Enerji Santrallarında Siber Güvenlik

Bülent Harput

Bölge Satış Yöneticisi

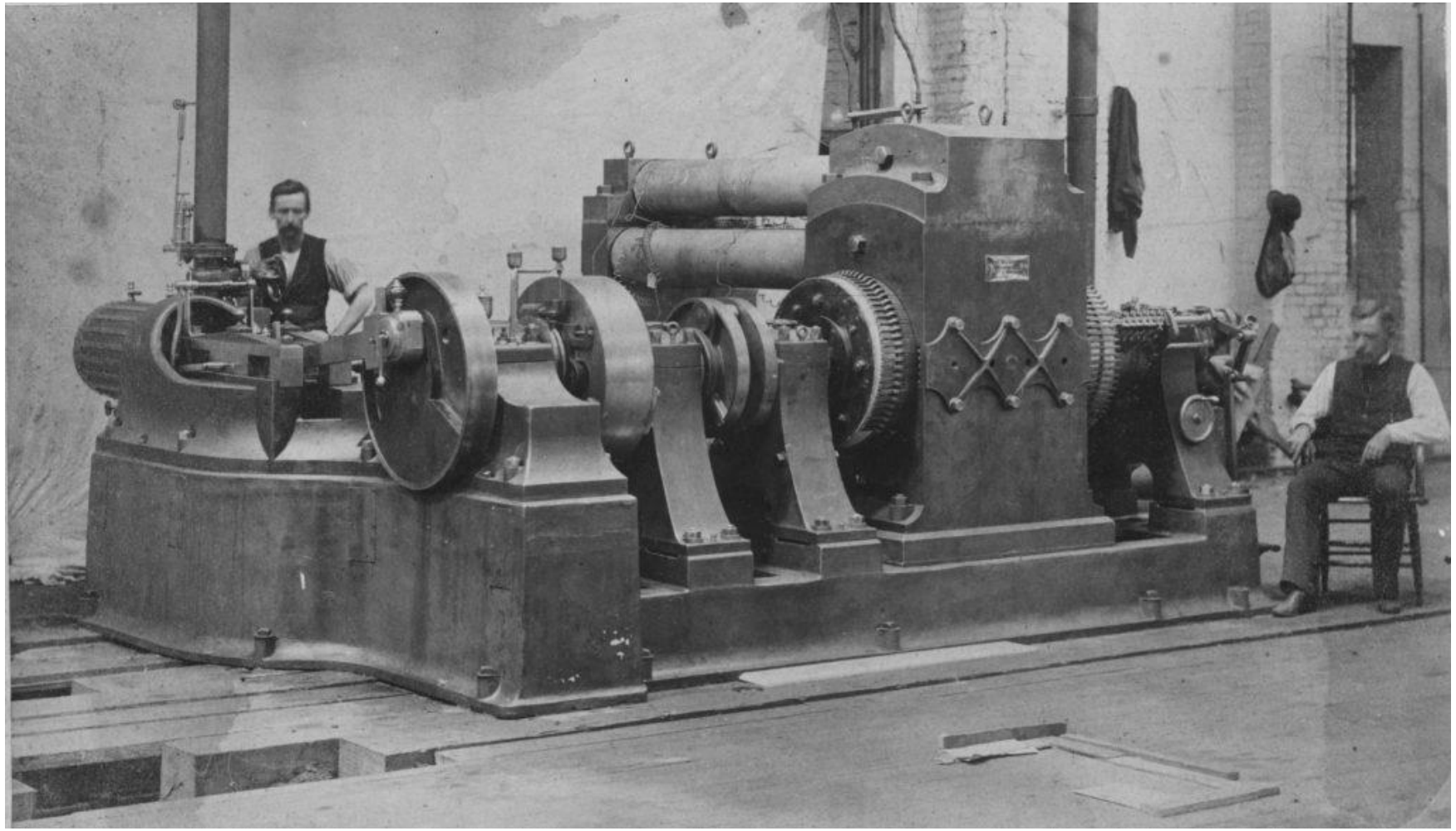
GE Dijital

ICCI

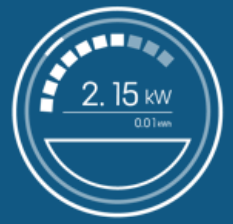
16 Ekim 2020

Imagination at work

Dijital Dönüşüm ve Siber Güvenlik



Bağlı Cihazlardaki Artış



1,6 MİLYAR

Akıllı sayaç

31 MİLYAR

Nesnelerin interneti cihazı

152 MİLYON

Bağlı otomobil sayısı

7,3 MİLYAR

Akıllı telefon ve
ağa bağlı kişisel bilgisayar

+$300 MİLYAR

İlave ciro, çoğunlukla servis alanında

$1.9 TRİLYON

Beklenen ekonomik katma değer

Source:
Gartner - The Internet of Things, Worldwide, 2013
IHS-Forbes Number of Internet of Things (IoT) Connected Devices Worldwide 2019

