
SafeBreach
BT
OT
EKS VE KRİTİK ALTYAPILARA YÖNELİK
Red - Teaming
SİBER SALDIRI B A S ÇÖZÜMÜ
Savunmanızı Geliştirmek için
"SALDIRILARDAN YARARLANIN"
OTD BİLİŞİM
GLOBAL VAD
ICT
OTD
PREFER EXPERIENCE ONLINE
Since 2011

Modern Kurum Güvenliği Giderek Daha Az Değil, **Daha Fazla** Karmaşık Hale Gelmektedir.

Ortalama olarak kurumlar ağlarında siber güvenlik konusunu ilgilendiren **75** araç kullanmaktadır

Başarıya ulaşan ihlallerin **%95**'i bilinen saldırıların birer sonucudur

Kurumların **%61**'i siber risk azaltma çalışmalarını önceliklendirmede zorluk yaşamaktadır.

BT ve OT Ekiplerinin Savunma Sistemlerini Güçlendirmek

Güvenlik kontrollerinin etkinliğinin test edilmesi, gelecek yatırımlara öncelik verilmesi

Raporlanabilir metriklere sahip veri güdümlü yaklaşım

Saldırganların kurum genelinde izleyeceği yüksek hassasiyetli varlıklara giden muhtemel yolların bulunması

Savunucuların tecrübesinin sürekli olarak iyileştirilmesi

OTD BİLİŞİM GLOBAL VAD

Bunları Biliyor musunuz...

%94

Son zamanlarda ankete katılan kuruluşlardan önceki 12 ayda bir OT/IoT güvenlik olayı yaşayanların yüzdesi

%80

Endüstriyel kuruluşların %80'i yılda yalnızca bir kez veya daha az bir EKS güvenlik değerlendirmesi gerçekleştiriyor

3

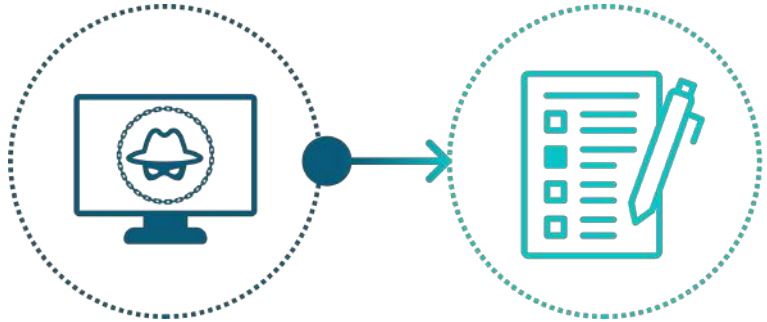
Mühendislik iş istasyonları, HMI'lar ve operasyon sunucuları (tümü Windows veya Linux gibi ticari bir işletim sistemi çalıştıran), bir OT saldırısında tehlikeye girme riski en yüksek olan ilk 3 kontrol sistemi bileşenidir

Birçok OT Saldırısı, BT Saldırıları Olarak Başlıyor

Birçok saldırı, BT ağı üzerinden girişle başlar.

Saldırganlar içeri girdikten sonra, kimlik bilgileri elde etmek ve OT ağına giden savunmasız yolları belirlemek için keşif yapar.

Saldırgan daha sonra, OT DMZ gibi daha yüksek güvenlik bölgelerindeki sistemlere erişmek için önceden güvenliği ihlal edilmiş sistemlerden, kimlik bilgilerinden veya uygulamalardan yararlanır.



Bilgi Kaynakları	Hedef Bilgisi
Sistem veya süreç belgeleri	Üst düzey ağ mimarisi diyagramları
Klavye Dinleme	Ana bilgisayar adları ve IP adresleri
Ekran izleme	İletişim yolları
Ağ yönetimi konsolları	Kullanıcı adları ve kimlik bilgileri
Port taraması (aktif ve pasif)	

Mükemmel Fırtına

Tasarımı Nedeniyle Güvensiz EKS

- **Düz ağlar**
- **Zayıf kimlik doğrulama**
- **Şifrelemesiz**
- **Güvenli olmayan EKS protokolleri**
- **Zor/nadir yama**

Artan şekilde bağlı

- **Entegre BT/OT ağlar**
- **En alttan en üste KPI'lar**
- **Veri analizi programları**
- **Tedarik zinciri entegrasyonu**
- **Uzaktan erişimi**

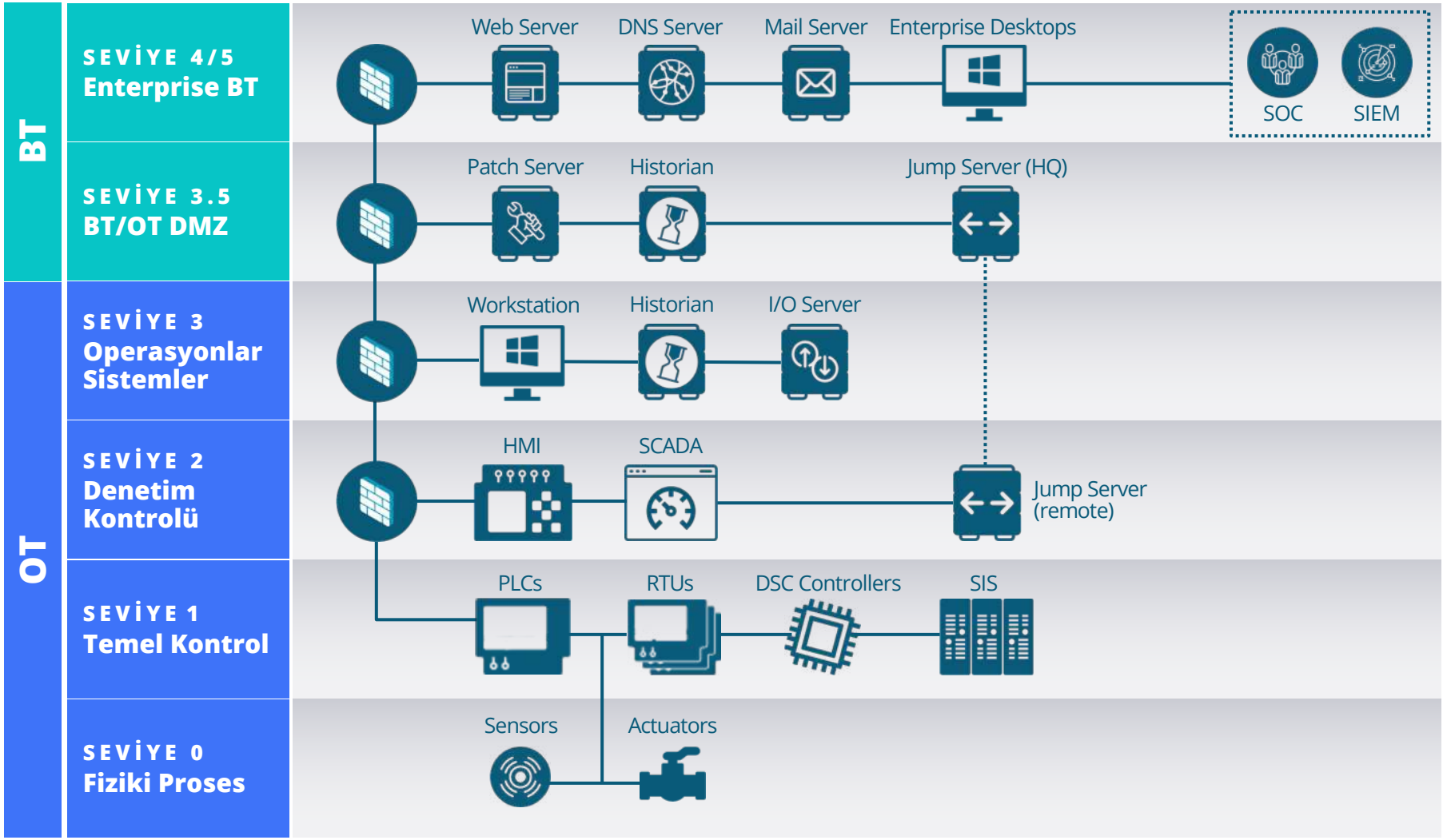
Aktif Tehdit Görünümü

- **Ulus-Devlet saldırıları EKS'yi hedefliyor**
- **DHS/FBI, GCHQ, Diğerlerinden tekrarlanan uyarılar**
- **Fidye yazılımı saldırılarından milyarlarca ikincil hasar**
- **Savunmasız sistemlere erişmek için gelişmiş bilgisayar korsanlığı bilgisi gerekmez**

EKS AĞINDA ZAYIF GÖRÜNÜRLÜK

OTD BİLİŞİM GLOBAL VAD

Purdue Mimarisi



SafeBreach

BAS ve BT/OT Ortamı

Bu, güvenlik programınıza nasıl uyuyor?

