HONEYWELL FORGE
Cybersecurity+

HONEYWELL PROAKTİF SİBER SAVUNMA

REAKTİF MÜDAHALEDEN PROAKTİF RİSK ÖNGÖRÜSÜNE OT GÜVENLİĞİNİN DÖNÜŞTÜRÜLMESİ

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

OT'Yİ HEDEF ALAN SİBER SALDIRILARI ÖNGÖRME VE MÜDAHALE ETME ZORLUĞU

OTD BİLİŞİM
GLOBAL VAD

PROAKTİF SAVUNMA ZORLUĞU

OT Siber Güvenliğindeki Temel Zorluklar

- **Eski Nesil OT Altyapısı**
  Eski nesil EKS / OT sistemlerinin, tamamen yenilenmeden güvence altına alınması zordur.

- **Hızlı Dijital Dönüşüm**
  Mobil, bulut, IoT ve uzaktan çalışma, saldırı yüzeyini genişleterek daha güçlü OT / IoT korumasını gerekli kılar.

- **Gelişmiş Kalıcı Tehditler (APT'ler)**
  Gelişmiş, hedefli saldırılar çoğu zaman fidye yazılımı veya jeopolitik motivasyonlu proaktif savunma gerektirir.

- **Sınırlı OT'ye Özgü Görünürlük**
  OT'ye uyarlanmış ele geçirme göstergelerine (IOC'ler) ilişkin içgörü eksikliği, erken tespit ve müdahaleyi zorlaştırır.

BİRÇOK ŞİRKET, OT AĞLARINA İLİŞKİN KAPSAMLI GÖRÜNÜRLÜKTEN HÂLÂ YOKSUN

OTD BİLİŞİM
GLOBAL VAD

İNSANLARINIZ, SÜREÇLERİNİZ VE SİSTEMLERİNİZ SİBER TEHDİTLERE KARŞI GÜVENDE Mİ?

DEĞERLENDİRİLMESİ GEREKEN SORULAR…

OT sistemleriniz genelinde tehditleri gerçek zamanlı olarak tespit edebiliyor musunuz?

- OT ağlarına yönelik sürekli görünürlük sağlamak, birçok kuruluş için önemli bir zorluk olmaya devam etmektedir.
- Geleneksel BT güvenlik araçları ve uygulamaları, OT ortamlarının kendine özgü gereksinimlerini çoğu zaman karşılayamaz.
- Kuruluşların yalnızca %13'ü OT siber güvenlik duruşlarını çok olgun olarak değerlendirmektedir; bu durum, BT ile karşılaştırıldığında kritik bir boşluğa işaret etmektedir (1).
- Honeywell Cyber Proactive Defense (CPD), OT verilerini zenginleştirip ilişkilendirerek tehditleri erken aşamada ortaya çıkartan, müdahaleyi otomatikleştiren ve genel görünürlüğü güçlendiren dijital bir SOC analisti gibi hareket ederek bu boşluğun kapatılmasına yardımcı olur.

OT Ortamınızda Bir Siber Saldırıyı Tespit Edebilir misiniz?

- Endüstriyel şirketlerin %10'undan daha azı OT ağlarında tam zamanlı görünürlüğe sahiptir.
- Kuruluşların çoğu, OT siber güvenliğini etkin şekilde yönetmek için gerekli kurum içi uzmanlıktan yoksundur.
- OT güvenlik araçları karmaşık, maliyetli ve uzman desteği olmadan devreye alınması zordur.

Müdahale Süreniz Yeterince Hızlı mı?

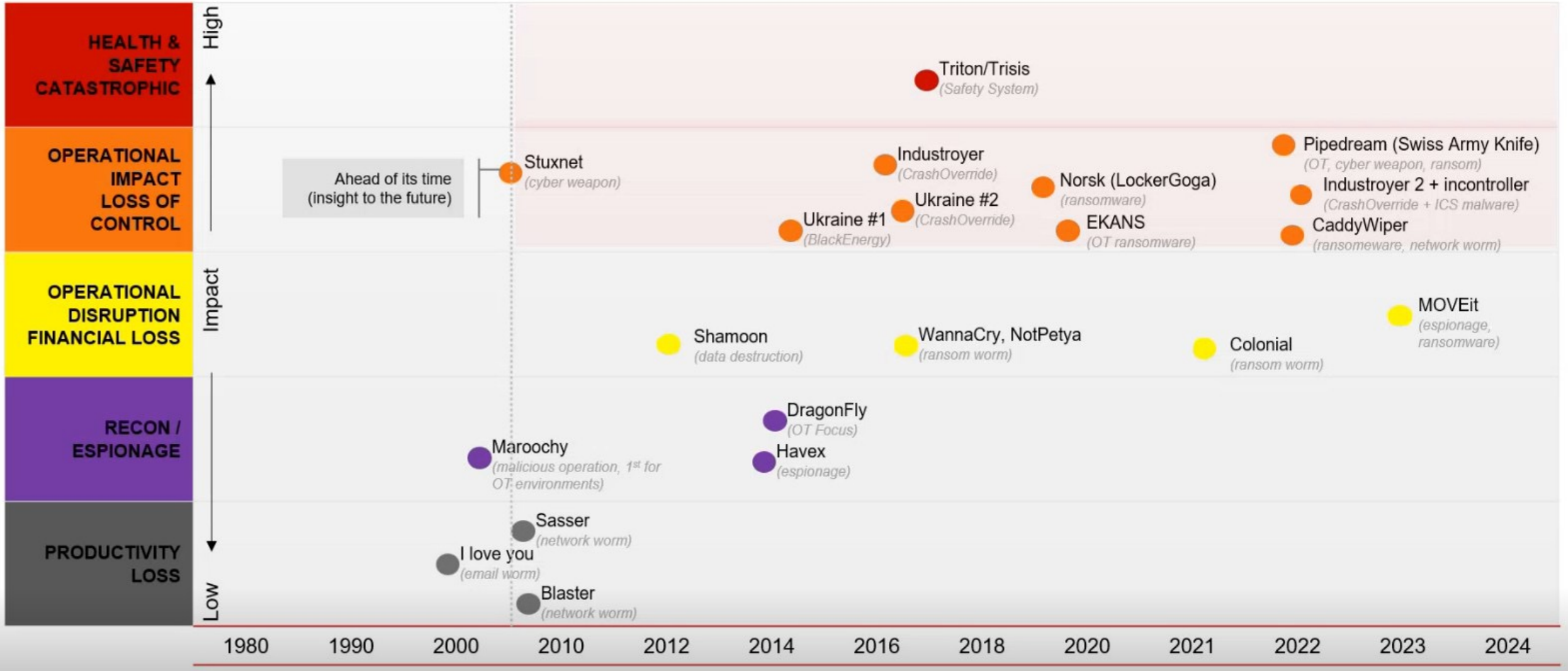
- Birçok kuruluş, OT'ye özgü olay müdahale planlarından yoksundur; bu durum siber saldırı sırasında hazırlıksız yakalanmalarına neden olur.
- OT ağlarına ilişkin sınırlı görünürlük, tehditlerin gerçek zamanlı olarak tespit edilmesini ve bunlara müdahale edilmesini zorlaştırır.
- OT sistemlerinin karmaşıklığı ve birbirine bağımlılığı, tehditlerin etkin biçimde izole edilmesini ve kontrol altına alınmasını engeller.
- OT sistemlerine yönelik siber saldırılar, geleneksel BT ihlallerinden farklı olarak fiziksel operasyonları doğrudan kesintiye uğratabilir.

