ila 0.80 sürümlerinin yanı sıra FileZilla, WinSCP, TortoiseGit ve TortoiseSVN gibi diğer bazı yazılım ürünlerini de etkilemektedir.

Sorumluluğun ifşa edilmesi, PuTTY 0.81 ve FileZilla 3.67.0 gibi etkilenen yazılım sürümleri için yamaların yayınlanmasına yol açmıştır.

Tedbirler:

Kullanıcıların bu güvenlik açığından yararlanan olası saldırılara karşı korunmak için yazılımlarını en son yamalı sürümlere güncellemeleri çok önemlidir.

Ayrıca, hassas sistemlere yetkisiz erişimi önlemek için SSH yapılandırmalarından tehlikeye atılmış anahtarların iptal edilmesi ve kaldırılması gereklidir.

Rapor
Sonuçları

1.Sayfa Değerlendirme

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

2.Sayfa Değerlendirme

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

3.Sayfa Değerlendirme

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.Sayfa Değerlendirme

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.Sayfa Değerlendirme

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.Sayfa Değerlendirme

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.Sayfa Değerlendirme

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.Sayfa Değerlendirme

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.Sayfa Değerlendirme

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.

Rapor'da Yer Alan
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)

BARİKAT
Siber Güvenlik

BARİKAT Siber Güvenlik
Operasyoları Merkezi

İletişim

barikat.com.tr

barikat.com.tr

BARİKAT Siber Güvenlik