OTD BİLİŞİM GLOBAL VAD

OTD ICT PREFER EXPERIENCE ONLINE Since 2011









Tesisin Her Yerinde Daha İyi Koruma ve Görünürlük

Üretim Çalışma Süresini Koruyun

BT/OT Güvenlik Testini Birleştirin, İyileştirin ve Raporlayın

OT Dijital Dönüşümünü Güvenle Destekleyin

Tedarik Zinciri Güvenliği Maruziyetini Kontrol Edin

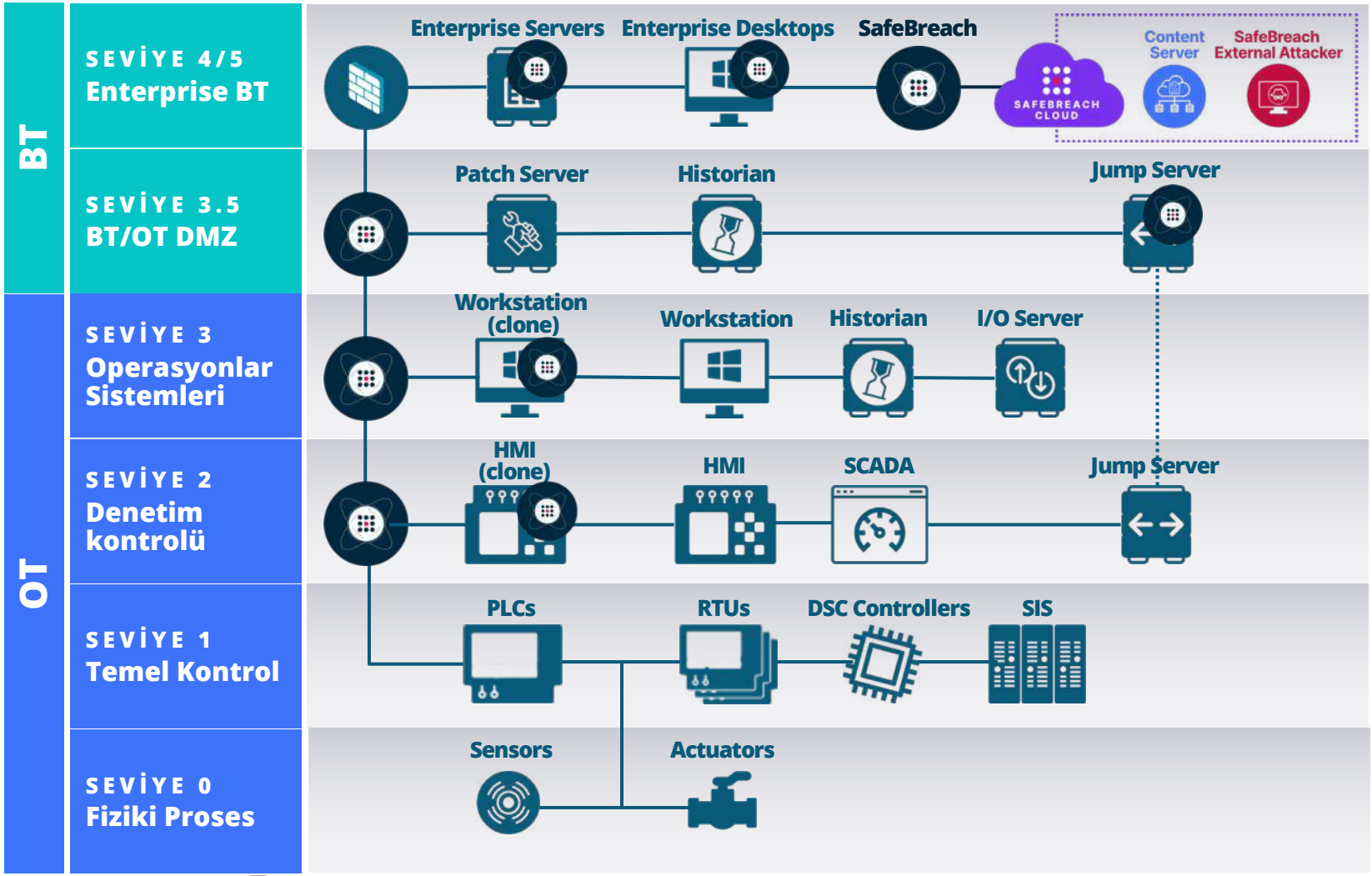
BT ve OT Paydaşları Arasındaki İşbirliğini Artırın

"SafeBreach ekibinin OT ağını riske atan boşlukları belirlemesine ve bir iyileştirme planı üzerinde fabrikadaki ekiple daha işbirliği içinde çalışmasına olanak sağladı."

SoC Direktörü

Güç ve Enerji Sağlayıcı

BT/OT Ortamında SafeBreach



SafeBreach, Seviye 4 ve 3.5'te hem Ağ hem de Ana Bilgisayar seviyesinde Saldırı Simülasyonları gerçekleştirir

- Ana Bilgisayar Düzeyinde Güvenlik Kontrolünü Doğrulayın (Dsktp, Srvr, Uzak)
- Güvenlik Duvarı Algılama Kurallarını Doğrulayın
- Güvenlik Duvarı EKS Kurallarını Doğrulayın
- Günlüğü SIEM ve Güvenlik Kontrol Düzeyinde Doğrulayın

SafeBreach, Ağda Seviye 3.5 ile 2 arasında ve klonlanmış Seviye 3 ana bilgisayarlarda saldırı simülasyonları gerçekleştirir

- Güvenlik Duvarı Algılama Kurallarını Doğrulayın (İş istasyonu klonu)
- Güvenlik Duvarı Algılama Kurallarını Doğrulayın
- Güvenlik Duvarı EKS Kurallarını Doğrulayın
- Günlüğü SIEM ve Güvenlik Kontrol Düzeyinde Doğrulayın

SafeBreach, Ağ üzerinde Seviye 2 ve 3+ ve klonlanmış Seviye 3 ana bilgisayarları arasında saldırı simülasyonları gerçekleştirir

- Ana Bilgisayar Seviyesi Güvenlik Kontrolünü Doğrulayın (HMI klonu)
- Güvenlik Duvarı Algılama Kurallarını Doğrulayın
- Güvenlik Duvarı EKS Kurallarını Doğrulayın
- Günlüğü SIEM ve Güvenlik Kontrol Düzeyinde Doğrulayın

Not: Tüm simülasyonlar, SafeBreach simülatörleri (simgeleri) arasında gerçekleşir. SafeBreach dışı sistemler arasında hiçbir simülasyon gerçekleşmez.Not: Test için ortamdaki tüm proxy'leri kullanacaktır.

SafeBreach, OT Riskinizin %99'una Işık Tutuyor

Güvenliği ihlal edilmiş sistemlerin %99'u bilgisayar iş istasyonları ve sunucuları (HMI'lar) olacaktır.

İzinsiz giriş bekleme süresinin %99'u, herhangi bir Purdue seviye 0-1 cihazı etkilenmeden önce ticari kullanıma hazır bilgisayar ekipmanında gerçekleşir.

Kötü amaçlı yazılımların %99'u bu bilgisayar iş istasyonları ve sunucuları için tasarlanacaktır.

Algılama fırsatlarının %99'u, bu bilgisayar iş istasyonlarına ve sunucularına bağlı etkinlikler için olacaktır.

Adli tıp işlemlerinin %99'u bu bilgisayar iş istasyonları ve sunucularında gerçekleştirilecek.