EN İYİ SINIFTAKİ ŞİRKETLER BU SORULARA GÜÇLÜ YANITLAR VERİR

HONEYWELL FORGE Cybersecurity+

ÖRNEKLER: ENDÜSTRİYEL SİBER GÜVENLİK

SALDIRI ETKİSİ ARTIYOR



OTD BİLİŞİM
GLOBAL VAD

BU APT SALDIRILARINDA KULLANILAN EN YAYGIN 6 DAVRANIŞ

01

Dosya Oluşturma / Değiştirme

Sistem üzerinde dosyaların oluşturulması veya değiştirilmesi.

02

Komut Çalıştırma

Varlıklar üzerinde PowerShell kullanılarak komutların çalıştırılması.

03

Process Creation

Varlıklar üzerinde yeni süreçlerin veya servislerin oluşturulması.

04

Ağ Trafiği Akışı

Uzak etkinliklerin örüntüleri, özellikleri ve imzaları.

05

OS API Yürütme / Modül Yükleme

Varlıklar üzerinde gerçekleştirilen gelişmiş işlemler.

06

Windows Kayıt Defteri Değişiklikleri

Varlıkların işleyişini bozmak amacıyla varlıkların oluşturulması, değiştirilmesi ve silinmesi.

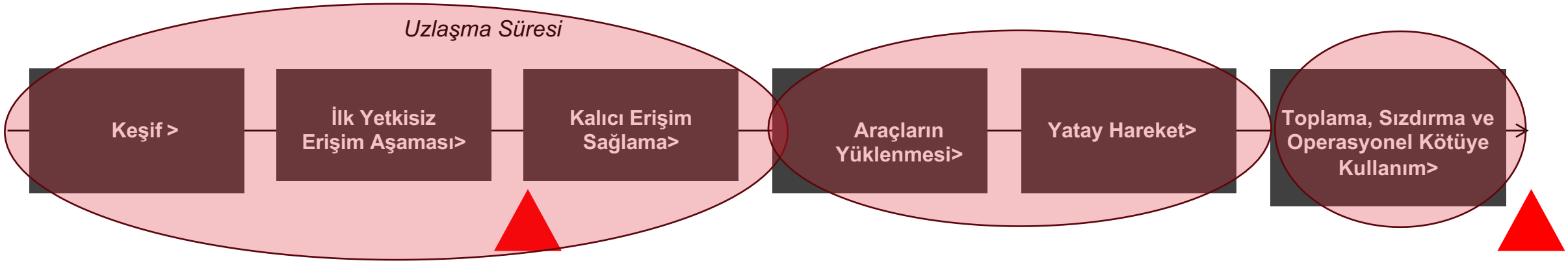
HONEYWELL FORGE
Cybersecurity+

BİR SALDIRININ ANATOMİSİ

Bir saldırgan genellikle ortalama olarak fark edilmeden kalır.

292 Gün[1]

GÜNLER – AYLAR | **DAKİKALAR – GÜNLER** | **DAKİKALAR – GÜNLER** | **GÜNLER – AYLAR**



İlk Bilgisayarın Ele Geçirilmesi

Saldırı Tespit Edildi

KEŞFET VE YERLEŞ

YERLEŞ VE GENİŞLE

HASAR

HONEYWELL FORGE
Cybersecurity+

REAKTİF SAVUNMADAN PROAKTİF RİSK ÖNGÖRÜSÜNE GEÇİŞ

OTD BİLİŞİM
GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

PROAKTİF SİBER SAVUNMAYA ULAŞMAK İÇİN EN İYİ UYGULAMALAR

CPD ile Proaktif Tehdit Tespiti

- Tamamen otomatikleştirilmiş süreç: veri toplamadan aksiyona dönüştürülebilir önerilere kadar
- Erken tehdit tanımlaması için OT ortamları genelinde verileri zenginleştirir ve ilişkilendirir
- Gelişmiş ML modelleri kullanarak davranışsal sapmaları tespit eder.
- Aldatma teknolojisi (OT honeypot) ile pasif izlemenin ötesine geçer.
- Birleşik tehdit görünürlüğü için birden fazla siber aracı entegre eder.
- Şüpheli olayları gruplayıp ilişkilendirerek erken tespiti destekler.
- Bölge tabanlı gezinme ile ağ segmentasyonu analizini güçlendirir.
- Kolaylaştırılmış triyaj için merkezi olay görünümü panosu sunar.
- Manuel iş yüklerini azaltmak ve müdahaleyi hızlandırmak için dijital bir SOC analisti gibi hareket eder.

OT için Tehdit Öngörüsü ve İstihbaratı

- Olay geri bildirimleri, SOC bulguları ve harici siber tehdit akışlarından gelen verileri ilişkilendirerek OT ortamlarına özel zenginleştirilmiş tehdit istihbaratı oluşturur.
- Davranışsal anomalilerin ve saldırgan taktiklerinin yapay zekâ destekli analiziyle aksiyona dönüştürülebilir içgörüler sunar.
- Gen AI destekli, OT'ye özgü çalışma kitaplarından yararlanarak operatörlerin riskleri azaltmasına ve öngörülen tehditlere karşı savunmaları güçlendirmesine rehberlik eder.
- Reaktif güvenliği proaktif savunmaya dönüştürerek endüstriyel sistemler genelinde daha erken tespit ve daha hızlı müdahale sağlar.

HONEYWELL FORGE Cybersecurity+

SİBER SALDIRILARI DAHA İYİ ÖNGÖRMEK İÇİN AI / ML KULLANAN 5 ADIMLI SÜREÇ

Temel Kolaylaştırıcı

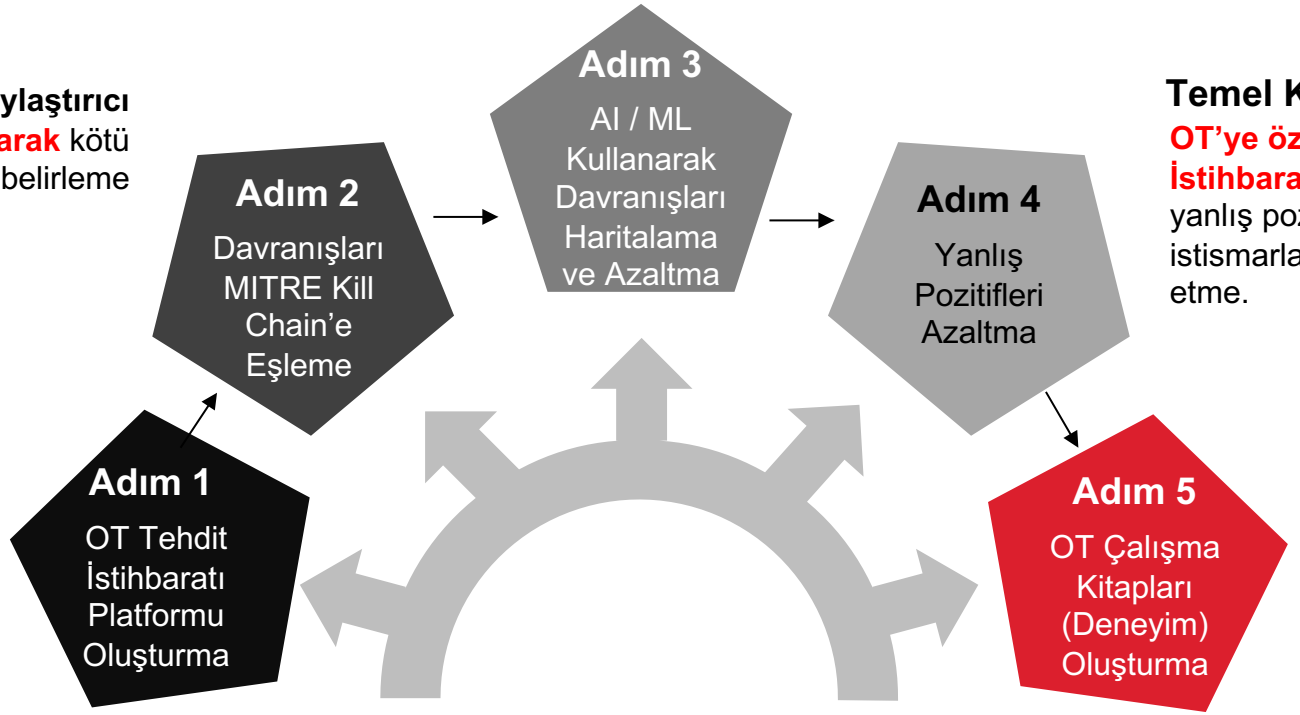
EKS / OT ortamı davranışlarındaki örüntüleri ve sapmaları belirleyerek bilinmeyen tehditleri ve anomalileri tespit etmek için **denetimsiz ML modellerini** kullanma

