SECURE MEDIA EXCHANGE SMX

Operasyonel Ortamlar İçin Uygulanabilir Kurumsal USB Cihazı ve Taşınabilir Medya Siber Güvenlik Çözümü

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

TAŞINABİLİR MEDYA OPERASYONLARI ÇALIŞIR TUTUYOR

Stuxnet bilgisayar virüsünün keşfinden bu yana endüstriyel organizasyonlar, taşınabilir medyayı güvenli şekilde kullanma ve izleme konusunda zorluk yaşamaktadır. Ne yazık ki birçok siber güvenlik aracı ve strateji gelişen operasyonel taleplere uyum sağlayamamıştır. Ayrıca fazla maliyet ve iş yükü doğurmakta, değişen zafiyetleri de ele almamaktadır.

Rafineri, kağıt ve kağıt hamuru, petrol ve gaz, madencilik ve mineraller, ilaç, enerji üretimi, binalar, üretim ve havacılık gibi sanayilerde, taşınabilir medya, tesis süreçlerinin kullanılabilirliğini ve güvenliği ni sağlamak için kritik öneme sahiptir, ancak bu durum potansiyel güvenlik riskleri de yaratmaktadır.

USB kullanımını yasaklayan BT politikaları na rağmen, taşınabilir medya, sanayi kontrol ağlarında aşağıdaki nedenlerden dolayı yaygın olarak kullanılmaktadır:

- Birden fazla satıcıdan gelen sistem platformlarının çeşitliliği, güncellemelerin merkezi olarak yönetilmesini zorlaştırır.
- Ekipmanların uzun ömrü, hem eski hem de yeni sistemlerin karışımını yaratır ve bunların her birinin sürekli güncellenmesi gerekir.

Mevcut Çözümlerin Sınırlamaları

Bir üretim tesisinde, yazılım güncellemeleri için hızla hareket etme gereksinimi ile kritik varlıkları kesinti ya da kötü niyetli saldırılar dan koruma görevini dengelemek gereklidir.

Bu, sanayi ağlarının hızla dijital olarak daha fazla birbirine bağlı yazılım ve sistemlerle değiştiği bir dönemde meydana gelmekte dir. Hava boşluğu olan mimarilerin artık sona erdiği ve dijital bağlantının daha fazla saldırgan fırsat sunduğu bir dönemdeyiz.

Maalesef, bilgi teknolojisi (BT) güvenlik yaklaşımları, üretim ve imalat ortamları için sıklıkla uygunsuzdur. Bu yaklaşımlar, bu ortamlarda kabul edilebilir olsa bile, genellikle işleme ve kontrol ağlarının aksamasına yol açacak şekilde kritik varlıkları korumakta yetersiz kalmaktadır.

USB güvenliği çözümleri gibi geçici çözümler, güncellemeler ve yamanamalar için yardımcı mühendislik iş istasyonları kullanmak ya da güvensiz dosya transfer teknikleri kullanmak, aşırı maliyet, yük ve risk oluşturabilir.

Son olarak, geleneksel USB tarayıcıları, endüstriyel tesislerdeki taşınabilir medya güvenlik sorununu gerçekten çözmez çünkü sürekli güncel kalabilmek için AV yazılımı güncellemeleri gerektirir ve yalnızca BT ile ilgili tehditleri tespit etmek için tasarlanmıştır.

HONEYWELL FORGE Cybersecurity+

HONEYWELL SMX

Riskleri azaltın ve **dosya politikaları ile verimliliği artırın.**

Honeywell SMX, Forge Siber Güvenlik Suite ile entegrasyon ve Kurumsal Tehdit Yönetimi portalı ile OT (Operasyonel Teknoloji) girişimleri üzerinden endüstriyel USB siber güvenliğini genişletir.

Honeywell SMX, organizasyon genelinde USB cihazları, faaliyet ve içeriklerin görünürlüğünü ve yönetimini sağlar; ayrıca tesis dışı ortamlar, hava boşluğu olan ortamlar ve diğer zorlu çevrelerde.

