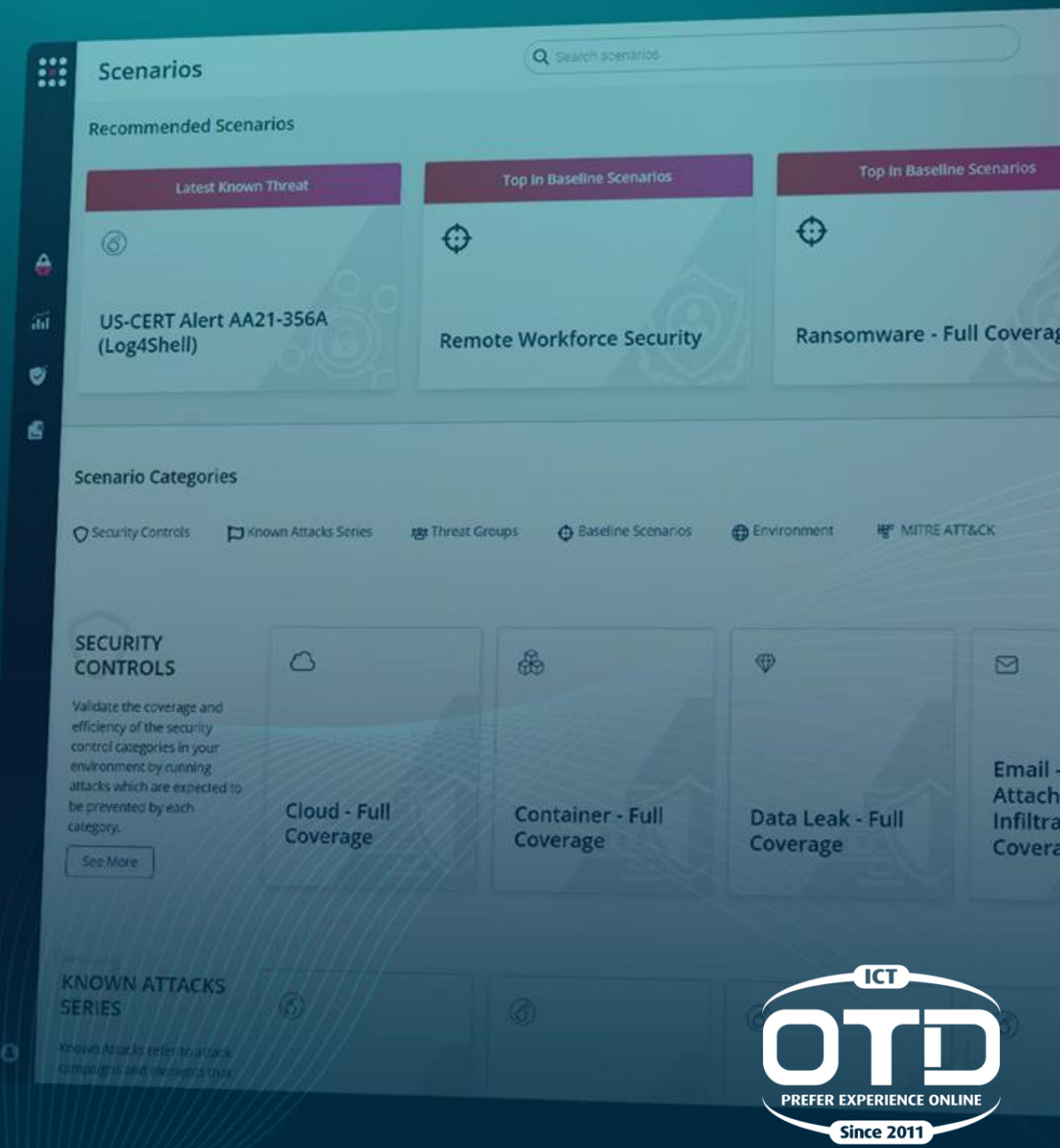
SafeBreach

Savunma Sistemlerinizi Güçlendirmek için Siber Saldırıların Kullanılması

Hedef Kişi:



Sunumu Yapanın Adı
Şubat 2022

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.

Ekiplerin
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

Saldırı. Çözüm. Raporlama. Tekrar.