Temel Kolaylaştırıcı

Yapay zekâ kullanarak kötü amaçlı davranışları belirleme

Temel Kolaylaştırıcı

OT'ye özgü Siber Tehdit İstihbaratı akışlarının Veri zenginleştirmede kullanımı



Temel Kolaylaştırıcı

OT'ye özgü Tehdit İstihbaratından yararlanarak, yanlış pozitifleri azaltırken istismarları öngörme ve tespit etme.

Temel Kolaylaştırıcı

Yapay zekâdan yararlanarak, siber değerlendirmeler ve iş birlikleriyle desteklenen OT uzmanlığını kullanıp Kurumsal Görünümde bir bilgi tabanı oluşturma

REAKTİF SİBER GÜVENLİKTEN PROAKTİF SİBER GÜVENLİĞE GEÇİŞ

HONEYWELL FORGE
Cybersecurity+

HONEYWELL PROAKTİF SİBER SAVUNMA TANITILIYOR

OTD BİLİŞİM
GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL PROAKTİF SİBER SAVUNMA: PROAKTİF OT SİBER GÜVENLİĞİ İÇİN TASARLANDI

Honeywell Cyber Proactive Defense (CPD), endüstriyel kuruluşların reaktif güvenlikten proaktif risk öngörüsüne geçişine yardımcı olmak üzere dijital bir SOC analisti gibi çalışmak üzere tasarlanmış, yapay zekâ destekli bir yazılım çözümüdür. CPD, OT ortamları genelinde verileri zenginleştirip ilişkilendirerek erken aşama tehditleri tespit eder, müdahaleyi otomatikleştirir ve genel siber dayanıklılığı güçlendirir.

Temel Yetkinlikler

Proses Entegrasyonu - Mühendislik veya operatör varlıklarında, siber olay süresi boyunca meydana gelen proses sapmalarını; proses verilerini (etiketler ile alarmlar/olaylar) entegre edip gömerek öğrenme ve ilişkilendirme.

Gömülü Proses Bilgisi ve Aldatma Teknolojisi- CPD, aksiyona dönüştürülebilir istihbaratı ortaya çıkaran ve alarmları tetikleyen OT honeypot gibi otomatik iş akışları ve entegrasyonlar aracılığıyla tehdit tespitini geliştirir. Gömülü endüstriyel bağlam, uyarlanmış tespit ve daha hızlı müdahale sağlar.

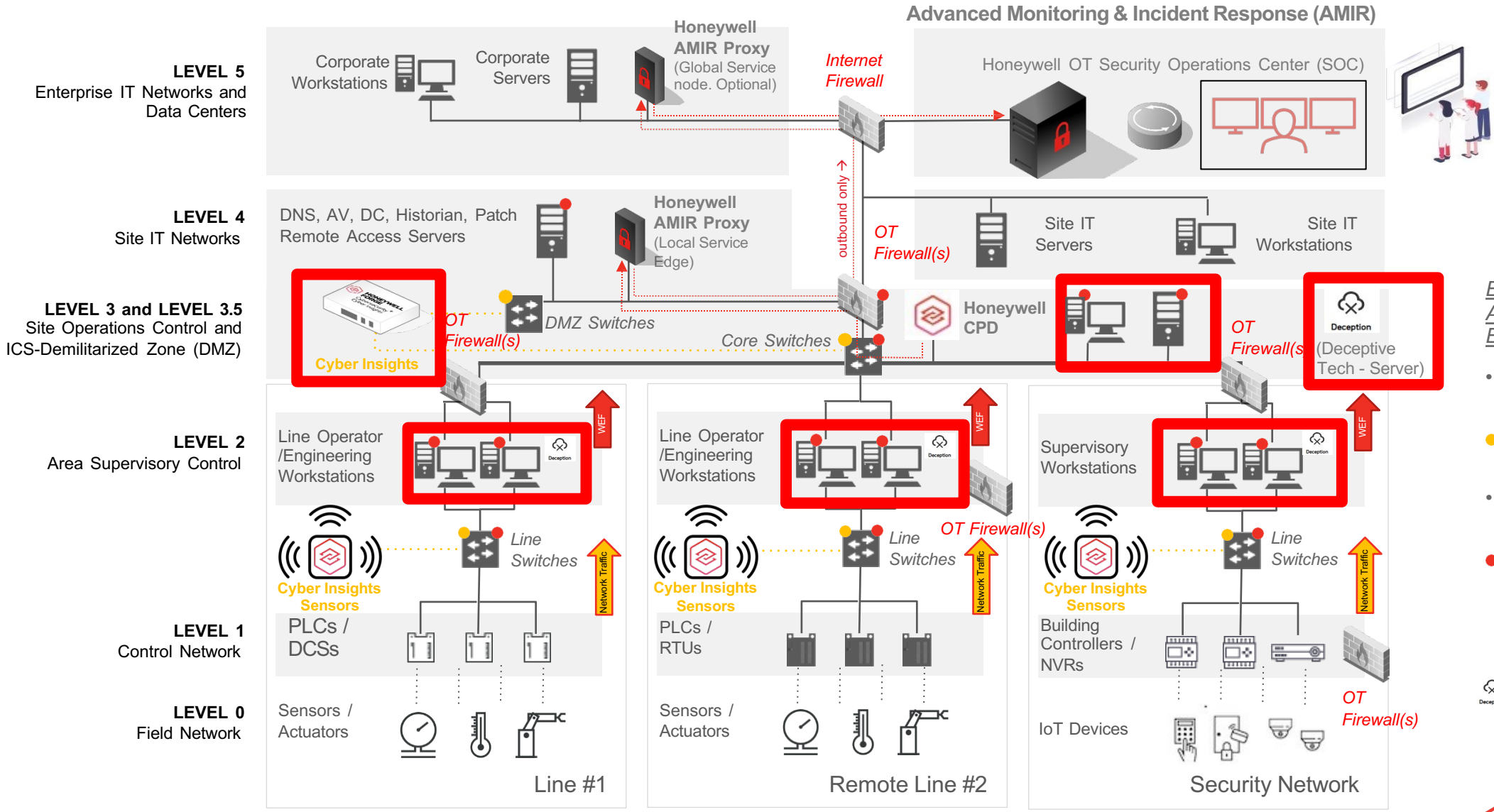
AI / ML Destekli Tespit - Makine öğrenimi kullanarak davranışsal anomalileri tespit eder ve zenginleştirilmiş tehdit istihbaratına dayanarak savunmaları sürekli olarak uyarlar.

