Awiron

AWIRON TANITIM KATALOĞU

Her şeyi görün.

Anında anlayın.

Akıllıca hareket edin.

Next-Gen AI Powered Cyber Security Platform

awiron.org

Problem & Vizyon

Günümüz siber tehditleri; uç noktalar, ağlar, kullanıcılar, uygulamalar ve bulut sistemleri boyunca hızla çeşitleniyor. Buna karşın birçok kurum, birbirinden kopuk güvenlik araçları, yoğun alarm trafiği ve manuel müdahale süreçleri nedeniyle tehditleri bütüncül olarak görmekte ve zamanında aksiyon almakta zorlanıyor.

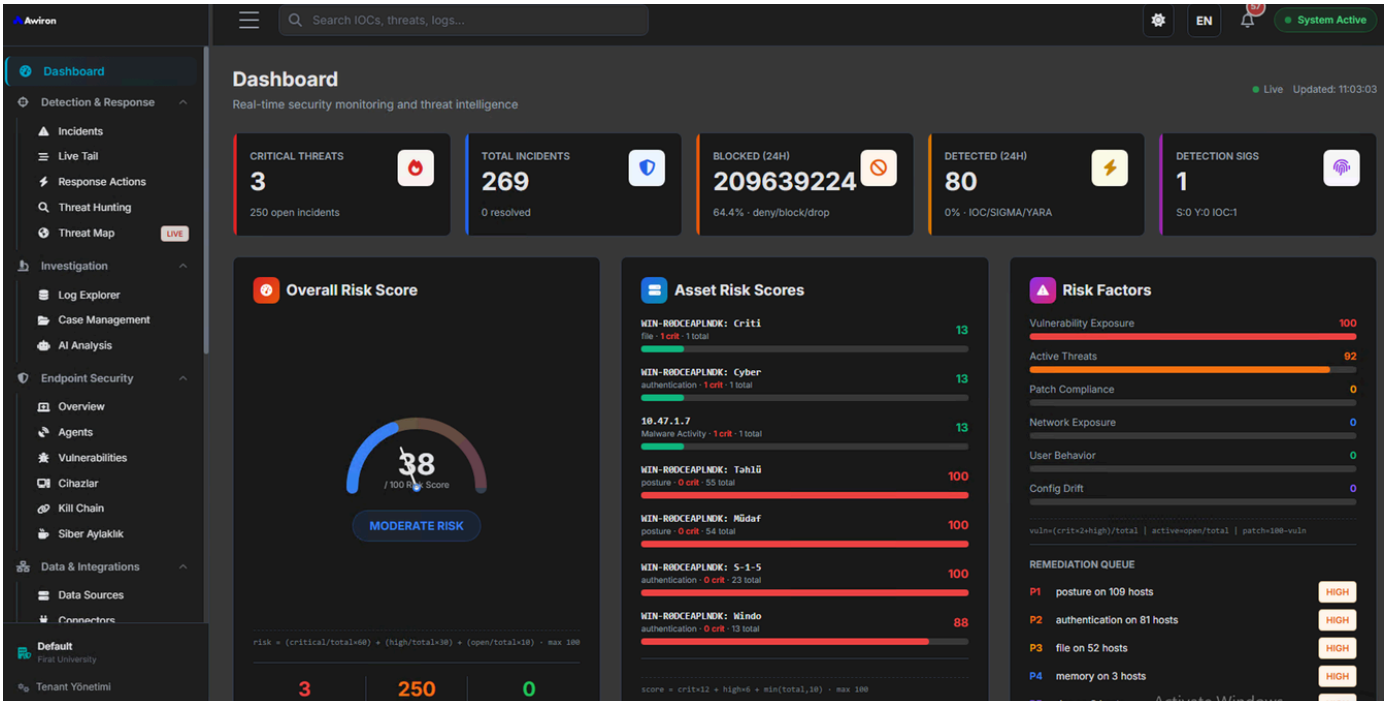
AWIRON Platform Mimarisi

AWIRON Platform Mimarisi, güvenlik verilerini farklı kaynaklardan toplayarak tek bir platform üzerinde birleştiren bütünleşik bir yapı sunar. SIEM, ajan tabanlı veri toplama, tehdit istihbaratı, risk skorlama ve yapay zekâ destekli analiz katmanları birlikte çalışarak tehditlerin daha hızlı, daha doğru ve daha bağlamsal şekilde değerlendirilmesini sağlar.

MITRE ATT&CK ile zenginleştirilen bu yapı sayesinde AWIRON; görünürlük, analiz, ilişkilendirme ve aksiyon süreçlerini tek merkezden yöneten modern bir güvenlik zekâ platformu sunar.

Tüm Güvenlik Operasyonlarınızı Tek Ekrandan Yönetin

Awiron, güvenlik operasyonlarını tek bir merkezde birleştirerek kurumların tehdit görünürlüğünü artırır ve karar alma süreçlerini hızlandırır. Gerçek zamanlı izleme, dinamik risk skorlama, olay yönetimi ve varlık bazlı analiz yetenekleri sayesinde güvenlik ekipleri tüm güvenlik ekosistemini tek panel üzerinden takip edebilir, önceliklendirebilir ve proaktif şekilde yönetebilir.



TEK PANEL. TAM KONTROL.

Awiron, tüm güvenlik süreçlerini tek noktada birleştirir.
Gerçek zamanlı **tehdit izleme**, **risk analizi** ve **olay yönetimi** tek panel üzerinden yönetilir.

Gerçek Zamanlı İzleme

Tüm sistemler ve tehditler anlık olarak izlenir.

Risk Skorlama

Organizasyonun güvenlik seviyesi dinamik olarak hesaplanır.

Varlık Bazlı Analiz

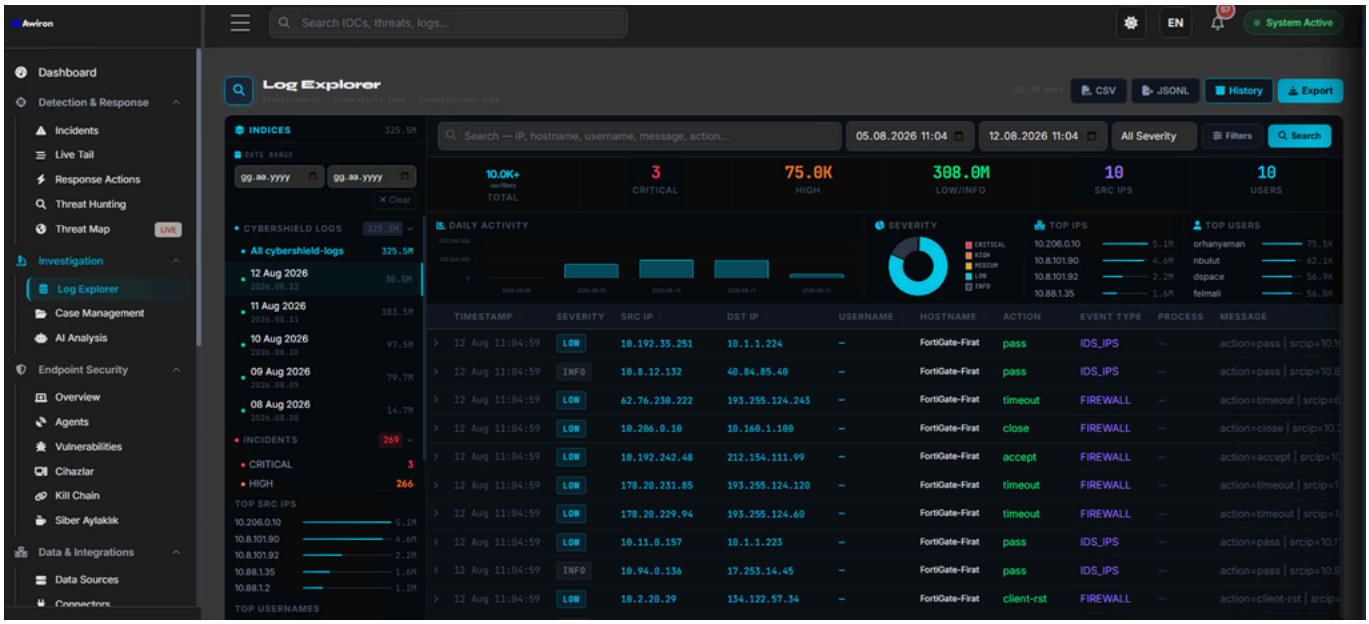
Kritik sistemler ve riskli varlıklar hızlıca tespit edilir.

Olay Görünürlüğü

Tüm güvenlik olayları merkezi olarak görüntülenir.

