RINT BİLGİ TEKNOLOJİLERİ

Wazuh Platinum Partner · Türkiye

TEKNİK WHITEPAPER

Wazuh

XDR ve SIEM Platformu

Mimari, Yetenekler ve Hizmet Modeli

VERSİYON	YAYIN	KAPSAM
1.0	**Nisan 2026**	**Dış Kullanım**

ÖNSÖZ

Bu Doküman Hakkında

Bu whitepaper; Wazuh açık kaynak güvenlik platformunu, bu platformun kurumsal ortamlardaki konumunu ve Rint Bilgi Teknolojileri'nin müşterilerine sunduğu hizmet modellerini tanıtmak amacıyla hazırlanmıştır.

Doküman iki farklı okuyucu kitlesini gözeterek yapılandırılmıştır. Üst yönetim ve karar vericiler için executive summary, platform konumlandırması ve hizmet modeli bölümleri stratejik bir genel bakış sunar. Teknik ekipler için ise mimari, yetenek detayları, deployment modelleri, entegrasyonlar ve uyumluluk başlıkları derinlemesine bir referans niteliğindedir.

Whitepaper süresince yer alan içerik; Wazuh Inc.'in resmi dokümantasyonuna, platform üzerindeki saha tecrübesine ve Rint Bilgi Teknolojileri ekibinin onlarca müşteri kurulumundan elde ettiği operasyonel bilgi birikimine dayanmaktadır.

> *Açık kaynak yazılımın gerçek değeri, doğru ellerde işletildiğinde ortaya çıkar.*
>
> — Rint Bilgi Teknolojileri Mühendislik Ekibi

DOKÜMAN BILGILERI

ALAN	BILGI
Doküman adı	Wazuh XDR ve SIEM Platformu — Teknik Whitepaper
Versiyon	1.0
Yayın tarihi	Nisan 2026
Hazırlayan	Rint Bilgi Teknolojileri — Security Engineering
Hedef kitle	Karar vericiler ve teknik değerlendirme ekipleri

ALAN	BILGI
Kapsam	Wazuh 4.13.x ve 4.14.x sürüm hattı
Dağıtım	Dış kullanım — açık paylaşım

İ Ç İ N D E K İ L E R

Yol Haritası

00

BÖLÜM

Yönetici Özeti

Karar vericiler için iki sayfalık genel bakış

Kurumsal güvenlik operasyonu, son beş yılda derin bir dönüşüm geçirdi. Tek başına antivirüs veya firewall ile savunma yapılabilen bir dünyadan; endpoint'ten cloud'a, container'dan SaaS uygulamalarına kadar çok katmanlı görünürlük gerektiren bir gerçekliğe geldik.

Bu yeni gerçeklikte Security Information and Event Management (SIEM) ve Extended Detection and Response (XDR) sistemleri, bir güvenlik ekibinin en temel aracı haline geldi. Wazuh, bu alanda ortaya çıkan en güçlü açık kaynak platformlardan biridir. Endpoint log toplama, dosya bütünlüğü izleme, zafiyet tespiti, güvenlik yapılandırma denetimi, tehdit istihbaratı, olay müdahalesi ve regülasyon uyumluluğu gibi on bir ana yetkinliği tek bir platformda birleştirir; kurumsal ölçekte on binlerce endpoint'i yönetebilecek şekilde ölçeklenir; modern bulut ve konteyner ortamlarını yerel olarak destekler.

Bu whitepaper; Wazuh platformunun ne olduğunu, hangi yetenekleri sunduğunu, nasıl bir mimari üzerine kurulduğunu ve hangi entegrasyonları desteklediğini tanıtır. Doküman iki farklı okuyucu kitlesine hitap edecek şekilde tasarlanmıştır: üst yönetim için yatırım getirisi ve stratejik konumlandırma, teknik ekipler için ise mimari, ölçeklenebilirlik ve entegrasyon detayları aynı belge içinde yer alır.

> *Wazuh açık kaynak lisansı maliyet avantajı sunar; ancak gerçek değer, doğru mimariyle kurulması ve operasyonel olarak sürdürülebilir tutulmasıyla ortaya çıkar.*

0.1 Üç Hizmet Seviyesi, Tek Partner

Rint Bilgi Teknolojileri, Türkiye'nin Wazuh Platinum Partner'ı olarak; on'dan fazla aktif mühendisten oluşan bir ekiple kurumlara üç farklı hizmet seviyesi sunar. Birinci seviye olan Kur ve Teslim Et modelinde platform anahtar teslim olarak kuruma devredilir. İkinci seviye olan Kur ve İzle modelinde kurulumun yanı sıra günlük bakım, haftalık tuning ve aylık raporlama Rint Bilgi Teknolojileri tarafından yürütülür. Üçüncü ve en kapsamlı seviye olan Tam SOC Hizmeti modelinde ise Rint Bilgi Teknolojileri bir Security Operations Center partneri olarak konumlanır; 7/24 alarm takibi ve aktif savunmayı üstlenir.

0.2 Bu Dokümanda Neler Var

- Wazuh platformunun tanımı, tarihçesi ve rekabet konumu
- On bir ana yetenek alanının detaylı tanıtımı ve kullanım senaryoları
- Platform mimarisi, bileşenler ve veri akışı
- Ölçeklenebilirlik modelleri ve deployment topolojileri
- Desteklenen işletim sistemleri, bulut servisleri ve konteyner platformları
- Entegrasyonlar, add-on'lar ve üçüncü parti araç desteği
- Compliance ve regülasyon uyumluluk kapsamı
- Rint Bilgi Teknolojileri hizmet modeli ve Platinum Partner yetkinlikleri

01

BÖLÜM

Wazuh Platformuna Giriş

Açık kaynak XDR ve SIEM platformunun tanımı

Wazuh; endpoint'ten cloud'a kadar tüm BT altyapısı üzerinde güvenlik olaylarını toplayan, ilişkilendiren ve analiz eden açık kaynak bir XDR ve SIEM platformudur.

2015 yılında OSSEC projesinin bir fork'u olarak hayata geçen Wazuh, bugün dünya genelinde 100.000'i aşkın kurumsal kurulumda kullanılan, aktif bir geliştirici topluluğu tarafından desteklenen modern bir güvenlik platformuna dönüşmüştür.

1.1 Wazuh Nedir?

Wazuh'u anlamanın en sade yolu, modern bir güvenlik ekibinin üç temel soruyu hangi araçla yanıtladığını düşünmektir. Ekip birinci soruyu sorar: altyapımda şu anda ne oluyor? Bu, görünürlük sorusudur ve log toplama, envanter ve file integrity monitoring ile cevaplanır. İkinci soruyu sorar: bu olayların içinde saldırı belirtisi var mı? Bu, tespit sorusudur ve kural motoru, tehdit istihbaratı ve davranışsal analiz ile cevaplanır. Üçüncü soruyu sorar: bu saldırıya nasıl müdahale ederim? Bu, müdahale sorusudur ve otomatik aksiyonlar, vaka yönetimi ve olay kayıtları ile cevaplanır.

Wazuh bu üç soruyu tek bir platform üzerinden yanıtlar. Geleneksel SIEM ürünleri yalnızca ilk iki soruya odaklanır ve müdahale için ayrı bir SOAR ürünü gerektirir; geleneksel EDR ürünleri ise yalnızca endpoint'e bakar ve cloud görünürlüğü sağlamaz. Wazuh, XDR yaklaşımıyla endpoint, server, cloud workload ve container'ı tek bir yönetim konsolunda birleştirerek bu bölünmüşlüğü ortadan kaldırır.