- **Otomatikleştirilmiş Çalışma Kitapları -** Operatörlere, olaylara müdahaleyi hızlandıran ve insan hatasını azaltan yapılandırılmış, yapay zekâ destekli iş akışlarıyla rehberlik eder.
- **Dijital Analist İşlevselliği -** Veri normalizasyonunu, korelasyon kontrollerini ve birinci seviye iyileştirmeyi otomatikleştirerek SOC ekiplerinin yüksek katma değerli incelemelere odaklanmasını sağlar.

OT SİBER SALDIRILARINI GERÇEKLEŞMEDEN ÖNCE TESPİT ETMEK İÇİN DAHA FAZLASINI YAPIN

HONEYWELL FORGE Cybersecurity+

OT Ağ Tasarım Mimarisi: Performans + Güvenlik

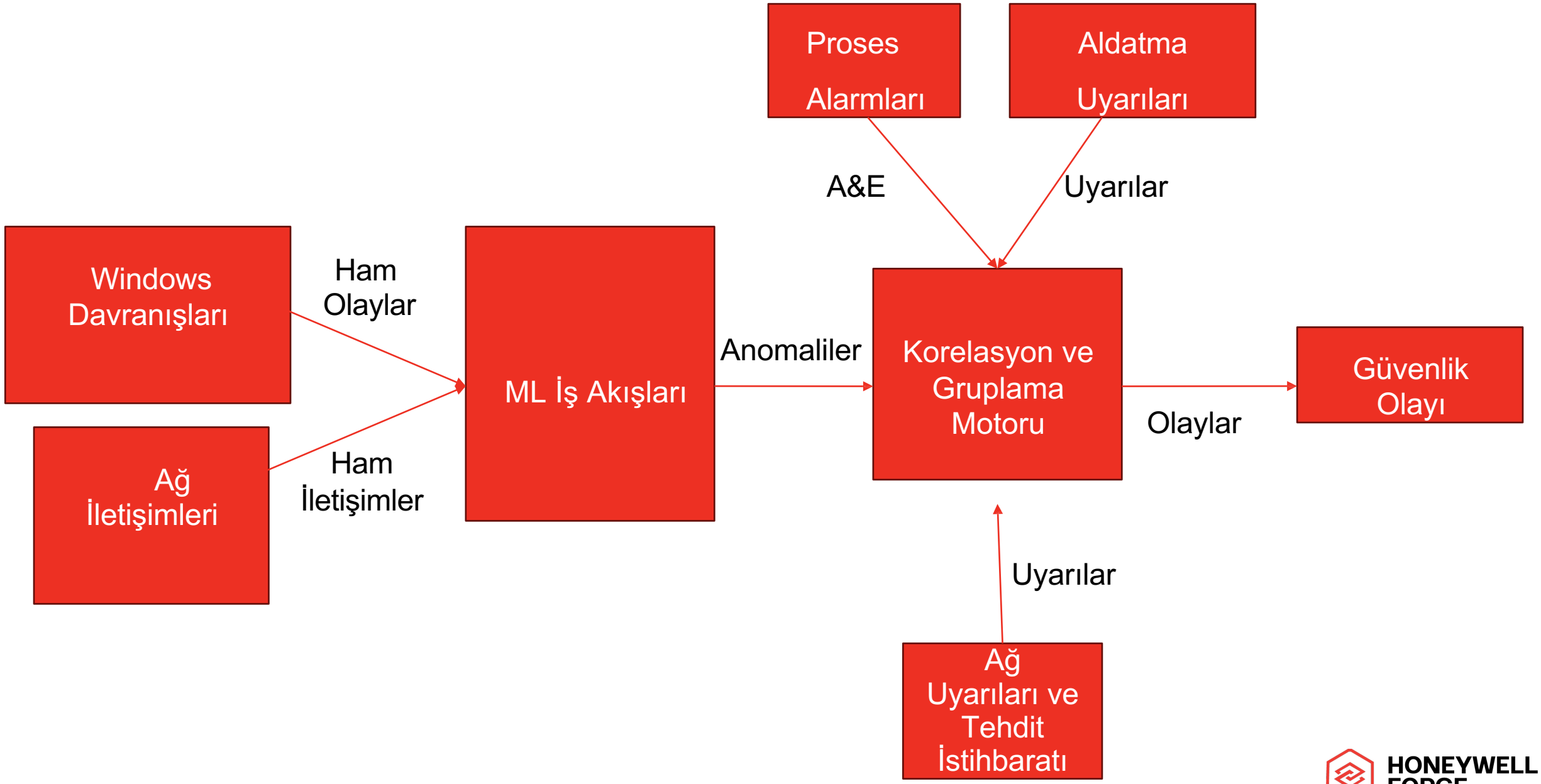


Bağımsız Çözüm veya AMIR için İsteğe Bağlı Eklenti:

- *Varlık tespiti, tehdit tespiti ve ağ anomalisi tespitine yardımcı olan siber içgörüler*
- *Honeywell Cyber Proactive Defense varlık alımı, güvenlik olaylarının oluşturulması için makine öğrenimi ve yapay zekâ ile analiz edilir.*
- *Honeywell Cyber Proactive Defense (Aldatma Sunucusu ve Sensör)*

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+


Proses Alarmları
Aldatma Uyarıları
A&E
Uyarılar
Windows Davranışları
Ham Olaylar
ML İş Akışları
Anomaliler
Korelasyon ve Gruplama Motoru
Güvenlik Olayı
Olaylar
Ağ İletişimleri
Ham İletişimler
Uyarılar
Ağ Uyarıları ve Tehdit İstihbaratı

HONEYWELL OT SİBER GÜVENLİK PORTFÖYÜ: BİRLEŞİK DERİNLEMESİNE SAVUNMA

OTD BİLİŞİM GLOBAL VAD

Ürün	Temel Yetkinlik	Değer Önerisi
Proaktif Siber Savunma	Davranışsal analizler, aldatma teknolojisi (honeypot) ve otomatik olay müdahale çalışma kitapları için AI/ML tabanlı platform.	Öngörüsel Savunma: Predicts and prevents unknown, zero-day, and living-off-the-land attacks to ensure operational resilience and uptime.
OT SOC / AMIR	Merkezi log toplama, uzman izleme, tehdit avcılığı ve olay incelemesi için 7/24 Yönetilen Hizmetler. Olay müdahalesi için retainer hizmeti sunar.	Uzmanlık-Hizmet-Olarak: Ek yük oluşturmadan, hızlı ve etkili olay müdahalesini güvence altına alan, dünya standartlarında, kendini adamış bir OT güvenlik ekibi sunar.
Cyber Insights	Ajan gerektirmeyen varlık keşfi; gerçek zamanlı zafiyet yönetimi, pasif ağ izleme ve risk puanlaması ile birlikte.	Bütüncül Görünürlük: Tüm OT varlıklarının ve güvenlik duruşlarının gerçek zamanlı, kapsamlı bir görünümünü oluşturarak risklerin önceliklendirilmesini ve uyumluluğu basitleştirir.
Secure Media Exchange (SMX)	Çoklu tehdit istihbaratı kaynaklarıyla kötü amaçlı yazılım taraması, dosya doğrulama, politika uygulama, kimliğe bürünen cihazlara ve donanım yazılımı değiştirme saldırılarına karşı koruma ile USB cihaz kontrolü sağlayan, çıkarılabilir medya için Honeywell çözümü.	Kritik Bir Saldırı Vektörünü Kapatır: Tehditler için birincil giriş noktası olan USB kaynaklı kötü amaçlı yazılımları proaktif olarak engelleyerek OT ağlarını fiziksel çevrede korur.