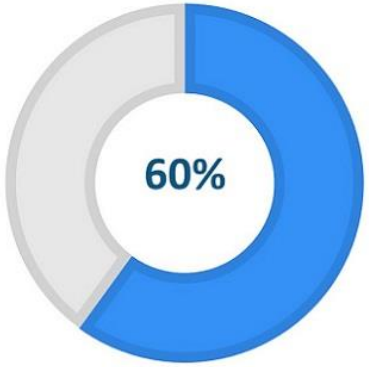
Kritik Altyapı Tesislerine Yönelik Siber Saldırılar

In 2018 **41,686** security Incidents [3] across **86** Countries [3]

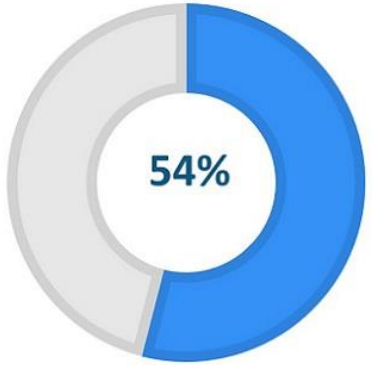
91%
of Power Generation organisations have experienced a Cyber Attack [5]

29%
of reported attacks are against Power & Water [6]

of companies experienced at least one attack against OT infrastructure resulted in downtime in the past 24 months [2]



expect a successful exploit on their OT Infrastructure in 2019 [2]



of companies believe their organization's cybersecurity posture to stay the same [4]

[2] T. Ponemon, "Cybersecurity in Operational Technology: 7 Insights you need to know," Ponemon Institute, 2019.
[3] Verizon, "Data Breach Investigations Report (DBIR) 2019," Verizon, 2019.
[4] P. Ratheon, "2018 Study on Global Megatrends in Cybersecurity," Ponemon Institute, 2018.
[5] T. Bayar, "Cybersecurity in the power sector," Power Engineering International, 2014.
[6] NCCIC, "ICS-CERT Year in Review 2016," NCCIC, 2016.

Enerji Sektöründe Siber Saldırılar

Risk Büyük

+300 bin Enfekte Bilgisayar
200 bin Fidye Yazılım Kurbanı
WannaCry Attack (2017)

Bir Alman Nükleer Santralinde Plant **18 Virüslü** USB bellek tespiti (2016)

Ukrayna'da **200 bin** üzerinde kişiyi etkileyen siber saldırı sonucu elektriğinin kesilmesi (2015)

Bir Alman Çelik tesisinde siber saldırı sonucu kontrol sistemi arızasının **yüksek fırında büyük hasar**a sebep olması (2014)

İran **nükleer santrifüjler**inin beşte birinin SCADA and PLC'leri hedef alan Stuxnet saldırısıyla aşırı hızdan hasarlanması (2010)

Açık Önlem İhtiyacı

Enerji sektöründe çalışan bilişim uzmanları ne diyor?