1.2 Kısa Tarihçe

Wazuh, ünlü açık kaynak HIDS projesi OSSEC'in bir türevi olarak 2015 yılında başladı. Kurucular OSSEC'in kural motoru ve agent mimarisini koruyarak; üzerine modern bir arama ve görselleştirme katmanı ekleyerek platformu SIEM kategorisine taşıdılar. Sonraki yıllarda Vulnerability Detection, Security Configuration Assessment, MITRE ATT&CK mapping, Cloud Security Monitoring ve Container Security gibi modüller eklenerek platform XDR kategorisine genişledi.

2022 yılında Wazuh Inc. 15 milyon dolarlık Seri A yatırımı aldı ve bu yatırımla birlikte ürün geliştirme hızı önemli ölçüde arttı. 2024-2025 döneminde 4.13 ve 4.14 sürümleriyle birlikte IT Hygiene Dashboard, Hot Reload, Microsoft Graph entegrasyonu ve yenilenmiş Vulnerability Detection mimarisi gibi kritik iyileştirmeler devreye alındı. 2026 itibarıyla 5.0 sürümü aktif geliştirme altındadır.

1.3 Rekabet Konumu

Wazuh, kurumsal güvenlik pazarında ticari SIEM ve XDR ürünleriyle aynı kategoride yer alır ancak açık kaynak lisansı sayesinde belirgin bir maliyet avantajı sunar. Aşağıdaki tablo platformun genel konumunu özetler:

KATEGORI	TICARI ÇÖZÜMLER	WAZUH'UN KONUMU
SIEM	Splunk, IBM QRadar, LogRhythm	Karşılaştırılabilir yetenek, önemli TCO avantajı
EDR / XDR	CrowdStrike, SentinelOne, Defender	Tam XDR yetenekleri, tek agent
Compliance	Tenable, Qualys	PCI, HIPAA, GDPR, NIST dashboard'ları
Vulnerability Mgmt	Rapid7, Qualys	Entegre inventory ve CVE keşfi
Cloud Security	Wiz, Prisma Cloud	AWS, Azure, GCP, M365 entegrasyonu

Wazuh'un en güçlü yanı; yukarıdaki kategorilerin her birini ayrı bir ürün olarak satın almak yerine tek bir platform üzerinden sunmasıdır. Bu, özellikle orta ve büyük ölçekli kurumlar için lisans maliyetlerinde ciddi tasarruf sağlar ve birden fazla aracın entegrasyon yükünü ortadan kaldırır.

1.4 Açık Kaynak Lisansı

Wazuh, AGPLv3 lisansı altında dağıtılır. Bu lisans; kaynak koda tam erişim, özgürce değiştirme ve dağıtma hakkı sağlar. Kurumsal kullanım için herhangi bir lisans ücreti ödenmez; müşteri yalnızca kendi altyapı kaynakları ve isteğe bağlı profesyonel destek için ödeme yapar. Bu model, yazılımın arkasındaki şirketin ticari başarısına bağımlı olmadan sürdürülebilirlik sunar.

Açık kaynak modelinin ikinci önemli avantajı şeffaflıktır. Ticari SIEM ürünlerinin kapalı kutu yapısı, güvenlik ekiplerinin ürünün içinde ne olduğunu bilmemesine yol açar. Wazuh'ta her satır kod, her kural, her decoder inceleme için açıktır. Bu; özellikle kamu kurumları, finans sektörü ve savunma sanayii gibi yüksek güven gerektiren ortamlarda büyük bir tercih sebebidir.

AÇIK KAYNAK ≠ ÜCRETSIZ

Wazuh yazılımı ücretsizdir; ancak kurumsal bir Wazuh deployment'ı bedava değildir. Doğru mimarinin tasarlanması, sertifikaların yönetilmesi, kural tuning süreci, kapasite planlama, upgrade operasyonları ve 7/24 izleme gerçek mühendislik emeği gerektirir. Rint Bilgi Teknolojileri'nin değer önerisi tam bu noktadadır: açık kaynak lisansın maliyet avantajını korurken, kurumsal kalitede bir operasyonel deneyimi müşterilere sunmak.

02

BÖLÜM

Platform Yetenekleri

Tek platformda on bir ana yetkinlik

Wazuh platformu on bir ana yetenek alanında çalışır. Bu yetenekler tek bir agent ve tek bir yönetim konsolu üzerinden sunulur; ekiplerin aynı olayı farklı ürünlerde ayrı ayrı araştırma ihtiyacını ortadan kaldırır.

Bu bölüm her yeteneği; ne işe yaradığı, nasıl çalıştığı ve hangi senaryolarda kritik olduğu açısından tanıtır. Yetenek matrisi platformun toplam kapsamını özetler.

YETENEK MATRISI

№	YETENEK	ANA KULLANIM
01	Log Data Collection	Merkezi log toplama ve normalize etme
02	File Integrity Monitoring	Kritik dosyalarda değişiklik tespiti
03	Vulnerability Detection	CVE bazlı zafiyet keşfi ve envanteri
04	Security Configuration Assessment	CIS benchmark bazlı sertleştirme denetimi
05	Intrusion Detection	Kural tabanlı saldırı tespiti

№	YETENEK	ANA KULLANIM
06	Active Response	Otomatik müdahale ve karantina
07	Regulatory Compliance	PCI, HIPAA, GDPR, NIST dashboard'ları
08	Cloud Security Monitoring	AWS, Azure, GCP, M365 entegrasyonu
09	Container Security	Docker ve Kubernetes görünürlüğü
10	MITRE ATT&CK Mapping	Saldırı tekniklerinin otomatik eşleştirilmesi
11	Threat Intelligence	IOC eşleştirme ve CTI entegrasyonu

2.1 Log Data Collection

Wazuh'un en temel yeteneği, izlenen sistemlerden log verilerini toplamak ve merkezi bir noktada birleştirmektir. Platform; Linux ve Windows işletim sistemi log'ları, uygulama log'ları, syslog formatında gelen network cihazı log'ları ve JSON formatındaki modern uygulama log'ları dahil olmak üzere çok geniş bir veri kaynağı yelpazesini destekler. Toplanan log'lar önce decoder'lar ile yapısal alanlara ayrılır, ardından kural motoruna gönderilir.

Log collection kapasitesi, bir SIEM ürününün omurgasıdır. Çünkü hem adli bilişim süreçlerinde geriye dönük inceleme için, hem compliance denetimlerinde kayıt delili olarak, hem de gerçek zamanlı tespit için temel veri kaynağıdır.

2.2 File Integrity Monitoring

File Integrity Monitoring, kritik dosya ve dizinlerde meydana gelen değişikliklerin tespiti için kullanılan bir tekniktir. Wazuh FIM modülü; dosya oluşturma, değiştirme ve silme olaylarını yakalar, bu değişiklikleri kim tarafından ve hangi process ile yapıldığını raporlar. Bu yetenek özellikle sistem dosyaları, web kök dizinleri, veritabanı konfigürasyon dosyaları ve PCI-DSS kapsamındaki ödeme uygulamaları için kritiktir.

FIM iki farklı modda çalışabilir. Periyodik tarama modu belirli aralıklarla tüm izlenen dizinleri karşılaştırır. Gerçek zamanlı mod ise OS-level event'leri dinleyerek değişiklikleri anında yakalar ve değişikliği yapan kullanıcı ile process bilgisini de kaydeder. Bu; ransomware tespiti, insider threat analizi ve compliance raporlamada büyük değer taşır.

2.3 Vulnerability Detection

Wazuh Vulnerability Detection modülü; izlenen her sistem üzerindeki yüklü paketleri envanter olarak çıkarır ve bu envanteri uluslararası güvenlik açığı veritabanları (NVD, Red Hat OVAL, Microsoft MSU, Debian Security Tracker, Ubuntu Security Notices, Amazon Linux Security Center ve Arch Linux Security Tracker) ile eşleştirir. Sonuç olarak her sistem için bir CVE listesi üretir ve bu listeyi zaman içinde günceller.