SafeBreach, BT/OT Güvenlik Entegrasyonunuzu Hızlı Başlatmaya Yardımcı Olur

OTD BİLİŞİM GLOBAL VAD

Temel

DEĞERLENDİRİN, PLANLAYIN VE DÜZENLEYİN

HEDEF:

Önemli OT varlıklarını belirleyin, mimariyi değerlendirin ve olaylar için yanıt planları hazırlayın

Anahtar Görevler ve Kilometre Taşları:

- Taç mücevher analizi [saldırı simülasyonu ve analizi] ile bir mimari inceleme gerçekleştirin
- Bir olay müdahale planını tamamlayın [sürekli güvenlik doğrulaması ve BAS planı]

Operasyonel Hale Getirin

OT RİSK KONTROLLERİ

HEDEF:

Olayları algılamak ve bunlara yanıt vermek için kaynaklara ve beceriye sahip OT güvenlik programı

Anahtar Görevler ve Kilometre Taşları:

- Taç mücevher OT varlıklarına sahip siteler için varlık/ağ izlemeyi uygulayın
- Yönetici, varlık doğrulama, tehdit algılama ve soruşturmayı operasyonel hale getirin
- Kritik OT güvenlik açıkları için hafifletme süreçleri uygulayın

Optimize

GELİŞMİŞ OT RİSK AZALTMA PROGRAMI

HEDEF:

Proaktif risk azaltma ve program iyileştirme

Anahtar Görevler ve Kilometre Taşları:

- Yüksek ve orta riskli OT tesislerinde varlık/ağ izlemeyi genişletin
- Savunma kontrollerini doğrulayın - envanter, topoloji, trafik izleme, güvenlik açıkları
- Aktif güvenlik açığı yönetimi ve tehdit avlama programları
- OT tehdit istihbaratını güvenlik operasyonları süreçlerine entegre edin

1-3 AY → 3-12 AY → 12-24 AY (+DEVAM EDİYOR)

Saldırı. Çözüm. Raporlama. Tekrar.

Devamlı Saldırı

Güvenlik kontrollerinizi otomatik ve güvenli bir şekilde doğrular

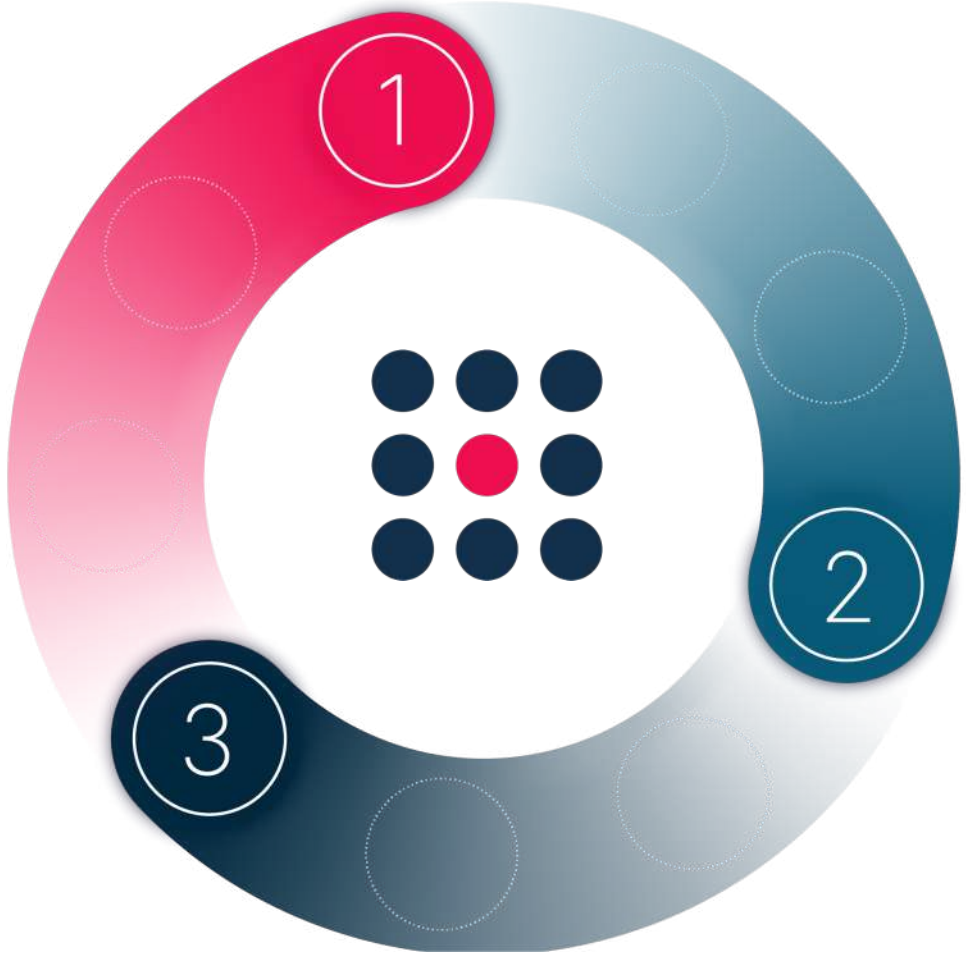
30.000+'den fazla saldırı yöntemi

24 saat içinde eklenen SLA - All US-CERT uyarısı

Riski Azaltın

Geniş ölçekte azaltmayı otomatik hale getirmek için benzersiz analizler ve entegrasyonlar

İlerlemeyi izlemek ve pano seviyesinde KPI'ları sunmak için CISO panosu



Sonuçların önceliklendirmesi

Güvenlik duruşunu görselleştirir

Güvenlik açığı yönetim platformlarıyla entegre eder

En etkili boşluklara odaklanmak için güvenlik kontrolleriyle ilişki kurar

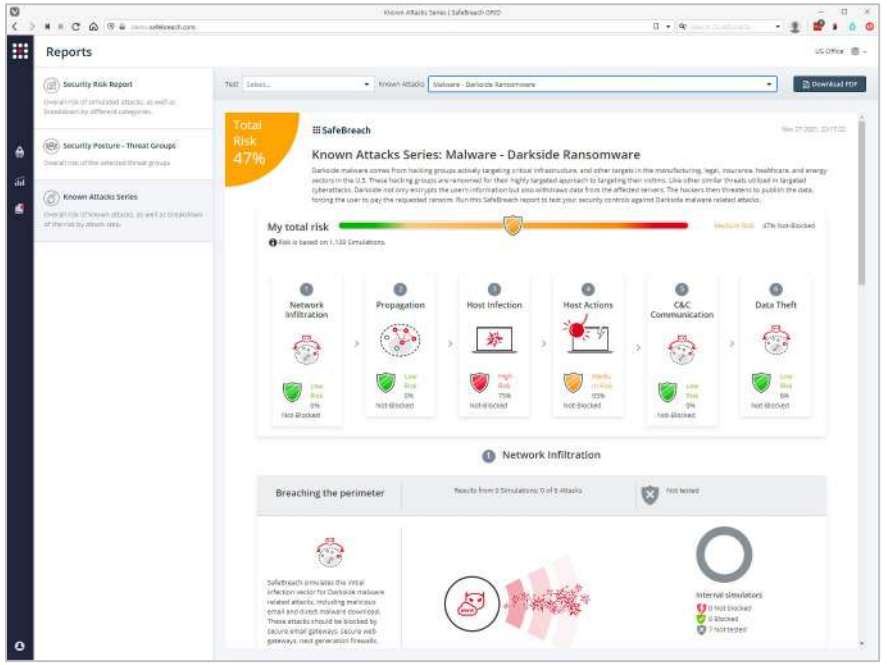
Amaçlı Saldırı

Endüstrinin en büyük saldırı taktikler PlayBook, **30.000+** ’den fazla saldırı yöntemi

Özel araştırma ekibi, yeni sertifikalar ve kritik saldırılardan sonraki **24 saat** içinde PlayBook’u günceller

Saldırılar oluşturur ve / veya özelleştirir

Tehdit istihbaratıyla entegre eder



Saldırı İstihbaratı

En son tehdidin IOC'lerinden oluşturulan saldırıları simüle eder

Alien Vault OTX

ThreatConnect

ThreatQ

Unit42

OTD BİLİŞİM GLOBAL VAD

Bulut ve şirket içi güvenlik denetimi etkinliğini sürekli olarak doğrular ve optimize eder

Etkinliği doğrulamak için güvenlik kontrollerinize yönelik saldırıları simüle eder

Sonuçları ilişkilendirmek ve güvenlik açıklarını verimli bir şekilde belirlemek için SIEM ve güvenlik kontrolleriyle entegre olur

Güvenlik ekosisteminin tamamını test eder:

Bulut, taşıyıcı, ağ, web, son nokta, e-posta, DLP

Güvenlik Kontrolleri

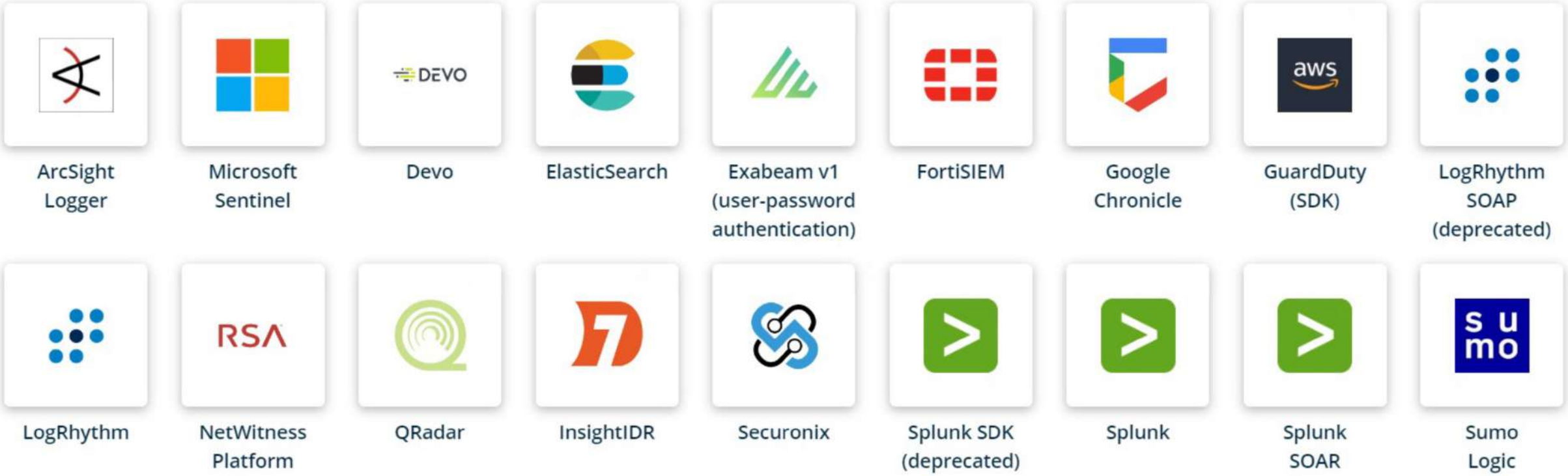
Simüle edilmiş saldırıları, belirli uç noktalardan ve ağ kontrollerinden alınan güvenlik olaylarıyla otomatik olarak ilişkilendirir

SIEM

Simüle edilmiş saldırıları birden çok kaynaktan gelen güvenlik olaylarıyla otomatik olarak ilişkilendirir

SIEM

Simüle edilmiş saldırıları birden fazla kaynaktan gelen güvenlik olaylarıyla otomatik olarak ilişkilendirin.



Güvenlik Kontrolleri

Simüle edilmiş saldırıları güvenlik olaylarıyla otomatik olarak ilişkilendiren belirli uç nokta ve ağ kontrollerinden alınmıştır.

OTD BİLİŞİM GLOBAL VAD

- Carbon Black Defense
- CheckPoint NGFW
- Cisco AMP
- Cisco Secure Email
- Cisco Umbrella
- Cortex™ XDR
- CrowdStrike Falcon
- Cybereason
- CylancePROTECT & OPTICS
- FireEye HX
- Firepower
- FortiGate NGFW
- BigQuery
- Trellix ePO
- Microsoft Defender for Endpoint
- Netskope SASE
- Microsoft Defender for Office 365
- Palo Alto Panorama
- SentinelOne
- Tanium Threat Response
- Trend Micro XDR
- Windows Events

Riski verimli bir şekilde azaltmak için iyileştirmeye öncelik verir ve otomatikleştirir

Azaltmayı kolaylaştırmak için eyleme dönüştürülebilir iyileştirme adımları

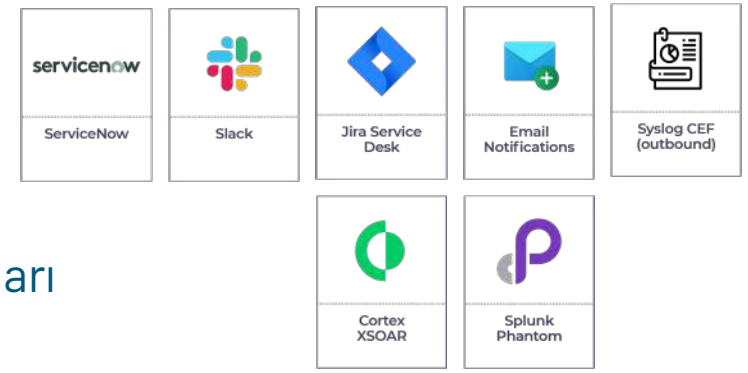
İş riskine göre iyileştirmeye öncelik verir

Düzeltmeyi otomatikleştirmek için SIEM, SOAR ve İş Akışı yönetimi ile entegre eder

Sömürülebilir güvenlik açıklarını belirlemek ve önceliklendirmek için güvenlik açığı yönetim platformlarıyla entegre eder

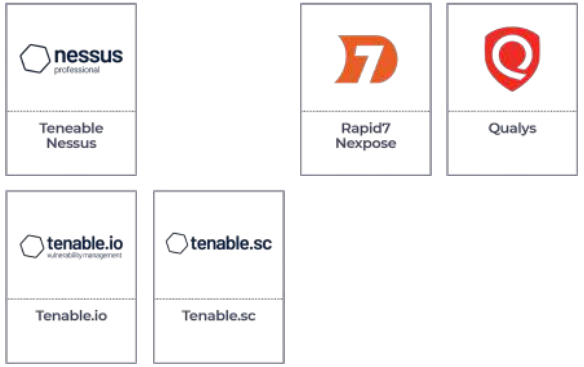
İş Akışı ve Otomasyon

Sistem olaylarıyla ilgili bildirimleri alır ve otomatik düzeltme eylemleri için olaylar üretir



Zafiyet Yönetimi

SafeBreach simülasyonlarına dayalı olarak istismar edilebilirlik ve etki ile güvenlik açığına öncelik verir



Güvenlik Açığı Yönetimi

Güvenlik açıklarını, SafeBreach simülasyonlarına dayalı olarak yararlanılabilirlik ve etkiye göre önceliklendirin.

Tenable Nessus | Qualys | Rapid7 Nexpose | Tenable.io | Tenable.sc

Tehdit İstihbaratı

En son tehditlerin IOC'lerinden oluşturulan saldırıları simüle edin.

AlienVault OTX | Anomali | Falcon Intelligence | Recorded Future | ThreatConnect | ThreatQ | Unit42

OTD BİLİŞİM GLOBAL VAD

Farklılaşma: İşinizi Geleceğe Hazırlama

Otomatik Azaltma

Geniş ölçekte orkestrasyonunuzla otomatik azaltma için eyleme dönüştürülebilir veriler sağlar.

CORTEX XSOAR BY PALO ALTO NETWORKS

splunk> phantom

Kurumsala Hazır

Ölçeklenebilir & Güvenli

Yerleştirme Kolaylığı

Otomatik ve Düşük Dokunma

En Yüksek Kapsama

Bulut tabanlı, şirket içi veya hava boşluklu dağıtım ile tüm saldırı zincirini takip edin.

>30K saldırı ile piyasadaki en büyük PlayBook.

SLA – 24 saat içinde eklenen yeni tehditler.

Windows

aws

docker

macOS

Azure

Google Cloud

Açık Platform

IBM Radar

CROWDSTRIKE

ThreatConnect

Microsoft

tenable

RSA

RAPID7

CYLANCE

paloalto NETWORKS

SafeBreach

SentinelOne

CISCO

now

CARBON BLACK

Qualys.

McAfee

splunk> phantom

OTD BİLİŞİM GLOBAL VAD

SafeBreach Panelleri

Güvenli Raporlama

Güvenlik duruşu ölçümlerini ve diğer raporları planlar

Eyleme geçirilebilir MITRE çerçevesi ve NIST eşlemesi

Zaman içindeki eğilimleri kolayca izler

Güvenlik görünürlüğünü yönetime bildirir

SafeBreach Dağıtımı

Simülatörler

Dahili ve harici temsili sistemlerde yerleştirilmiş hafif yazılım aracısı

Güvenliği sağlamak için saldırılarda saldırgan ve hedef rolü üstlenin

Windows, Linux, Mac, AWS, Azure, GCP ve diğerleri

Yönetim

SaaS, Şirket İçi veya Bağlantısız seçenekleri

Sonuç verilerini raporlar, görselleştirmeler ve analizler halinde planlar, düzenler ve toplar

Güvenlik Kontrolleri, SIEM, SOAR, VM, TI ve Workflow platformları ile entegre olur

Saldırı PlayBook

Binlerce güncellenmiş saldırı yöntemini barındıran bulut hizmeti

Yeni saldırılar için yazılım güncellemesi gerekmez, saldırılar otomatik olarak güncellenir

Bağlantısı kesilen yönetimde manuel olarak güncellenir

BAS Gücünü Kullanın

Güvenlik Kontrol Doğrulaması

SC1	Kuruluş Çapında Güvenlik Duruşu
SC2	OU/BU başına Duruş Değerlendirmesi
SC3	Çevresel Sürüklenme Algılama
SC4	MITRE ATT&CK Değerlendirmesi
SC5	Uç Nokta Teknikleri Değerlendirmesi
SC6	E-posta Güvenlik Değerlendirmesi
SC7	Çevre Doğrulaması
SC8	Veri Sızıntısı Değerlendirmesi
SC9	Segmentasyon Kontrol Doğrulaması
SC10	Güvenlik Kontrollerini Karşılaştırması
SC11	SoC/IR Doğrulaması
SC12	M&A Risk Değerlendirmesi

Tehdit Değerlendirme

TA1	Yakın Tehdit Değerlendirmesi
TA2	MITRE Tehdit Aktör Değerlendirmesi
TA3	TI Entegre Değerlendirme

Bulut Güvenlik Değerlendirme

CS1	Bulut Tehditleri Değerlendirmesi
CS2	CWPP Kontrol Doğrulaması
CS3	Konfigürasyon Kontrol Doğrulaması

Risk Bazlı VM

VM1	Güvenlik Açığı Önceliklendirmesi
VM2	Tehdide Göre Güvenlik Açığı Önceliklendirmesi

Bize güven duyan firmalar...