Birleşik Savunma Stratejisi:

Honeywell portföyü, uyumlu ve katmanlı bir savunma yapısı olarak birlikte çalışır. SMX, fiziksel çevrede ilk savunma hattı olarak görev yapar. Cyber Insights, tüm varlıkların temel gerçek zamanlı bağlamını sağlar. Cyber Proactive Defense ise, AI / ML kullanarak ince davranışsal anormallikleri öngören ve tespit eden istihbarat katmanıdır. Son olarak, OT SOC ve AMIR yönetilen hizmetleri, tehditler operasyonları etkilemeden önce etkisiz hâle getirmek için gerekli uzman insan gözetimini ve hızlı müdahaleyi sağlar.

HONEYWELL FORGE Cybersecurity+

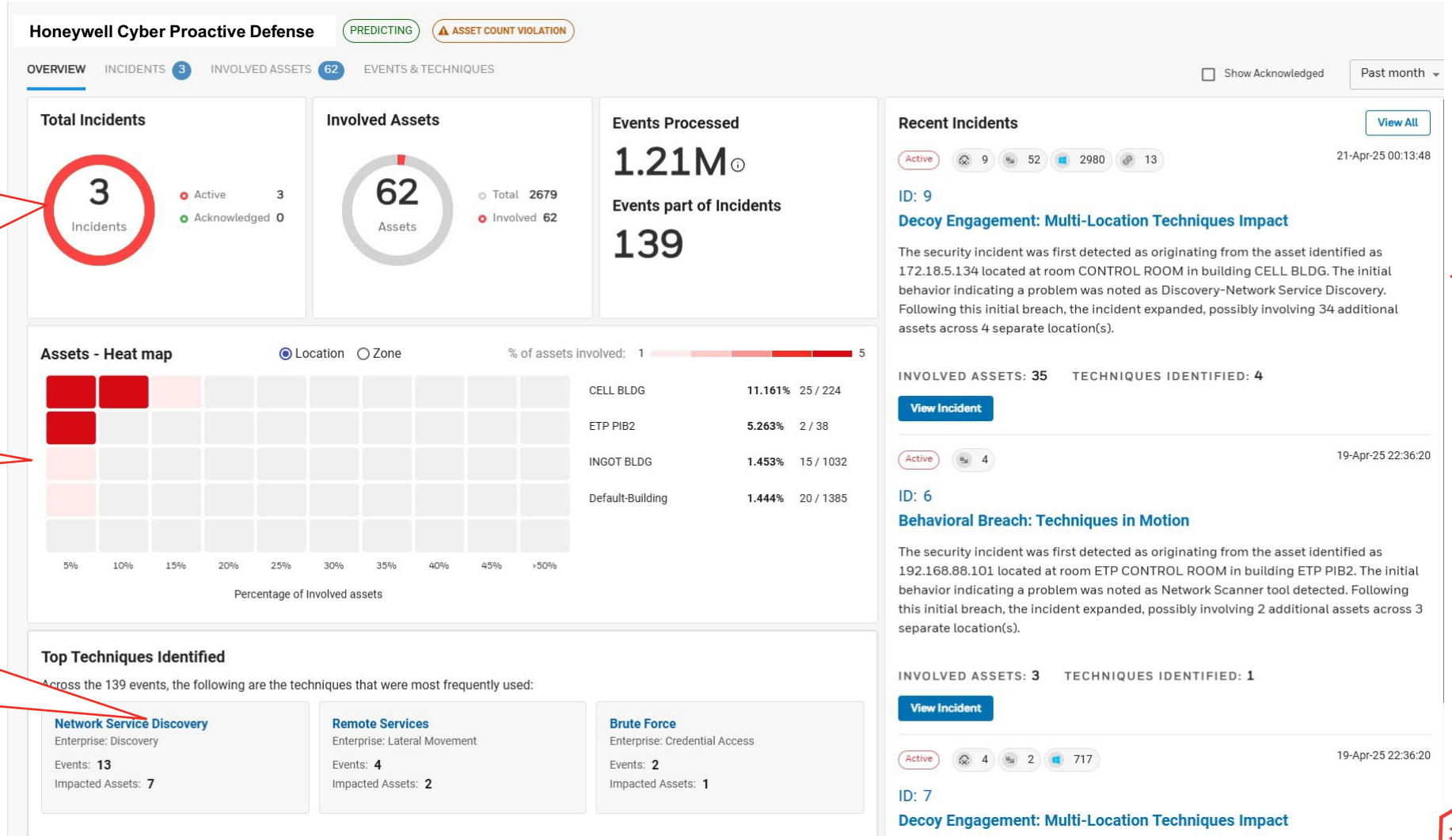
YAPAY ZEKA DESTEKLİ İLİŞKİLENDİRME, ZENGİNLEŞTİRİLMİŞ TEHDİT İSTİHBARATI VE YÖNLENDİRİLMİŞ MÜDAHALE

OTD BİLİŞİM GLOBAL VAD

Müşteri ortamındaki güvenlik olaylarına ilişkin mevcut durumları ve çözüm ilerlemeleri dâhil olmak üzere ayrıntılar.