Klasik vulnerability scanner'ların aksine Wazuh'un yaklaşımı agent tabanlıdır. Bu; bir VPN arkasındaki çalışanın laptop'unun da, bir DMZ'deki sunucunun da, hatta bir Kubernetes node'unun da sürekli izlenebileceği anlamına gelir. Tarama için bir zaman penceresi beklemek gerekmez; agent'ın envanter verisi her güncellemesinde otomatik olarak CVE eşleştirmesi tetiklenir.

2.4 Security Configuration Assessment

Security Configuration Assessment (SCA), izlenen sistemlerin güvenlik sertleştirme kontrollerinden geçip geçmediğini denetleyen modüldür. Wazuh; CIS benchmark'larını Ubuntu, RHEL, Debian, Amazon Linux, Windows 10/11, Windows Server ve macOS için kutudan hazır olarak sunar. Her sistem yüzlerce check üzerinden skorlanır; geçen ve kalan check'ler ayrı ayrı raporlanır ve iyileştirme önerileri otomatik olarak üretilir.

SCA'nın değeri; bir kurumun güvenlik duruşunu rakam olarak ölçülebilir hale getirmesidir. Linux sunucularımızın yüzde kaçı CIS Level 1 benchmark'ına uygun sorusu, SCA olmadan cevaplanamaz. Ek olarak; kurum kendi iç güvenlik politikasını custom policy olarak yazabilir ve Wazuh bu politikayı da tüm filoya uygular.

2.5 Intrusion Detection ve Rule Engine

Wazuh'un kural motoru; gelen tüm log'ları ve event'leri binlerce önceden tanımlı kural karşısında değerlendirir. Varsayılan ruleset brute-force login denemelerinden web saldırılarına, privilege escalation denemelerinden şüpheli process çalıştırmalara kadar geniş bir yelpazede tespit yapar. Her kural bir seviye (1-15) ile etiketlenir; seviye 12 ve üzeri kurallar kritik olarak işaretlenir ve otomatik olarak email veya SOAR entegrasyonunu tetikleyebilir.

Kural motorunun en güçlü yanı, özelleştirilebilir olmasıdır. Her kurum kendi custom kurallarını yazabilir, mevcut kuralları kendi ortamına göre tune edebilir ve MITRE ATT&CK framework'ü ile otomatik olarak eşleştirebilir. Bu esneklik, Wazuh'u sabit kurallara mahkum olan ticari ürünlerin önüne geçiren en önemli farklılıklardan biridir.

2.6 Active Response

Active Response; bir kural tetiklendiğinde otomatik olarak bir eylemin çalıştırılması yeteneğidir. Tipik örnekler: brute-force saldırısı tespit edildiğinde kaynak IP'nin firewall'da otomatik olarak bloklanması, şüpheli bir process tespit edildiğinde sonlandırılması, bir kullanıcı hesabı risk sinyali verdiğinde otomatik olarak disable edilmesi. Active Response, Wazuh'un Response harfini temsil eder ve platformu salt bir tespit aracından, bir müdahale aracına dönüştürür.

2.7 Regulatory Compliance

Wazuh her kural ve her SCA check'i için regulatory compliance mapping'i taşır. Bir kural fire ettiğinde, ilgili compliance standartları otomatik olarak alert metadata'sına eklenir. Bu sayede dashboard'da her standart için ayrı bir görünüm sunulur; bir denetçi PCI DSS 10.2.4 kontrolünün nasıl uygulandığını sorduğunda, ilgili ekran hazırdır.

2.8 Cloud Security Monitoring

Modern kurumsal altyapı artık tamamen on-premises değildir. Çoğu kurumda workload'ların önemli bir kısmı AWS, Azure veya GCP üzerinde çalışır; kullanıcı kimlik yönetimi Microsoft 365 üzerinden yapılır; çeşitli SaaS uygulamaları kurumsal verinin büyük bir kısmını tutar. Wazuh bu servislerle native entegrasyonlar sunar.

Bu cloud entegrasyonları sayesinde güvenlik ekipleri; on-premises log'larını ve cloud log'larını aynı dashboard'da, aynı arama dili ile ve aynı kural motoru içinde inceleyebilir. Bu; olay müdahalesi sırasında bir saldırganın on-prem'den cloud'a veya tersine hareketini izlemenin tek yoludur.

2.9 Container Security

Container ve Kubernetes ortamları, klasik endpoint izleme yaklaşımlarından farklı bir model gerektirir. Wazuh; Docker daemon event'lerini, Kubernetes audit log'larını ve container image güvenlik bilgilerini yakalar. DaemonSet pattern ile her Kubernetes node'una bir agent deploy edilir ve o node üzerinde çalışan tüm workload'lar izlenir. Sidecar pattern ise daha izole senaryolar için kullanılır.

2.10 MITRE ATT&CK Mapping

MITRE ATT&CK; siber saldırı tekniklerinin standartlaştırılmış bir katalogudur. Wazuh ruleset'indeki her kural, ilgili ATT&CK tekniklerine otomatik olarak eşleştirilmiştir. Bu sayede bir saldırı zinciri oluştuğunda; güvenlik ekibi olayı hangi tekniklerin gerçekleştirildiği açısından hızlıca görebilir ve

kalan saldırı adımlarını tahmin edebilir. Dashboard'da özel bir ATT&CK görselleştirmesi; saldırganların hangi teknikleri ne sıklıkla kullandığını heat map olarak sunar.

2.11 Threat Intelligence

Wazuh 4.13 ile birlikte platform, hazır tehdit istihbaratı listeleri ile gelmeye başladı. Bilinen kötü niyetli IP adresleri, domain'ler ve dosya hash'leri CDB list olarak platform içinde sunulur ve kurallar bu listelere referans verebilir. Ek olarak; kurum kendi CTI beslemelerini (MISP, OTX AlienVault, ticari feed'ler) entegre edebilir.

03

BÖLÜM

Mimari Genel Bakış

Bileşenler, veri akışı ve iç tasarım

Wazuh platformu dört temel bileşenden oluşur. Bu bileşenler küçük ortamlarda tek bir sunucuda birlikte, büyük ortamlarda ise ayrı kümelerde yatay ölçeklenmiş olarak çalışabilir.

Bu bölüm mimari bileşenleri, bileşenler arası veri akışını ve platformun nasıl büyüdüğünü anlatır. Mimari kavrayışı; doğru deployment modelini seçmenin ve operasyonel sorunları erken teşhis etmenin temelidir.