NEDEN SMX?

Sürpriz yok! USB cihazlarını güvenli bir şekilde yönetmek için:

- Özelleştirilmiş dosya politikaları ile güncelleme ve yamanama yaparken verimliliği artırın.
- Yeni ortaya çıkan OT tehditlerini proaktif araştırmalar, zararlı yazılım analizleri ve derin web madenciliği ile takip edin.

Üretim ortamınızı güncellerken ve yamalarken verimliliği artırın, özel dosya politikalarıyla

Proaktif araştırma, kötü amaçlı yazılım analizi ve derin web madenciliği ile ortaya çıkan OT tehditlerinin önüne geçin

HONEYWELL SMX NEDİR?

Kurumsal Tehdit Yönetimi Portalı – Taşınabilir medya, günlükler ve dosyaları uzaktan yönetme.

Yürütme Sürücüsü – Tüm depolama medyası taranmalıdır.

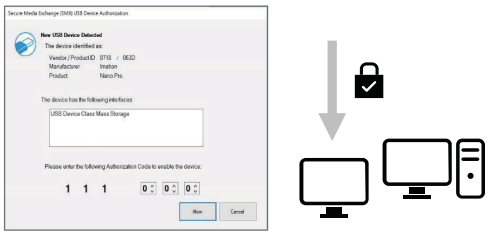
SMX Sistemi – Herhangi bir ortam için tam yönetilen sağlam veya taşınabilir tarama istasyonu.

GARD Motoru – Donanım tabanlı tehditlerden (örneğin, rubber ducky, cep telefonları) daha iyi koruyun.

GARD Motoru – Endüstri lideri OT tehdit algılama.