96% : IIoT siber saldırılarında artış bekleyenler

64% : Kritik varlıklarının korunmasına ihtiyaç duyanlar

51% : Siber saldırılara hazırlıksız olduklarını düşünenler

*1 Source: Dimensional Research by Tripwire. Survey to 403 IT professionals

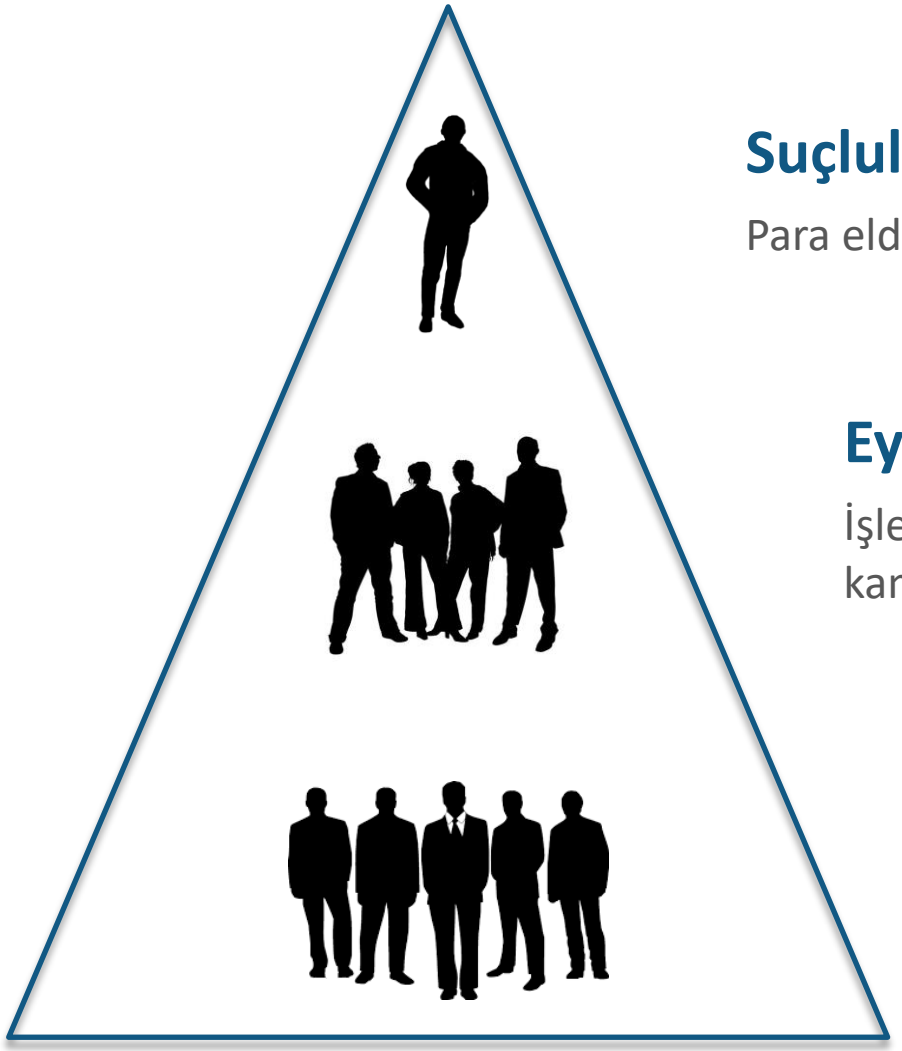
En Önemli Siber Riskler : Bulgular

GE Siber Güvenlik Durum Tespitleri

- 2016'dan beri
- Dünya çapında

Özet	
Saldırıya açık işletim sistemi kullanılan en az bir sistem bulunanlar	96%
En az bir çift bağlantı noktalı sistemi (güvenlik duvarında açık) olanlar	96%
Uçnokta çözümünün süresi geçmiş en az bir sistemi olanlar	92%
Kullanıcı girişleri uygun olmayanlar	88%
En az bir sisteminde kötü niyetli yazılım tespit edilenler	8%
Etkin siber güvenlik gözetimi yapanlar	0%
Yönetici şifresi değişmeden kalan en uzun süre	?

Siber Tehditlerin Arkasında Kim Var?



Kaynaklar

Unutulmaması Gereken Tehdit:

İnsan Hatası

Suçlular:

Para elde etme ya da dikkat çekme amaçlı sızmalar (ör: fidye yazılımları)

Eylemciler:

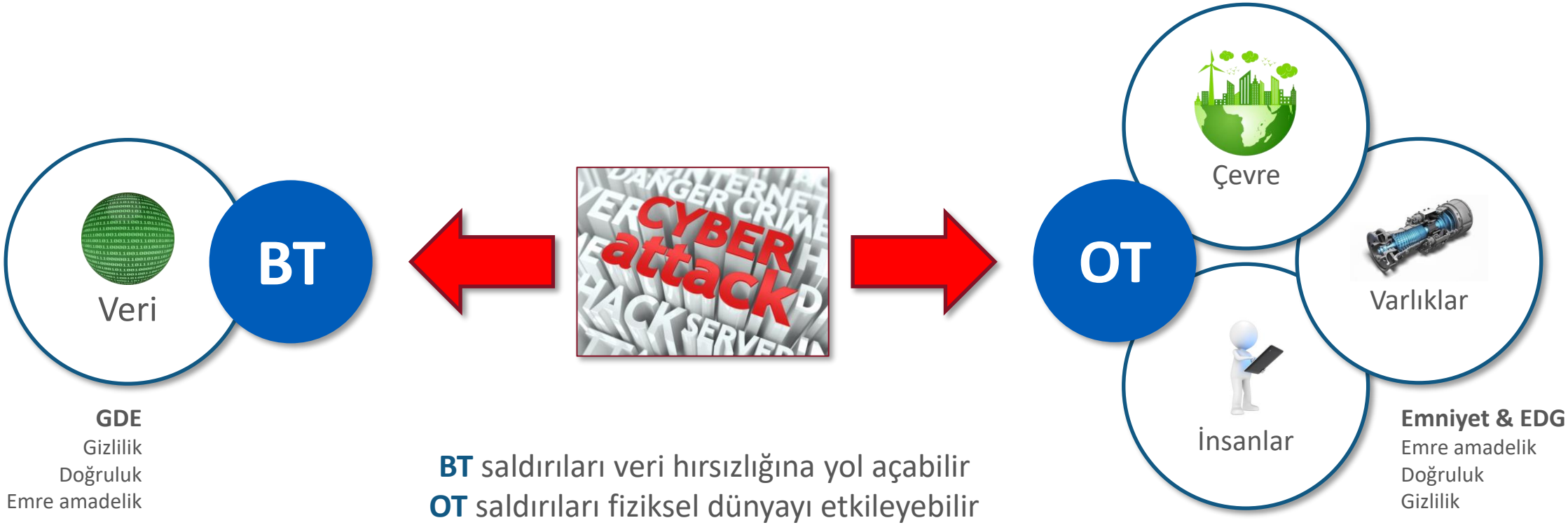
İşletmelerin güvenlik açıklarını ortaya çıkararak ilgili tesisin kapatılması için kamuoyu oluşturmak veya başka sosyal amaçlar için dikkat çekmek

Kamu kurumları:

Siber savaş programı çerçevesinde enerji, su, haberleşme benzeri kritik sanayi kuruluşlarına sızarak rakip bir devleti yıpratma amaçlı kurulan özel birimler

Kritik Altyapı Tesislerinde Siber Güvenliğin Sağlanması

Bilişim Teknolojisi güvenliği ve **Operasyon Teknolojisi** güvenliği birkaç açıdan farklıdır.
Ama en önemli farkları saldırıların sonuçları açısındandır.



GDE
Gizlilik
Doğruluk
Emre amadelik

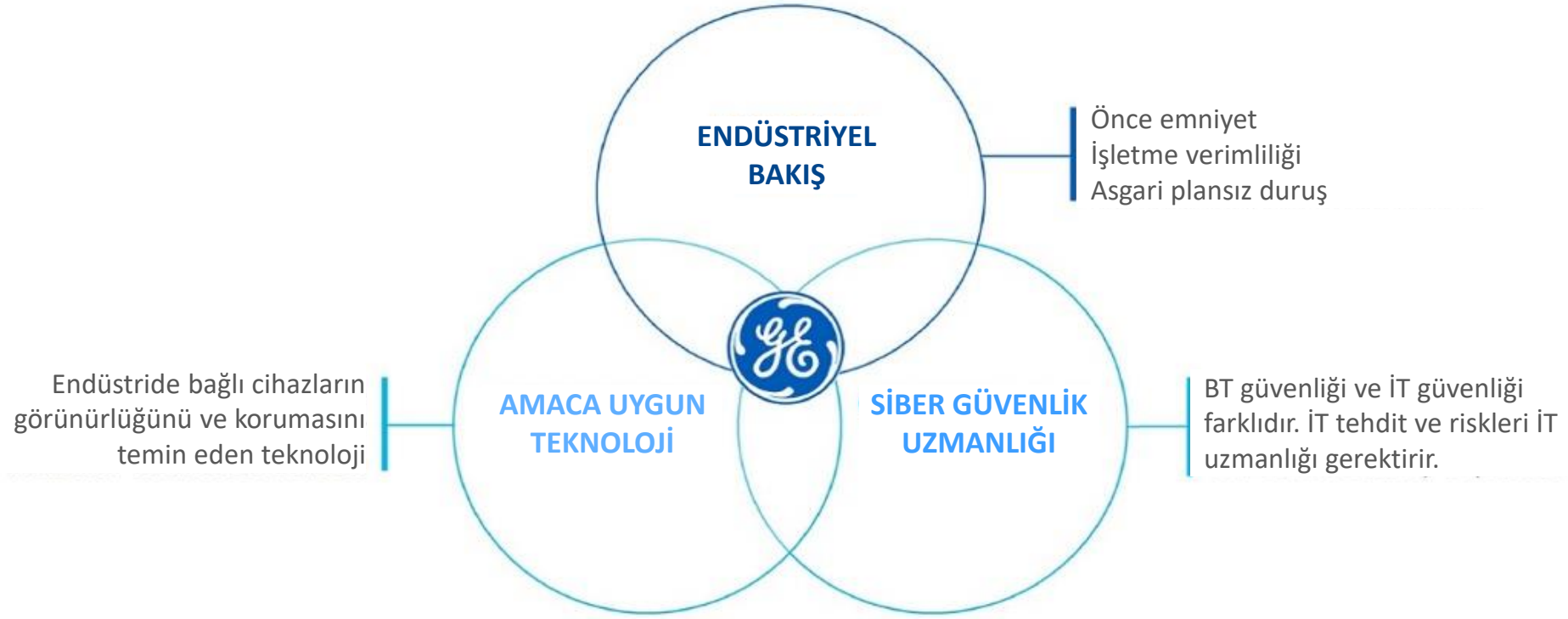
Emniyet & EDG
Emre amadelik
Doğruluk
Gizlilik