3.1 Temel Bileşenler

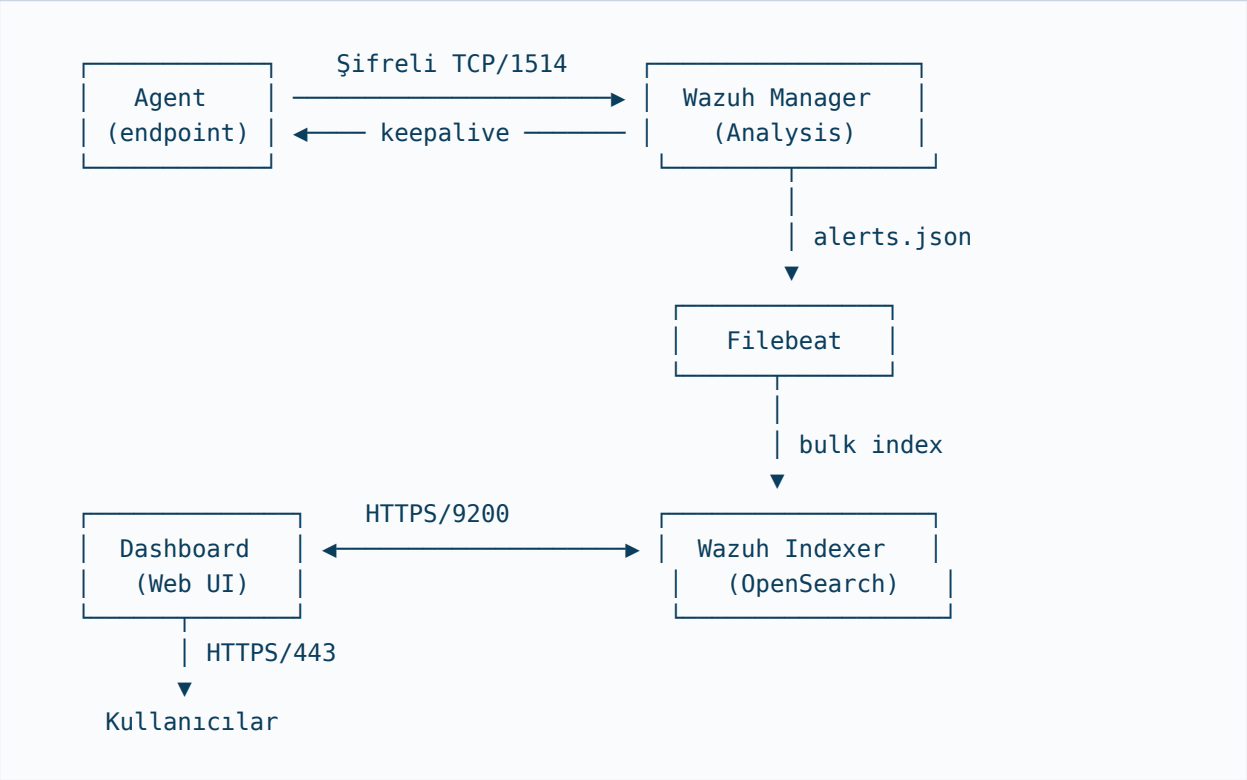
Wazuh dağıtımı dört ana bileşenden oluşur. Her bileşenin net bir sorumluluğu vardır ve bağımsız olarak ölçeklenebilir.

BILEŞEN	GÖREV	ÖLÇEKLENME
Wazuh Agent	Endpoint üzerinde log toplar, FIM ve envanter yapar	Endpoint başına 1 agent
Wazuh Manager	Veriyi decode eder, kural motorunu çalıştırır	Master/worker cluster
Wazuh Indexer	Alarm ve inventory verisini indeksler, arama sağlar	Multi-node cluster

BİLEŞEN	GÖREV	ÖLÇEKLENME
Wazuh Dashboard	Görselleştirme, sorgulama ve yönetim arayüzü	Tek veya çoklu instance

3.2 Veri Akışı

Platformun çalışma mantığını kavramanın en iyi yolu, bir log olayının agent'tan dashboard'a kadar izlediği yolu takip etmektir. Aşağıdaki şema bu akışı özetler.



Şekil — Wazuh platformunda bir olayın agent'tan dashboard'a yolculuğu

Akışın her adımı bağımsız bir sorumluluk taşır. Agent yalnızca veri toplama ve iletme ile ilgilenir; Manager tüm analiz ve kural motorunu çalıştırır; Indexer arama ve saklama ile, Dashboard ise sunum ile ilgilenir. Bu ayrım sayesinde herhangi bir katmanın yükü arttığında; sadece o katman yatay olarak büyütülebilir.

3.3 Agent Mimarisi

Wazuh agent, izlenen her sistem üzerine kurulan hafif bir yazılımdır. Linux, Windows, macOS, AIX, Solaris ve HP-UX dahil olmak üzere çok geniş bir işletim sistemi yelpazesini destekler. Agent; log toplama, dosya bütünlüğü izleme, rootkit tespiti, yapılandırma denetimi, envanter çıkarma ve active response modüllerini tek bir process altında çalıştırır. CPU ve bellek tüketimi oldukça düşüktür; tipik bir endpoint'te yüzde bir civarında CPU ve 50-100 MB bellek kullanır.

Agent ve manager arasındaki tüm iletişim AES tabanlı simetrik şifreleme ile korunur. Her agent benzersiz bir key ile enroll olur ve manager bu key üzerinden agent'ın kimliğini doğrular. Bu model; ortadaki adam saldırılarına karşı dayanıklıdır ve agent'ın manager'a bağlandığı hat ne olursa olsun (açık internet dahil) güvenli bir kanal sağlar.

3.4 Manager Mimarisi

Wazuh Manager, platformun beynidir. İç yapısında birden fazla daemon çalışır: wazuh-remoted agent bağlantılarını karşılar, wazuh-analysisd decoder ve kural motorunu yürütür, wazuh-modulesd çeşitli zenginleştirme modüllerini çalıştırır, wazuh-db agent state verisini tutar, wazuh-authd yeni agent enrollment'larını yönetir ve wazuh-apid yönetim API'sini sunar.

Büyük ortamlarda tek bir manager yetersiz kalır. Bu durumda master-worker topolojisi kullanılır: bir master node konfigürasyonun kaynağı olarak çalışır, bir veya daha fazla worker node ise agent yükünü master ile paylaşır. Ruleset değişiklikleri yalnızca master üzerinde yapılır ve otomatik olarak worker'lara senkronize edilir.

3.5 Indexer Mimarisi

Wazuh Indexer, OpenSearch tabanlı bir arama ve depolama motorudur. Manager tarafından üretilen alarmlar; Filebeat aracılığıyla Indexer'a gönderilir ve burada indekslenir. Indexer tek node veya çoklu node cluster olarak çalışabilir. Çoklu node yapısı; hem arama performansını artırır hem de replica shard mekanizması sayesinde veri kaybına karşı koruma sağlar.

Indexer'ın veri modeli tarih bazlı indekslerden oluşur. Her gün yeni bir index yaratılır ve eski indeksler ISM policy'lerine göre otomatik olarak silinir veya arşivlenir. Bu; disk kullanımının öngörülebilir olmasını ve uzun dönemli saklama stratejilerinin kolayca uygulanmasını sağlar.

3.6 Dashboard Mimarisi

Wazuh Dashboard, OpenSearch Dashboards tabanlı bir web arayüzüdür. Kullanıcılar bu arayüz üzerinden alarm akışını izler, geçmiş olayları sorgular, envanter ve vulnerability raporlarını görüntüler, agent'ları yönetir ve kendi özel dashboard'larını oluşturabilir. Dashboard SAML, OpenID

Connect, LDAP ve Active Directory ile entegre olarak kurumsal kimlik yönetim sistemlerine bağlanabilir. Multi-tenancy özelliği sayesinde MSSP ve partner senaryolarında tek bir dashboard üzerinden birden fazla müşteri verisi izole olarak sunulabilir.

04

BÖLÜM

Deployment Modelleri

Ölçeklenebilirlik ve topoloji seçenekleri

Wazuh; 10 endpoint'ten 100.000 endpoint'e kadar farklı ölçeklerde dağıtılabilir. Seçilecek mimari; izlenecek endpoint sayısına, günlük üretilen alarm hacmine ve beklenen yüksek erişilebilirlik seviyesine göre değişir.

Bu bölüm dört temel deployment modelini ve her birinin hangi senaryoya uygun olduğunu açıklar.

4.1 All-in-One Kurulum

All-in-one modelde Manager, Indexer, Dashboard ve Filebeat tek bir sunucu üzerinde çalışır. POC ortamları, küçük ölçekli kurulumlar ve test ortamları için en hızlı yoldur. Hızlı kurulum ve düşük operasyonel maliyet avantajı sunar; ancak yüksek erişilebilirlik sağlamaz ve tek bir donanım arızasında tüm görünürlük kesilir.

