

Kritik OT Altyapıların Sibergüvenliği

Yasin Yiğit Günaydın

07.10.2026



OT Ağlarında Siber Risk Yönetimi

“Sıfır Siber Risk” gerçek dışıdır.

- İzole ağların riskleri:
 - USB (örn. Stuxnet), fabrika çıkışı kötü niyetli bilgisayar (pager explosion), sorunlu çalışan vb.
- Deprem analojisi

Risk Gerçekleştğinde...

Muleshoe, Texas

HMI'nin zayıf bir şifreyle internete açık olması sonucu su arıtma tesisi hedef alındı.

FrostyGoop

600 dairelik bir binada ısıtma kesildi. Ucuz bir router arkasındaki düz (flat) ağ...

Jaguar Land Rover

IT tarafını vuran büyük bir fidye yazılımı saldırısı, OT tarafında da büyük bir duruşa neden oldu.

Lake Risevatnet Barajı

Ele geçirilmiş yazılım güncellemesi, fiziksel varlıklar üzerinde yetkisiz kontrol elde edilmesine neden oldu.

WORLD > MIDDLE EAST • 4 MIN READ

Hacked traffic cameras and US intelligence: How a plot to kill Iran’s supreme leader came together

UPDATED MAR 4, 2026 ▾

Russian hackers breached Polish power grid thanks to bad security, report says

The Polish government said Russian government hackers broke into parts of the country’s energy grid infrastructure, taking advantage of its poor security.

Pro-Ukrainian hackers claim massive cyberattack on Russia's Aeroflot

Zaman daralıyor...

- Mythos/Astra/Qwen27B
- OT içi yanal hareketler
- 20 saat!
- 28 dakika!
- Amaç: Hasar alanını limitlemek



Alican Kiraz @AlicanKiraz0 · 14 Eyl

Dostlar ürkütmek gibi olmasın ama, Siber güvenlik odaklı Uncensored 27B parametrelili finetune ettiğim modelin saldırı odaklı kullanıldığında (açık kaynak paylaşılmayacaktır, akademik amaçlıdır) çıktılarını paylaşmak istedim.

Hackthebox'da (izole ve deneysel çalışmalar yapabileceğiniz Siber güvenlik ortamlarından biri) yer alan laboratuvar alanında hiçbir bilgi vermeden iki makinenin sadece IP bilgisi verilerek hedef gösterdim