HONEYWELL SMX'İN 5 TEMEL BİLEŞENİ

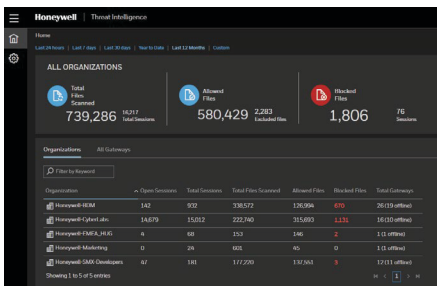
1 SMX SİSTEMLERİ



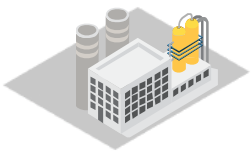
3 SMX İstemci Yürütme Sürücüsü

2 GARD TEHDİT MOTORU
Global Analiz, Araştırma & Savunma

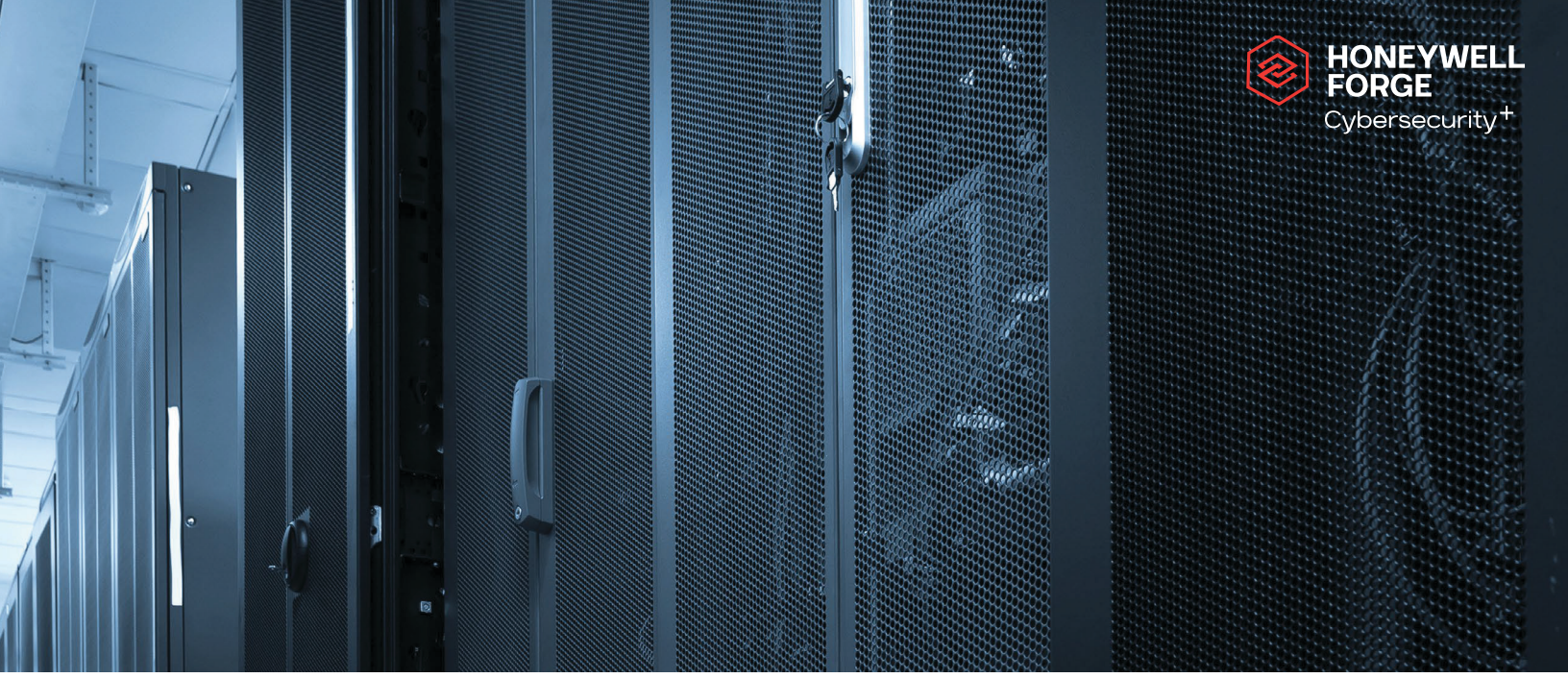
4 Kurumsal Tehdit Yönetimi Portalı



5 GARD TEHDİT ARAŞTIRMA EKİBİ
Global Analiz, Araştırma & Savunma



OTD BİLİŞİM GLOBAL VAD



İLK TEHDİT TESPİT ARACI

Secure Media Exchange, endüstriyel tesislerde çıkarılabilir medya kullanımı izleyerek, koruyarak ve kaydederek siber güvenlik risklerini azaltır ve operasyonel kesintileri sınırlar. SMX ağ geçidi güvenlik cihazı, fiziksel "ön masanızda" veya seçtiğiniz site konumunda basitçe yer alır. Eldivenle bile çalışan bir tüketici odaklı dokunmatik ekran, ziyaretçilerin çıkarılabilir medyalarını kontrol prosedürünün bir parçası olarak yerleştir melerini doğal bir şekilde hatırlatır. Kötü amaçlı yazılımlar ve diğer güvenlik tehditleri, USB'ler aracılığıyla kritik altyapıya iletilmeden önce tespit edilir.

SMX, evergreen koruma için satıcıdan bağımsız ICS (Endüstriyel Kontrol Sistemi) tehdit güncellemeleri sunar.

SMX güvenlik denetimleri, istihbarat akışları ve endüstriyel tehdit tespiti tekniklerinin bir araya geldiği güçlü bir kombinasyonu içerir. Ayrıca Honeywell'in Siber Güvenlik Küresel Analiz, Araştırma ve Savunma (GARD) tehdit araştırma ekibiyle birlikte çalışır.