Derin Log Analizi ile Gerçeği Ortaya Çıkarın

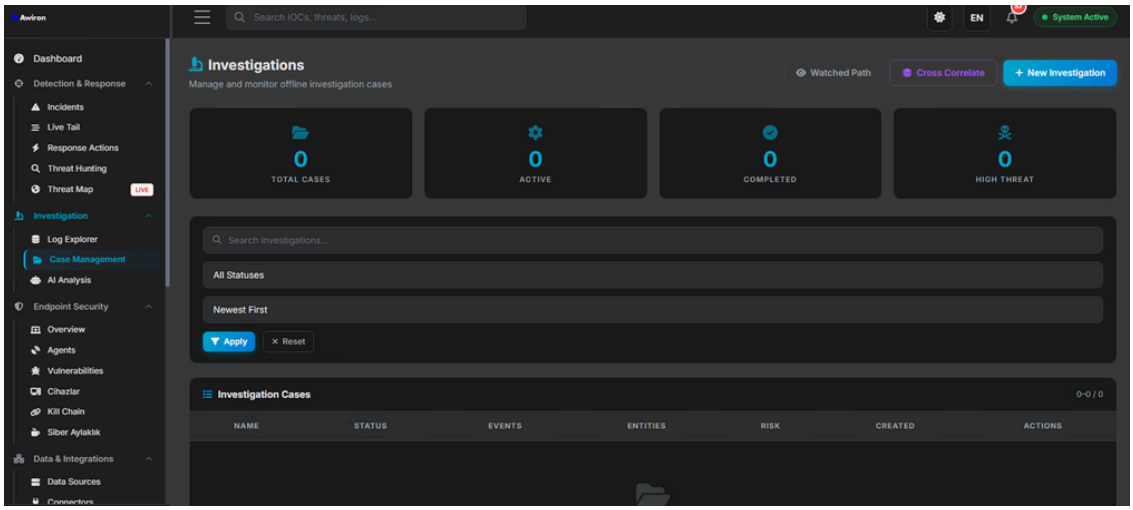
Awiron Forensic modülü, milyonlarca log verisini anlık olarak analiz ederek güvenlik olaylarının kök nedenini ortaya çıkarır. Gelişmiş filtreleme, zaman bazlı analiz ve detaylı veri inceleme yetenekleri sayesinde analistler, tehditleri hızlı ve doğru bir şekilde tespit eder.



Awiron Forensic modülü, güvenlik olaylarını yüzeyde bırakmaz; her detayı derinlemesine analiz ederek görünmeyeni ortaya çıkarır. Gelişmiş sorgulama, zaman bazlı korelasyon ve yüksek hacimli veri işleme yetenekleri sayesinde analistler, karmaşık saldırı senaryolarını hızlıca çözümleyebilir. Böylece güvenlik operasyonları yalnızca tepki veren değil, anlayan ve öngören bir yapıya dönüşür.

Olay Sonrasında Bile Kontrol Sizde

Awiron Investigation modülü, güvenlik olaylarının yalnızca tespit anında değil, olay sonrasında da ayrıntılı biçimde incelenmesini sağlar. Analistler farklı zaman aralıklarındaki olayları, ilişkili varlıkları ve güvenlik kayıtlarını vaka bazında bir araya getirerek saldırının gelişimini bütüncül şekilde değerlendirebilir.

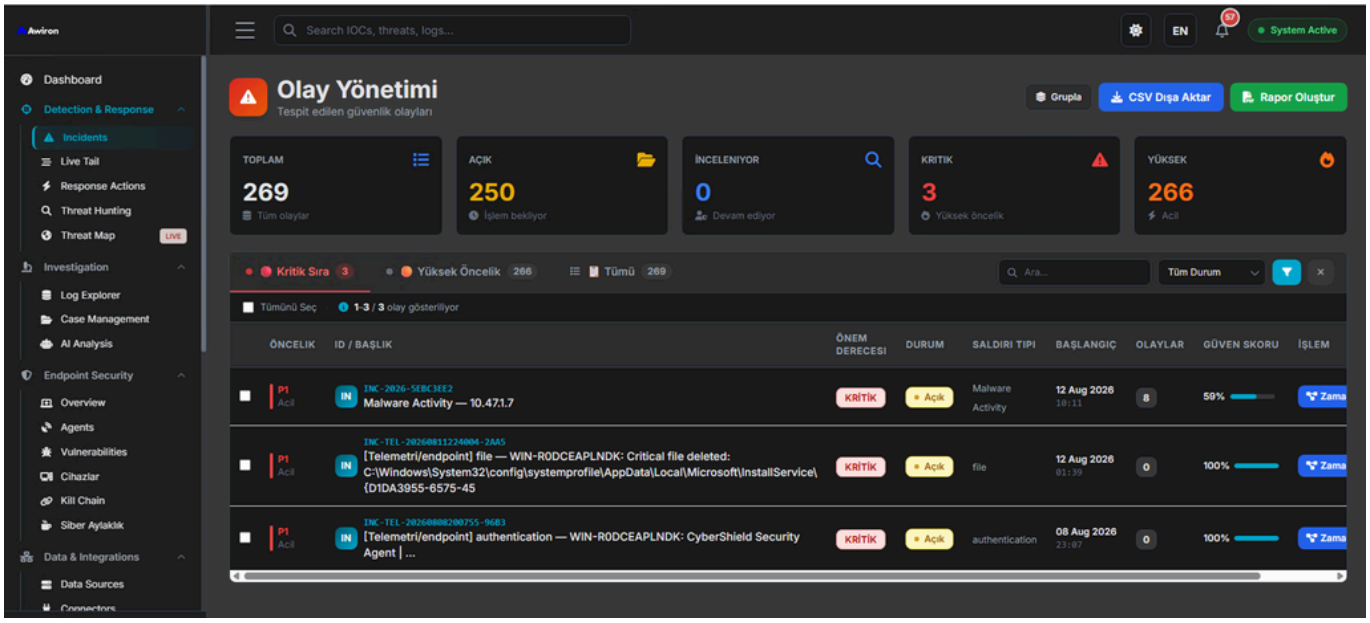


Çapraz korelasyon ve vaka yönetimi yetenekleri sayesinde birbirinden bağımsız görünen olaylar ortak bir bağlam altında ilişkilendirilebilir. Böylece SOC ekipleri yalnızca alarmı değil; olayın öncesini, gelişimini, ilişkili kanıtları ve etkilenen varlıkları da inceleyerek kök nedene daha hızlı ulaşır.

“Olay bittikten sonra bile analiz bitmez...”

Tehditleri Tespit Edin, Önceliklendirin ve Hızlıca Müdahale Edin

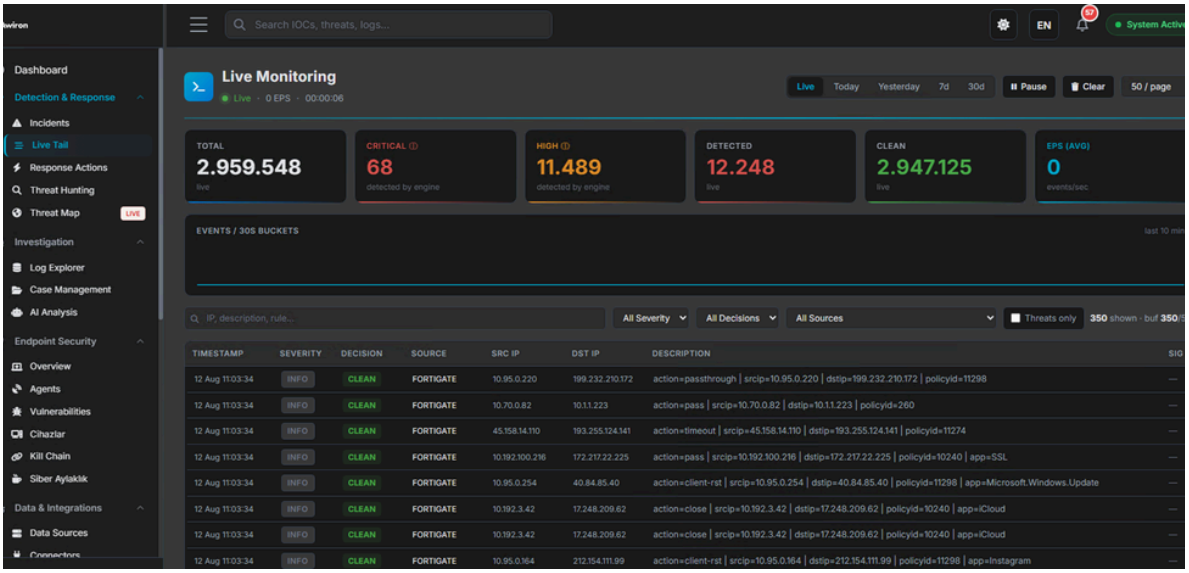
Awiron Olay Yönetimi, farklı güvenlik kaynaklarından elde edilen tespitleri merkezi bir olay kuyruğunda birleştirir. Kritik ve yüksek öncelikli olaylar otomatik olarak öne çıkarılır; önem derecesi, durum, saldırı tipi, zaman bilgisi ve güven skoru ile birlikte analistin karşısına gelir. Önceliklendirilmiş olay görünümü sayesinde SOC ekipleri yüksek riskli tehditlere odaklanır, araştırma süresini kısaltır ve müdahale süreçlerini daha kontrollü yönetir. Olayların gruplandırılması, filtrelenmesi, raporlanması ve dışa aktarılması aynı merkezi yapı üzerinden gerçekleştirilebilir.