FİNANSAL HİZMETLER

SAĞLIK HİZMETİ

ÜRETİM

İLAÇ & BİYOTEKNOLOJİ

SİGORTA

OTD BİLİŞİM GLOBAL VAD

Bize güven duyan firmalar...

TEKNOLOJİ

Microsoft
ByteDance
paloalto NETWORKS
Trustwave
CRYPSIS
mimecast
IBM
TREND MICRO
WIZ
FORTIVE
virsec
IAS Integral Ad Science
netskope
VARONIS
JUNIPER NETWORKS
PEGA

YİYECEK & İÇECEK

PEPSICO
Carlsberg Group
Kellogg's
OTD BİLİŞİM GLOBAL VAD
OTD

DANIŞMANLIK

Deloitte.
CYNERGISTEK A Clearwater Company
softserve
HCL
seek
PARAGON CONSULTING GROUP
SP6

HUKUK

HUSCH BLACKWELL
FOLEY FOLEY & LARDNER LLP
pillsbury
BakerHostetler

SERVİSLER

Service Corporation International
ADT

EĞİTİM

CARIBBEAN EXAMINATIONS COUNCIL
Singapore Institute of Management

ARAÇLAR

Marathon Petroleum Corporation
ICEPCO
PG&E
NORTHLAND POWER
Ameren
Southern Company

TAŞIMACILIK

UNION PACIFIC
SINGAPORE AIRLINES
American Airlines

İLETİŞİM

TIM
.izzi telecom
at&t
Ministry of the Interior and Safety National Information Resources Service
ECHOSTAR
NOS
orange