Kendini öğrenen yetenekler ve otomasyon, SMX ve Tehdit İstihbarat çözümünün mevcut ve ortaya çıkan USB kaynaklı tehditlere karşı daha iyi koruma sağlamasını garantiler. İlk güvenlik analizinden sonra, SMX, hizmet sağlayıcılarının ve çalışanların ekipman güncellemeleri için çıkarılabilir medya kullanarak daha güvenli bir şekilde faaliyet göstermelerini sağlar.

SMX, tesis güvenliğini modernize eder, bir tüketici dostu USB tarama cihazını bulut tabanlı endüstriyel siber güvenlik tehdit güncellemeleriyle birleştirir.

SMX, çıkarılabilir medya etkinliklerinin tesis boyunca kaydını tutarak uyumu ve site incelemelerini basitleştirir.

SMX, ISA-99 ve IEC 62443 gereksinimler ine destek sağlar. Honeywell'in ek çözümleriyle, örneğin Honeywell Forge Cybersecurity Site, süreç kontrol ağı riskleri ve tehditlerinin önceliklendirilme sini ve daha güçlü bir endüstriyel güvenlik duruşu için daha iyi bir şekilde azaltıl masını sağlar.

HONEYWELL FORGE Cybersecurity+

UYGULANABİLİR GÜVENLİK TEKNOLOJİSİNE GÜVENİN, SADECE BİR ONUR SİSTEMİ POLİTİKASI DEĞİL

Bazı siber güvenlik sağlayıcıları mevcut durumu göz ardı eder ve endüstriyel operasyonların güvenlik nedeniyle durmasını bekler, bu ise gerçekçi değildir. Çıkarılabilir medyanın kullanımını yasaklayan politikalar önerirler ve fiziksel portları işlevsiz hale getirirler.

Şimdi, Honeywell'in inovasyonu, tesis korumasını çıkarılabilir medya için genişletir ve güvenlik risklerini ve operasyonel kesintileri dijital ve fiziksel olarak en aza indirerek operasyonel metriklerin takibini sağlar.

Honeywell, kritik altyapıyı siber tehditlerden daha iyi korumaya yardımcı olacak insanlara, süreçlere ve teknolojilere ciddi yatırımlar yapmaktadır. Dijital kontrol sistemlerine yönelik artan tehditlere rağmen tesislerin kesintisiz çalışmasını sağlama taahhüdümüz devam etmektedir. Ürün ve hizmetlerimiz yalnızca Honeywell kontrol sistemleriyle sınırlı değildir, aynı zamanda çeşitli operasyonel altyapıları da daha iyi korur.

SMX, tesisinizin politikasını uygulamak için çıkarılabilir medya izlemesini sürdürür. Onaylanmamış USB cihazlarının USB portlarını kullanmasını engellerken, portu yetkilendirilmiş cihazlar için açık tutar. Ziyaretçi veya çalışan çıkışı sırasında, SMX cihazı tekrar kontrol eder, anormallikleri tespit eder ve cihaz bilgilerini kaydederek adli analizleri destekler.

