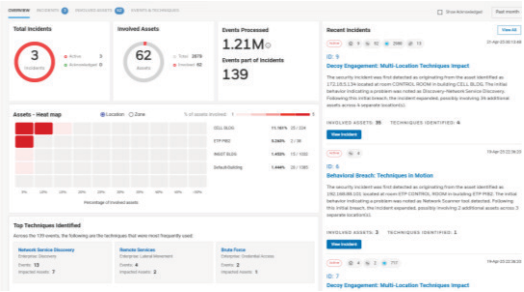
HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE

ÜRÜN BİLGİ NOTU

Honeywell Cyber Proactive Defense, endüstriyel operasyonel teknoloji (OT) ortamlarını giderek artan karmaşıklıktaki ve yapay zekâ destekli siber tehditlere karşı korumak üzere tasarlanmış, ileri teknoloji bir siber güvenlik çözümüdür. Bu gelişmiş platform, potansiyel riskleri tam ölçekli saldırılara dönüşmeden önce proaktif olarak belirlemeye, önceliklendirmeye ve azaltmaya kuruluşlara destek sağlar. Yapay zekâ destekli davranışsal analitiğin entegrasyonu ve Google Threat Intelligence (GTI) tarafından desteklenen Honeywell Cyber Threat Intelligence platformundan yararlanılması sayesinde çözüm; OT sistemlerinin özgün gereksinimlerine uyarlanmış, zenginleştirilmiş ve neredeyse gerçek zamanlı içgörüler ile gelişmiş analitik yetkinlikler sunar.

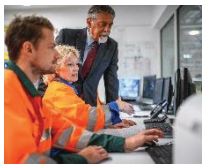


Cyber Proactive Defense'in temel özelliklerinden biri, sistemlerin normal davranışına ilişkin kapsamlı bir baseline oluşturabilme yeteneğidir. Bu sayede kötü niyetli faaliyet göstergesi olabilecek anormallikler erken aşamada tespit edilebilir. Platform ayrıca, ağ içerisinde stratejik olarak konumlandırılan OT decoy (honeypot) bileşenleri devreye alarak deception teknolojisini entegre eder; böylece saldırganlar yanıltılır ve kritik varlıklardan uzaklaştırılır. Buna ek olarak, yapay zekâ destekli incident response playbook'lar tehditlere karşı yapılandırılmış ve akıllı yönlendirme sağlar; kesinti süresini en aza indirir ve hızlı toparlanmayı güvence altına alır.

Honeywell Cyber Proactive Defense, siber analiz süreçlerine derin proses bilgisi entegre ederek ve endüstriyel iş akışlarıyla hizalanarak kuruluşların siber güvenliğe yönelik proaktif ve istihbarat odaklı bir yaklaşım benimsemelerini sağlar; böylece kritik altyapıyı hem mevcut hem de ortaya çıkan tehditlere karşı güçlendirir.

OT SİBER GÜVENLİK DURUŞUNUZ İÇİN PROAKTİF GÖRÜNÜRLÜK ELDE EDİN

Honeywell Cyber Proactive Defense, operasyonel teknoloji (OT) ortamlarını; siber tehditleri operasyonları kesintiye uğratmadan önce öngörerek, tespit ederek ve etkisiz hâle getirerek korumak üzere tasarlanmış ileri görüşlü bir siber güvenlik çözümüdür.
Geleneksel reaktif güvenlik modellerinden farklı olarak Honeywell'in proaktif savunma stratejisi; sürekli izleme, zenginleştirilmiş tehdit istihbaratı ve yapay zekâ destekli analitiği entegre ederek anormalliklerin ve zafiyetlerin siber saldırı zincirinin erken aşamalarında daha etkin şekilde tespit edilmesini sağlar.



Bu proaktif metodoloji, özellikle legacy sistemlerin çoğu zaman yerleşik güvenlik özelliklerinden yoksun olduğu ve kesinti sürelerinin operasyonel, finansal ve güvenlik açısından ciddi sonuçlar doğurabildiği OT ortamlarında kritik öneme sahiptir. Google Threat Intelligence (GTI) tarafından desteklenen Honeywell Cyber Threat Intelligence platformundan yararlanılması sayesinde çözüm; endüstriyel ortamların özgün dinamiklerine uyarlanmış, neredeyse gerçek zamanlı içgörüler ve gelişmiş analitik yetkinlikler sunar.