EĞLENCE

NETFLIX

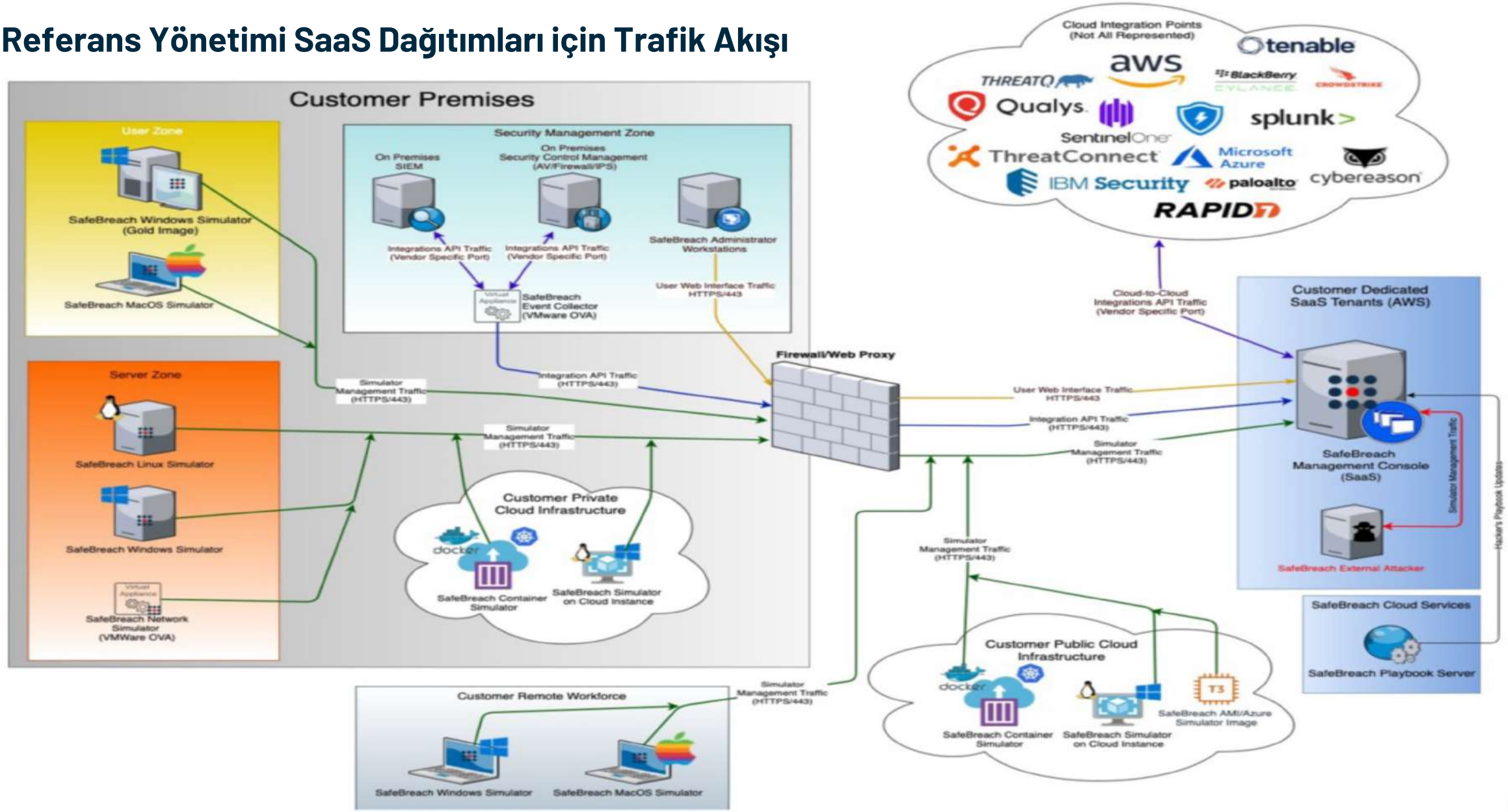
PERAKENDE

ABC Supply Co. inc.
7 ELEVEN
SPAR
ASBURY AUTOMOTIVE GROUP

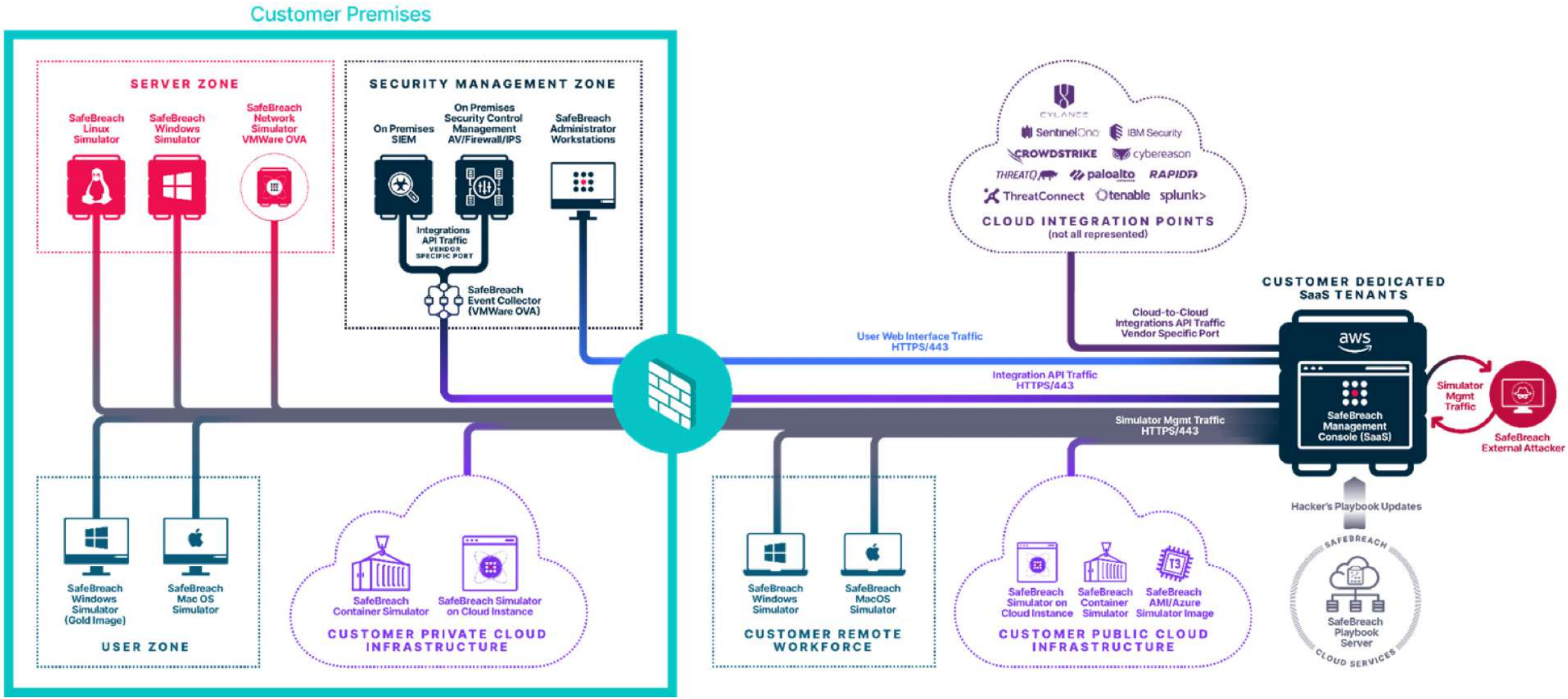
DEVLET

New Jersey Courts
Independence • Integrity • Fairness • Quality Service
ROWAN COUNTY NORTH CAROLINA Be an original.
RivCoNOW COMMUNITY NOW. SERVICES NOW.

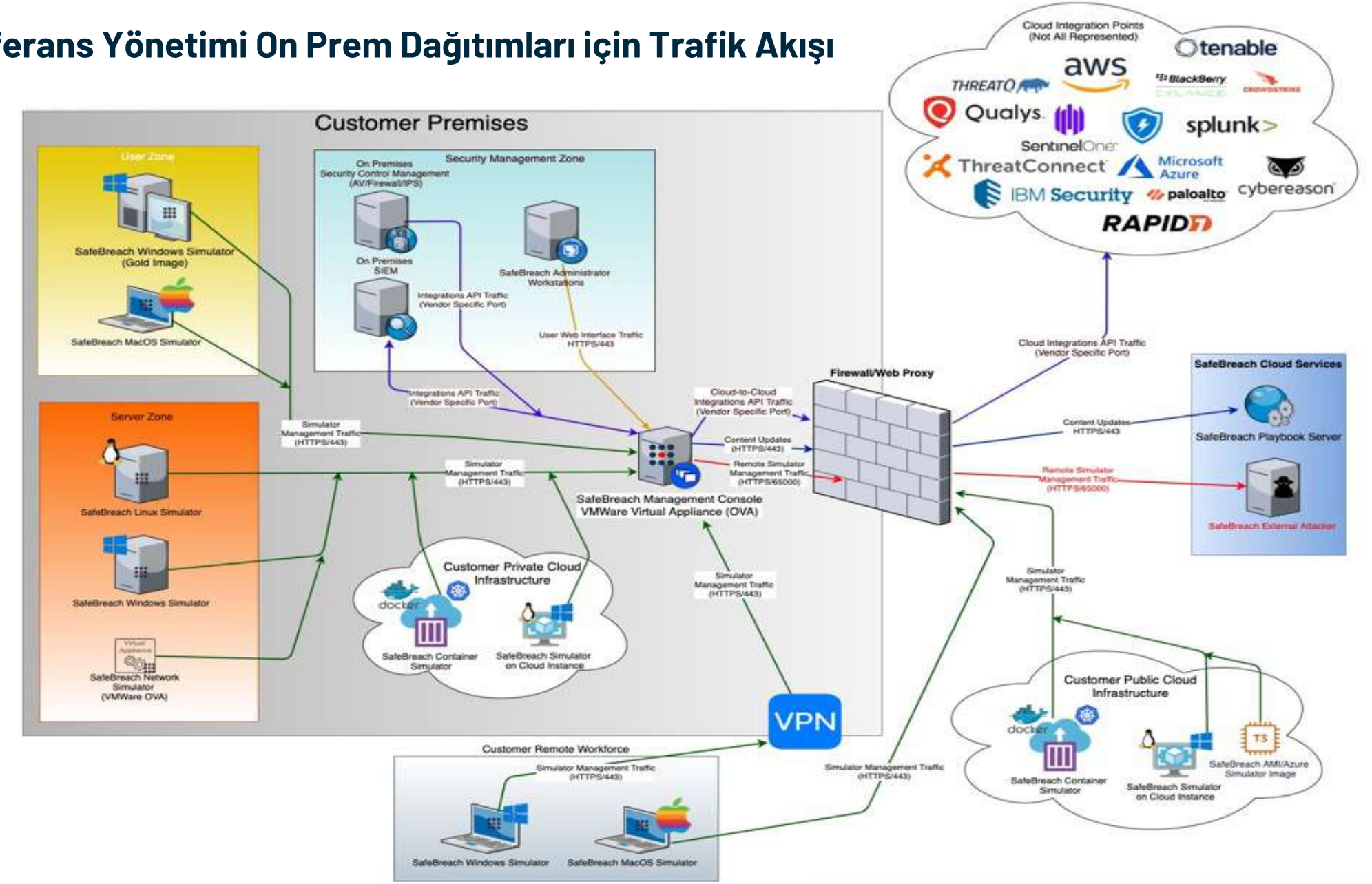
Referans Yönetimi SaaS Dağıtımları için Trafik Akışı



Referans Yönetimi SaaS Dağıtımları için Trafik Akışı

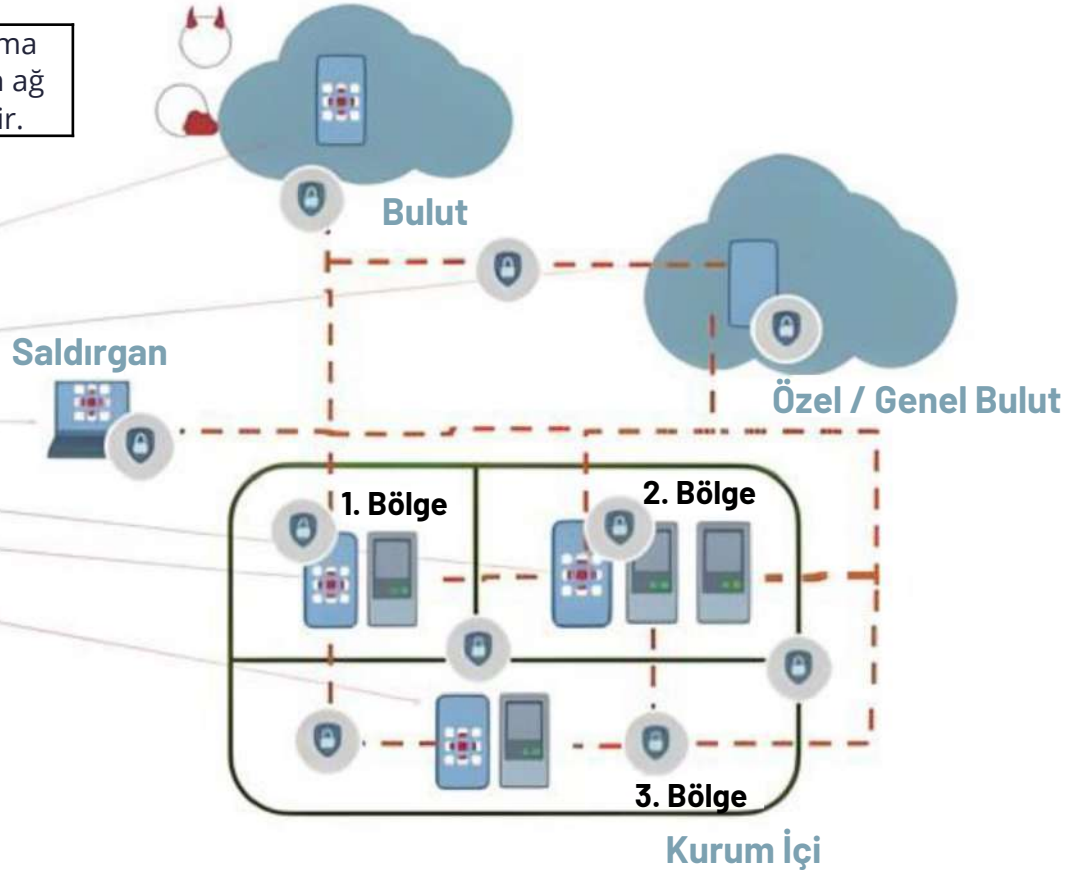


Referans Yönetimi On Prem Dağıtımları için Trafik Akışı



Yönetim Konsolu

Sızmaya yardımcı olmak ve sızma hedefi olarak hizmet etmek için ağ dışına bir Simülatör yerleştirilir.