“Doğru tehdit, doğru öncelik, doğru aksiyon.”

Gerçek Zamanlı Veri Akışı ile Anında Tespit

Awiron Live Monitoring modülü, farklı güvenlik kaynaklarından gelen yüksek hacimli olayları gerçek zamanlı olarak izler ve tek bir canlı akışta sunar. Kritik, yüksek ve normal olaylar anlık olarak sınıflandırılır; kaynak, hedef, karar ve önem derecesine göre filtrelenerek SOC ekiplerinin hızlı değerlendirme yapması sağlanır.

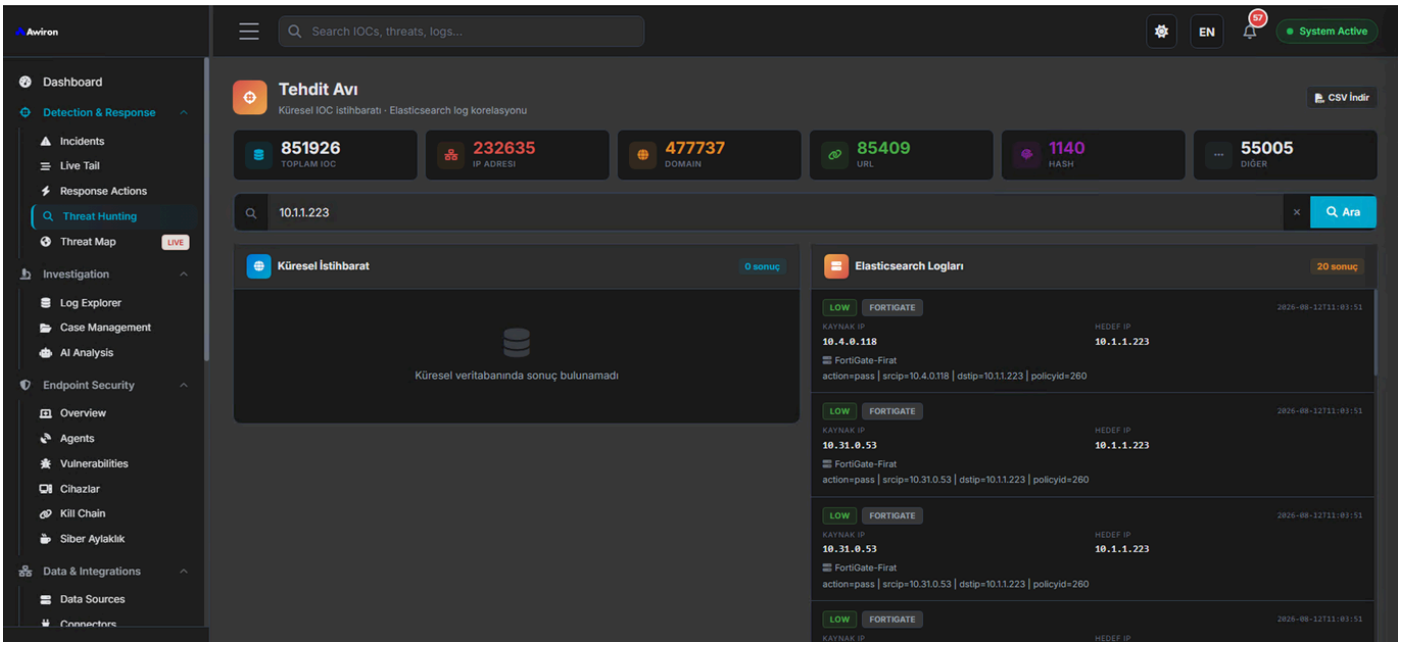


Canlı izleme yeteneği sayesinde güvenlik ekipleri sistemlerdeki güncel hareketliliği gecikmeden görebilir. Farklı kaynaklardan gelen olayların tek akışta birleştirilmesi; şüpheli aktivitelerin erken fark edilmesini, kritik olayların hızla ayrıştırılmasını ve operasyonel farkındalığın sürekli korunmasını sağlar.

“Veri akışı durmaz, Awiron da durmaz.”

Tehditleri Beklemeyin, Bulun

Awiron Threat Hunting modülü, kurum içi güvenlik verilerini küresel tehdit istihbaratı ile ilişkilendirerek proaktif tehdit araştırması yapılmasını sağlar. IP adresi, alan adı, URL, hash ve diğer IOC türleri üzerinden gerçekleştirilen sorgular, kurumun kendi loglarıyla eş zamanlı olarak karşılaştırılır.



Bu yaklaşım sayesinde analistler yalnızca alarm üreten olayları değil, henüz bir güvenlik alarmına dönüşmemiş şüpheli göstergeleri de araştırabilir. Küresel IOC havuzu ile kurumun kendi telemetrisinin aynı ekranda korele edilmesi, tehditlerin daha erken keşfedilmesine ve olayların bağlamsal olarak değerlendirilmesine yardımcı olur.

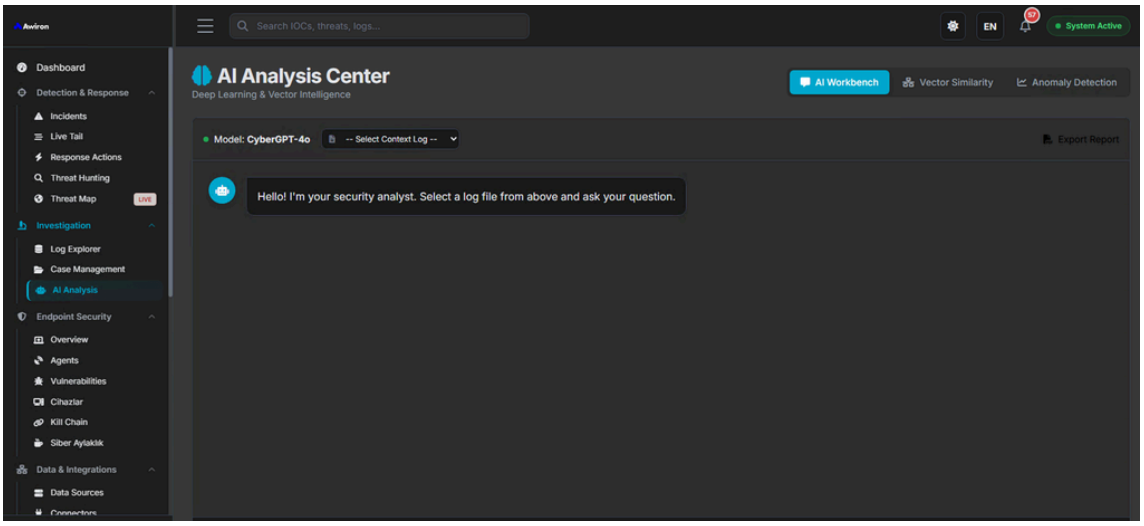
"Güvenliği izlemeyin, anlayın."

Tehditleri Küresel Ölçekte Görün

Awiron Threat Map modülü, güvenlik olaylarının coğrafi dağılımını ve saldırı kaynaklarını gerçek zamanlı olarak görselleştirir. Kaynak ülkeler, hedef bölgeler, saldırı türleri ve ağ saldırı vektörleri tek bir operasyonel görünümde bir araya getirilerek SOC ekiplerine küresel ölçekte durum farkındalığı kazandırılır. Canlı tehdit haritası, tekil güvenlik olaylarının ötesine geçerek saldırıların hangi coğrafyalarda yoğunlaştığını, hangi bölgelerin hedef alındığını ve hangi saldırı vektörlerinin öne çıktığını gösterir. Böylece güvenlik ekipleri değişen saldırı eğilimlerini daha hızlı yorumlayabilir ve operasyonel önceliklerini buna göre belirleyebilir.

Yapay Zekâ ile Güvenliği Anlamlandırın

Awiron AI Analysis Center, güvenlik verilerini yapay zekâ destekli analiz ile yorumlayarak analistlerin karmaşık olayları daha hızlı değerlendirmesine yardımcı olur. Seçilen log ve olay bağlamı üzerinden çalışan analiz ortamı; benzer davranışların ilişkilendirilmesini, şüpheli örüntülerin incelenmesini ve güvenlik verilerinin daha anlamlı hale getirilmesini sağlar. Yüksek hacimli log ve güvenlik olayları içerisinde önemli sinyalleri bulmak zaman alabilir. Awiron'un yapay zekâ destekli analiz yetenekleri, analistin doğru bağlama daha hızlı ulaşmasını destekler; benzer olayları ilişkilendirir ve olağan dışı davranışların incelenmesini kolaylaştırır.

