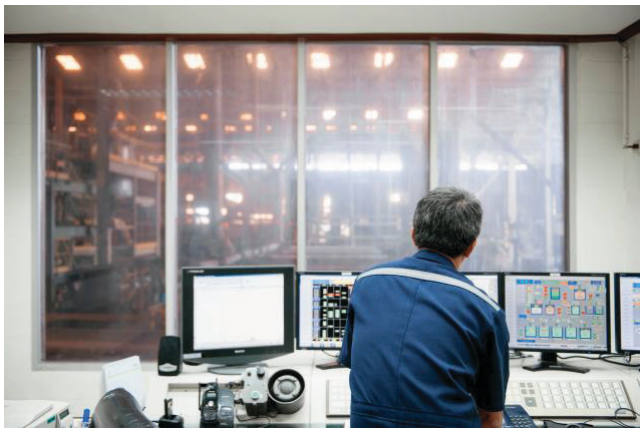
HONEYWELL FORGE Cybersecurity+

HONEYWELL FORGE CYBERSECURITY+ | CYBER INSIGHTS

ÜRÜN BİLGİ NOTU

Endüstriyel varlıkları siber saldırılardan korumak söz konusu olduğunda, bilgi güçtür. Ancak veriyi bilgiye dönüştürmek, özellikle de bilgi teknolojileri (BT) çözümleriyle sınırlı kalındığında, operasyonel teknoloji (EKS) alanındaki birçok kuruluş için hâlâ zorluk teşkil etmektedir. Bu noktada Honeywell Forge Cybersecurity+ Cyber Insights, dünya genelindeki benzersiz EKS ortamlarını daha iyi korumak için EKS siber güvenlik uzmanları tarafından tasarlanmıştır. Gerçek zamanlı varlık, tehdit ve zafiyet verilerine erişim sağlayarak, kuruluşların siber risklerini azaltmalarına ve operasyonlarını kesintisiz sürdürmelerine yardımcı olur.



EKS SİBER GÜVENLİK DURUŞUNUZU DAHA NET GÖRÜN

Cyber Insights, OT ve IoT ağları için en kapsamlı siber güvenlik çözümlerinden biridir. Ağınızdaki tüm varlıkları keşfetmek, envanterini çıkarmak ve tesisinizin siber güvenlik durumuna dair bilinen sömürülebilir zafiyetler ve aktif tehditler dahil tam görünürlük sağlamak için tasarlanmıştır. Ayrıca şüpheli aktiviteleri araştırmanıza yardımcı olur.

AĞINIZA BAĞLI OLAN HER ŞEYİ BİLİN

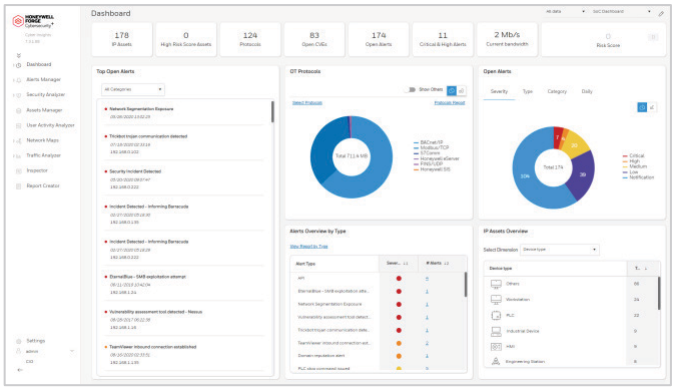
Ağda hangi varlıkların bulunduğunu bilmek, herhangi bir siber güvenlik programı için temel başlangıç noktasıdır. Bu manuel olarak yapılabilir, ancak yeni eklenen cihazları gecikmeden tespit etmek için pratik bir yöntem değildir. Cyber Insights, EKS'ye özel ağ izleme yetenekleriyle yalnızca ilk kurulumda ağınızdaki tüm varlıkların kapsamlı ve doğru envanterini oluşturmakla kalmaz, aynı zamanda ağa yeni eklenen cihazları da tespit eder ve ileri inceleme için uyarı oluşturur. Eğer ağa eklenen cihaz kötü niyetli bir "sahte düğüm" ise, bu uyarılar sayesinde hızlı müdahale operasyonların güvenliği ve sürekliliği üzerindeki olumsuz etkileri önemli ölçüde azaltabilir.