Yönetim Konsolu (MC), her bir Simülatör ile bağımsız ve güvenli bir şekilde iletişim kurar (Port 443) ve simülasyonları yürütme talimatı verir. Simülatörler, sonuçlarını daha sonra çeşitli gösterge tablolarını, olası öldürme zinciri görünümlerini, önerileri ve raporları analiz edecek ve üretilecek olan MC'ye geri iletir.

Bu ortam, AV, EDR, Proxy, Secure Web Gateway, NexGen güvenlik duvarı, IPS Sandbox vb gibi çeşitli güvenlik kontrollerine sahip 3 segmentli bölgeyi temsil eder.

Açıklama

- SafeBreach Simülatörü
- Güvenlik Kontrolü
- Temsili Sistemler
- Simülatörlü Uzak Kullanıcı
- MC'den Simülatörlere İletişim Yolu
- Potansiyel Simülasyon Yolları
- Ağ Segmentasyonu
- Tanımlanmış Sızma Hedefi
- Tanımlanmış Sızma Hedefi

SafeBreach-as-a-Service ile Savunmadan Saldırıya Geçin: En Eksiksiz BAS Çözümü

Platformu yönetmede SafeBreach'in tüm avantajları

Strateji, iyileştirme, azaltma ve standart oluşturmaya odaklanmanıza ve güvenlik duruşunuzu güçlendirmenize imkan sağlar

Aracısız web uygulaması güvenlik doğrulaması aracılığıyla bütün atak öldürme (full-kill chain) zincirinin kilidini açın

Web Uygulaması Güvenliği için SafeBreach

- Bütün atak öldürme zincir doğrulaması
- Kapsam, OWASP® Foundation'ın ilk on güvenlik riskini içerir
- Web uygulaması güvenlik duruşunun bağlamsallaştırılmış bir görünümü
- Hızlı ve kolay yerleşim
- WAF'ınız için eyleme dönüştürülebilir ROI raporlaması

OTD BİLİŞİM

GLOBAL VAD

Kullanım Örnekleri

Bu, güvenlik programınıza nasıl uyuyor?

Müşteri Vaka Çalışması

En İyi 3 ABD Sigortacısı

Meydan Okuma

OU'lar ve entegre olmayan kuruluşlarda siber riski değerlendirmek ve duruşu iyileştirmek

Çözüm

SafeBreach OU'lar ve NIE'lerde dağıtılır ve sızma, ana bilgisayar düzeyi, yanal hareket ve sızmayı sürekli olarak test eder

SafeBreach panelleri, üç ayda bir C-seviyesine ve BoD'ye raporlanır

Fayda / ROI (Yatırım Üzerinden Getiri)

Tek tip bir KPI setine dayalı olarak program ilerlemesini takip etme yeteneği

Zaman içinde duruşta iyileşme gösterme yeteneği

Binlerce boşluğu tespit etme ve düzeltme yeteneği

MÜŞTERİ VAKA ÇALIŞMASI

Ik 3 ABD FIS

Meydan Okuma

En değerli segmentlerde segmentasyon kontrollerini değerlendirme

Yakın tehditlere karşı dayanıklılığı kısa sürede değerlendirme

Çözüm

SafeBreach, değerli segmentler arasında dağıtılır, SIEM'e entegre edilir ve segmentasyonu sürekli olarak doğrular

US-CERT güvenlik duruşunu test etmek için SafeBreach SLA kullanılır

Fayda / ROI (Yatırım Üzerinden Getiri)

Ağ kontrollerinde saldırı yüzeyinin > %80'den < %5'e düşürülmesi

Yakın tehdit esnekliği ve azaltma planını günler içinde bildirebilme

MÜŞTERİ VAKA ÇALIŞMASI

PayPal

Meydan Okuma

Boşlukları belirlemek ve birleşmeyi planlamak için birleşme ve satın alma siber riskini sürecin başında değerlendirme

Çözüm

Birleşme ve Satın Alma ekibi, her DD sürecinde SafeBreach temel testini devreye sokar ve çalıştırır ve günler içinde siber durumu değerlendirir

Fayda / ROI (Yatırım Üzerinden Getiri)

Etki yaratmak için edinilen riski zamanında değerlendirir

İlişkili birleşme bütçesini ve etkisini değerlendirir

Etkin ve hızlı değerlendirme süreci

VAKA ÇALIŞMASI

Spear-phishing ve "living-off-the-land" (LOTL) araçları, OT saldırı keşiflerini başlatır

E-posta, Uç Nokta ve Ağ Kontrolü Doğrulaması

Saldırganlar, bir kimlik avı kampanyasıyla Üretim çalışanlarını hedef aldı. Katıştırılmış bir bağlantı, kötü amaçlı yazılımı bir C&C sunucusuna atfedilemez bir iletişim yolu oluşturmaya itti. Saldırganlar, LOTL araçlarını kullanarak, genişletilmiş ağ mimarisini haritalamaya ve ilgilenilen OT hedeflerini keşfetmeye başlamak için kimlik bilgilerini ele geçirdi ve ayrıcalıkları artırdı.

Amaç	Kötü amaçlı yazılım etkinliğinin bir parçası olarak uç nokta ve ağ denetimlerini, görünürlüğü ve kötü amaçlı ana bilgisayar eylemlerinin önlenmesini doğrulamak.
Test	Anormal davranış tespiti, uygulama beyaz listesi ve sistem kilitleme politikaları dahil olmak üzere ana bilgisayar kontrollerini test etmek için kötü amaçlı yazılım öldürme zincirinin farklı aşamalarında saldırı simülasyonları gerçekleştirdik. Filtreleme kurallarını, kilitleme ilkelerini ve ağ çevre güvenlik kontrollerinin uzlaşma göstergelerine (IOC) karşı etkili olup olmadığını doğrulamak için ağ sızma/sızma simülasyonları çalıştırdık.
Sonuçlar	Belirlenen ağ bölümleme ve filtreleme kuralları, genel olarak bilinen güvenlik açıklarından yararlanma ve hassas ağlara erişim elde etmek için birden çok açık kaynak araçtan yararlanma potansiyel riskiyle yetersizdi. EDR politikasının kötü niyetli davranışları tespit etme ve önleme etkinliğinin iyileştirilmesi gerekiyor.Onaylanmış güvenlik kontrolleri, en az ayrıcalık ilkesi uygulanarak güçlendirilebilir. Ayrıca, tehdit aktörleri ayrıcalıkları yükseltmekte ve/veya yanal olarak hareket etmekte zorluk çekeceğinden, komut satırı komut dosyası oluşturma etkinliklerinin ve izinlerinin devre dışı bırakılması da önerilir. Kötü amaçlı C2 iletişimine karşı web filtreleme kontrolleri güçlendirildi.

VAKA ÇALIŞMASI

Kritik altyapıyı devre dışı bırakan ve çalışamaz hale getiren kötü amaçlı yazılım

Uç Nokta ve Ağ Kontrolü Doğrulaması

Saldırganlar, WhisperGate ve Hermetic kötü amaçlı yazılımı kullanarak EKS ağındaki Windows tabanlı HMI'ları hedef aldı. Ana önyükleme kaydını manipüle etmeye, cihazları çalışmaz hale getirmeye ve güç üretimini kapatmaya çalıştılar.