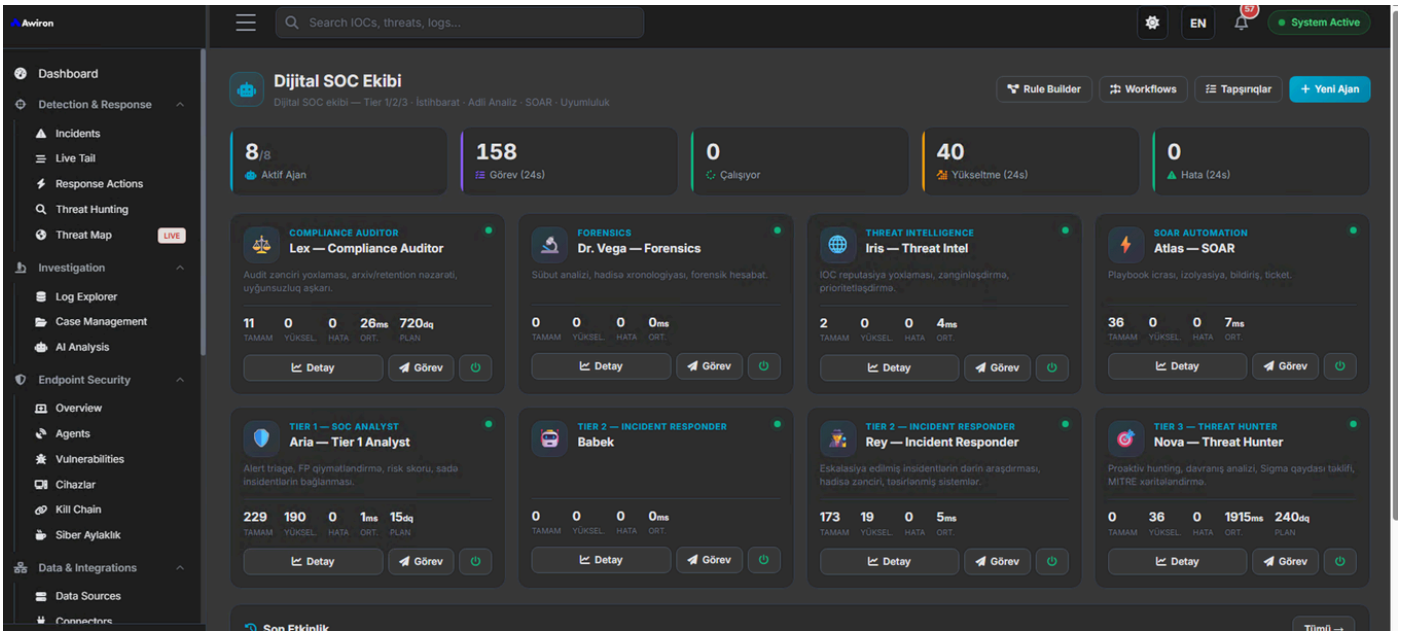


"Veriyi okuyun. Bağlamı anlayın. Kararı hızlandırın."

Dijital SOC Ekibiniz Her An Hazır

Awiron AI SOC Team, güvenlik operasyonlarını farklı uzmanlık alanlarına sahip dijital ajanlarla destekleyen yapay zekâ tabanlı bir SOC çalışma katmanı sunar. Tehdit analizi, adli inceleme, tehdit istihbaratı, uyumluluk kontrolü, olay müdahalesi ve SOAR süreçleri; kendi görev alanlarında çalışan uzman ajanlar tarafından sürekli ve koordineli biçimde yürütülür.

Tier 1 analizinden gelişmiş tehdit avcılığına kadar farklı sorumlulukları üstlenen dijital ajanlar, olayları değerlendirir, gerektiğinde üst seviyeye eskale eder ve operasyonel görevleri ortak bir iş akışı içerisinde paylaşır. Böylece rutin analiz yükü azalırken insan analistler kritik kararlar, karmaşık araştırmalar ve stratejik güvenlik operasyonlarına daha fazla odaklanabilir.

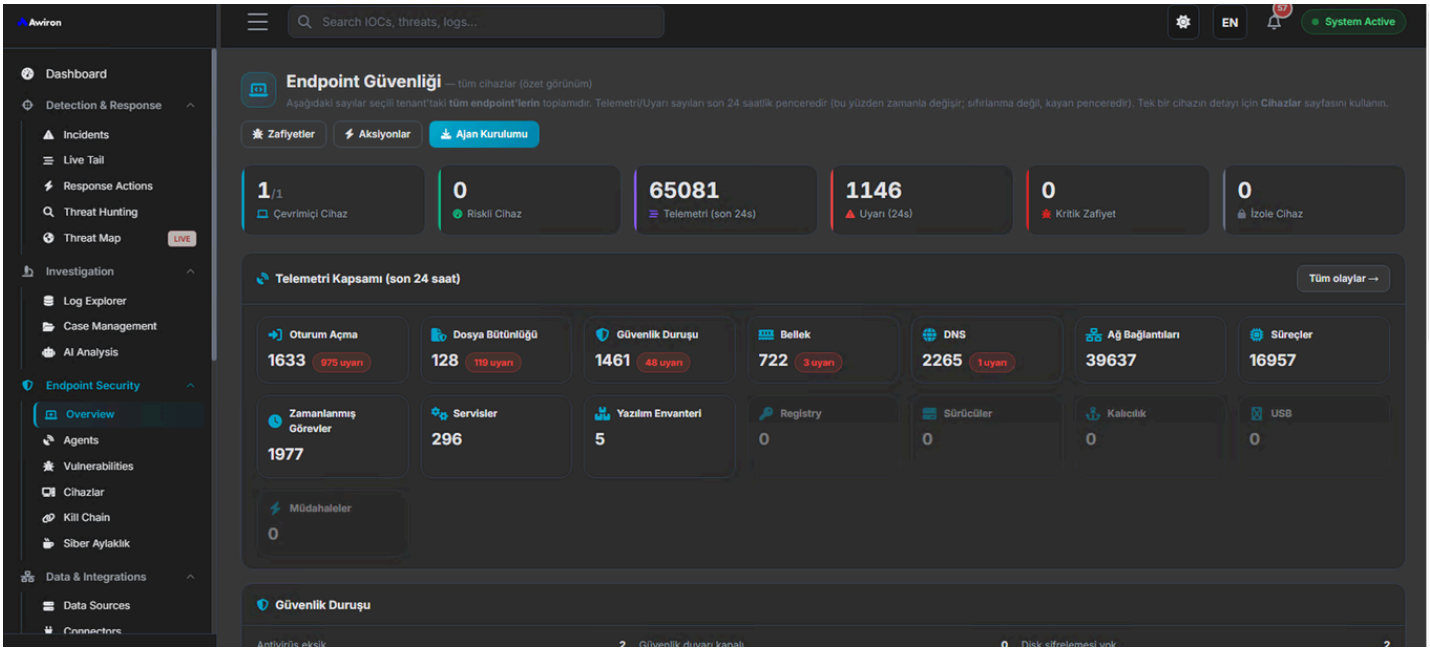


“Tek bir yapay zekâ değil, birlikte çalışan bir SOC ekibi.”

Uç Nokta Güvenliğinde Tam Görünürlük

Awiron Endpoint Security, kurum genelindeki uç noktaları merkezi olarak izleyerek cihazların güvenlik durumunu, telemetri hacmini, oluşan uyarıları ve risk göstergelerini tek ekranda görünür hale getirir. Oturum açma aktivitelerinden dosya bütünlüğüne, DNS sorgularından ağ bağlantılarına, çalışan süreçlerden yazılım envanterine kadar farklı endpoint telemetrileri sürekli olarak takip edilir.