Devamlı Saldırı

Güvenlik kontrollerinizi otomatik ve güvenli bir şekilde doğrular

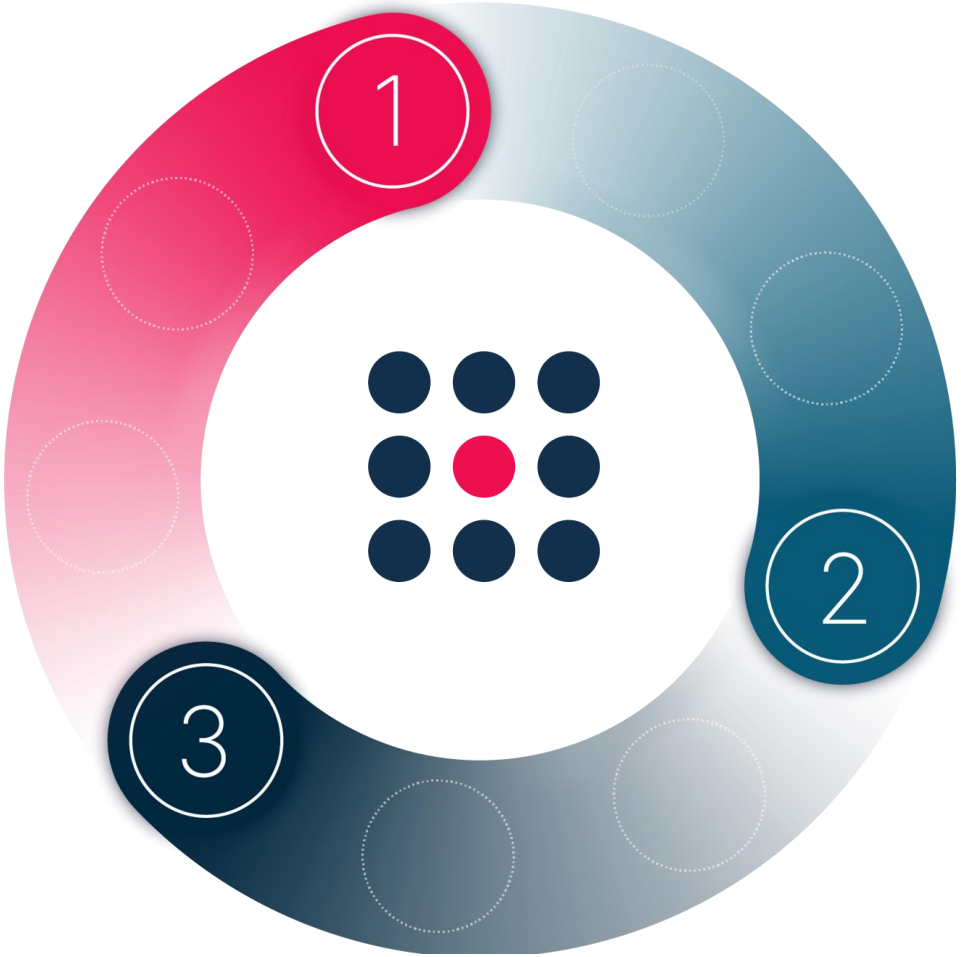
20K'dan fazla saldırı yöntemi

24 saat içinde eklenen SLA - All US-CERT uyarısı

Drive Down Risk

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

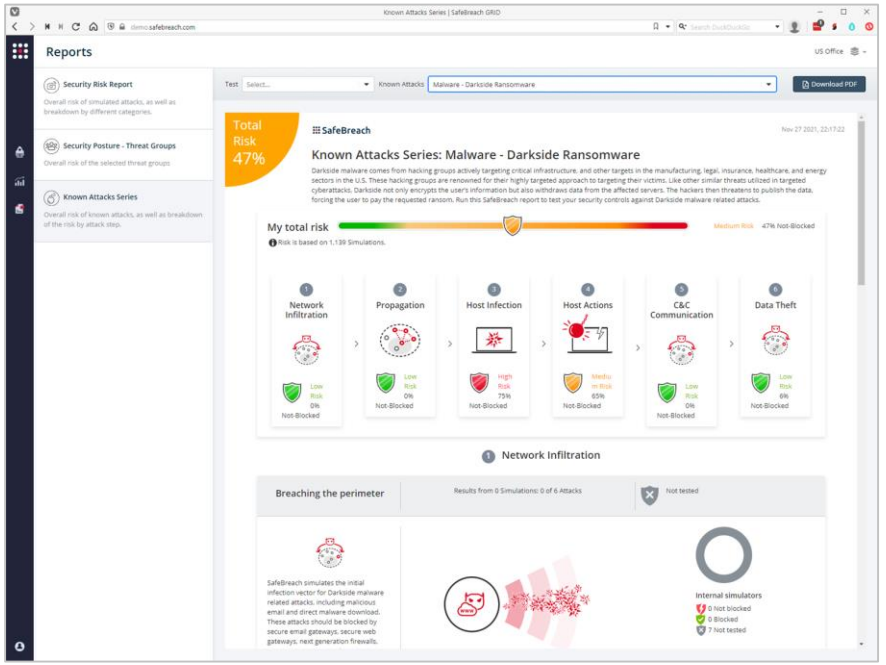
Amaçlı Saldırı

Endüstrinin en büyük saldırı taktikler (çalışma) kitabı, 20.000'den fazla saldırı yöntemi