Amaç	Ağ yapılandırmasını ve ağ güvenlik kontrollerinin, uç nokta kontrollerinin ve iyileştirme yanıtının etkinliğini doğrulayın.
Test	SPAN bağlantı noktası yapılandırmasını doğruladık.OT güvenlik araçlarının düzgün çalıştığını doğrulamak için seviye 2 ve seviye 3 HMI'lara ve Mühendislik iş istasyonlarına karşı ağ saldırısı simülasyonu çalıştırdık. OT Ağı güvenlik kontrollerini SafeBreach EKS Saldırıları (Ağ Transferleri) ile test ettik.
Sonuçlar	Yanal hareket saldırıları, ağ tabanlı erişim kontrol listelerinin (ACL'ler) yanlış yapılandırılmasını ve kötü amaçlı yazılım yayılmasına izin veren sistem açıklarını belirledik. Sonuçlar, ağ bölümleme ve filtreleme kurallarının, yapılandırma özniteliklerini kaldırma/değiştirme veya bellenim veya sistem ikili dosyalarını yok etme potansiyel riskleri açısından yeterli olmadığının altını çizdi; bunlar, kritik ağ kaynaklarının kullanılabilirliğini izole edebilir veya azaltabilir.

VAKA ÇALIŞMASI

Amaca Yönelik OT Fidye Yazılımı

BT/OT Güvenlik Doğrulaması

WannaCry ve SNAKE fidye yazılımı saldırıları, ilk 10 otomobil üreticisinden ikisini üretim hatlarını kapatmaya zorladı. Her iki saldırının da kimlik avından kaynaklandığı ve Windows tabanlı EKS uç noktalarını başarıyla ele geçirdiği düşünülüyor.

Amaç	Ağ yapılandırmasını ve ağ güvenlik kontrollerinin, uç nokta kontrollerinin ve iyileştirme yanıtının etkinliğini doğrulamak.
Test	Üretim süreçlerini içeren verilere erişimin nerede sınırlanacağını belirlemek ve sisteme kötü amaçlı yazılım bulaştırabilecek güvenlik kontrollerindeki zayıflığı belirlemek amacıyla sistem güvenlik kontrollerini doğrulamak için simüle edilmiş saldırılar gerçekleştirdik. Uç nokta algılama ve yanıt (EDR) entegrasyon aracımız ile uç nokta kontrollerinin etkinliğini doğrulamak ve EDR tarafından oluşturulan bu uyarıların doğru bir şekilde önceliklendirildiğini doğrulamak için belirli tehdit davranışları simüle edildi.
Sonuçlar	Yanal hareket simülasyonları, güvenlik kontrollerini doğruladı ve ağ bölümleme ve filtreleme kurallarının minimum düzeyde etkili olması, en kritik iletişim ve verilerin en güvenli ve güvenilir katman olan Whisper Gate'te bulunduğu çok katmanlı ağ bölümlemenin uygulanmasına ve uygulanmasına yol açtı. Web filtreleme kontrolleri, kötü amaçlı uzaktan izleme ve yönetim yazılımları ile kötü niyetli açıklardan yararlanmaya yardımcı olan uzak masaüstü yazılım uygulamaları için güçlendirildi.

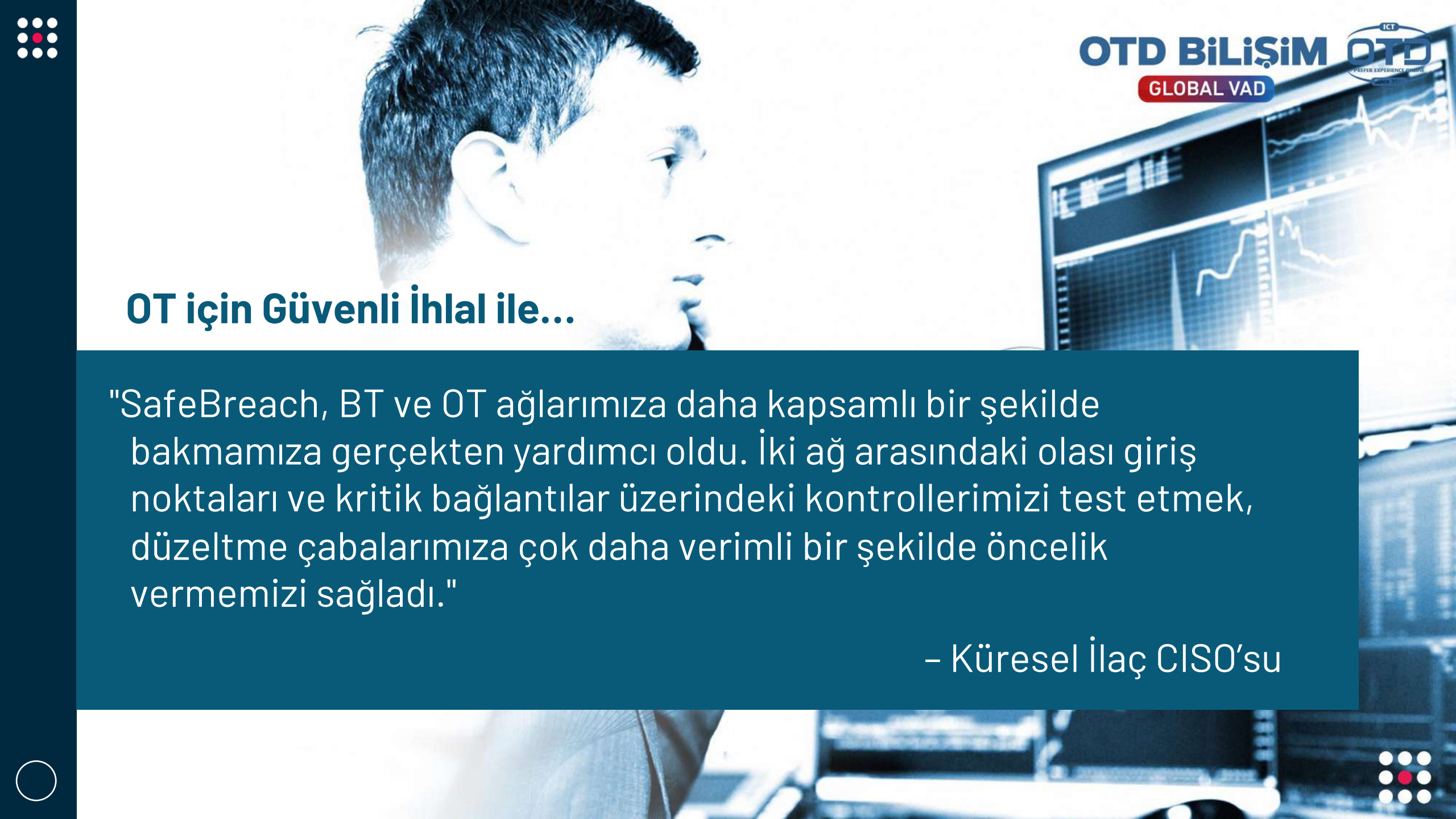
VAKA ÇALIŞMASI

Tedarik zinciri saldırısı, OT ortamına sızmak için zayıf ağ segmentasyonundan yararlanır

Ağ Çevresi ve Segmentasyon Doğrulaması

Siber suçlular, müşterilerinin OT ağına uzaktan erişim elde etmek için bir HVAC satıcısını hedef aldı. Saldırganlar içeri girdikten sonra, Tesisler ağından yanal olarak üretim tesisindeki OT ağına geçti.

Amaç	OT ortamında telafi edici kontrollerin etkinliğine dair görünürlük elde etmek. Doğrulamak için OT sistemleri, yama yaşam döngüsüne rağmen yeterince korunmaktadır.
Test	Saldırıları kritik süreç alanları arasında yürüttük. Her bir süreç alanı içinde ve süreç alanları arasında olmak üzere kritik segmentlerde segmentasyon politikalarını, ağ denetimini ve tehdit önlemeyi doğruladık.Uygulama beyaz listesi ve kilitleme politikaları gibi yerel korumaların belirli saldırgan tekniklerine karşı etkili olduğunu doğrulamak için uç nokta saldırıları gerçekleştirdik.
Sonuçlar	Simülasyon sonuçları, başarılı istismar girişimlerini önlemeye yardımcı olmak için en az erişim modelleri ve derinlemesine savunma uygulanarak güvenlik kontrollerinin güçlendirilebileceğini doğruladı.Yanal hareket simülasyonları, OT ağlarını rollere ve gereksinimlere göre alt bölgelere ayırarak gelişmiş ağ segmentasyonu ihtiyacını doğruladı.



OTD BİLİŞİM
GLOBAL VAD

OT için Güvenli İhlal ile...

"SafeBreach, BT ve OT ağlarımıza daha kapsamlı bir şekilde bakmamıza gerçekten yardımcı oldu. İki ağ arasındaki olası giriş noktaları ve kritik bağlantılar üzerindeki kontrollerimizi test etmek, düzeltme çabalarımıza çok daha verimli bir şekilde öncelik vermemizi sağladı."

– Küresel İlaç CISO'su

SafeBreach

Teşekkürler

OTD BİLİŞİM GLOBAL VAD