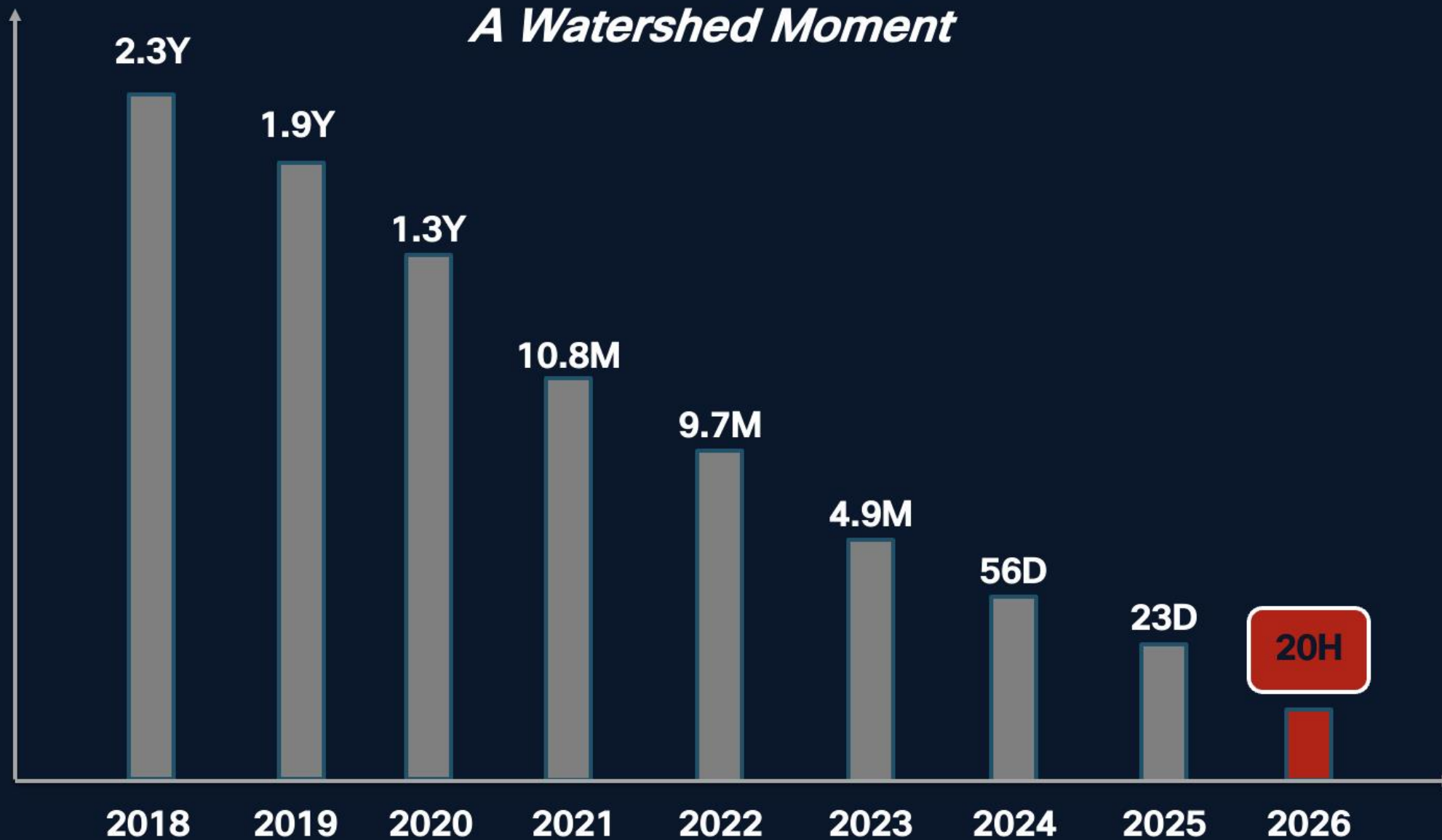
Klasik bir harness ile çalıştırdığımda, ortalama 25 adımda ve 28 dakika da iki makinenin de kullanıcı yetkilerini, ardından da administrator yetkilerini zafiyetleri kullanarak elde etti.

Üstelik bu ortalama 300K token yani base modelin 1M/\$ fiyatı üzerinden değerlendirecek olursak 0.7 dolara başardı.



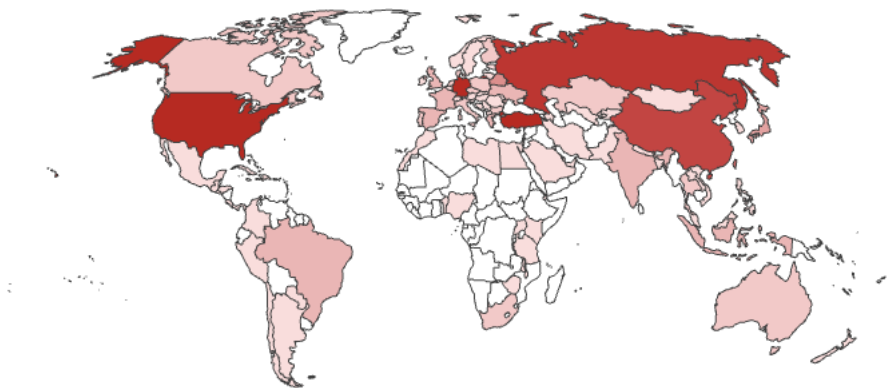
From Vulnerability to Exploitation

A Watershed Moment



Peki nasıl?