Endüstriyel tesislerdeki bir diğer yaygın zorluk ise kullanım ömrünün sonuna yaklaşan varlıkları takip edebilme yeteneğidir. Cyber Insights, üretici tarafından sağlanan bilgilere dayanarak varlıkların mevcut yaşam döngüsü durumunu ve kullanım ömrü bitiş tarihini görüntüleyerek bu süreci kolaylaştırır. Bu sayede tesisler, yükseltme ve göç (migration) planlarını daha etkin biçimde hazırlayabilir.

TEHDİTLERİ DAHA HIZLI TESPİT EDİN, ZAFİYETLERİ DAHA ETKİLİ YÖNETİN

EKS ortamlarında, kontrolörler ve PLC'ler gibi alt seviye varlıklardan bilgi almak genellikle zordur.
Cyber Insights, bu cihazlarla ilgili verileri pasif ağ izleme veya gerekirse aktif protokol sorgulama yöntemiyle toplamak üzere tasarlanmıştır. Toplanan bu veriler, Ulusal Zafiyet Veritabanı (NVD) ile karşılaştırılır ve öncelikli giderim çalışmaları için anlamlı bilgilere dönüştürülür. Cyber Insights ayrıca tanımlanan zafiyetleri Bilinen Sömürülen Zafiyetler (KEV) listesine göre filtreler, böylece yalnızca aktif tehdit oluşturan zafiyetler önceliklendirilir.

Bu özellik, NVD'den alınan CVSS skorlaması ile birleşerek, EKS siber güvenlik ekiplerinin öncelikli olarak ilgilenmesi gereken en kritik açıkların belirlenmesini sağlar.



Cyber Insights ayrıca topladığı verileri MITRE ATT&CK for EKS çerçevesiyle karşılaştırmak üzere tasarlanmıştır. Bu yaklaşım, gerçek dünyada gözlemlenen saldırı taktik ve teknikleriyle karşılaştırıldığında tesisin mevcut güvenlik durumunu anlamak için değerli bir görünürlük sağlar. Bu sayede, bir olayın yalnızca izole bir olay mı yoksa zincirleme bir saldırının parçası mı olduğu daha kolay tespit edilir. Bir uyarı araştırılırken, Cyber Insights sistem yöneticisine olayın hangi kullanıcı eylemiyle tetiklendiğini izleme imkânı tanır ve aynı zamanda kullanıcının başka hangi faaliyetlerde bulunduğunu da gösterebilir. Honeywell tehdit araştırmacıları, hedefli siber saldırılara karşı tesisleri daha iyi korumak amacıyla sürekli olarak yeni siber tehditleri ve istismar yöntemlerini belirler. Bu tehdit istihbaratı, Cyber Insights'a entegre edilir ve tesislerin EKS siber güvenlik ekiplerine özel olarak düzenlenmiş tehdit bilgileri sağlanır. Bu sayede ekipler, en güncel tehditlerin farkında olarak odaklarını doğru noktalara yöneltebilir.

TESİS İÇİ VE TEDARİKÇİDEN BAĞIMSIZ ÇÖZÜM

Cyber Insights, kontrol ağı üzerinde çalışarak sınırlı veya kurumsal ağa bağlı olmayan tesislerde bile siber güvenlik verileri sağlar. Honeywell Experion® PKS kontrol sistemi üzerinde kullanım için sertifikalıdır. Bu çözüm, Honeywell veya üçüncü taraf cihazlardan gelen ağ trafiğini izleyerek tesis dışına veri çıkarmadan güvenli bilgi akışı sağlar. Bu nedenle Cyber Insights, hem Honeywell sistemlerine hem de farklı tedarikçilerin cihazlarına sahip tesislerde yerinde kullanım (on-premise) için idealdir. Birden fazla tesisin merkezi görünümünü sağlamak isteyen organizasyonlar için, Honeywell Forge Cybersecurity+ | Cyber Watch çözümü eklenebilir. Bu tamamlayıcı çözüm, çok sahalı organizasyonlarda merkezi bir noktadan toplanan verileri birleştirerek kapsamlı bir siber güvenlik görünürlüğü sağlar.