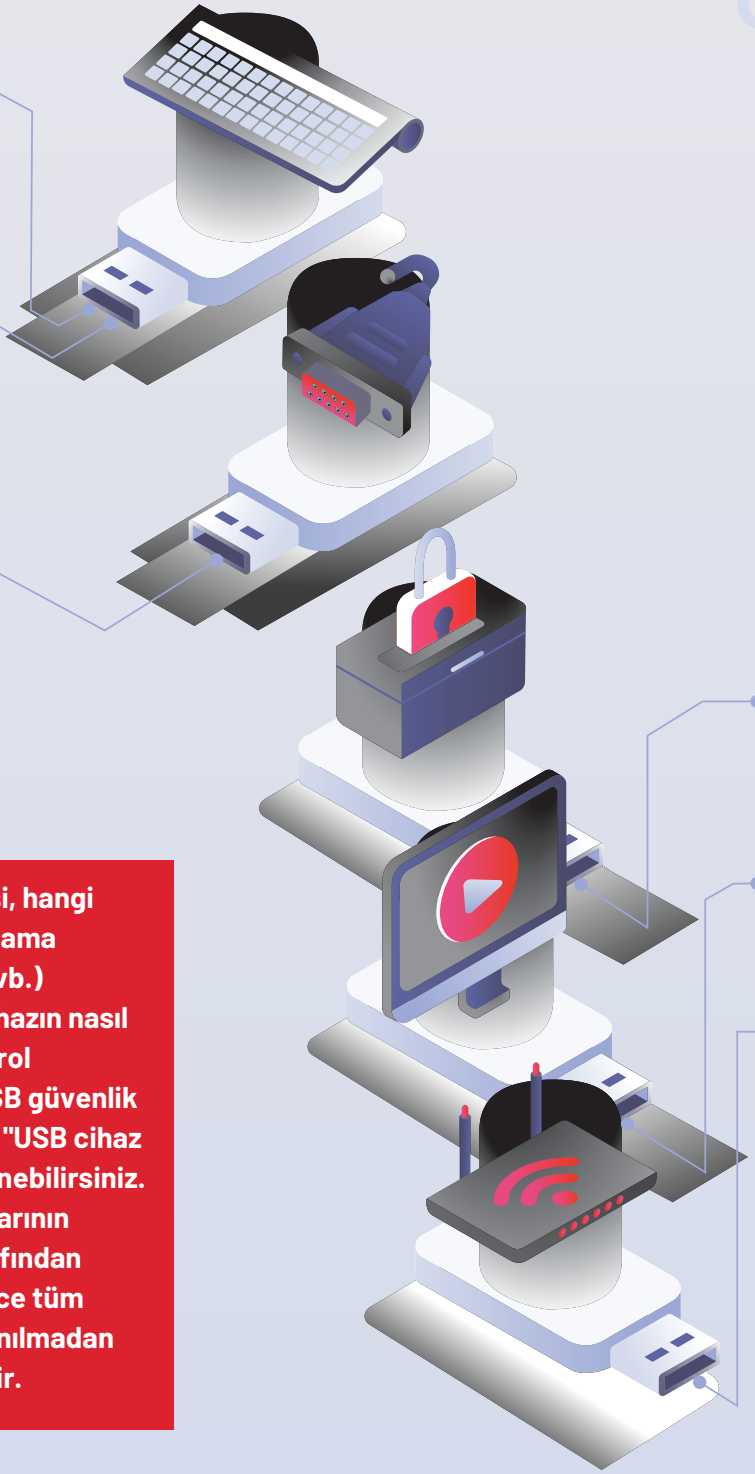
SMX, GELİŞMİŞ USB TEHDİTLERİNE KARŞI DAHA İYİ KORUMA SAĞLAR

Honeywell SMX, işlem üretiminde IT ve OT gereksinimleri arasındaki farkı kapatarak daha güvenli bir ortam sunar.

ANAHTAR KAYDEDİCİLER (Keyloggers): Veri çıkarımı ve şifre hırsızlığı

TUŞ VURUŞU ENJEKTÖRLERİ (Keystroke Injectors): Gizli "içeriden" saldırılar, anti-malware'yi geçebilen saldırılar

SERİ PORT: Ağa güvenliği aşabilen doğrudan COM erişimi



Depolama (Storage): Zararlı yazılım ile veri çıkarımı

Ses / Görüntü (Audio/Visual): Casus yazılım, gizli izleme

Ağ (Network): Yasadışı erişim noktaları ve ağ arka kapıları

Honeywell TRUST Teknolojisi, hangi USB tabanlı cihazların (depolama medyası, fare, cep telefonu vb.) bağlanabileceği ve her bir cihazın nasıl çalışacağı üzerinde sıkı kontrol sağlayan uygulanabilir bir USB güvenlik programı yaratır. Bu durumu "USB cihaz güvenlik duvarı" olarak düşünebilirsiniz. Ayrıca, tüm depolama cihazlarının bağlanmadan önce SMX tarafından taranması gerektiğini, böylece tüm dosyaların kritik ağlara kullanılmadan önce kontrol edildiğini belirtir.