Konum veya Bölgeye Göre Varlık Isı Haritası

Saldırı Taktikleri ve Tekniklerine İlişkin Bilgiler



Yapay Zeka / Makine Öğrenimi Destekli Olay Önceliklendirme ve İlişkilendirme

HONEYWELL FORGE Cybersecurity+

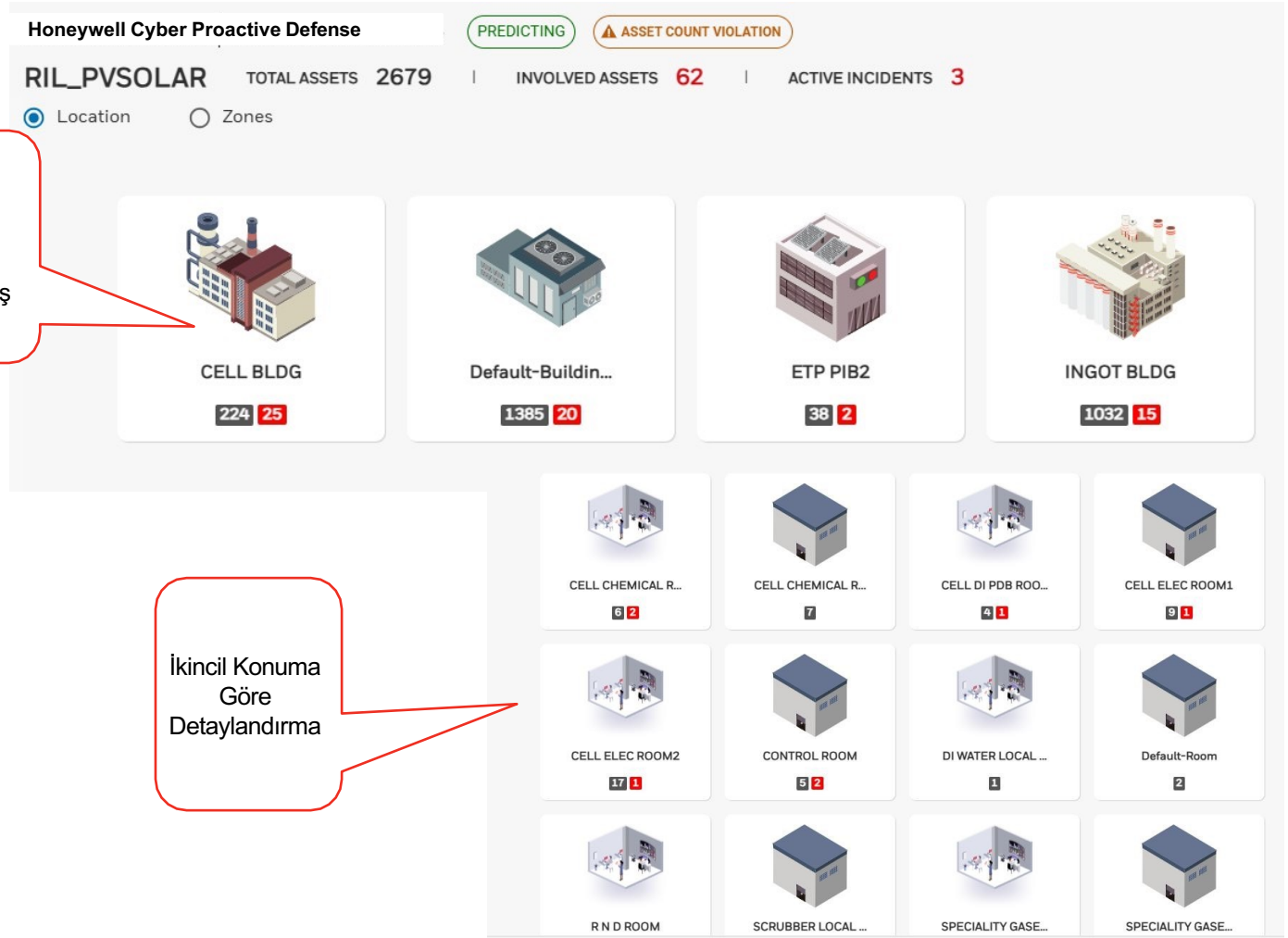
PROAKTİF TEHDİT YÖNETİMİ İÇİN DETAYLI İÇGÖRÜLER

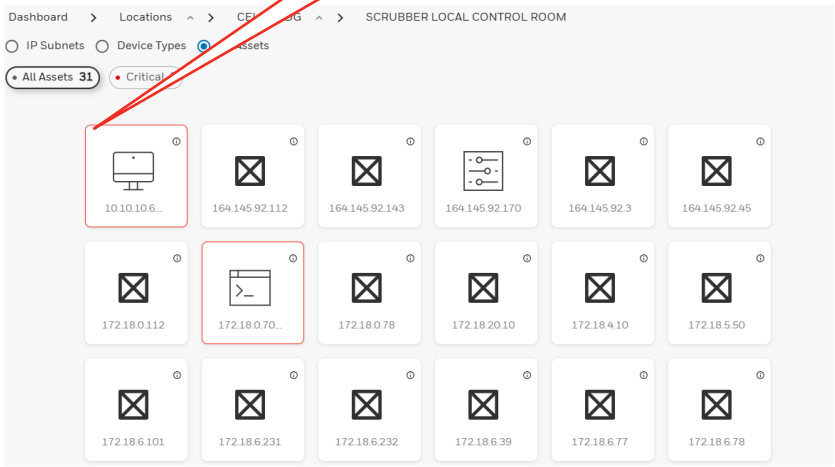
Konuma Göre Üst Düzey Genel Bakış

İkincil Konuma Göre Detaylandırma

(3)
IP / Cihaza Göre Gelişmiş Detaylandırma

Örn. 10.79.218.9/varlıklar





SİBER SALDIRILARI DAHA İYİ ÖNGÖRMEK İÇİN AI / ML KULLANAN 5 ADIMLI SÜREÇ

OTD BİLİŞİM GLOBAL VAD

Temel Kolaylaştırıcı

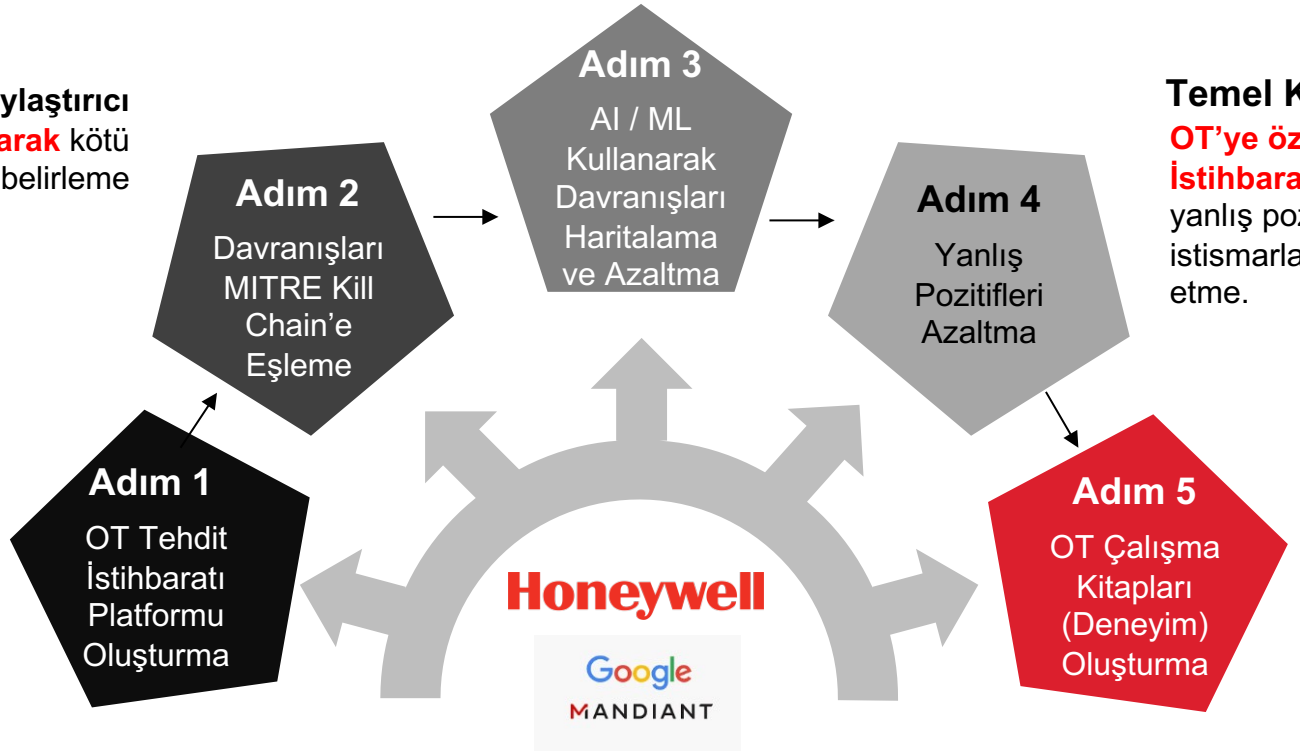
EKS / OT ortamı davranışlarındaki örüntüleri ve sapmaları belirleyerek bilinmeyen tehditleri ve anomalileri tespit etmek için **denetimsiz ML modellerini** kullanma

Temel Kolaylaştırıcı

Yapay zekâ kullanarak kötü amaçlı davranışları belirleme

Temel Kolaylaştırıcı

OT'ye özgü Siber Tehdit İstihbaratı akışlarının Veri zenginleştirmede kullanımı – **Google Tehdit İstihbaratı tarafından, önleyici siber güvenlik teknolojilerinden (deception) elde edilen verilerle desteklenmektedir**



Temel Kolaylaştırıcı

OT'ye özgü Tehdit İstihbaratından yararlanarak, yanlış pozitifleri azaltırken istismarları öngörme ve tespit etme.