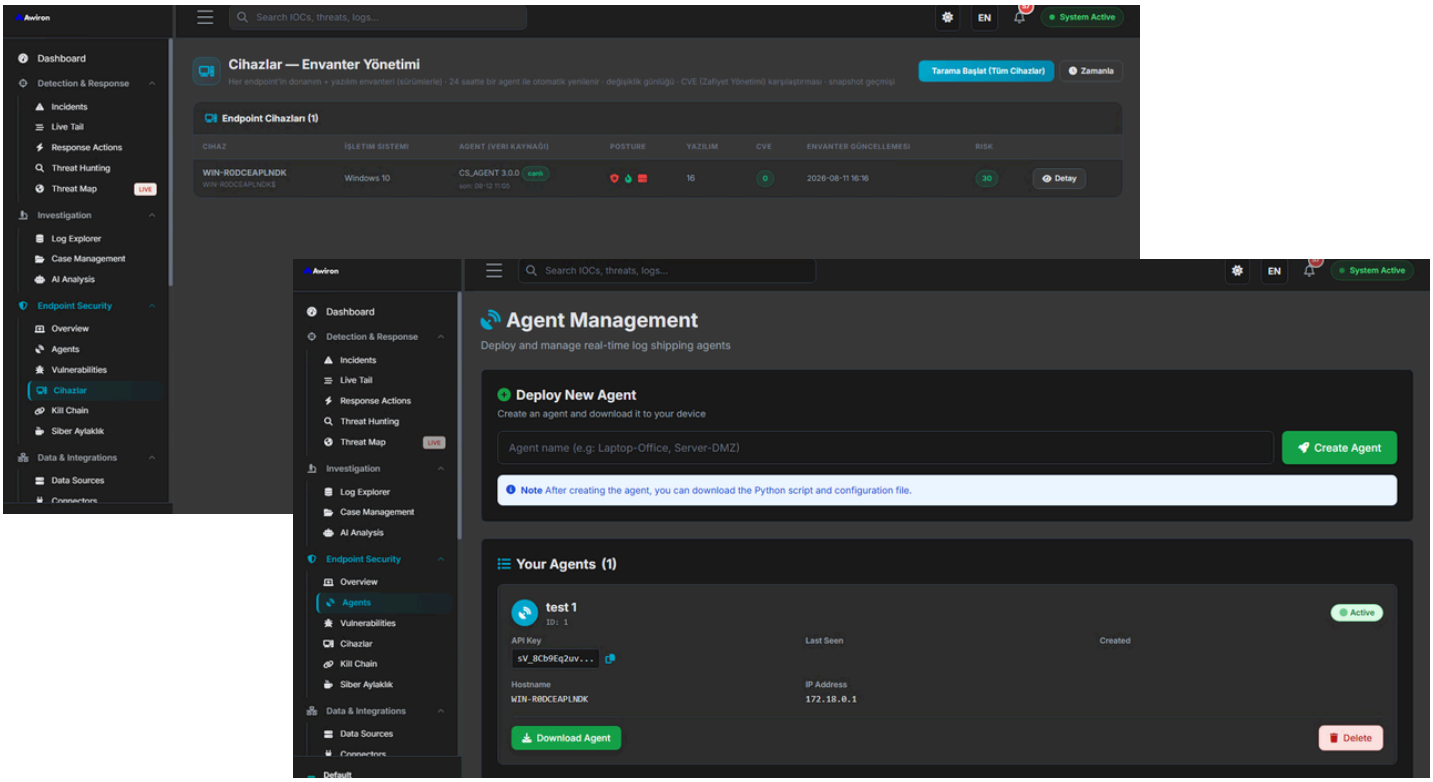
Bu bütünleşik görünürlük sayesinde SOC ekipleri yalnızca oluşan tehditleri değil, uç noktaların genel güvenlik duruşunu da değerlendirebilir. Riskli cihazların belirlenmesi, kritik aktivitelerin önceliklendirilmesi ve gerektiğinde müdahale süreçlerinin başlatılması merkezi bir endpoint güvenlik yaklaşımı içerisinde yürütülür.



“Her uç noktayı görün. Her riski anlayın. Tek merkezden yönetin.”

Uç Noktaları ve Ajanları Tek Merkezden Yönetin

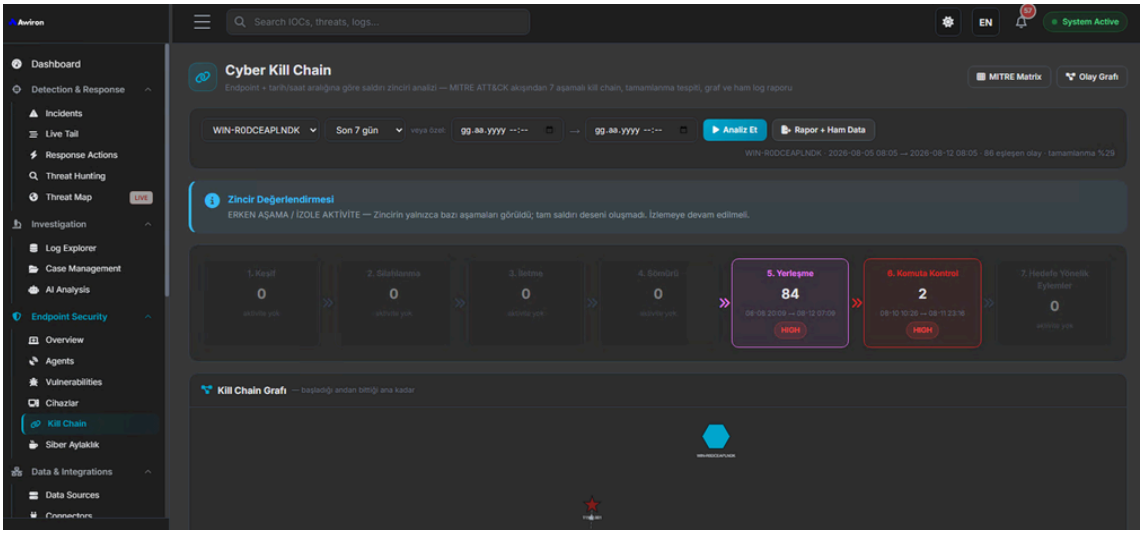
Awiron, uç nokta güvenliğini yalnızca cihaz görünürlüğü ile sınırlamaz; bu cihazlardan veri toplayan ajanların yönetimini de aynı operasyon akışı içinde sunar. Envanter ekranı üzerinden cihazların işletim sistemi, ajan durumu, güvenlik duruşu, yazılım bilgisi ve risk seviyesi izlenirken; ajan yönetimi ekranı ile yeni ajan oluşturma, dağıtım, aktivasyon ve izleme süreçleri merkezi olarak kontrol edilir. Bu bütünleşik yapı sayesinde güvenlik ekipleri hem hangi varlıkların korunduğunu hem de bu varlıklardan veri akışını sağlayan ajanların ne durumda olduğunu tek merkezden yönetebilir. Böylece görünürlük, veri toplama ve operasyonel kontrol tek bir güvenlik katmanında birleşir.

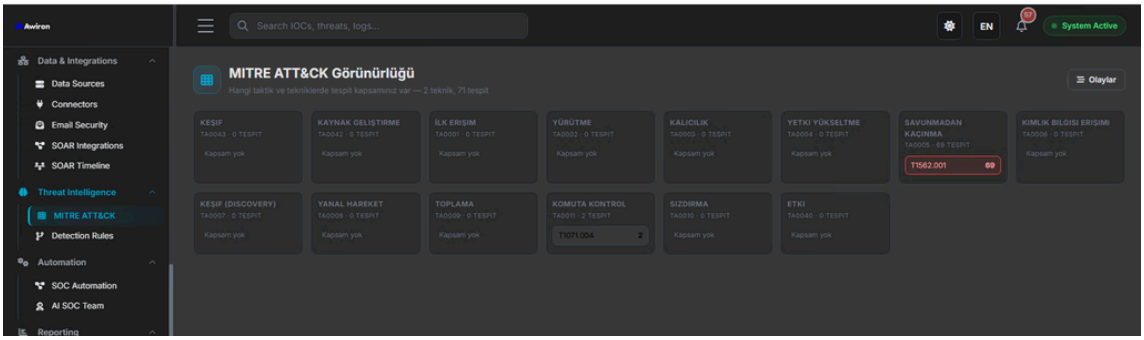


“Cihazı görün, ajanı yönetin, görünürlüğü tamamlayın.”

Saldırı Zincirini MITRE ATT&CK ile Uçtan Uca Görün

Awiron, güvenlik olaylarını yalnızca bağımsız alarmlar olarak değil, bir saldırının birbirini takip eden aşamaları içerisinde analiz eder. Cyber Kill Chain yaklaşımı ile saldırının keşiften komuta-kontrol ve hedefe yönelik eylemlere kadar nasıl ilerlediği ortaya çıkarılır; MITRE ATT&CK eşleştirmesi ile tespit edilen davranışların hangi taktik ve tekniklerle ilişkili olduğu görünür hale getirilir. Kill Chain ve MITRE ATT&CK görünürlüğünün birlikte kullanılması, analistlerin saldırının yalnızca ne olduğunu değil, nasıl ilerlediğini ve hangi davranış tekniklerini kullandığını anlamasını sağlar. Böylece saldırının mevcut aşaması belirlenebilir, tespit kapsamındaki boşluklar görülebilir ve müdahale kararları tehdit davranışının gerçek bağlamına göre şekillendirilebilir.