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

GARD NASIL ÇALIŞIR?

Bir dosyanın "iyi" olduğunu nasıl anlarsınız?
Dikkate almanız gereken birçok faktör var

ÇOK KAYNAKLI TEHDİT İSTİHBARATI

- Birden fazla tehdit itibar beslemesi
- Sıfırıncı gün ve erken dönem tehdit tespiti
- Zararlı yazılım çoklu taramaları
- Tehdit avcılığı ve Darkweb madenciliği

İÇERİK BEYAZ LİSTELEME

- Çoklu satıcı yazılım ve donanım doğrulaması
- Özel dosya politikalar

OPERASYONEL TELEMETRİ

- Binlerce dağıtılmış sensör
- Honeywell'in küresel SOC'sinden gelen olay verisi
- Kamu ve özel sektör

İNSANİ ZEKÂ

- 7 Honeywell siber güvenlik mükemmeliyet merkezi tarafından yapılan araştırmalar

---

ZORLUK

Çok fazla tehdit var ki, uç nokta anti-malware yazılımları, zararlı yazılımların %1'inden daha azını tespit edebiliyor ve bu da endüstriye özel tehditler için yer bırakmıyor. Bulut tabanlı tehdit tespiti yardımcı olabilir, ancak ağdan izole edilmiş (air-gapped) ağlarda kullanılamaz.

ÇÖZÜM

GARD, daha güvenli, bağlı tehdit tespit motoru sağlayarak ticari çözümlerden daha fazla tehdidi bulmak için tasarlandı... ve Honeywell Forge Siber Güvenlik çözümleriyle, ağdan izole ağları korumak için kullanılabiliyor.

ETKİ

Honeywell müşterilerini, endüstriyel, bina ve havacılık müşterilerine yönelik en önemli tehditlerden korumaya yardımcı olacak daha iyi tehdit tespiti.

+20 %

HİBRİD TEHLİKELER, EN ÇOK TİCARİ ANTI-VİRÜS ÇÖZÜMLERİNİ GERİDE BIRAKIYOR.

-7%

POTANSİYEL YALAN POZİTİFLER, EK DOĞRULAMA KATMANLARI DAHA AZ YALAN POZİTİF DEMEKTİR.

Bir araştırmaya göre, Enterprise Strategy Group, anket yapılan işletmelerin neredeyse yarısının başarılı bir zararlı yazılım saldırısı yaşadığını, ancak yine de antivirüs çalıştırdıklarını ortaya koymuştur.

– ENTERPRISE STRATEGY GROUP

HONEYWELL FORGE Cybersecurity+

SMX ve GELENEKSEL ANTI-VIRUS USB TARAMASI

SMX sadece bir AV tarama istasyonu değildir!
Çok daha fazlası...

SMX

- ✓ GARD'ın tam gücüyle dosyaları analiz etme
- ✓ Yerel AV'yi güvenlik önlemi olarak kullanarak tarama yapar
- ✓ Yönetim gerektirmez: Tamamen kendi kendine hizmet veren bir kiosk
- ✓ Hava boşluğu (air-gapped) ortamlarında çalışır
- ✓ Check-in' işlemi ile taramayı zorunlu kılar
- ✓ Uç noktalarda (end node) taramaları zorunlu kılar
- ✓ Dosya saldırıları ve kötü niyetli USB cihazları ve UAP'lere karşı koruma sağlar

ANTI-VIRUS
GELENEKSEL TARAMA İSTASYONU

- ✓ Bilinen zararlı yazılımların bir alt kümesi için dosya taraması yapar
- ✗ Sunucuyu yönetme ve yama yapma gereksinimi vardır
- ✗ AV imza dosyalarını güncellemek için yönetim gerektirir (hava boşluğu (air-gapped) ortamlarında otomatik güncelleme yoktur)
- ✗ Müşteri etkileşimi gerektirir: Giriş yapmak, taramaları başlatmak, sonuçları yorumlamak
- ✗ Uç noktalarda tarama sonuçlarını zorunlu kılma yolu yoktur
- ✗ Kötü niyetli cihazlar veya UAP'ler için koruma sağlamaz