TOP COUNTRIES



Türkiye	1,044
United States	256
Germany	208
Russian Federation	193
China	157

[More...](#)

TOTAL RESULTS

36,944

TOP CITIES

Istanbul	14,083
İzmir	4,257
Ankara	3,854
Bursa	2,494
Antalya	2,157

[More...](#)

TOP PORTS

80	17,226
81	2,965
8010	1,981
82	946
8080	665

[More...](#)

IEC-60870-5-104

CCTV Kameralar

shodan.io/host/188.

Form Doldurma Araç Çubuğunu Göster

188.

Regular ViewRaw DataTimelineWhois

İstanbul

BuyukçekmeceBeyliközüKucukçekmeceBahçelievlerZeytinburnuAtaşehirSancaktepeKurtdoğanEmirliBallicaGöztepe

OpenMapTiles SatelliteMapTilerOpenStreetMap contributors

// TAGS: ics self-signed

// LAST SEEN: 2026-09-15

General Information

Hostnames

host17

Domains

Country

Turkey

City

Istanbul

Organization

ISP

ASN

AS

Vulnerabilities

All portsCVSS

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

Critical (5)

CVE-2015-7705

9.0

The rate limiting feature in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to have unspecified impact via a large number of crafted requests.

Open Ports

531231701808047808

// 53 / TCP {}1245902056 | 2026-09-14T14:23:51

dnsmasq-2.91
Recursion: enabled

// 53 / UDP {}1245902056 | 2026-09-15T04:29:29

dnsmasq-2.91
Recursion: enabled

// 123 / UDP {}-374011215 | 2026-09-15T01:53:57

ntpd 428

NTP
version: ntpd 4.2.8p15@1.3728-o Wed Jan 7 06:54:31 UTC 2026 (1)
processor: aarch64
system: Linux/4.14.98
leap: 0
stratum: 4
precision: -22
rootdelay: 126.990
rootdisp: 20.315
refid: 16:
reftime: 0xee532361.b362f6eb
clock: 0xee5323b5.c4ba9755
peer: 18942
tc: 8

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO

CVE-2024-25117 zafiyetinin nasıl çalıştığını ve profesyonel bir ortamda nasıl ele alınması gerektiğini aşağıda özetledim:

Zafiyetin Çalışma Mekanizması

- **Bileşen:** Bu zafiyet, web uygulamalarının SVG dosyalarını ayrıştırmak veya işlemek için kullandığı php-svg-lib kütüphanesinde bulunmaktadır.
- **Hata:** Kütüphane, SVG kodu içindeki font-family özniteliğini işlerken katı bir doğrulama yapmamaktadır.
- **Saldırı Yöntemi:**
 - Bir saldırgan, font-family kısmına özel olarak oluşturulmuş bir dize (string) yerleştirerek bir PHP Arşivi (PHAR) dosyasına işaret edebilir.
 - Kütüphane bu dosyayı işlerken, farkında olmadan PHAR protokolüyle ilişkili dosya işlemlerini veya serileştirme (deserialization) rutinlerini tetikleyebilir.
 - Sunucu ortamı bu işlemlere izin veriyorsa, bu durum **Uzaktan Kod Çalıştırma (RCE)** ile sonuçlanabilir ve saldırganın web sunucusu yetkileriyle komut çalıştırmasına olanak tanır.

php

 Copy

```
// TEHLİKELİ KULLANIM (Zafiyetli)  
$svgContent = $_POST['user_uploaded_svg']; // Kullanıcıdan gelen kontrolsüz veri  
$renderer = new Svg\Renderer();  
  
// Kütüphane, içerideki 'font-family' değerini kontrol etmeden işlerse:  
// Saldırgan bu SVG içine 'phar://malicious.phar' gibi bir değer enjekte edebilir.  
$renderer->render($svgContent);
```

**Sibergüvenlik, siber riskleri
anlama ve etkilerini hafifletme
sanatıdır.**

Anahtar Terimler (CISA Cybersecurity Performance Goals)

Risk Değerlendirmesi

Neyin ters gidebileceğini ve bunun ne kadar zarara yol açacağı.