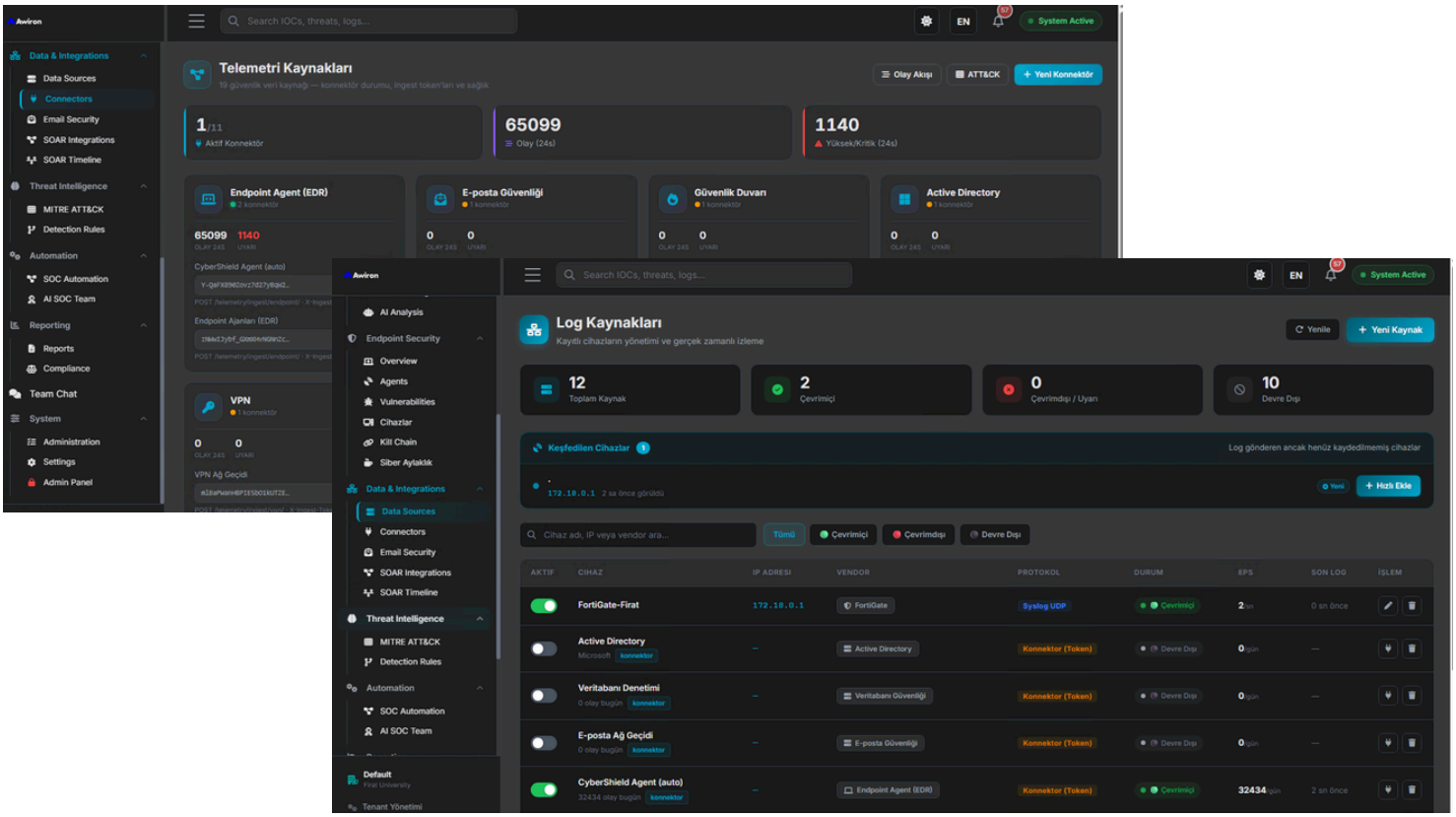




“Saldırının hangi aşamada olduğunu bilin, hangi teknikle ilerlediğini görün.”

Güvenlik Verilerinizi Tek Ekosistemde Birleştirin

Awiron, farklı güvenlik sistemlerinden gelen verileri tek platform üzerinde bir araya getirerek merkezi bir veri ve entegrasyon katmanı oluşturur. Güvenlik duvarları, endpoint ajanları, Active Directory, e-posta güvenliği, VPN, veritabanları ve ağ tespit sistemlerinden üretilen telemetri; ortak bir güvenlik veri modeli içerisinde toplanarak analiz ve korelasyon süreçlerine aktarılır. Konnektör ve entegrasyon yapısı sayesinde mevcut güvenlik yatırımlarının değiştirilmesine gerek kalmadan Awiron ekosistemine dahil edilmesi mümkün olur. Böylece dağınık veri kaynakları merkezi görünürlüğe, merkezi görünürlük ise daha güçlü tehdit tespiti ve müdahale kabiliyetine dönüşür.



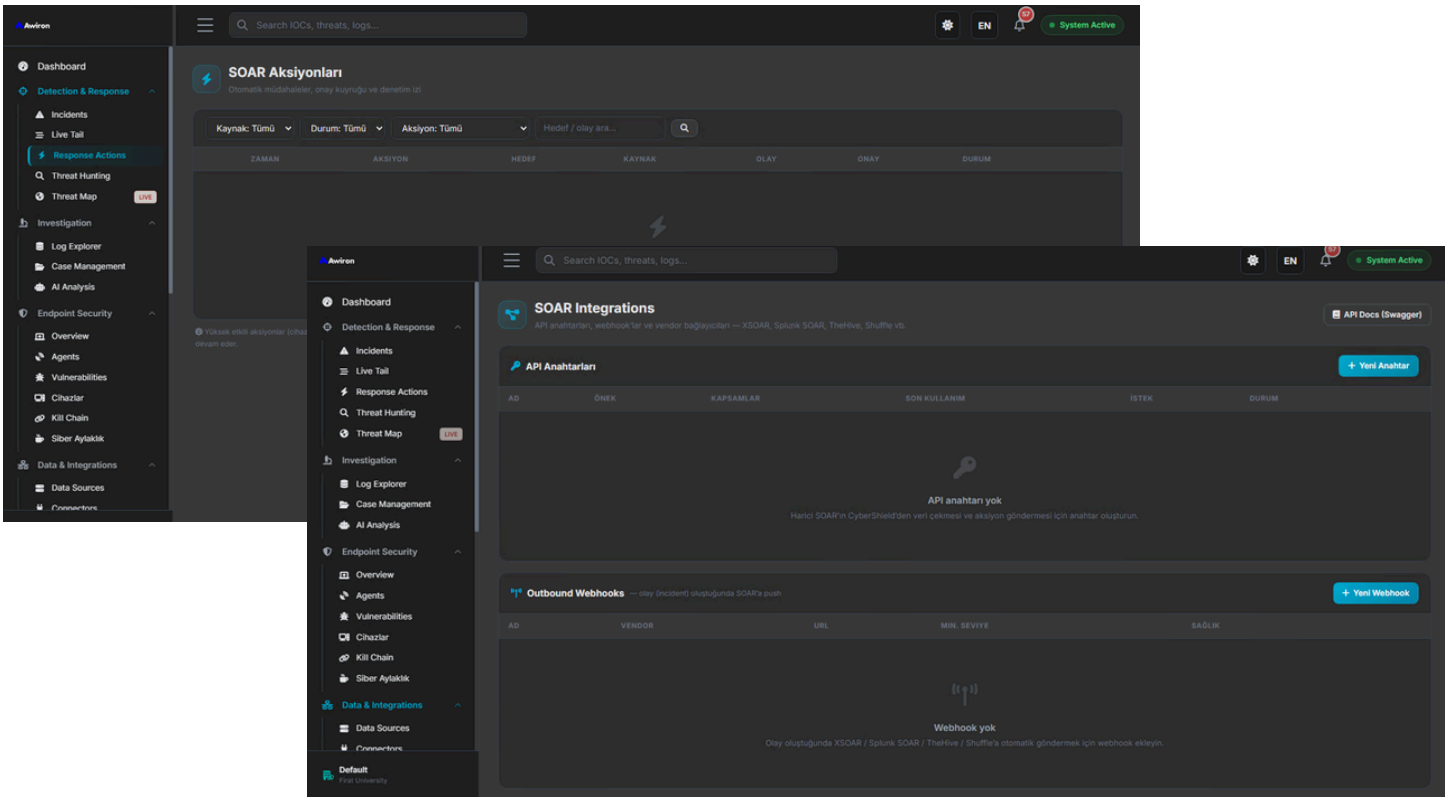
Merkezi entegrasyon yaklaşımı, veri kaynaklarının durumunu ve veri akışını sürekli görünür tutarken üçüncü taraf güvenlik platformlarıyla çift yönlü operasyon imkânı sağlar. API ve webhook desteği sayesinde Awiron, mevcut SOC mimarisinin yerine geçen kapalı bir sistem değil; farklı güvenlik teknolojilerini ortak operasyon katmanında buluşturan genişletilebilir bir platform olarak konumlanır.

“Farklı kaynaklar. Tek veri katmanı. Ortak güvenlik görünürlüğü.”

Otomasyonla Müdahaleyi Hızlandırın

Awiron SOAR, tespit edilen güvenlik olaylarına yönelik müdahale adımlarını merkezi olarak yönetir ve tekrarlayan operasyonları otomatikleştirir. IP engelleme, cihaz izolasyonu, süreç sonlandırma, bildirim gönderme ve vaka oluşturma gibi aksiyonlar; önceden tanımlanmış iş akışları üzerinden hızlı ve kontrollü biçimde yürütülebilir.

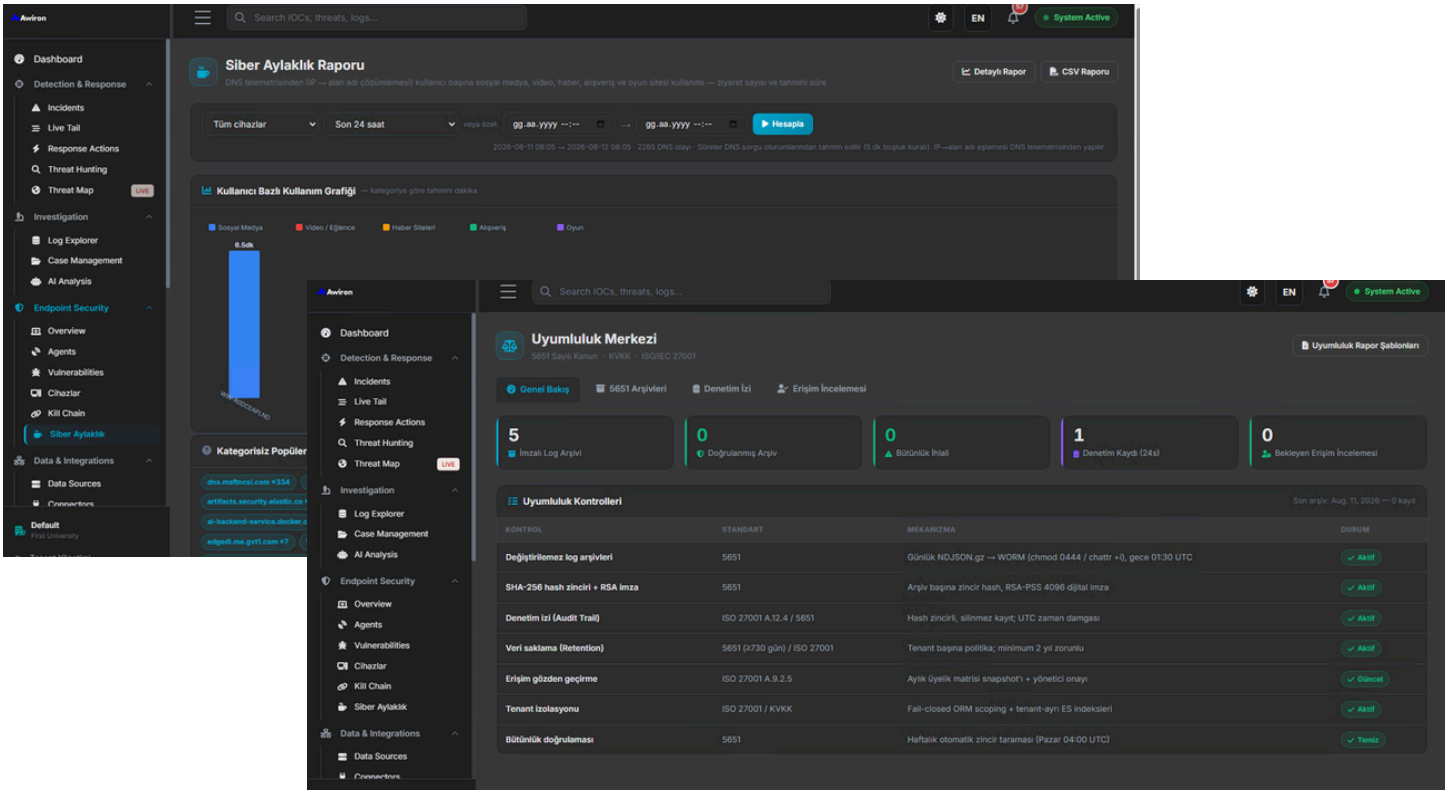
Kritik veya yüksek etkili müdahalelerde analist onayı devreye alınabilir; böylece otomasyon hızı ile operasyonel kontrol dengelenir. Tüm aksiyonlar zaman çizelgesi üzerinden izlenerek hangi olayın hangi playbook'u tetiklediği ve hangi müdahalenin gerçekleştirildiği kayıt altına alınır.



“Tespit ile aksiyon arasındaki zamanı kısaltın.”

Uyumluluğu ve Raporlamayı Tek Merkezden Yönetin

Awiron, güvenlik operasyonlarından üretilen verileri yalnızca analiz etmekle kalmaz; denetim ve yönetim süreçlerinde kullanılabilecek izlenebilir çıktılara dönüştürür. Uyumluluk Merkezi üzerinden 5651, KVKK ve ISO/IEC 27001 gibi gereksinimlere ilişkin kontroller takip edilirken, raporlama altyapısı güvenlik verilerinin yönetici, denetçi ve teknik ekipler için anlaşılır biçimde sunulmasını sağlar.
İmzalı log kayıtları, erişim izleri, bütünlük kontrolleri ve güvenlik olayları merkezi olarak değerlendirilerek kurumun uyumluluk durumuna ilişkin sürdürülebilir bir görünürlük oluşturulur.

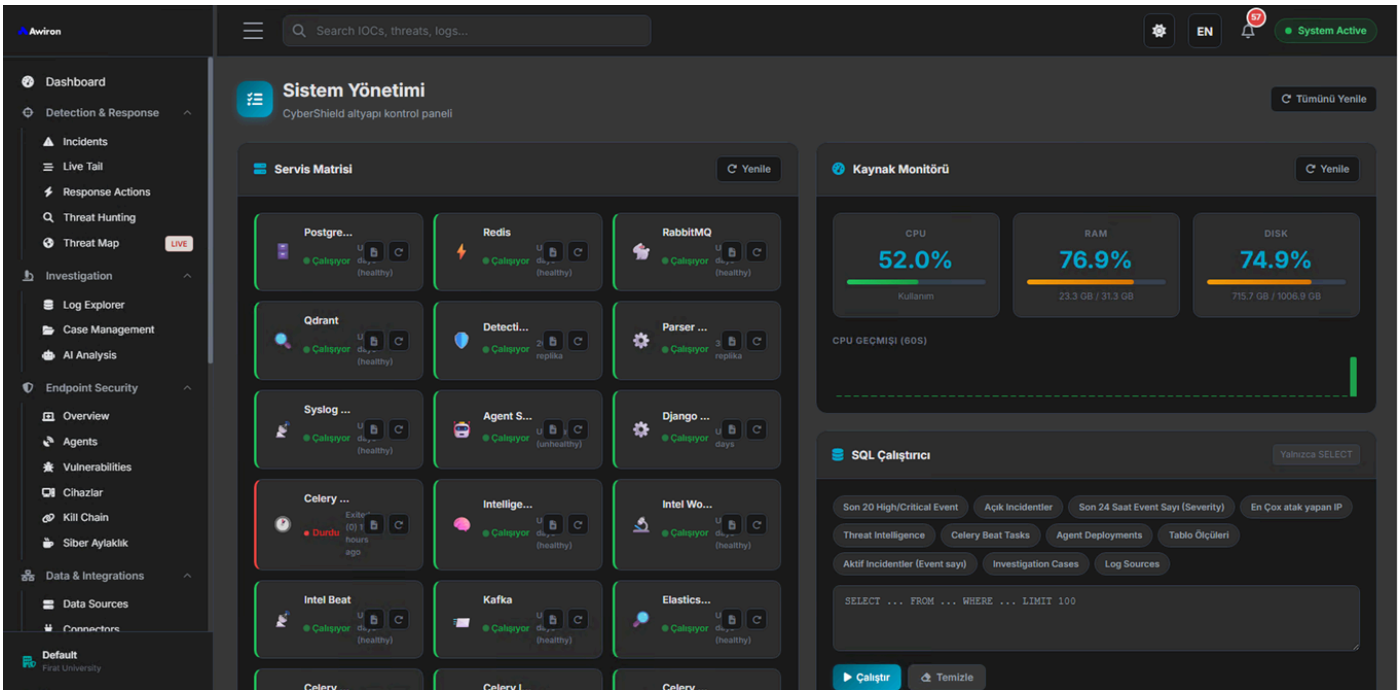


“Güvenliği ölçün. Uyumluluğu kanıtlayın.”

Platform Sağlığını ve Sistem Kaynaklarını Tek Merkezden Yönetin

Awiron Sistem Yönetimi, güvenlik platformunun çalışmasını sağlayan temel servisleri, sistem kaynaklarını ve operasyonel durumu merkezi bir panel üzerinden izlenebilir hale getirir. CPU, bellek ve disk kullanımı gibi altyapı metrikleri ile servislerin çalışma durumları aynı ekranda takip edilerek olası performans sorunları ve hizmet kesintileri daha erken fark edilebilir.