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

HONEYWELL ENDÜSTRİYEL SİBER GÜVENLİK

USB TEHDİT RAPORU 2021

ENDÜSTRİYEL SİSTEMLERE USB TEHDİTLERİNİN ARTAN RİSKİ

79 %

ENDÜSTRİYEL KONTROL SİSTEMLERİNDE (EKS) BÜYÜK BİR KESİNTİYE YOL AÇMA POTANSİYELİNE SAHİP USB TEHDİTLERİ (GEÇEN YILDAN %59 ARTIŞ)

↑30 %

ÜRETİM TESİSLERİNDE USB KULLANIMINDAKİ YILLIK ARTIŞ

37 %

TEHDİTLERİN, TAŞINABİLİR MEDYA KULLANIMI İÇİN TASARLANMIŞ OLDUĞU ORAN (GEÇEN YILDAN %19 ARTIŞ)

50 %

UZAK ERİŞİM SAĞLAYAN USB TEHDİTLERİNİN ORANI

45 %

USB TEHDİTLERİNİN TOPLAMI, GEÇEN YILDAN (%44) DEĞİŞMEDİ

OTD BİLİŞİM
GLOBAL VAD

Honeywell Endüstriyel Siber Güvenlik Tehdit Raporu

Endüstriyel kontrol sistemlerinde bulunan kötü amaçlı yazılımların önemli bir kısmı taşınabilir medya aracılığıyla yayıldığından, günümüz fabrikalarında taşınabilir cihazlar olmadan çalışmak neredeyse imkansızdır. Flash bellekler ve USB hafıza kartları gibi taşınabilir medya, endüstriyel kontrolleri yönetmek için çalışanlara sağlanırken, üçüncü parti entegratörler ve hizmet sağlayıcılar da, müşteri tesislerine sık sık güncellemeler uygulamak amacıyla USB değişimlerini yoğun bir şekilde kullanmaktadır.

TROJANLAR **30 %**

USB İÇİN TASARLANMIŞ **37 %**

OT'Yİ HEDEF ALAN **30 %**

UZAK ERİŞİM SAĞLAMA **51 %**

USB kaynaklı kötü amaçlı yazılım tehdidi, ciddi ve artan bir endişe olmaya devam etmektedir. USB üzerinden yayılan tehditler ya da özellikle USB'yi başlatma vektörü olarak kullanabilen tehditler, 2019'daki %19'luk orandan 2020'de %37'ye yükselmiştir. Bu ardışık ikinci yıl olarak önemli bir büyümeyi göstermektedir. Bu tehditlerin çoğunda TROJANLAR, tespit edilen kötü amaçlı yazılımların %76'sını oluşturmuştur. Ayrıca, 2020'deki daha fazla tehdit, taşınabilir olmuştur ve %52'si (%34'ten artış) uzaktan erişim veya kontrol sağlamaya olanak tanımıştır. Bu durum, geçen yılın raporunda tanımlanan bir trendin devam ettiğini göstermektedir: kötü niyetli kişiler, USB taşınabilir medyasını ilk başlatma vektörü olarak kullanarak uzaktan bağlantı kurmak, ek veri indirmek ve kontrol sağlamak amacıyla hedef sektörlerdeki tehditlerde artışa yol açmıştır (sektörlerdeki artış %28'den %30'a çıkmıştır), bu da USB taşınabilir medyasının, birçok endüstriyel ve OT (operasyonel teknoloji) ortamlarında sızmaya devam ettiğini desteklemektedir.

TEHDİTLER DEVAM EDİYOR, DAHA ŞİDDETLİ

Engellenen tehditlerde, 2019'dan devam eden bir diğer trend, kötü amaçlı yazılımın endüstriyel kontrol sistemlerine zarar verme kapasitesinin artmış olmasıdır; bu durum, 2019'da büyük bir ransomware (fidye yazılımı) düşüşüne rağmen, 2020'de %79'a kadar çıkmıştır. Kötü amaçlı yazılımın artan şiddeti, giderek daha sofistike olan zararlı yazılım kaynaklıdır; bu yazılım, hedeflenen sistemlerde geri izleme yapabilen backdoor'lar (geri kapılar), uzaktan erişim sağlama ve komut-veri alma gibi etkiler yaratmaktadır (%20), veya dosya arşivlerini indirip çalıştıran saldırılar (%9).

İÇERİK-BASED MALWARE: OT'YE İLK SALDIRI VETÖRÜ OLARAK

2020'de tanımlanan yeni bir tehdit, büyük oranda meşru yazılım gibi görünerek endüstriyel sistemlere sızan tehditlerdi. Artık kötü amaçlı yazılımlar, özellikle değiştirilmiş veya enfekte olmuş belgeleri hedef alıyor. Bu yıl önemli bir artış, trojanlarda ve özellikle içerik-based malware türlerinde görülmüştür. Bununla birlikte, birçok kuruluş 2020'de daha fazla açık oluşturdu ve kötü niyetli kişiler belgelerdeki içerikleri hedef aldı.

GÖMME KOMUT DOSYALARI VE MAKROLAR

Bu trenddeki artış, daha önceki değişimlere yönelik bazı kişisel fikirleri desteklemektedir. 2020'de birçok organizasyon içerik-based malware'a daha fazla duyarlıydı. Kötü niyetli kişiler, dokümanlardaki değişikliklerden faydalandı. Ancak içerik-odaklı yazılımlar, zaten bazı sistemler üzerinde geçici tehditler haline geldi.

HONEYWELL NASIL YARDIMCI OLABİLİR?

Son yıllarda endüstriyel kontrol sistemleri ile ilgili güvenlik olaylarında büyük bir artış yaşanmıştır. Yeni tehditler ortaya çıktıkça ve endüstriyel güvenlik ortamı geliştikçe, tesis otomasyon sisteminizin kullanılabilirliğini, güvenilirliğini ve güvenliğini korumak için deneyimli ve güvenilir bir ortağa ihtiyacınız vardır. Ayrıca, operasyonunuzun tüm yönlerinde yer alan insanlar ve süreçleri korumanız gerekir.

Honeywell Endüstriyel Siber Güvenlik Çözümleri, kontrol altyapınızı ve tesis operasyonlarınızı daha iyi korumak için özel olarak tasarlanmıştır. Bu geniş çözümler, endüstri lideri proses kontrolü ve siber güvenlik bilgi birikimi ile tanınan uzmanlığımızı kullanmaktadır ve şu özellikleri sunmaktadır:

Endüstriyel kontrol sistemlerini daha iyi güvence altına almak için özelleştirilmiş çözümler

Müşterilerimize yakın küresel/bölgesel endüstriyel siber güvenlik hizmet merkezi hub'ları

Endüstriyel kontrol ağlarının kapsamlı güvenliği

Müşterilerimize siber güvenlik programı geliştirmeden güvenlik değerlendirmelerine kadar destek olabilme

HONEYWELL KİMDİR?

- **Operasyonel Teknoloji (OT) siber güvenliği konusunda güvenilir bir ortak**
- **100+ yıllık OT ve 20+ yıllık OT siber güvenliği alanında uzmanlık**
- **300+ çalışan OT siber güvenliğine odaklanmış**
- **1000'lerce güvenli uzaktan erişim kurulumu ve 5000'den fazla proje teslimi**
- **Endüstri kanıtlanmış siber güvenlik ürünleri, hizmetleri ve çözümlerinin tam portföyü**
- **Tedarikçi bağımsız çözümler**
- **Küresel yetenekler ve yerel deneyim**

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

ISA GLOBAL CYBERSECURITY ALLIANCE Founding Member