NIST'e göre:

- Vendor
- Model
- Yazılım versiyonu
- İşletim sistemi

detayları kritiktir.

Risk Toleransı

Bir organizasyonun hedeflerine uygun olarak kabul ettiği risk miktarı.

- Kabul edilebilir maksimum kesinti süresi
- Kabul edilebilir veri kaybı miktarı ve türü
- Maksimum finansal kayıp tahmini
- Ağ kurtarma hedefi

Risk Kabulü

Riski azaltmadan dinamik biçimde tutmaya karar vermek.

Örneğin:

- Çok nadir görülebilecek bir risk
- Risk azaltma masrafının daha yüksek olması
- İyileştirme planlarken belirli bir süre boyunca riski kabul etmek

Cisco OT Güvenlik Çözümü

Ağa entegre kapsayıcı güvenlik

Cisco Cyber Vision

Splunk / XDR



Risk maruziyetine
görünürlük



Etki alanını kısıtlama
için segmentasyon

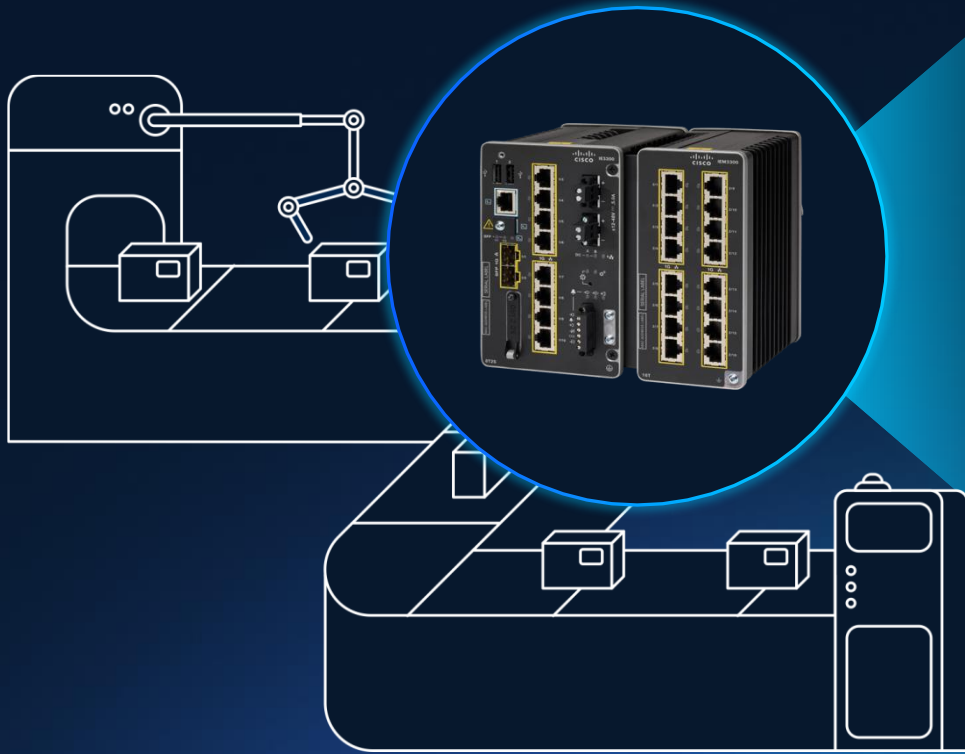


OT varlıklarına güvenli
uzaktan erişim



OT ağı için SOC
izlemesi

Cisco Endüstriyel Switchler ile riski anlama ve azaltma



Görünürlük

Risk maruziyetini SPAN olmadan anlama



Segmentasyon

Ağ tarafından uygulanan line-rate koruma



Güvenli Uzaktan Erişim

Ek donanımsız OT ZTNA

Cisco Endüstriyel Routerlar ile riski anlama ve azaltma



Visibility

Risk maruziyetini SPAN olmadan anlama



NGFW

OT uygulamalarını tanıyan NGFW



Secure Remote Access

Ek donanımsız OT ZTNA

Splunk ile Saldırı Zaman Çizelgesi Analizi