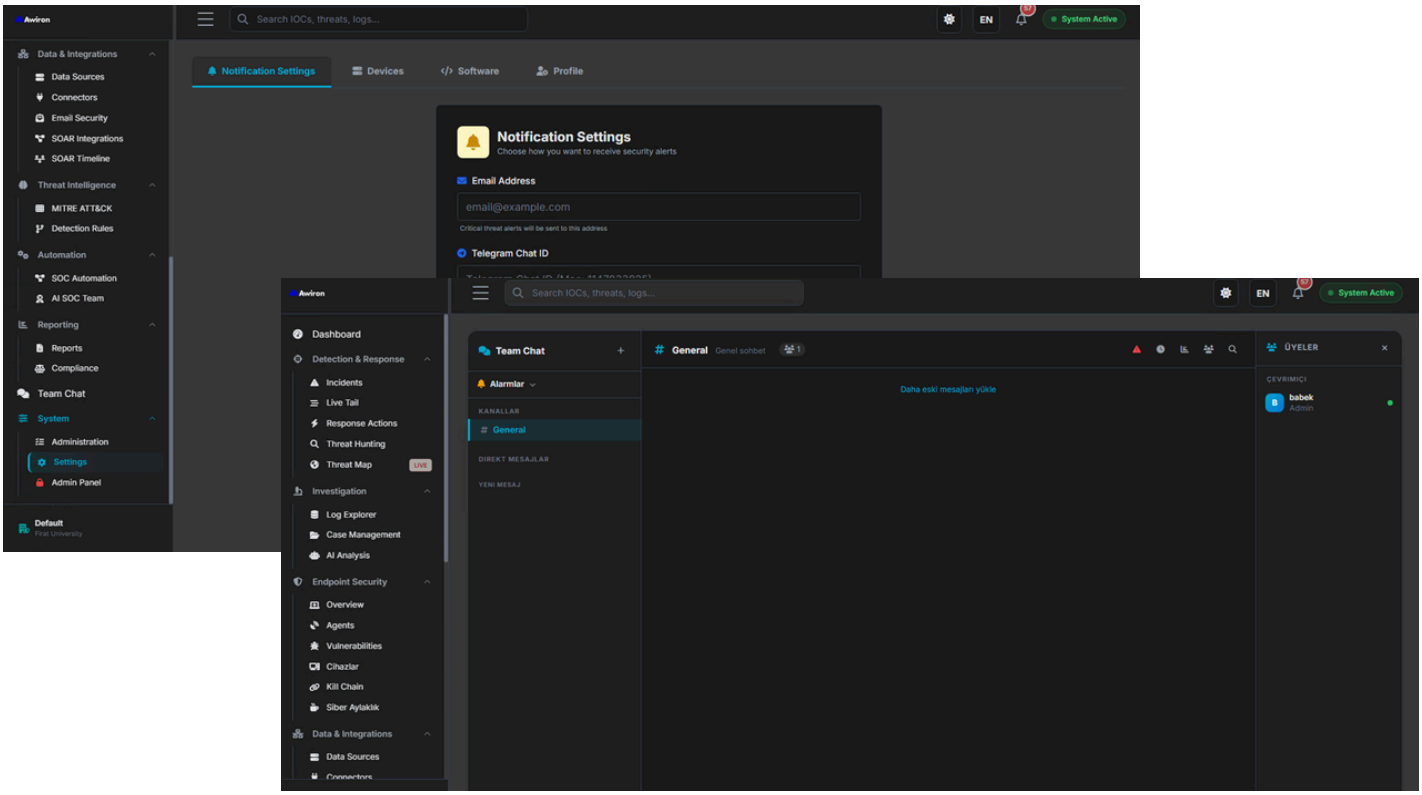
Güvenlik operasyonlarının kesintisiz sürdürülebilmesi için yalnızca tehditlerin değil, bu tehditleri analiz eden altyapının da sürekli izlenmesi gerekir. Awiron, platform sağlığını görünür kılarak operasyon ekiplerine sistem sürekliliği ve kaynak yönetimi konusunda merkezi kontrol sağlar.



“Tehditleri izlerken platformunuzu da kontrol altında tutun.”

Güvenlik Ekiplerinizi ve Bildirim Akışını Bir Araya Getirin

Awiron, güvenlik operasyonlarının yalnızca tespit ve analiz aşamasını değil, ekip içi iletişim ve bildirim süreçlerini de tek platform içerisinde destekler. Entegre Team Chat sayesinde SOC analistleri olaylar, tehditler ve operasyonel gelişmeler hakkında hızlıca iletişim kurabilir; bildirim yönetimi ile kritik güvenlik uyarıları ilgili ekiplere doğru kanallar üzerinden ulaştırılabilir.
Bu bütünleşik yaklaşım, güvenlik olaylarında bilgi kaybını ve iletişim gecikmelerini azaltarak ekiplerin daha koordineli hareket etmesine yardımcı olur.

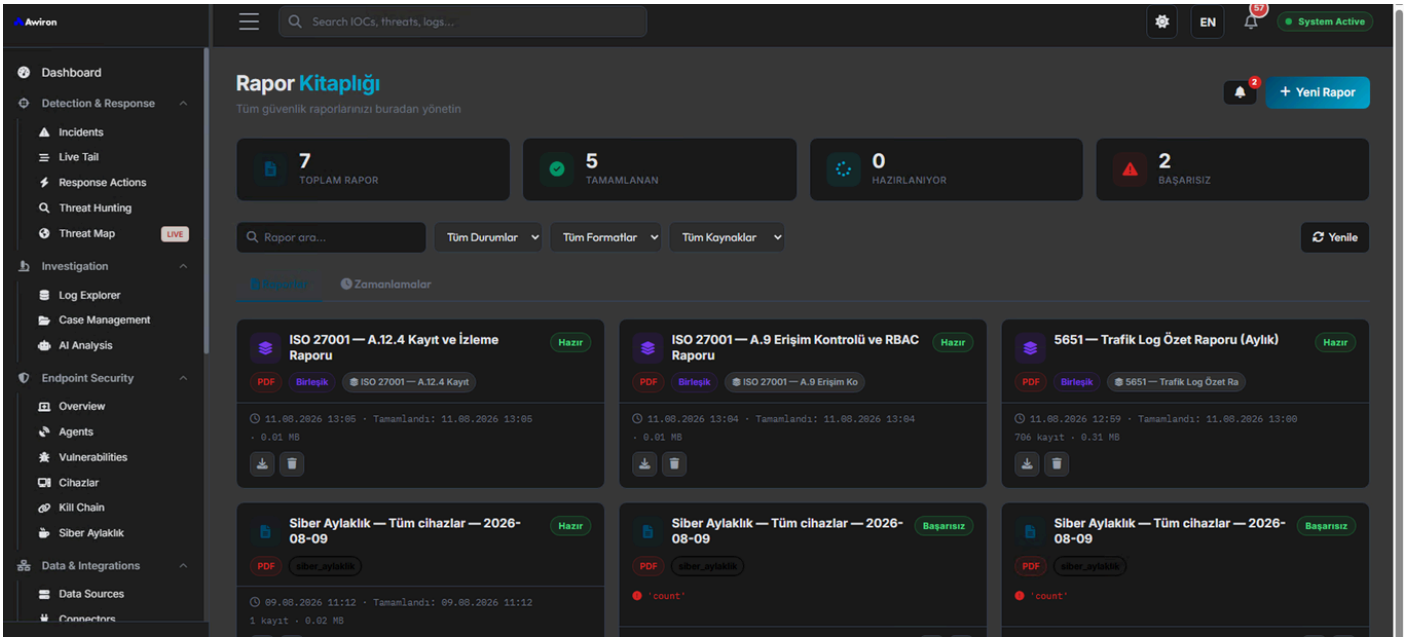


“Doğru olay. Doğru ekip. Doğru zamanda aksiyon.”

Güvenlik Verisini Karara Dönüştürün

Awiron Raporlama Merkezi, platform genelinde üretilen güvenlik verilerini teknik ekipler, yöneticiler ve denetçiler için anlaşılır ve aksiyon alınabilir raporlara dönüştürür. Olaylar, güvenlik logları, kullanıcı aktiviteleri ve farklı veri kaynaklarından elde edilen bilgiler; seçilebilir tarih aralıkları, filtreler ve görselleştirme seçenekleri ile raporlanabilir.

Hazırlanan raporlar yalnızca anlık analiz amacıyla değil, dönemsel güvenlik değerlendirmeleri, yönetici bilgilendirmeleri ve denetim süreçleri için de kullanılabilir. PDF, Excel ve CSV gibi farklı çıktı seçenekleri sayesinde Awiron, operasyon sırasında oluşan veriyi kurumsal karar süreçlerinde kullanılabilecek kalıcı bir bilgi kaynağına dönüştürür. Güncel ürün dokümanında da raporların farklı veri kaynaklarından üretilebildiği, çeşitli grafik türlerinin desteklendiği ve zamanlanmış raporlamanın bulunduğu belirtiliyor.



“Veriyi görün. Sonucu ölçün. Kararı güçlendirin.”

Awiron

prodrom.com

info@prodrom.com