Özel araştırma ekibi, yeni sertifikalar ve kritik saldırılardan sonraki 24 saat içinde çalışma kitabını 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

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

Riski verimli bir şekilde azaltmak için iyileştirmeye öncelik veri ve otomatikleştirir

Azaltmayı kolaylaştırmak için eyleme dönüştürülebilir iyileştirme adımları

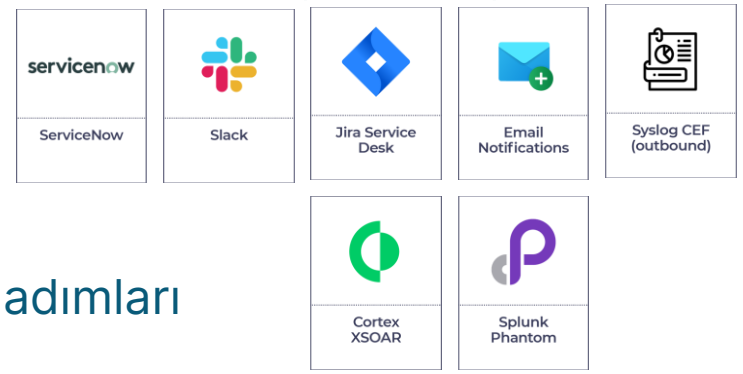
İş riskine göre iyileştirmeye öncelik verir

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 olayları hakkında bildirimler alır ve otomatik düzeltme eylemleri için olaylar oluşturur



Zafiyet Yönetimi

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

ICT OTD
PREFER EXPERIENCE ONLINE
Since 2011

SafeBreach Panelleri

Güvenli Raporlama

SafeBreach Dağıtımı

Simülatörler

Dahili ve harici temsili sistemlerde yerleştirilmiş hafif yazılım aracısı

Güvenliği sağlamak için saldırılarda saldırgan ve hedef rolü üstlenenin

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 Çalışma Kitabı

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

Pazar Liderleri Tarafından Güvenilen

"SafeBreach'in ABD Sertifika Uyarılarına dayalı yeni saldırıları Hacker's Playbook'da hemen güncellemesi bizim için büyük bir değerdir. SolarWinds'e karşı kullanılan saldırılarda; bu kontrollerimizi, süreçlerimizi ve ekiplerimizi hızlı bir şekilde test etmemize olağanüstü yardımcı oluyor. Saldırı simülasyonlarını başlattığımızı ve ekibin saldırıyı hızlı bir şekilde tespit ettiğin yönetim kuruluna bildirmek, onlara ekibimizin tetikte olduğuna ve hızlı bir şekilde algılama ve yanıt verme yeteneğine sahip olduğuna dair bir ek güven sağladı.

CISO, Top 10 U.S. Insurance Company

Ek Slaytlar

SafeBreach

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

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 Paneller 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 SafeBreach SLA, için 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

Farklılaşma: İşinize 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.

>20K saldırı ile piyasadaki en büyük çalışma kitabı.

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

SafeBreach hakkında

Kuruluş: 2014

Merkez: Sunnyvale and Tel Aviv

Kurucuları: Guy Bejerano, CEO ve Itzik Kotler, CTO. Bejerano şirketi kurmadan önce bilgi güvenliği şefi olarak çalışırken Kotler de İsrail Savunma Kuvvetleri'nin teknoloji biriminde hacker olarak zaman harcamıştı.

Fonlama: 106 milyon dolar. Sequoia Capital, DTCP, DNX Ventures, OCV Ortakları, PayPal. Son D Serisi turu, Sands Capital ve Leumi Partners'ın ek katılımıyla Sonae IM ve srael Growth Partners (IGP) tarafından yönetildi.

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

Platformu yönetmeden SafeBreach'in tüm avantajları

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

Aracısız web uygulaması güvenlik doğrulaması aracılığıyla tam öldürme (full-kill) zincirinin kilidini açın

Web Uygulaması Güvenliği için SafeBreach

- Full kill-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

SafeBreach

Teşekkürler

Adınız
Email
Telefon

ICT OTD PREFER EXPERIENCE ONLINE Since 2011