4.2 Distributed Kurulum

Distributed modelde her bileşen kendi sunucusu üzerinde çalışır ancak henüz yatay ölçekleme yoktur. 100 ile 500 arası endpoint ölçeğinde ve kaynak ayrımı isteyen kurulumlar için uygundur. Bileşenler kaynak yarışmaz; her birinin CPU, RAM ve disk ihtiyacı bağımsız olarak planlanabilir. Bu model; ileride cluster'a geçişi kolaylaştıran bir ara basamaktır.

4.3 Manager Cluster ve Load Balancer

500 ile 2000 arası endpoint ölçeğinde en sık tercih edilen modeldir. Bir master ve bir veya daha fazla worker manager, bir load balancer arkasında çalışır. Agent'lar load balancer üzerinden bağlanır ve trafikleri manager'lar arasında dağıtılır. Bu yapı; manager tarafında yüksek erişilebilirlik, rolling upgrade ve bakım sırasında alarm akışının kesilmemesi gibi kritik operasyonel avantajlar sağlar.

4.4 Tam Yüksek Erişilebilirlik

En büyük ortamlar için kullanılan tam yüksek erişilebilirlik mimarisidir. Hem manager katmanı hem de indexer katmanı çoklu node olarak çalışır. 2000 ve üzeri endpoint'lerde standart seçimdir. Indexer cluster'ı en az üç node'dan oluşur; replica shard'lar sayesinde bir node kaybedilse dahi cluster green durumunda kalır ve veri kaybı yaşanmaz.

4.5 Karşılaştırma

KRITER	ALL-IN-ONE	DISTRIBUTED	CLUSTER + LB	TAM HA
Önerilen endpoint	≤ 100	100—500	500—2000	2000+
Sunucu sayısı	1	3	4—5	6+
Toplam vCPU	8	16	24+	40+
Toplam RAM	16 GB	32 GB	56 GB	120 GB+
HA seviyesi	Yok	Yok	Manager HA	Tam HA
Rolling upgrade	Hayır	Hayır	Evet	Evet

DOĞRU MODEL SEÇIMI

Seçilen deployment modeli; platformun ilerleyen yıllardaki operasyonel maliyetini ve esnekliğini belirler. Az kaynakla kurulan bir mimari birkaç ay içinde darboğaza girer; aşırı kaynakla kurulan bir mimari ise gereksiz maliyet üretir. Rint Bilgi Teknolojileri her müşteri için bu seçimi mevcut endpoint envanteri, büyüme projeksiyonu ve SLA gereksinimleri üzerinden özel olarak planlar.

05

BÖLÜM

Desteklenen Ortamlar

İşletim sistemleri, bulut ve container'lar

Modern bir kurumsal altyapıda tek bir işletim sistemi veya tek bir platform nadiren yeterli olur. Çoğu kurum; Windows sunucular, Linux sunucular, Kubernetes cluster'ları, AWS veya Azure workload'ları ve çeşitli SaaS uygulamalarını aynı anda kullanır.

Wazuh bu çeşitliliği desteklemek üzere tasarlanmıştır. Bu bölüm platformun desteklediği ortamları özetler.

5.1 İşletim Sistemleri

Wazuh agent; aşağıdaki işletim sistemlerinde native olarak desteklenir. Agent paketleri resmi repository üzerinden imzalı olarak dağıtılır ve standart paket yöneticileri ile kurulabilir.

PLATFORM	DESTEKLENEN SÜRÜMLER
Red Hat Enterprise Linux	RHEL 7, 8, 9 — Rocky, Alma, Oracle Linux türevleri dahil
Ubuntu	18.04, 20.04, 22.04, 24.04 LTS
Debian	10, 11, 12
Amazon Linux	2 ve 2023

PLATFORM	DESTEKLENEN SÜRÜMLER
SUSE Linux	SLES 12, 15
Windows Server	2012 R2, 2016, 2019, 2022, 2025
Windows Client	10, 11
macOS	11 (Big Sur) ve üzeri
AIX	7.1, 7.2, 7.3
Solaris	11

5.2 Bulut Platformları

Wazuh, büyük bulut sağlayıcılarıyla yerel entegrasyonlara sahiptir. Bu entegrasyonlar iki yönlüdür: hem bulut sağlayıcısının audit ve aktivite log'larını çekmek, hem de bulut üzerindeki workload'lara agent deploy etmek.

SAĞLAYICI	DESTEKLENEN SERVISLER
Amazon Web Services	CloudTrail, GuardDuty, VPC Flow, WAF, Inspector, CloudWatch, S3 Access, ALB
Microsoft Azure	Activity Log, Sign-in Log, Audit Log, Security Center, Log Analytics
Google Cloud Platform	Cloud Audit Logs (Admin, Data Access, System Event), Pub/Sub ingest
Microsoft 365	Unified Audit, Exchange, SharePoint, Teams, Entra ID, DLP events

5.3 Container ve Orchestration

Wazuh, modern konteyner altyapılarını izlemek için özelleşmiş deployment pattern'leri sunar. Docker Engine ve Kubernetes ortamları için DaemonSet, Sidecar ve StatefulSet deployment modelleri ile hem node seviyesinde hem de workload seviyesinde izleme mümkündür.

PLATFORM	DESTEK ŞEKLI
Docker Engine	Native wodle, daemon events, container inventory
Kubernetes	DaemonSet, Sidecar, StatefulSet pattern'leri, audit ingest
OpenShift	Kubernetes pattern'leri, Red Hat resmi destek
Amazon EKS	IRSA ile native entegrasyon, CloudWatch köprüsü
Azure AKS	Azure Monitor entegrasyonu ile birlikte
Google GKE	Cloud Audit Logs ve Pub/Sub üzerinden

06

BÖLÜM

Entegrasyonlar

SIEM, SOAR, kimlik yönetimi ve API

Wazuh'un en güçlü yönlerinden biri, mevcut güvenlik ekosistemine kolayca entegre olabilmesidir.

Platform; kurum içindeki ticketing sistemleriyle, SOAR çözümleriyle, tehdit istihbaratı platformlarıyla, ITSM araçlarıyla ve kimlik yönetim sistemleriyle native veya esnek API üzerinden bağlantı kurar. Bu bölüm başlıca entegrasyon alanlarını özetler.

6.1 SIEM ve SOAR Entegrasyonları

Wazuh'un kendisi bir SIEM olarak kullanılabilir; ancak bazı kurumlar halihazırda bir SIEM yatırımı yapmış olabilir. Bu durumda Wazuh; detection katmanı olarak konumlanır ve ürettiği alarmları mevcut SIEM'e forward edebilir. Aynı zamanda müdahale katmanı için SOAR ürünleriyle entegre çalışabilir ve otomatik playbook'lara tetikleyici olarak hizmet verir.

KATEGORI	DESTEKLENEN ÜRÜNLER
SIEM Forward	Splunk, IBM QRadar, LogRhythm, Microsoft Sentinel, Elastic SIEM
SOAR	Shuffle, TheHive, Cortex, Palo Alto XSOAR, Tines, Splunk SOAR

KATEGORI	DESTEKLENEN ÜRÜNLER
Ticketing	Jira, ServiceNow, Zendesk, Freshdesk (webhook üzerinden)
Notification	Slack, Microsoft Teams, PagerDuty, Opsgenie, email, SMS
Threat Intel	MISP, OTX AlienVault, VirusTotal, AbuseIPDB, ticari CTI feed'leri

6.2 Kimlik ve Erişim Yönetimi

Wazuh Dashboard; OpenSearch Security plugin üzerinden çeşitli kimlik sağlayıcıları ile entegre olabilir. SAML 2.0, OpenID Connect, LDAP ve Active Directory protokolleri native olarak desteklenir. Bu sayede Okta, Azure Entra ID, Keycloak, OneLogin, Auth0 ve Google Workspace gibi kurumsal kimlik sağlayıcılarla Single Sign-On kurulabilir. Role-Based Access Control sayesinde farklı kullanıcı gruplarına farklı yetki seviyeleri verilebilir.