SÜREKLİ DEĞİŞEN TEHDİT ORTAMINDA OPERASYONLARI KORUYUN

EKS ortamlarında tehditler giderek karmaşıklaşmaktadır. Siber tehditleri ve zafiyetleri erken tespit edebilen kuruluşlar, kötü amaçlı yazılım veya güvenlik ihlalleri nedeniyle yaşanabilecek plansız duruş riskini önemli ölçüde azaltır. Anlık siber güvenlik duruşunu bilmek, siber riskleri azaltmak açısından kritik öneme sahiptir. Cyber Insights, bir tesisin varlıklarını, zafiyetlerini ve tehditlerini analiz ederek EKS güvenlik ekiplerine, sistemlerini korumak için ihtiyaç duydukları derinlemesine bilgileri sağlar. Ayrıca, güncel tehdit bilgilerine dayalı olarak düzenli olarak erişilebilen bir kaynak olarak tasarlanmıştır. Bu sayede kullanıcılar, tesisin genel siber güvenlik duruşunu iyileştirmeye odaklanabilir.

HONEYWELL FORGE Cybersecurity+

ÖZELLİKLER VE FAYDALAR

ŞU YETENEKLERİ SAĞLAMAK ÜZERE TASARLANDI

Daha İyi Varlık Yönetimi
Tam otomatik varlık keşfi ve envanterleme sağlayarak, kontrol ağındaki BT ve EKS cihazlarına kapsamlı görünürlük sunmak üzere tasarlanmıştır.
Cihazların yaşam döngüsü (lifecycle) durumlarını ve kullanım ömrü sonu (EOL) bilgilerini de içerir.

Kapsamlı Görünürlük
EKS ağları, iletişim kalıpları ve saldırı vektörleri hakkında görünürlük sağlamak üzere tasarlanmıştır. Tedarikçiden Bağımsız (Vendor Neutral) EKS ortamları için, EKS siber güvenlik uzmanları tarafından geliştirilmiş, yerinde çalışan bağımsız bir çözümdür.

Geliştirilmiş Risk Yönetimi
Siber güvenlik risk yönetimini iyileştirmek ve siber hijyeni artırmak amacıyla, Ulusal Zafiyet Veritabanı (NVD) verilerine dayalı ayrıntılı güvenlik bilgileri ve mevcut zafiyetleri görüntülemek için tasarlanmıştır.

ŞU FONKSİYONLARI SAĞLAMAK ÜZERE TASARLANDI

Tehditlerin ve Anormalliklerin Neredeyse Gerçek Zamanlı Tespiti
İhlal göstergelerini (IOC) pasif olarak tanımlayarak erken saldırı tespiti sağlar.
Ayrıca tesisin ağındaki kullanıcı faaliyetlerini izleyerek olası siber güvenlik tehditlerine karşı erken uyarı oluşturur.

MITRE ATT&CK Çerçevesi
Siber güvenlik olaylarını daha iyi analiz için MITRE ATT&CK for EKS çerçevesine haritalamak üzere tasarlanmıştır.

Hedefe Yönelik Tehdit İstihbaratı
Raporlanmış kötü niyetli aktiviteler hakkında, belirli konumlar, endüstriler ve ekipmanlarla ilişkili özel tehdit istihbaratı sağlamak üzere tasarlanmıştır.

ŞU FAYDALARI SAĞLAMAK ÜZERE TASARLANDI

Esnek Kurulum
Kolay kurulum imkânı sunar; mevcut bir tesisin güvenlik mimarisine entegre olacak şekilde tasarlanmıştır.

Experion Sertifikalı
Endüstriyel otomasyon için Honeywell Experion kontrol sistemi üzerinde kullanım için sertifikalıdır.

HONEYWELL FORGE Cybersecurity+

NEDEN HONEYWELL?

Honeywell, endüstri alanında 100 yılı aşkın deneyime ve endüstriyel siber güvenlikte 20 yılı aşkın uzmanlığa sahiptir. Dünya genelinde tamamlanmış binlerce proje ile Honeywell, endüstriyel varlıkların erişilebilirliğini, güvenliğini ve sürekliliğini koruyan siber güvenlik çözümleri sunmaktadır.
Honeywell'in kapsamlı portföyü şunları içerir: Siber güvenlik yazılımları, Yönetilen güvenlik hizmetleri, Endüstriyel güvenlik danışmanlığı, Entegre güvenlik çözümleri.
Honeywell, sektörde lider siber güvenlik deneyimini proses kontrolündeki onlarca yıllık bilgi birikimiyle birleştirerek, operasyonel teknoloji (OT) ortamları için en üst düzey endüstriyel çözümleri sunar.