Ayrıca Honeywell Cyber Proactive Defense, siber analiz süreçlerine derin proses bilgisini entegre eder ve OT honeypot gibi deception teknolojilerini devreye alarak saldırganları yanıltır ve kritik varlıkları korur. Yapay zekâ destekli incident response playbook'lar ise ortaya çıkan tehditlere karşı hızlı ve yapılandırılmış müdahale imkânı sağlayarak dayanıklılığı daha da güçlendirir. Bu kapsamlı ve önleyici yaklaşım sayesinde Honeywell; kritik altyapının korunmasını güçlendirir, operasyonel sürekliliği destekler ve küçük kesintilerin dahi geniş çaplı etkiler yaratabileceği ortamlarda güvenliği muhafaza eder.

PROAKTİF SAVUNMA GENEL KULLANIM SENARYOSU

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE

Karmaşık ve eski nesil bir operasyonel teknoloji (OT) altyapısı işleten bir endüstriyel kuruluş, sofistike tehdit aktörleri tarafından gerçekleştirilen hedefli saldırılar dâhil olmak üzere artan siber güvenlik tehditleriyle karşı karşıya kalmıştır.

Sınırlı siber güvenlik personeli ve OT ağına ilişkin gerçek zamanlı görünürlük eksikliği nedeniyle kuruluş; tehditleri etkin şekilde tespit etmekte, önceliklendirmekte ve müdahale etmekte zorlanmış, bu durum kritik altyapı ve operasyonel sürekliliği riske atmıştır.

Bu zorlukları gidermek amacıyla kuruluş, OT ortamlarını proaktif olarak güvence altına almak üzere tasarlanmış kapsamlı bir çözüm olan Honeywell Cyber Proactive Defense'i devreye almıştır. Yapay zekâ ve makine öğreniminden yararlanan platform, ağ davranışlarını sürekli izleyerek kötü niyetli faaliyet göstergesi olabilecek anormallikleri tespit etmek amacıyla dinamik bir baseline oluşturmuştur. Bu erken tespit kabiliyeti sayesinde tehditler olay seviyesine yükselmeden belirlenebilmiştir.

Uygulama kapsamında ayrıca, stratejik olarak konumlandırılmış OT honeypot'lar gibi deception teknolojileri devreye alınmıştır. Bu yapı, saldırganları yüksek değerli varlıklardan uzaklaştırırken aynı zamanda tehdit aktörlerinin taktikleri hakkında değerli istihbarat sağlamıştır. Bunun yanı sıra, yapay zekâ destekli incident response playbook'lar tehdit azaltma süreçlerini otomatikleştirerek müdahale sürelerini önemli ölçüde kısaltmış ve sınırlı bir güvenlik ekibiyle dahi tutarlı ve etkili aksiyon alınmasını mümkün kılmıştır.

Sonuç olarak kuruluş, operasyonel kesinti yaşamadan birden fazla siber tehdidi başarıyla tespit etmiş ve etkisiz hâle getirmiştir. Otomasyon, gerçek zamanlı tehdit istihbaratı ve proaktif savunma mekanizmalarının entegrasyonu sayesinde güvenlik ekibi güçlü bir güvenlik duruşu sağlamış, dayanıklılığı artırmış ve sınırlı kaynaklarla kritik altyapıyı korumuştur.

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE

ÖZELLİKLER VE FAYDALAR

DECEPTION YETENEĞİ

• OT ağı içerisinde decoy ve tuzak bileşenler konuşlandırarak saldırganları kritik varlıklardan uzaklaştırır.

• Aldatıcı unsurlarla etkileşimleri izleyerek tehditleri erken aşamada tespit eder ve erken uyarı sinyalleri üretir.

• Sistemlerin ifşa edilmesi riskine maruz kalmadan saldırgan davranışları ve taktikleri hakkında tehdit istihbaratı toplar.

YAPAY ZEKÂ VE ML

• Gelişmiş makine öğrenimi modelleri kullanarak ağ ve sistem davranışlarındaki anormallikleri tespit eder.

• Çoklu veri kaynakları arasında desen analizi ve korelasyon yaparak ortaya çıkan tehditleri öngörür.

• Yeni verilerden sürekli öğrenerek savunma mekanizmalarını gerçek zamanlı olarak adapte eder ve tespit doğruluğunu artırır.

YAPAY ZEKÂ DESTEKLİ PLAYBOOK'LAR

• Önceden tanımlanmış ve özelleştirilebilir iş akışları aracılığıyla incident response süreçlerini otomatikleştirir.

• Müdahale süresini saatlerden dakikalara indirerek hızlı containment ve mitigation sağlar.

• Olaylar arasında tutarlı aksiyon alınmasını sağlayarak insan hatasını minimize eder ve operasyonel verimliliği artırır.