Temel Kolaylaştırıcı

Yapay zekâdan yararlanarak, siber değerlendirmeler ve iş birlikleriyle desteklenen OT uzmanlığını kullanıp Kurumsal Görünümde bir bilgi tabanı oluşturma

REAKTİF SİBER GÜVENLİKTEN PROAKTİF SİBER GÜVENLİĞE GEÇİŞ

HONEYWELL FORGE Cybersecurity+

CYBER PROAKTİF SAVUNMA – DİJİTAL SOC ANALİSTİNİZ

SOC Analisti Görevleri	Honeywell Cyber Proactive Defense Bunu Nasıl Ele Alır (Otomatik ve Öngörücü)
Alarm Önceliklendirme ve İnceleme: Tier 1 analistleri, yanlış pozitifleri elemek ve gerçek tehditleri belirlemek için SIEM, EDR vb. kaynaklardan gelen yüksek hacimli alarmları inceler.	**Yapay Zeka Destekli İzleme ve Alarm Azaltma** OT ağ davranışını temel almak için ML kullanır, zararsız olayları filtreler ve verileri yüksek doğruluklu alarmlara dönüştürerek alarm yorgunluğunu ve önceliklendirme süresini azaltır.
Tehdit Avcılığı: Tier 3 analistleri, saldırgan davranışlarına ilişkin derin bilgi ve manuel teknikler kullanarak tespit edilmemiş tehditleri proaktif olarak araştırır.	**Gömülü Süreç Bilgisi ve Aldatma Teknolojisi** CPD, OT honeypots gibi entegrasyonlar ve otomatik iş akışları aracılığıyla uygulanabilir istihbaratı ortaya çıkarır ve alarmları tetikleyerek tehdit tespitini güçlendirir. Gömülü endüstriyel bağlam, özelleştirilmiş tespit ve daha hızlı müdahale sağlar.
Olay Müdahalesi ve Kontrol Altına Alma: Analistler, zaman açısından kritik koşullar altında etkilenen sistemleri izole eder, kötü amaçlı trafiği engeller ve tehditleri kontrol altına alır.	**Yapay Zeka Destekli Müdahale Oyun Kitapları** Özelleştirilebilir iş akışlarıyla olay müdahalesini otomatikleştirerek cihazları izole eder, C2 trafiğini engeller ve tehditleri kontrol altına alır; müdahale süresini önemli ölçüde kısaltır.
Tehdit İstihbaratı ve Analizi: Analistler, çoğu zaman manuel taramalar ve rapor incelemeleri kullanarak tehditleri belirler ve alınması gereken aksiyonları önerir.	**Tehdit İstihbaratı Entegrasyonu**: Ortaya çıkan tehditler konusunda güncel kalmak ve iyileştirme çalışmalarını önceliklendirmek için Honeywell ve Google tehdit akışlarını entegre eder.
Kök Neden Analizi ve Raporlama: Olay sonrası analistler adli analizler gerçekleştirir, bulguları dokümante eder ve etkiyi değerlendirmek ile tekrarını önlemek amacıyla raporlar oluşturur.	**Otomatik Veri Toplama ve Raporlama:** CPD, mevcut telemetriyi endüstriyel bağlamla zenginleştirerek izlemeyi çoğaltmadan kök neden analizini mümkün kılar. Otomatik ilişkilendirme, raporlamayı yalınlaştırarak analistlerin stratejik kararlara odaklanmasını sağlar.

OTD BİLİŞİM
GLOBAL VAD

CPD'NİN DİJİTAL SOC ANALİSTİNİZ OLARAK NASIL HAREKET ETTİĞİ

- **Akıllı bir yardımcı olarak hareket eder:** Platform, zenginleştirilmiş, gerçek zamanlı içgörüler ve önceliklendirilmiş tehdit alarmları sunarak SOC ekibinin daha hızlı ve daha doğru kararlar almasını sağlar.
- **SOC analistlerini güçlendirir:** Cyber Proactive Defense, SOC analistlerinin yetkinliklerini artıran gelişmiş bir çözümdür ve onların karmaşık, yüksek etki yaratan görevlere odaklanmasına olanak tanır.
- **Rutin işleri otomatikleştirir:** Veri ilişkilendirme ve ilk tehdit tanımlama gibi sürekli ve tekrarlayan görevleri üstlenerek analistlerin derinlemesine incelemelere ve stratejik tehdit avcılığına zaman ayırmasını sağlar.
- **Verimliliği ve hızı artırır:** Yapay zeka destekli müdahale oyun kitaplarıyla olay müdahalesini otomatikleştirerek tehditlere hızlı ve tutarlı bir yanıt verilmesini sağlar ve SOC ekibinin daha verimli çalışmasına olanak tanır.
- **İnsan uzmanlığını ölçeklendirir:** Bir kuvvet çarpanı gibi davranarak insan ekibinin erişimini ve etkinliğini genişletir; artan siber tehdit hacmi ve karmaşıklığıyla başa çıkılmasını sağlar.

HONEYWELL FORGE
Cybersecurity+

HONEYWELL FORGE
Cybersecurity+

KULLANIM SENARYOSU
HONEYWELL CYBER PROAKTİF SAVUNMA

OTD BİLİŞİM
GLOBAL VAD

POWER GENERATION USE CASE

GÜÇ ÜRETİMİ KULLANIM SENARYOSU

Kamu hizmeti kuruluşu, gelişmiş kalıcı tehditlerden (APT'ler) gelen sofistike sızma girişimleri de dâhil olmak üzere operasyonel teknoloji (OT) ağını hedef alan artan siber tehditlerle karşı karşıya kaldı. Sınırlı OT siber güvenlik personeli ve gerçek zamanlı tehdit görünürlüğünün olmaması nedeniyle kuruluş, hızlı ve etkili şekilde müdahale etmekte zorlandı.

Çözüm

OT siber güvenlik duruşunu proaktif olarak güçlendirmek amacıyla kamu hizmeti kuruluşu, dijital bir SOC analisti olarak tasarlanmış yapay zeka destekli bir yazılım çözümü olan Honeywell Cyber Proactive Defense (CPD)'i devreye aldı. CPD:

Ağ verilerini zenginleştirip ilişkilendirerek davranışsal anormallikleri olaylara dönüşmeden önce ortaya çıkardı.

- Stratejik olarak konumlandırılmış OT honeypot gibi aldatma teknolojileri dâhil olmak üzere çoklu entegrasyonlar aracılığıyla tehdit tespitini zenginleştirdi; şüpheli faaliyetleri görünür kılarak saldırganları yüksek değerli varlıklardan uzaklaştırdı.
- Yapay zeka odaklı oyun kitaplarını etkinleştirerek olay müdahalesini otomatikleştirdi ve müdahale süresini saatlerden dakikalara indirdi.