BT saldırıları veri hırsızlığına yol açabilir
OT saldırıları fiziksel dünyayı etkileyebilir

Önemli bir fark…

Farklılıklarıyla beraber **BT** ve **OT** güvenliği birbiriyle örtüşür ve birleşir.

GE Enerji - Dijitalizasyonda Siber Güvenlik Yaklaşımı



GE's Solution Mapping to CIS Critical Security Controls

CIS Controls™ V7

Esas

1. Donanım envanterinin çıkarılması ve takibi
2. Yazılım envanterinin çıkarılması ve takibi
3. Zaafların düzenli yönetimi
4. Yönetsel erişim hakların kontrollü kullanımı
5. Mobil cihaz, bilgisayar, iş istasyonu ve sunucuların donanım ve yazılımlarının güvenli yapılandırılması
6. Denetim kayıtlarının bakım, takip ve analizi

Temel

7. E-posta ve tarayıcı koruması
8. Kötü niyetli yazılım savunması
9. Ağ kapılarının, protokol ve servislerin sınırlanması ve kontrolü
10. Ver kurtarma kabiliyetleri
11. Güvenlik duvarı, yönlendirici ve anahtarların güvenli yapılandırılması
12. Sınır savunması
13. Veri koruma
14. İhtiyaca dayalı kontrollü erişim
15. Kablosuz erişim kontrolü
16. Hesap takip ve kontrolü

Organizasyonel

17. Güvenli farkındalığı ve eğitim programı
18. Uygulama yazılımı güvenliği
19. Olay müdahale yönetimi
20. Sızma testleri ve Kırmızı Takım Çalışmaları

GE Digital: Siber Güvenlik Çözüm Portföyü

Profesyonel Hizmetler

Saha incelemesi, sızma testi, eğitim ve benzeri bir seri siber güvenlik hizmeti sunuyoruz.

Yama Doğrulama Programı

İhtiyaç duyduğunuz yamaları test edilmiş, doğrulanmış ve kolayca yüklenebilecek paketler halinde sunuyoruz.

Temel Güvenlik Merkezi

Bu çözümle işletmelerin santral ortamında sağlam ve derinliğine savunma kontrollerini tek bir entegre platform içinde kapsamlı güvenlik yetkinlikleri sunuyoruz.

Sızma Tespit Sistemi

Bu çözümle endüstriyel kontrol sistemlerinde siber tehdit ve süreç anomalilerini hızla tespit ederek benzersiz işletme görünürlüğü ve geliştirilmiş siber dayanıklılık sağlıyoruz.

Uzaktan İzleme ve Olay Müdahalesi

Bu hizmet İT kontrol ortamlarındaki güvenlik olayları için uzaktan izleme ve teşhis hizmetleri sunacak.

Dijital Hayalet

Verileri makine öğrenmesi yoluyla dijital ikiz modelleriyle karşılaştırıp ağ bileşenlerindeki hata ya da saldırı kaynaklı anormallikleri tespit edip etkisiz hale getirecek.

Endüstriyel Siber Güvenlik

Bütünlüklü bir siber güvenlik çözümü **ekipman, veri, insan** ve **çevre** unsurlarını dikkate almalıdır.

Teşekkürler