6.3 Vulnerability ve CTI Feed'leri

Vulnerability Detection modülü; birden fazla resmi CVE kaynağından beslenir: National Vulnerability Database, Red Hat OVAL, Microsoft Security Update, Debian Security Tracker, Ubuntu Security Notices, Amazon Linux Security Center, Arch Linux Security Tracker ve SUSE. Bu feed'ler Wazuh CTI platformu üzerinden otomatik olarak çekilir ve güncel tutulur. Air-gapped ortamlar için offline feed senkronizasyonu da desteklenir.

6.4 Custom Entegrasyonlar ve API

Wazuh Manager, RESTful bir API sunar. Bu API üzerinden; agent yönetimi, group yönetimi, custom rule deployment, alarm sorgulama, RBAC yapılandırması ve çok daha fazlası programatik olarak yapılabilir. Bu; mevcut CI/CD pipeline'larına entegrasyon, custom monitoring araçlarına veri besleme ve multi-cluster senkronizasyonu gibi gelişmiş senaryoları mümkün kılar. API dokümantasyonu OpenAPI standardında sunulur ve bir geliştirici ekibi saatler içinde entegrasyon yazabilir.

07

BÖLÜM

Uyumluluk Kapsamı

PCI, HIPAA, GDPR, KVKK, ISO 27001, NIST

Modern bir güvenlik platformunun değeri yalnızca tehditleri yakalamasıyla ölçülmez; aynı zamanda kurumun tabi olduğu yasal ve sektörel düzenlemelere uyumu kanıtlamasıyla da ölçülür.

Wazuh bu açıdan güçlü bir konumdadır: varsayılan ruleset ve SCA check'leri, büyük uluslararası uyum standartlarıyla önceden eşleştirilmiştir. Bu eşleştirme sayesinde bir denetim esnasında PCI DSS 10.2.4 kontrolüne dair kanıtınız nerede sorusuna birkaç tıkla yanıt verilebilir.

7.1 Desteklenen Standartlar

STANDART	KAPSAM	NOTLAR
PCI DSS 4.0	Ödeme kartı verisi koruması	BKM ve bankalar için geçerli
HIPAA	ABD sağlık verisi koruması	KVKK sağlık hükümleriyle örtüşür
GDPR	AB kişisel veri koruması	KVKK ile ilkeler paralel
KVKK	Türkiye kişisel veri koruması	GDPR çerçevesi üzerinden

STANDART	KAPSAM	NOTLAR
ISO 27001	Bilgi güvenliği yönetim sistemi	Sertifikasyon denetimleri
NIST 800-53	ABD federal güvenlik kontrolleri	Savunma ve kamu projeleri
SOC 2 (TSC)	Service organization trust criteria	SaaS sağlayıcıları
CIS Benchmarks	İşletim sistemi sertleştirme	Tüm SCA politikalarının temeli

7.2 KVKK Özelinde Wazuh'un Rolü

Türkiye'de faaliyet gösteren kurumlar için KVKK uyumu yasal bir zorunluluktur. Wazuh; KVKK'nın teknik ve idari tedbirler başlığı altında istenen birçok kontrolü doğrudan destekler. Erişim log'larının tutulması ve düzenli olarak denetlenmesi, kişisel veri içeren dosyalara yapılan değişikliklerin izlenmesi, yetkisiz erişim girişimlerinin tespit edilmesi ve veri ihlali durumunda 72 saat içinde yapılması gereken bildirim için gerekli delil toplama; bunların hepsi Wazuh üzerinden gerçekleştirilebilir.

Ek olarak; KVKK'nın veri sorumlusu kavramı kapsamında kurumların kişisel veri işleme envanterini güncel tutması ve işleme faaliyetlerini denetlenebilir kılması gerekir. Wazuh'un envanter ve audit log yetenekleri, bu tür bir kayıt rejiminin teknik temelini sağlar.

7.3 Otomatik Compliance Dashboard'ları

Wazuh Dashboard; desteklenen her uyum standardı için ayrı bir görsel sunum sağlar. PCI DSS dashboard'u; kart sahibi verisi erişimi, başarısız login denemeleri, konfigürasyon değişiklikleri ve antivirüs durumunu tek bir ekranda özetler. Aynı mantık HIPAA, GDPR ve NIST için de geçerlidir. Bu dashboard'lar; denetim ziyaretleri sırasında denetçilere gösterilebilen hazır raporlardır.

08

BÖLÜM

Güvenlik ve Veri Yönetimi

Şifreleme, yetkilendirme ve backup

Bir güvenlik platformunun kendisi; izlediği sistemler kadar güvenli olmalıdır. Wazuh, bu prensibi tasarımın merkezine alır.

Tüm bileşenler arası iletişim şifrelidir, kimlik doğrulama zorunludur ve hassas verilerin erişim kontrolü granüler olarak yapılandırılabilir. Bu bölüm platformun güvenlik mimarisini ve veri yönetimi yaklaşımını özetler.

8.1 Şifreleme ve Sertifika Yönetimi

Wazuh bileşenleri arasındaki tüm trafik şifrelidir. Agent ile manager arasındaki iletişim AES-256 tabanlı simetrik şifreleme ile korunur; manager ile indexer arasındaki trafik TLS 1.3 üzerinden gerçekleşir; dashboard ile indexer arasındaki sorgular da TLS ile korunur. Sertifikalar; kurulum sırasında otomatik olarak üretilen bir iç CA ile imzalanır veya kurumun kendi PKI altyapısı ile değiştirilebilir.

8.2 Kimlik Doğrulama ve Yetkilendirme

Platform iki katmanlı bir yetkilendirme modeli kullanır. Birinci katman Wazuh Server RBAC'tir ve manager API'si üzerindeki izinleri yönetir: hangi kullanıcı hangi agent'ı listeler, hangi group'u değiştirebilir, hangi rule'u deploy edebilir. İkinci katman OpenSearch Security'dir ve indexer tarafındaki document-level security, index pattern ve dashboard izinlerini yönetir. İki katmanın

birlikte kullanılması; MSSP ve çok-tenant senaryolarında müşteri verilerinin birbirinden izole edilmesini sağlar.

8.3 Veri Saklama ve Retention

Wazuh; toplanan verilerin ne kadar süreyle saklanacağını belirleyen esnek policy'ler sunar. ISM ile eski indeksler otomatik olarak silinebilir, arşive taşınabilir veya cold storage'a gönderilebilir. Bu; hem disk maliyetlerini kontrol altında tutar hem de KVKK gibi regülasyonların gerektirdiği gereği olduğundan daha uzun süre saklama yasağına uyumu sağlar.

8.4 Backup ve Disaster Recovery

Wazuh; hem konfigürasyon hem de veri katmanında backup stratejilerini destekler. Konfigürasyon dosyaları (manager ayarları, custom rule'lar, sertifikalar, agent key'leri) tar arşivi olarak düzenli yedeklenebilir. Veri katmanında; OpenSearch snapshot repository'si üzerinden filesystem, S3, Azure Blob veya GCS hedeflerine otomatik snapshot alınabilir. Bu snapshot'lar; disaster recovery senaryolarında yeni bir ortama hızlıca restore edilebilir ve RPO/RTO hedefleri karşılanabilir.

09

BÖLÜM

Hizmet Modeli

Üç hizmet seviyesi ve mühendislik ekibi

Wazuh yazılımı açık kaynak olarak ücretsizdir; ancak bir platformun kurumsal kalitede operasyonu, özel uzmanlık ve sürekli mühendislik emeği gerektirir.

Rint Bilgi Teknolojileri, Türkiye'nin Wazuh Platinum Partner'ı olarak; platformun yaşam döngüsünün her aşamasında müşterilerine eşlik eder. Bu bölüm sunulan üç temel hizmet seviyesini ve her birinin kapsamını ayrıntılı olarak açıklar.

9.1 Üç Hizmet Seviyesi

Her kurumun Wazuh platformundan beklentisi ve iç kapasitesi farklıdır. Bazı kurumlar yalnızca platformu kurulu ve çalışır halde teslim almak ister; bazıları kurulumun ötesinde platformun sürekli izlenmesini bekler; bazıları ise platformun yanı sıra gerçek bir SOC hizmeti almak, güvenlik olaylarına 7/24 müdahale edilmesini talep eder.

Rint Bilgi Teknolojileri bu üç farklı ihtiyacı üç net hizmet seviyesi altında sunar:

SEVİYE	İSİM	KAPSAM
I	Kur ve Teslim Et	Mimari tasarım, kurulum, entegrasyon, kabul testi, eğitim, dokümantasyon

SEVIYE	İSIM	KAPSAM
II	Kur ve İzle	Seviye I'in tamamı + günlük bakım, haftalık tuning, aylık raporlama, 7/24 destek
III	Tam SOC Hizmeti	Seviye II'nin tamamı + 7/24 alarm takibi, aktif savunma, olay müdahalesi

> *Rint Bilgi Teknolojileri yalnızca bir kurulum partneri değildir. On'dan fazla aktif mühendisten oluşan ekip; bugün birden fazla müşteriye günlük bakım, raporlama ve aktif savunma hizmeti veriyor.*

9.2 Seviye I — Kur ve Teslim Et

Bu model; Wazuh platformunu kuruma anahtar teslim şekilde teslim etmeyi amaçlar. Rint Bilgi Teknolojileri ekibi ihtiyaç analizi yapar, doğru mimariyi tasarlar, tüm bileşenleri kurar, mevcut sistemlerle (Active Directory, firewall, ticketing, SIEM) entegre eder, kabul testini gerçekleştirir ve müşteri ekibine kullanıcı ve yönetici eğitimi verir. Kurulum süreci sonunda müşteri çalışan bir platform, ayrıntılı bir as-built dokümantasyonu, ilk ay için runbook ve eğitim materyallerini alır.

Bu modelde operasyonel sorumluluk tamamen müşteri ekibine devredilir; ancak Rint Bilgi Teknolojileri garanti süresi boyunca teknik destek sağlamaya devam eder. Kur ve Teslim Et modeli özellikle kendi içinde güçlü bir güvenlik ekibi bulunan kurumlar için uygundur.

9.3 Seviye II — Kur ve İzle

İkinci seviye; kurulumun ötesinde platformun sağlığının sürekli olarak Rint Bilgi Teknolojileri tarafından izlenmesini ve bakımının yapılmasını içerir. Günlük rutin kontroller (servis durumu, disk kullanımı, cluster sağlığı, filebeat akışı), haftalık sağlık raporları, aylık tuning toplantıları ve üç aylık kapasite planlama seansları bu hizmete dahildir.

Bu modelde müşteri ekibi; Wazuh platformunun kendisi ile ilgili hiçbir operasyonel yükü taşımaz. Bunun yerine kendi iç kaynaklarını gerçek güvenlik olaylarına ve kurum içi süreçlere odaklayabilir. Rint Bilgi Teknolojileri, ayda bir detaylı bir yönetici raporu sunar; bu rapor platform sağlık skorlarını, işlenen olay istatistiklerini, üretilen alarm hacmini, top risk kategorilerini ve bir sonraki ay için önerilen iyileştirmeleri içerir.

SEVIYE II'YE DAHIL OLAN HIZMETLER

- Günlük servis sağlığı kontrolü ve proaktif alarm takibi
- Haftalık performans ve kapasite raporu
- Aylık kural tuning ve false positive azaltma çalışması
- Aylık yönetici özet raporu (executive summary)
- Üç aylık health check ve kapasite projeksiyonu
- Wazuh minor sürüm upgrade operasyonları
- 7/24 platform destek ve SLA taahhüdü

9.4 Seviye III — Tam SOC Hizmeti

Üçüncü ve en kapsamlı seviye; Rint Bilgi Teknolojileri'nin bir Security Operations Center partneri olarak konumlandığı modeldir. Bu modelde platform kurulumu ve izlenmesinin yanı sıra, Wazuh tarafından üretilen güvenlik alarmları da Rint Bilgi Teknolojileri ekibi tarafından 7/24 takip edilir. Kritik seviyedeki alarmlar analiz edilir, gerçek tehdit olan olaylar için olay müdahale süreci başlatılır, yanlış pozitifler kural tuning ile temizlenir ve tüm bu süreç müşteriye düzenli raporlarla aktarılır.

Tam SOC hizmetinin en ayırt edici özelliği aktif savunma boyutudur. Rint Bilgi Teknolojileri ekibi yalnızca olayları izlemekle kalmaz; aynı zamanda Wazuh'un Active Response yetenekleri üzerinden otomatik müdahaleler yapılandırır ve bunları müşterinin iç süreçleriyle uyumlu hale getirir. Bu; kurumların kendi SOC'sini kurma maliyetinden kaçınarak, deneyimli bir ekibi doğrudan savunma hattına yerleştirebilmesi anlamına gelir.

SEVIYE III'E DAHIL OLAN EK HIZMETLER

- 7/24 güvenlik alarm takibi ve triaj
- Kritik olayların analizi ve olay müdahale desteği
- Aktif savunma ve Active Response senaryolarının yönetimi
- Tehdit istihbaratı entegrasyonu ve IOC takibi
- Aylık threat landscape raporu
- Adli bilişim ve post-incident analiz desteği
- Tabletop egzersizleri ve kriz tatbikatları
- Compliance denetimlerine teknik kanıt desteği

9.5 Mühendislik Ekibi

Rint Bilgi Teknolojileri'nin sunduğu hizmet kalitesinin temelinde güçlü bir mühendislik ekibi bulunur. On'dan fazla aktif mühendisten oluşan Wazuh operasyon ekibi; bugün birden fazla müşterinin platformunu aynı anda yönetmektedir. Ekip üyeleri Wazuh platformu, OpenSearch, Linux sistem yönetimi, cloud entegrasyonları ve SIEM operasyonu alanlarında sertifikasyonlara ve saha tecrübesine sahiptir.

Ekip yapısı vardiyalı operasyon modeline uygun tasarlanmıştır. Gündüz saatlerinde platformların aktif bakımı, tuning çalışmaları, müşteri toplantıları ve proje aktiviteleri yürütülür. Gece ve hafta sonlarında ise on-call mühendisler kritik alarmları izler ve gerektiğinde müdahale eder. Bu model, Rint Bilgi Teknolojileri'nin yalnızca bir entegratör değil, aynı zamanda bir operasyonel güvenlik sağlayıcısı olarak konumlanmasını mümkün kılar.

9.6 Fiyatlandırma

Rint Bilgi Teknolojileri'nin sunduğu hizmet seviyelerinin fiyatlandırması; kurumun endpoint sayısı, seçilen hizmet seviyesi, beklenen SLA düzeyi ve ek entegrasyon ihtiyaçları gibi çeşitli faktörlere göre belirlenir. Her kurum için özel bir fiyat teklifi hazırlanır; bu teklif ihtiyaç analizi toplantısının ardından detaylı bir kapsam dokümanıyla birlikte sunulur.

FIYAT BILGISI IÇIN İLETIŞIM

Bu whitepaper kapsamında fiyat bilgisi paylaşılmamaktadır. Kurumunuzun ihtiyaçlarına özel bir teklif, kapsam analizi ve hizmet seviyesi önerisi için lütfen Rint Bilgi Teknolojileri pazarlama ekibi ile iletişime geçiniz. İlk değerlendirme toplantısı ücretsizdir ve herhangi bir yükümlülük doğurmaz.

10

BÖLÜM

Neden Rint Bilgi Teknolojileri

Platinum Partner statüsü ve farklılıklar

Wazuh deployment'ı için partner seçimi; yalnızca yazılım bilgisi değil, aynı zamanda saha tecrübesi, ekip derinliği ve uzun vadeli sürdürülebilirlik gerektirir.

Rint Bilgi Teknolojileri'nin Türkiye'deki konumu; bu üç alanın üçünde de belirgin avantajlar sunar.

10.1 Platinum Partner Statüsü

Rint Bilgi Teknolojileri, Wazuh Inc.'in Türkiye'deki resmi Platinum Partner'ıdır. Platinum seviye; Wazuh'un ortak ağındaki en üst yetkinlik seviyesidir ve şu kriterleri karşılamayı gerektirir: minimum sertifikalı mühendis sayısı, yıllık deployment hacmi, müşteri memnuniyet skoru ve Wazuh'a katkıda bulunulan teknik içerik. Platinum Partner, Wazuh engineering ekibi ile doğrudan iletişim kanalına ve escalation önceliğine sahiptir; müşteriler için bu; kritik bir problemde bug fix ve destek taleplerinin hızlı çözüme kavuşması demektir.

10.2 Saha Tecrübesi

Rint Bilgi Teknolojileri; Türkiye'de çeşitli sektörlerden kurumlara Wazuh deployment'ı yapmış ve operasyonel olarak yönetmiştir. Finans, telekom, enerji, kamu, sağlık ve üretim sektörlerinde; KOBİ ölçeğinden on binlerce endpoint'li büyük kurumsal ortamlara kadar farklı büyüklüklerde referans projeler gerçekleştirilmiştir. Bu çeşitlilik; Rint Bilgi Teknolojileri ekibinin karşılaşılabilecek hemen her senaryoya hazır olmasını sağlar.

10.3 Türkçe Destek ve Yerelleşme

Rint Bilgi Teknolojileri'nin tüm teknik ekibi; Türkiye'de konumlu ve Türkçe anadil seviyesinde iletişim sağlar. Bu; özellikle kritik olay müdahalesi sırasında yabancı bir destek ekibi ile İngilizce iletişim kurma zorunluluğunu ortadan kaldırır. Dokümantasyon, raporlar ve eğitim materyalleri Türkçe olarak sunulur. Türkiye'nin regülasyon ortamı (KVKK, BTK, bankacılık ve finans otoriteleri) konusunda yerel bilgi birikimi; global partner'ların sunamadığı bir ek değerdir.

10.4 Bilgi Paylaşımı ve Topluluk

Rint Bilgi Teknolojileri; sahada biriktirdiği tecrübeyi iç dokümantasyon olarak saklamakla yetinmez. Ekip düzenli olarak blog yazıları, konferans sunumları, Türkçe teknik rehberler ve açık kaynak katkıları üretir. Bu şeffaflık; müşterilerin Rint Bilgi Teknolojileri'nin uzmanlığını herhangi bir NDA imzalamadan önce doğrulayabilmesini sağlar.

10.5 Uzun Vadeli Partnerlik

Rint Bilgi Teknolojileri'nin müşteri ilişkilerine yaklaşımı, tek seferlik bir kurulum projesi değil, uzun vadeli bir teknoloji partnerliğidir. Kurulum sonrası ilk yılda müşteri ortamının stabilize olması, ikinci yılda tuning ve optimizasyon, üçüncü yılda ise genişleme ve yeni modül devreye alma gibi doğal bir olgunlaşma eğrisi izlenir. Bu süreç boyunca; çeyreklik business review toplantıları, yıllık strateji gözden geçirmeleri ve platform roadmap paylaşımları gerçekleştirilir.

İLETİŞİM

Bir Sonraki Adım

Kurumunuz için Wazuh platformunun nasıl konumlanabileceğini ve hangi hizmet seviyesinin uygun olduğunu konuşmak için Rint Bilgi Teknolojileri ekibine ulaşabilirsiniz.

rint.com.tr

bilgi@rint.com.tr

0 (216) 801 99 06

A

BÖLÜM

Glossary

Teknik terimler sözlüğü

Whitepaper boyunca kullanılan teknik terimlerin kısa açıklamaları. Konuya yabancı okuyucular için hızlı referans niteliğindedir.

TERIM	AÇIKLAMA
Agent	Endpoint üzerinde çalışan, log toplayan ve manager'a ileten lightweight yazılım
APS	Alerts Per Second — saniyede üretilen alarm sayısı
Active Response	Bir alarm fire olduğunda otomatik çalıştırılan müdahale eylemi
CDB List	Constant Database List; whitelist veya blacklist amaçlı lookup tablosu
CTI	Cyber Threat Intelligence; tehdit istihbaratı
CVE	Common Vulnerabilities and Exposures; standart zafiyet tanımlayıcısı
Dashboard	Kullanıcı arayüzü bileşeni; OpenSearch Dashboards tabanlı
Decoder	Ham log'u yapısal alanlara ayıran tanım

TERIM	AÇIKLAMA
EPS	Events Per Second — saniyede işlenen olay sayısı
FIM	File Integrity Monitoring; dosya bütünlüğü izleme
HIDS	Host-based Intrusion Detection System
Indexer	OpenSearch tabanlı arama ve depolama motoru
IOC	Indicator of Compromise; uzlaşma göstergesi
ISM	Index State Management; eski indeksleri otomatik yönetme policy'si
Manager	Agent'lardan gelen veriyi işleyen merkezi bileşen
MITRE ATT&CK	Saldırı tekniklerinin standart katalog ve framework'ü
PCI DSS	Payment Card Industry Data Security Standard
RBAC	Role-Based Access Control; rol tabanlı erişim kontrolü
SCA	Security Configuration Assessment; güvenlik sertleştirme denetimi
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
Whodata	Dosya değişikliğini kim ve hangi process yaptığını yakalama özelliği
XDR	Extended Detection and Response

B

BÖLÜM

Kaynaklar

Referanslar ve ek okuma

Bu whitepaper'da bahsedilen konularda daha fazla bilgi edinmek isteyen okuyucular için başlıca referanslar.

RESMI WAZUH KAYNAKLARI

- Wazuh resmi dokümantasyonu — documentation.wazuh.com
- Wazuh resmi web sitesi — wazuh.com
- Wazuh GitHub organizasyonu — github.com/wazuh
- Wazuh sürüm notları ve yol haritası — wazuh.com/blog ve GitHub Releases
- Wazuh topluluk forumu — groups.google.com/g/wazuh

UYUM VE REGÜLASYON KAYNAKLARI

- PCI Security Standards Council — pcisecuritystandards.org
- NIST Cybersecurity Framework — nist.gov/cyberframework
- KVKK Kurumu — kvkk.gov.tr
- ISO/IEC 27001 standartları — iso.org
- MITRE ATT&CK framework — attack.mitre.org
- CIS Benchmarks — cisecurity.org

RINT BILGI TEKNOLOJILERI

- Web sitesi — rint.com.tr
- İletişim — bilgi@rint.com.tr
- Telefon — 0 (216) 801 99 06

BELGE SONU