SONUÇ

Birkaç hafta içinde kamu hizmeti kuruluşu, operasyonlarda herhangi bir kesinti yaşanmadan çok sayıda sızma girişimini tespit etti ve etkisiz hâle getirdi. CPD'nin otomatik oyun kitapları, yalın güvenlik ekibinin verimli şekilde müdahale etmesini sağlarken, aldatma katmanı erken uyarı ve zenginleştirilmiş istihbarat sunarak reaktif savunmayı proaktif dayanıklılığa dönüştürdü.

OTD BİLİŞİM
GLOBAL VAD

ÖZET

- Müşteriler, karmaşık OT ortamları genelinde tehdit avcılığını ve analizi ölçeklendirme konusunda giderek artan zorluklarla karşı karşıya kalmaktadır.
- Honeywell Cyber Proactive Defense (CPD), tehditler zarar vermeden önce tespit etmek, aldatmak ve müdahale etmek üzere katmanlı ve proaktif bir siber güvenlik stratejisi sunar.
- CPD, davranışsal verileri yapay zeka kullanarak zenginleştirir ve ilişkilendirir; anormallikleri belirleyerek potansiyel saldırıları öngörür.
- CPD, OT honeypot gibi entegrasyonlar ve otomatik iş akışları aracılığıyla uygulanabilir istihbaratı ortaya çıkarır ve alarmları tetikleyerek tehdit tespitini güçlendirir. Gömülü endüstriyel bağlam, özelleştirilmiş tespit ve daha hızlı müdahale sağlar.
- Yapay zeka destekli oyun kitapları, olay müdahalesini otomatikleştirir ve orkestre ederek daha hızlı ve tutarlı tehdit azaltımı sağlar.
- CPD, dijital bir SOC analisti olarak hareket ederek yalın güvenlik ekiplerinin reaktif savunmadan proaktif dayanıklılığa geçişini sağlar.

Honeywell Cyber Proactive Defense Tarafından Sağlanan Kritik İş Sonuçları

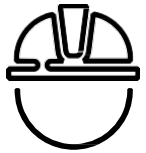
HONEYWELL FORGE
Cybersecurity+

NEDEN HONEYWELL'İ SEÇMELİSİNİZ

OTD BİLİŞİM
GLOBAL VAD

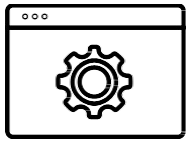
OTD BİLİŞİM
GLOBAL VAD

HONEYWELL'İN OT SİBER GÜÇLÜ YÖNLERİ



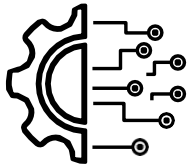
İNSANLAR

- OT siber güvenliği alanında 25 yılı aşkın deneyim
- 37 ülkede, OT siber güvenliğine adanmış 500'den fazla çalışanla küresel varlık
- 130'dan fazla ülkede tamamlanmış 7000'den fazla proje



UZMANLIK

- Honeywell genelinde en üst düzey uzmanlara ve sektör içgörülerine erişim
- Atlanta, Singapur ve Dubai'de Küresel Siber Güvenlik Mükemmeliyet ve İnovasyon Merkezleri
- Sektörel uzmanlık sunan Küresel OT Yönetilen Güvenlik Hizmetleri
- OT siber güvenliği alanında 38 patent



ÇÖZÜMLER

- Uçtan uca kapsamlı çözümler için ürünler ve hizmetler
- Ürünler, siber tehditlerin etkin şekilde giderilmesi için üçüncü taraf çözümlerle sorunsuz biçimde entegre olur.
- Hizmetler, Google ve Fortinet gibi en iyi sınıf güvenlik sağlayıcılarıyla yapılan iş birlikleriyle de desteklenmektedir.

İŞ BİRLİĞİ

- Sektör iş ortakları (örn. OT Cyber Coalition – kurucu üye)
- Standart iş ortakları (örn. ISASecure – kurucu üye)
- Devlet kurumlarını destekleme (örn. CISA, CSA Singapur)

HONEYWELL FORGE
Cybersecurity+

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL CYBER PROAKTİF SAVUNMA, DAHA GENİŞ BİR OT SİBER GÜVENLİK ÇÖZÜMÜNÜN PARÇASIDIR

★ Yakında

VARLIK KEŞFİ, RİSK VE ZAFİYET ANALİZİ

DAHA ETKİN TEHDİT TESPİTİ VE MÜDAHALESİYLE PROAKTİF SAVUNMA

OT'YE ÖZGÜ TEHDİT İSTİHBARATINA ERİŞİM

RİSK, ZAFİYETLER VE UYUMLULUĞA İLİŞKİN KURUMSAL GÖRÜNÜM

Cyber Insights* Cyber Watch*	Cyber Proactive Defense Secure Media Exchange	Cyber Threat Intelligence	Cyber Governance, Risk and Compliance ★

*Single and Multi-Site

HONEYWELL OT SİBER GÜVENLİK HİZMETLERİ

PROFESYONEL HİZMETLER

- OT siber güvenliğinin tüm yaşam döngüsünü destekleyen 30'dan fazla profesyonel hizmet (değerlendirmeler, iyileştirme, mimari ve tasarım, eğitimler ve çok daha fazlası)
- Cyber Care hizmetleri (yerinde)
- Üçüncü taraf teknolojilerin entegrasyonu

YÖNETİLEN GÜVENLİK HİZMETLERİ

- Secure remote access
- Yama / AV yönetimi
- Cyber Care hizmetleri (uzaktan)

OT GÜVENLİK OPERASYON MERKEZİ (OT SOC)

Yerleşik gelişmiş güvenlik analitiği, derinlemesine olay incelemesi ve orkestre edilmiş olay müdahalesi ile birlikte 7/24 gerçek zamanlı tehdit izleme ve tespit sağlar.

ELE GEÇİRİLME OLASILIĞINI VE ETKİNİN ŞİDDETİNİ AZALTIN

EYLEME ÇAĞRI

HONEYWELL FORGE Cybersecurity+

- Tüm OT varlıkları ve ortamları genelinde görünürlüğünüzden emin misiniz?
- Kuruluşunuzun siber risk profilini ve maruz kaldığı noktaları anlıyor musunuz?
- Davranışları ilişkilendiren ve tehdit tespitini zenginleştiren — saldırılar gerçekleşmeden önce öngörmenize yardımcı olan AI- powered içgörülerden fayda sağlar mıydınız?

OT'nizin gözden geçirilmesinde paydaşlar kimlerdir?

- CIO/CISO
- Kurumsal BT
- Tesis Yöneticisi
- Mühendis

- Tehditler ortaya çıkmadan önce OT ortamlarını güçlendirmek üzere tasarlanmış bir strateji olan Cyber Proactive Defense'e geçişte liderliğinizi desteklemek için Honeywell ile etkileşime geçin.
- Endüstriyel ortamınız genelinde zenginleştirilmiş ve ilişkilendirilmiş, OT'ye özgü tehdit istihbaratından yararlanarak siber riski azaltın.
- Davranışsal anormallikleri ve maruz kalma noktalarını ortaya çıkaran yapay zeka destekli içgörülerle kuruluşunuzun siber güvenlik duruşuna netlik kazanın.
- Gelişmiş izleme ve otomatik olay müdahalesini mümkün kılmak için Honeywell'in uzmanlığından faydalanarak ekibinizi dijital SOC analisti yetkinlikleriyle güçlendirin.

OTD BİLİŞİM GLOBAL VAD

TEŞEKKÜRLER

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD