SİBER GÜVENLİK

STM

SİBER GÜVENLİK

SİBER GÜVENLİK HEDEFLERİ

- Siber Güvenlik Alanında Yetkin Bir Kurum Olmak ve Katma Değeri Yüksek Hizmetler Sağlamak
- Siber Güvenlik Alanında Özgün ve Milli Çözümler Geliştirmek
- Siber Güvenlik Eğitimi Hizmeti
- Ulusal Düzeyde Siber Güvenlik Farkındalığı Oluşturma
- Siber Güvenlik Personelinin Beceri ve Bilgi Seviyesini Yükseltmek

STM SİBER GÜVENLİK YETENEKLERİ

- Siber Tehdit İstihbaratı
- Siber Durumsal Farkındalık
- Siber Risk Yönetimi ve Değerlendirme
- Siber Bilgi Paylaşım ve Uyarı Sistemleri
- Siber Karar ve Süreç Destek Sistemleri
- Akıllı ve Otonom Siber Güvenlik Altyapıları
- Sızma (Pen-Test) Testi Hizmetleri
- Siber Tatbikat ve Hazırlık Altyapıları
- Siber Savunma Birlikte Çalışabilirlik
- Siber Olay/Veri Görselleştirme Altyapıları

SİBER GÜVENLİK FAALİYET ALANLARI

- Siber Füzyon Merkezi Hizmetleri
- Araştırma ve Ürün Geliştirme
- Projeler
- STM Akademi Eğitimleri
- Siber Güvenlik Raporları
- Bayrağı Yakala/Capture The Flag (CTF) Yarışmaları
- Ortak Kriter Test Merkezi

STM AKADEMİ

Teorik ve Pratik Eğitimler

- STM Akademi'de verilen eğitimler teorik ve pratik unsurları içermektedir.

Siber Güvenlik Temel Farkındalık

- Bilgi güvenliği farkındalığının yetersiz olduğu bilinmektedir.
- Güncel saldırı yöntemleri ve önlemleri hakkında teorik ve pratik eğitimler verilmektedir.

Siber Güvenlik Uzmanı Eğitimleri

- Siber güvenlik konusunda çalışan personelin eğitim seviyesinin ortaya çıkan yeni saldırı teknikleri ve yöntemlerini de kapsayacak şekilde güncel tutulması gerekmektedir.

İleri Seviye Siber Güvenlik Eğitimleri

- Geniş yelpazedeki birçok konunun yanı sıra, derinlemesine belirli konuların araştırılması ve eğitimine yönelik programlar hazırlanmıştır.

Siber Güvenlik Yönetici Eğitimleri

- STM Akademi'de yöneticiler için stratejik seviyede siber güvenlik eğitimleri verilmektedir.

Siber Laboratuvar

- Zararlı yazılım analizi, tehdit analizi ve sızma testi,
- Dayanıklı ağ sistem mühendisliği,
- Yüksek performans bilgi işleme ve veri analitiği,
- Tersine mühendislik, zafiyet ve açıklık belirleme vb.

STM AKADEMİ SİBER GÜVENLİK EĞİTİMLERİ

- Saldırı Tespit ve Kayıt Yönetimi Eğitimi
- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi
- Uygulamalı Web Sızma Testi
- Siber Güvenlik ve Risk Değerlendirme
- Merkezi Güvenlik İzleme ve Olay Yönetimi
- Zararlı Yazılım Analizi Eğitimi
- Temel Açık Kaynak İstihbarat - OSINT ve Siber Tehdit İstihbaratı
- Web Uygulama Güvenliği Eğitimi
- Güvenli Yapılandırma Denetimi
- Yöneticiler İçin Bilgi Güvenliği
- İş Sürekliliği ve Felaketten Kurtarma
- Sosyal Mühendislik Saldırı ve Korunma Yöntemleri
- ISO 27001 Uygulama Eğitimi
- Etik Bilgisayar Korsanı Eğitimi
- Uygulamalı Büyük Veri Bilimsel Eğitimi
- Uygulamalı Büyük Veri Mühendislik Eğitimi

STM ORTAK KRİTER TEST MERKEZİ (CCEL-Common Criteria Evaluation Laboratory)

- Güvenlik ürünlerinin ISO 17025 Standartları'na (Common Criteria) uygun test ve değerlendirmesi,
- EAL 4+ seviyesine kadar test.

STM SİBER GÜVENLİK RAPORLARI

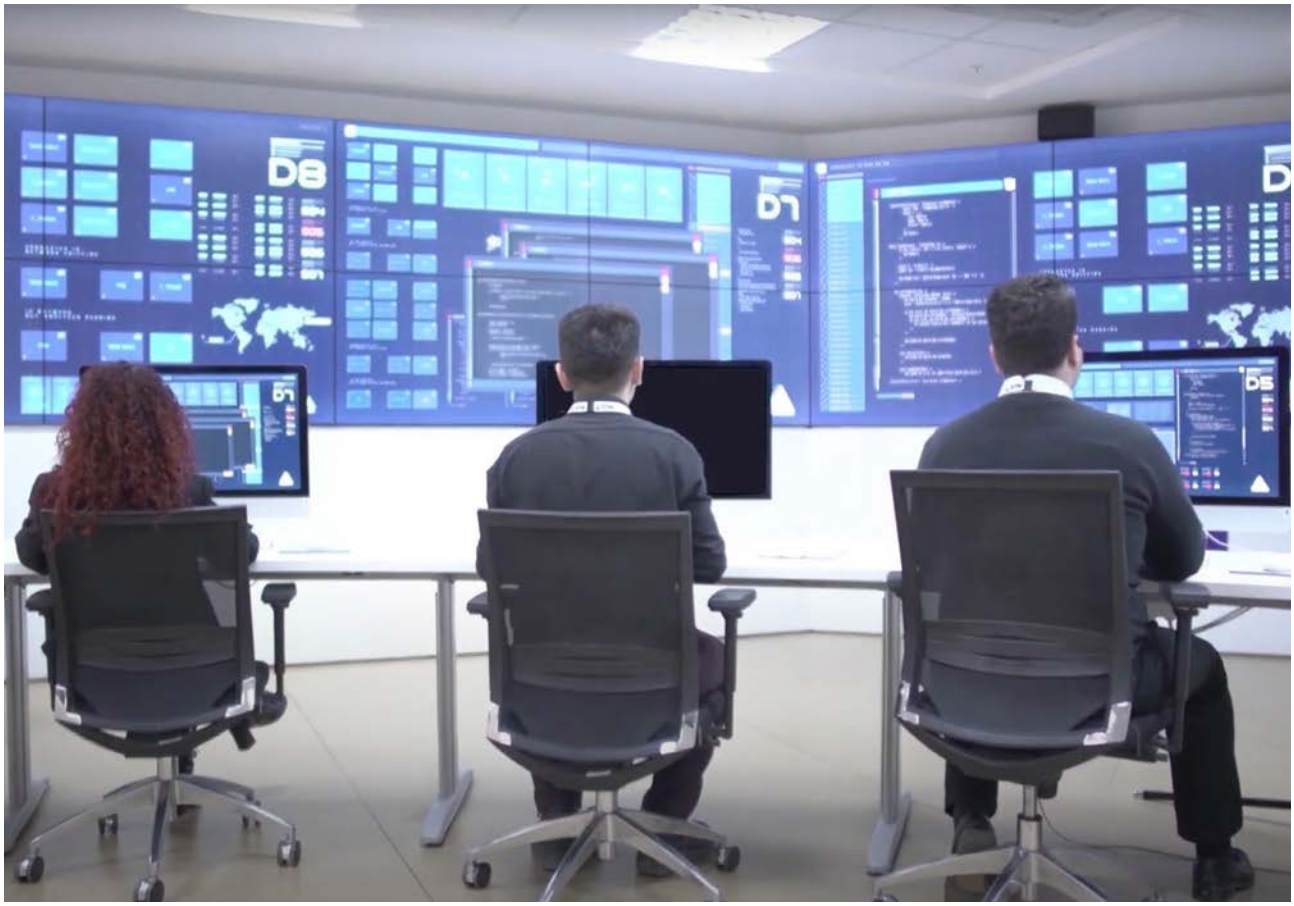
- Üçer aylık dönemlerde yayımlanan "Türkiye Siber Tehdit Durum Raporu" yaşanan siber olaylar konusunda genel bilgi sunmaktadır ve ülkemizde siber güvenlik farklılığının gelişmesine katkı ve destek sağlamaktadır.
- Raporlar, siber tehdit değerlendirmesi ile öngörüler ışığında hazırlanan muhtemel siber saldırı bilgilerini de içermektedir.

BAYRAĞI YAKALA ETKİNLİĞİ, CAPTURE THE FLAG (CTF)

- STM liderliğinde kamu, özel sektör ve üniversitelerin tek çatı altında birleştirilmesi ve siber güvenlik alanında bilgi paylaşım ağının oluşturulması hedeflenmiştir.
- 2015, 2016 ve 2017 yıllarında düzenlenen ve gelecek yıllarda da devam edecek olan etkinlik, bu alanda ülkemizdeki en yüksek katılımlı çalışmasıdır.

SİBER FÜZYON MERKEZİ

Kritik teknoloji ve bilgi varlıklarını koruyan proaktif ve önleyici faaliyetleri içeren **Siber Füzyon Merkezi (SFM)**; Siber Tehdit İstihbarat Merkezi, Siber Operasyon Merkezi ve Zararlı Yazılım Analiz Laboratuvarı (Z-Lab) olmak üzere bütünleşik ve entegre 3 ana merkezden oluşmaktadır.



STM SİBER FÜZYON MERKEZİ (SFM)

- Geleneksel siber güvenlik işlevselliklerini, yeni yeteneklerle birleştirerek tek ve entegre siber güvenlik yaklaşımı
- Siber tehdit istihbaratının güvenlik ve teknolojik ve müdahaleleri ile entegre eden çok yönlü yaklaşım
- Bu entegrasyon ile kritik teknoloji ve bilgi varlıklarını koruyan proaktif eylemleri yönlendirme
- İş, insan, süreç ve teknolojinin bütünleşmesi

STM SFM HİZMETLERİ

- Siber Operasyon Merkezi Hizmetleri
- Dinamik Risk Yönetimi
- Olay Müdahale
- Siber Tehdit İstihbaratı
- Zararlı Yazılım ve Sistem Analizi
- Trafik Analizi ve İzleme

SİBER TEHDİT İSTİHBARAT MERKEZİ

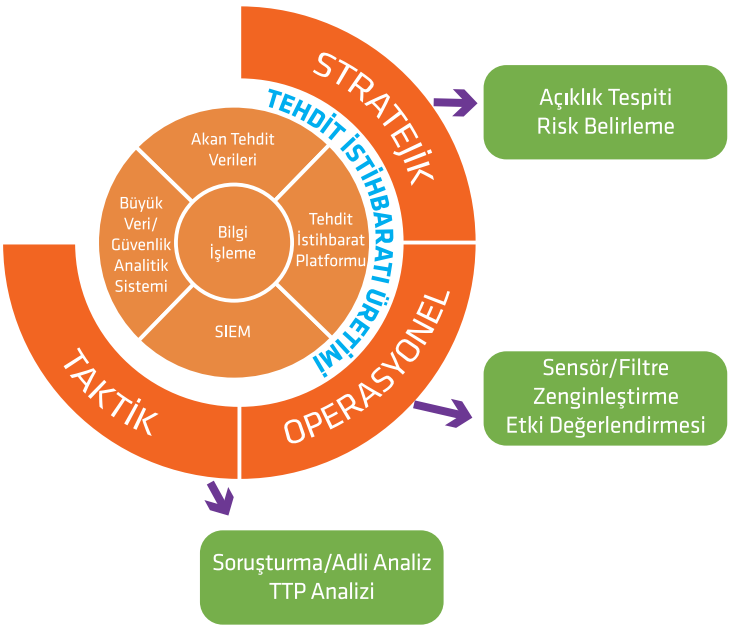
- Sürekli Atak Yüzey Analizi
- Açık Kaynak Tehdit İstihbaratı Analizi
- Siber Tehdit İstihbaratı Platformu
- Tehdit Aktörü Analizi
- Müşteriye Özel Hazırlanmış Tehdit Raporları

SİBER OPERASYON MERKEZİ

- Siber Operasyon Merkezi Danışmanlığı
- Olay Müdahale ve Tehdit Avcılığı Hizmeti
- Güvenlik Ürünleri Kural Seti Geliştirme ve Optimizasyon Danışmanlığı
- 7/24 Güvenlik ve Altyapı İzleme Hizmeti

STM ZARARLI YAZILIM ANALİZ LABORATUVARI (Z-LAB)

- Sanal veya fiziksel platformlarda farklı işletim sistemlerinin statik ve dinamik zararlı yazılım analizleri gerçekleştirilir



STM SİBER OPERASYON MERKEZİ

Siber Operasyon Merkezi'nde; siber olayların tespiti için altyapı tesis edilmesi, güvenlik politikalarının uygulanması ve izlenmesinden başlayan, olay inceleme ve yerinde olay müdahalesini kapsayan hizmetler verilmektedir. Kurumların ihtiyaçlarına binaen bu hizmetlerin bir veya birkaçı kuruma özel plan dahilinde verilmektedir.

OLAY İLİŞKİLENDİRME (KORELASYON) HİZMETİ

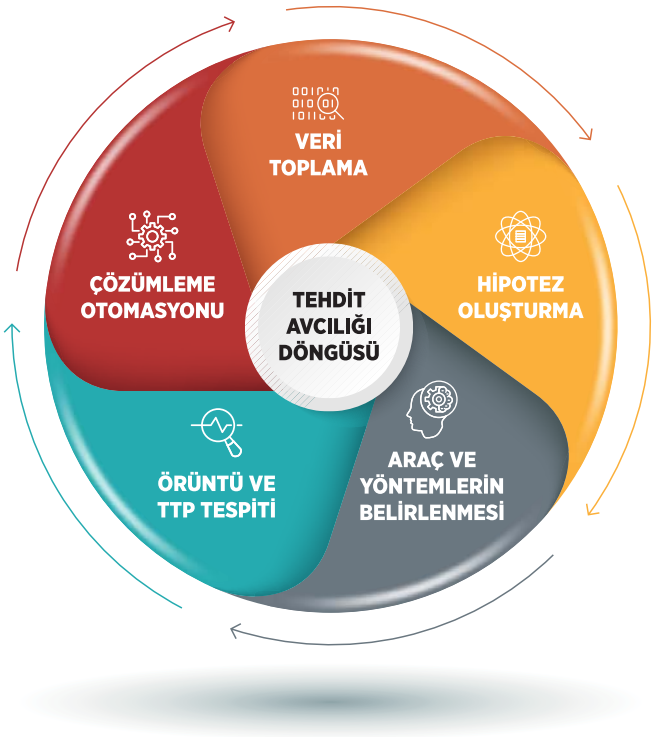
Olay kaynakları ve SIEM çözümünün yetenekleri doğrultusunda kayıtların ilişkilendirilmesi ve sonuçlar çıkarılması için ihtiyaç duyulan korelasyon kuralları belirlenir ve sisteme tanımlanır. Tanımlı kurallar neticesinde oluşan alarmlar incelenerek güvenlik ihlallerinin nedenleri detaylı şekilde araştırılır.

SIEM İZLEME HİZMETİ

SIEM tarafından toplanan kayıtlar, SIEM izleme yeteneklerinin yanı sıra STM mühendisleri tarafından geliştirilen ilave uygulamalar, açık kaynak kodlu ve ticari araçlar yardımıyla siber güvenlik analistleri tarafından izlenir, araştırılır, değerlendirilir ve müdahale ihtiyacı raporlanır. İzleme Hizmeti kapsamında 5/8 ya da 7/24 hizmet verilebilmektedir.

DANIŞMANLIK VE YERİNDE DESTEK HİZMETİ

Hizmet verilen kuruma ait siber güvenlik bileşenleri analiz edilerek, kuruma ait sistemlerin güvenliğinin analiz edilmesi ve arttırılması konusunda kurum ile birlikte gerekli çalışmalar yapılır. Güvenliğin bütünleşik olarak sağlanması hedeflenir.



OLAY İNCELEME

Siber Ölüm Zinciri (Cyber Kill Chain) metodolojisi referans alınarak yapılan olay incelemelerinde; siber saldırının kaynağı, hedefi, kapsamı, atak vektörü ve etkilediği sistemler tespit edilir. Yapılan çalışmaların ardından elde edilen bulgular tüm detaylarıyla birlikte raporlanır ve müteakip dönemde gerçeklesmemesi için ihtiyaç olan tedbirler sunulur.

YERİNDE OLAY MÜDAHALE

Hizmet verilen kurumun kaynaklarına bir saldırı olduğunda olaya müdahale edilir ve saldırı esnasında oluşabilecek kaybın yok edilmesi veya en aza indirilmesi amacıyla gerekli çalışma, görevli personel ve kurum yetkilileriyle birlikte yapılır.

TEHDİT AVCILIĞI

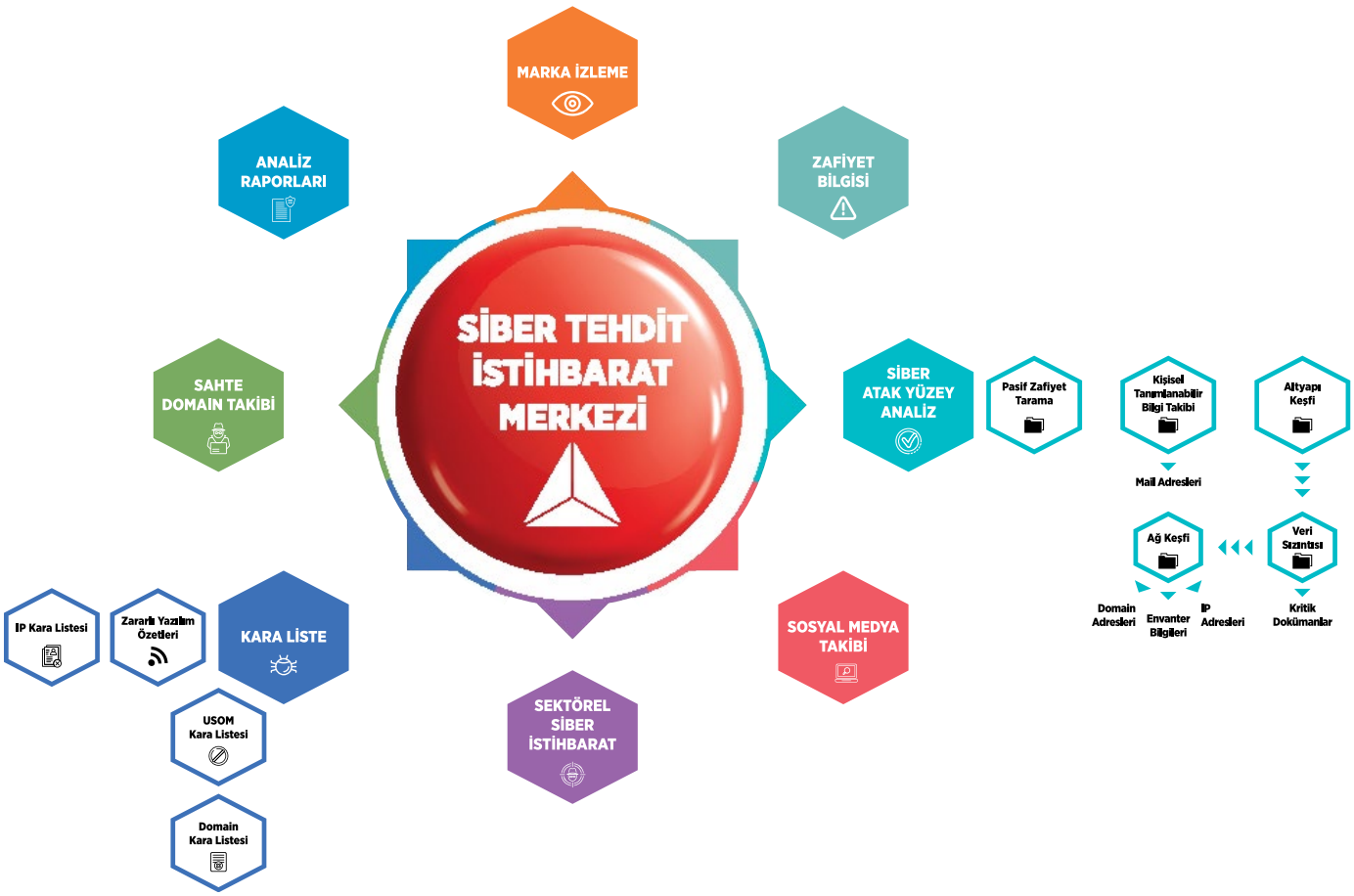
Kuruma ait olan ağ ve sistemlerde proaktif bir şekilde gelişmiş düzeydeki siber tehdit varlığı farklı senaryolar göz önünde bulundurularak araştırılır. Potansiyel saldırganlar, bu saldırganların kullandıkları teknikler, kullanılan araçlar ve saldırı süreçleri aktif olarak takip edilir ve tanımlanır. Bu sayede Hedef Odaklı Saldırılara (Advanced Persistent Threat – APT) karşı alınması gereken önlemler tespit edilir ve kurumun bilişim teknolojileri altyapısındaki boşluklar belirlenir. Açık kaynak kodlu ve ticari araçlardan faydalanılarak potansiyel tehditler, şüpheli ve anormal aktiviteler, kötü amaçlı yazılımlar gibi tehlikeleri tanımlamak için gösterge tabloları ve raporlar oluşturulur. PCAP dosyaları, ağ akış verileri, uygulamalar ve diğer güvenlik araçları üzerinden gelen bilgiler düzenli bir şekilde ve derinlemesine analiz edilir.

STM SİBER TEHDİT İSTİHBARAT MERKEZİ (STIM)

Siber uzayda gerçekleşen saldırıların önceden tespit edilebilmesi ve önlem alınabilmesi amacıyla STM SiberTehdit İstihbarat Merkezi'nde açık kaynaklar üzerinden veri toplama, veriyi zenginleştirme ve veriye bilgi statüsü kazandırma ile bilginin analiz edilerek istihbarata dönüştürülmesi işlemleri gerçekleştirilmektedir.

Siber tehdit istihbaratı için gerekli veriler, tehdit unsurlarının ve küresel tehdit ekosisteminin teşhisi ve sürekli izlenmesini içeren bir süreçle toplanmaktadır. Bu süreçte tehdit verileri açık kaynaklardan, ticari kaynaklardan ve MISP benzeri platformlardan toplanarak aksiyon alınabilir istihbarat haline getirilmekte ve kendi yazılımlarımız üzerinden sunulmaktadır. Aynı zamanda elde edilen bu istihbarat verisi, siber tehdit analistlerince sektöre veya kuruma özel siber tehdit istihbaratına dönüştürülmektedir.

STIM tarafından toplanan verilerin, zenginleştirilmesi, depolanması ve doğrulanmasını müteakip elde edilen nihai siber tehdit istihbarat bilgileri, STM Siber Tehdit İstihbarat Platformu (CyThreat) üzerinden kurumlara servis olarak sunulmaktadır.



STM ZARARLI YAZILIM ANALİZ LABORATUVARI (Z-LAB)

Zararlı Yazılım Analiz Laboratuvarı'nda, zararlı olduğu değerlendirilen veya şüphelenilen dosyaların analizleri profesyonel analistler tarafından gerçekleştirilmektedir. Söz konusu analizler ile yazılımın zararlı olup olmadığı, şüpheli dosyanın arka planda neler yaptığı, asıl amacının ne olduğu ve kendisini nasıl gizlediği gibi özel davranışlar ortaya çıkarılmaya çalışılmaktadır.

Zararlı Yazılım Analiz Laboratuvarı'nda Windows, Linux ve MacOSX işletim sistemlerine ek olarak akıllı telefonlar ve tablet bilgisayarlarda kullanılan Android ve iOS işletim sistemleri üzerinde çalışan zararlı yazılımların analizi yapılabilmektedir.

Analistlerin analiz yapabilecekleri birbirinden bağımsız ağlar ve simülasyon ortamları sayesinde, zararlı yazılımın ihtiyaç duyduğu internet ortamı simüle edilebileceği gibi hiçbir internet bağlantısı olmadan da analiz yapılabilmesi sağlanabilmektedir.

ZARARLI YAZILIM ANALİZİ YAPILAN PLATFORMLAR

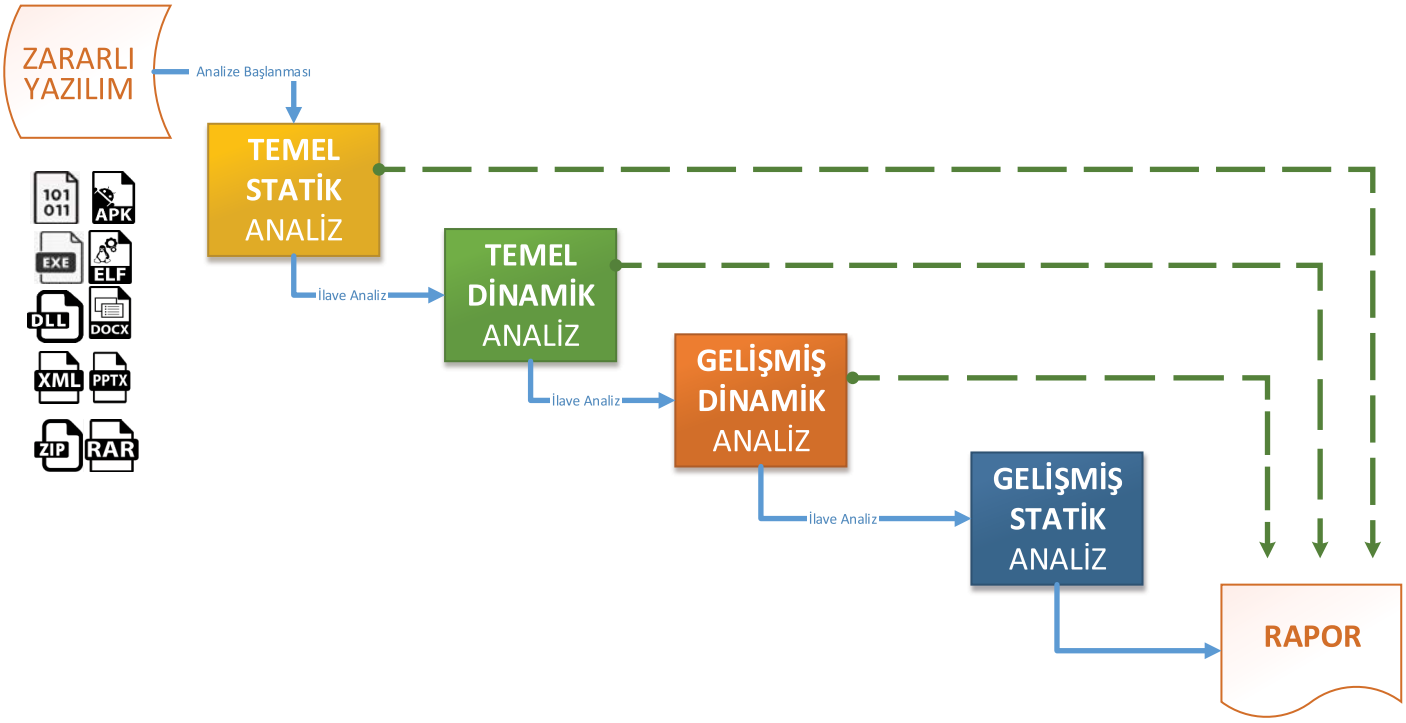
- Windows
- Linux
- OSX
- iOS
- Android

ANALİZ YÖNTEMLERİ

- Temel Statik Analiz
- Temel Dinamik Analiz
- Gelişmiş Statik Analiz
- Gelişmiş Dinamik Analiz

ANALİZ MECRALARI

- Sanal bilgisayarlar üzerinde analiz
- Kum havuzları üzerinde analiz
  - Ticari kum havuzları kullanılarak
  - Açık kaynak kum havuzları kullanılarak
- Fiziki cihazlar
  - Cep telefonu
  - Tablet
  - Bilgisayar



CyDecSys®

Zafiyet Temelli Risk Yönetim Aracı ve Karar Destek Sistemi

- Bütünleşik siber güvenlik durum tespit, analiz ve karar destek sistemidir.
- Bilgisayar ağlarının siber güvenlik resmini sunarak durumsal farkındalık oluşturur.
- Karar vericilere analiz sonuçları ile destek sağlar.

ANA ÖZELLİKLER

- Ağ topolojisi oluşturulması ve ağdaki varlıkların tespiti ile durumsal farkındalık yaratılması
- Ağ topolojisi ve varlıklar üzerindeki zafiyetlerin tespiti ile saldırı yüzeyinin belirlenmesi
- Zafiyetlerin ağ ve varlıklar üzerinde yarattığı risklerin ayrıntılı analizi (Temel ve tehdit tabanlı metodolojik risk algoritmaları ile)
- Saldırı ağacı üzerinde tehdit tabanlı ve çok adımlı saldırı simülasyonu
- Koruyucu önlem senaryoları ile risk analizi
- Zafiyet analizi yapabilmek için zenginleştirilmiş ve doğrulanmış zafiyet veri tabanı

AĞ KEŞFİ, CİHAZ VE ZAFİYET TARAMA

- Fiziksel ağ topolojisinin (alt ağlar, aktif ağ cihazları ve yapılandırmaları) keşfi
- Ürün spesifik ve açık protokol (SNMP vb.) tabanlı yöntemlerle ağ keşfi
- Ağ üzerindeki cihazların, yazılımların, açık port ve servislerin tespiti
- Zafiyetlerin dağıtık mimaride yüksek performanslı olarak taranması ve tespiti

SİBER GÜVENLİK RİSK ANALİZİ VE SİMÜLASYONU

- Tehditlerin tanımlanması ve yönetimi
- Çok adımlı saldırı yollarının tespit edilmesi ve saldırı ağacı ile gösterimi
- Cihaz, zafiyet, alt ağlar, ürünler vb. bileşenlerin risklerinin temel ve tehdit bazlı istatistiksel gösterimi
- Zafiyetlerin giderilmesine yönelik koruyucu önlemlerin sonuçlarının simüle edilmesi
- Koruyucu önlem senaryoları ile sağlanabilecek iyileştirmenin / risk değişiminin incelenebilmesi

ZENGİNLEŞTİRİLMİŞ ZAFİYET VERİ TABANI

- Zafiyet verilerinin ilişkilendirilmesi, sınıflandırılması, hata ayıklaması ve zenginleştirilmesi ile oluşturulan zafiyet veri tabanı
- Zafiyet, zayıflık, ürün, istismar (exploit) vb. bilgilerin ilişkilendirilmesi
- Zafiyetlerin istismarı için ayrıcalık ön koşulları ve olası sonuçlarının (makine öğrenimi gibi yöntemlerle) üretilmesi
- Zafiyetlerin analizi için detaylı sorgu yeteneği

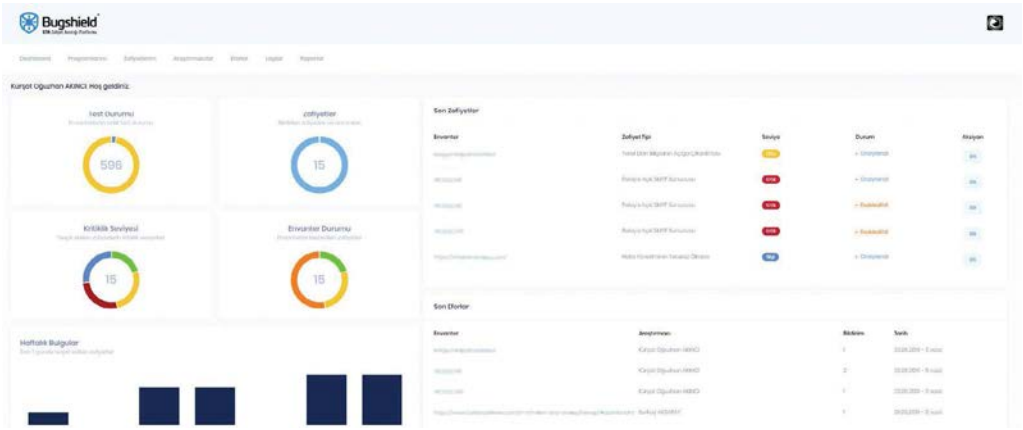
BUGSHIELD®

Kesintisiz Siber Güvenlik

STM Bugshield; “hacker” bakış açısı ile müşteri kaynaklarındaki zafiyetlerin araştırıldığı, bulunan zafiyetlerin raporlandığı Sürekli Sızma Testi ve Ödül Avcılığı Platformudur.

STM Bugshield; müşteri, analist ve araştırmacı profilleri bulunan rol tabanlı yönetim yeteneğine sahiptir. Araştırmacı rolünde farklı alanlarda yetkin siber güvenlik uzmanları zafiyet araştırması yapar; analist ise tespit edilen zafiyetleri doğrular ve onay süreci sonrasında müşteriyi platform üzerinden bilgilendirir ve bu sayede müşteri, tespit edilen zafiyetlere hızlı yanıt verebilir. Platforma bütünleşik geliştirilen biletleme (ticketing) mekanizması ile bulgular ve durum değişiklikleri anlık olarak izlenebilir. Bugshield üzerinden gönderilen uyarılara ek olarak e-posta ve SMS ile de bildirimler iletilebilmektedir.

- Sistemlerin “Sürekli Sızma Testi Metodolojisi” ile müşteri tarafından belirlenen zaman aralıklarında farklı güvenlik araştırmacıları tarafından test edilmesiyle, yeni çıkan zafiyetlerin hızlı bir şekilde tespiti hedeflenmektedir. Tespit edilen zafiyetler iki aşamalı onay sürecine tabi tutularak, doğruluğu onaylanan bulgular müşteriye anlık bildirimlerle iletilmektedir. Bu sayede zafiyetin bulunması ile kapatılması arasındaki süre kısaltılmaktadır.
- Testlerin durumu, bulunan zafiyetler, zafiyetlerin kritiklik seviyeleri, zafiyetlere yönelik yapılan işlemler ve zafiyet envanteri portal üzerinden izlenebilmektedir.
- Kurumlar, envanter listelerini ve test politikalarını belirleyerek zafiyet araştırması talep edebilmektedir.
- Kurumlar, zafiyet araştırması sonuçlarını pdf, word (docx), csv ve json formatlarında ve istedikleri filtrelemeyi uygulayarak otomatik rapor oluşturabilmektedir.



Test Durumu
Test edilen veya edilmesi planlanan envanterin görüldüğü ekrandır.

Zafiyetler
Bildirilen zafiyetlerin onay durumlarının yer aldığı ekrandır.

Kritiklik Seviyesi
Kritik, yüksek, orta ve bilgi seviyesinde tespit edilen zafiyetlerin görüldüğü ekrandır.

Envanter Durumu
Zafiyetlerin kaç adet uygulama, IP adresi veya alan adında (domain) bulunduğunu gösteren ekrandır.

ÖNE ÇIKAN ÖZELLİKLER

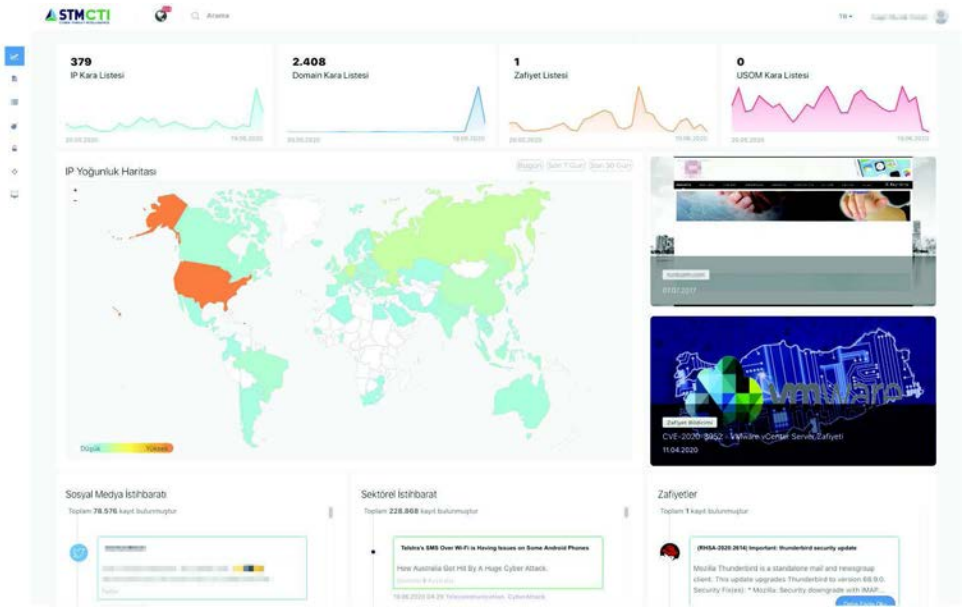
Güvenilirlik: Zafiyetlerin gizlilik sözleşmesi imzalamış güvenilir bir araştırmacı grubu tarafından tespit edilmesi
Kalite: Envantere birden fazla araştırmacının bakması ve tespit edilen zafiyetlerin STM analistleri tarafından kontrol edilip onaylanması
Çeviklik: Tespit edilen tüm zafiyetlere anlık bildirim gönderilmesi ve aksiyon alınabilmesi
Süreklilik: Dönemsel sızma testlerinin aksine daha sık aralıklarla testlerin gerçekleştirilmesi

Bugshield®
STM Zafiyet Avcılığı Platformu

CyThreat

Siber Tehdit İstihbarat Platformu

CyThreat, çeşitli kaynaklardan (deep/dark webten, sosyal medyadan, bloglardan, forumlardan vb.) otomatize bir şekilde topladığı siber tehdit istihbarat verilerini STM analistlerinin konu ve olay bazındaki raporları ile zenginleştirerek müşterilerine sunar. Bu sayede, siber tehdit aktörlerinin aktivitelerinin tespit edilmesi, siber saldırıların gerçekleşmeden önüne geçilmesi ve koruyucu önlem alınması mümkün olmaktadır. Böylece, olası saldırılar sonucunda meydana gelebilecek finansal kayıplar ve itibar kaybı önlenebilmektedir. İstihbarat verileri (kara liste IP adresleri, alan adları, zararlı yazılım hash değerleri, zafiyet verileri), API ve STIX/TAXII aracılığıyla güvenlik cihazlarına entegre edilebilmektedir. Görev yönetimi özelliği ile tespit edilen bulgular için müşteriye manuel/otomatik olarak görev tanımlanabilmekte ve bu sayede olay takibi yapılabilmektedir.



KARA LİSTELER

- IP Adresleri
- URL & Alan Adları
- Zararlı Yazılım Hash Değerleri
- USOM Zararlı Bağlantılar

ZAFİYET LİSTESİ

- Zafiyet tanımı
- CVSS skoru
- Zafiyetin etkilediği ürünler

ANALİZ RAPORLARI

- Zararlı yazılım analiz raporları
- Siber tehdit durum raporları
- Atak yüzey analiz raporları

POTANSİYEL OLTALAMA SİTELERİ

- Kuruma yönelik oltalama saldırısı yapmak amacıyla kullanılabileceği değerlendirilen alan adlarının tespit edilmesi ve ilgili müşteriye sunulması

SOSYAL MEDYA İZLEME

- Sosyal medya platformlarından müşteriye yönelik elde edilen verilerin sunulması

GÖREV YÖNETİMİ

- Manuel ve otomatik görev tanımlamalarıyla olay takibinin yapılmasını sağlar.

SEKTÖREL SİBER İSTİHBARAT

- Müşterinin bulunduğu sektöre yönelik tehdit verileri açık kaynaklardan, çeşitli forumlardan, haber kaynaklarından ve deep/dark web üzerinden toplanarak kullanıcılara sunulmaktadır.

MARKA İZLEME

- Markaya yönelik veriler bloglardan, forumlardan, haber sitelerinden ve deep/dark web üzerinden toplanarak arayüzde kullanıcılara sunulmaktadır.

İHLAL VERİLERİ

- Tespit edilen kurumsal e-posta adreslerinin kullanıcılara sunulduğu arayüzdür. Her bir e-posta adresine ait sızıntı bilgisi, nereden sızdırıldığı ve tespit edildiği tarih bilgisi paylaşılmaktadır.

RAPORLAMA

- Raporlama özelliği ile kullanıcılar, arayüz üzerinden sunulan verileri filtreleyerek tek seferlik veya zamanlanmış rapor oluşturabilir.

API

- Kara liste IP adresleri
- Kara liste alan adları
- USOM zararlı bağlantılar
- Zararlı yazılım hash değerleri
- Ürün bazlı zafiyet verisi

CYTHREAT
SİBER TEHDİT İSTİHBARATI

IoT MEDIC

IoT Medic; hastane ortamlarında bulunan kablolu veya kablosuz medikal IoT cihazlarının ağ trafiğini pasif bir şekilde dinleyerek medikal IoT cihazlarına ait envanter dökümünü (IP/MAC bilgisi, cihaz türü, marka/model, yazılım sürümü vb.) ve bu cihazlara özelleşmiş saldırıları tespit edebilen bir sistemdir.

ANA BİLEŞENLER

- IoT envanter çıkarımı
- Saldırı tespiti ve alarm yönetimi
- İstihbarat verisi destekli saldırı tespiti
- Sistem yönetimi ve raporlama

STM ITSEF LABORATUVARI

IT ürünlerinin ve IT çözümleri kullanılan ürünlerin iddia edilen güvenlik garanti seviyesine (EAL) uygun olarak uluslararası ortak değerlendirme metodolojisine (CEM) göre ürünün değerlendirilmesi, TÜRKAK tarafından ISO 17025 standardından akredite edilmiş laboratuvarımızda gerçekleştirilmektedir.

STM ITSEF EAL 4+ seviyesine kadar IT ürün değerlendirme hizmeti vermektedir.

TSE'den lisanslı laboratuvarımızda gerçekleşen değerlendirme sonucunda TSE tarafından verilen belgeler resmi olarak 30 ülkede tanınmaktadır.

ORTAK KRİTERLER STANDARDI

- Bilişim Teknolojisi ürünleri için geliştirilmiş uluslararası kabul gören tek BT ürün güvenlik değerlendirme modelidir. Dünyada 30 ülke tarafından resmî olarak tanınmaktadır.

HİZMETLERİMİZ

ASE: Güvenlik Gereksinimleri
- Güvenlik gereksinimlerinin değerlendirilmesi

ADV: Geliştirme – Tasarım
- Tasarımın değerlendirilmesi
- Güvenlik fonksiyonlarının değerlendirilmesi
- Kaynak kodun değerlendirilmesi

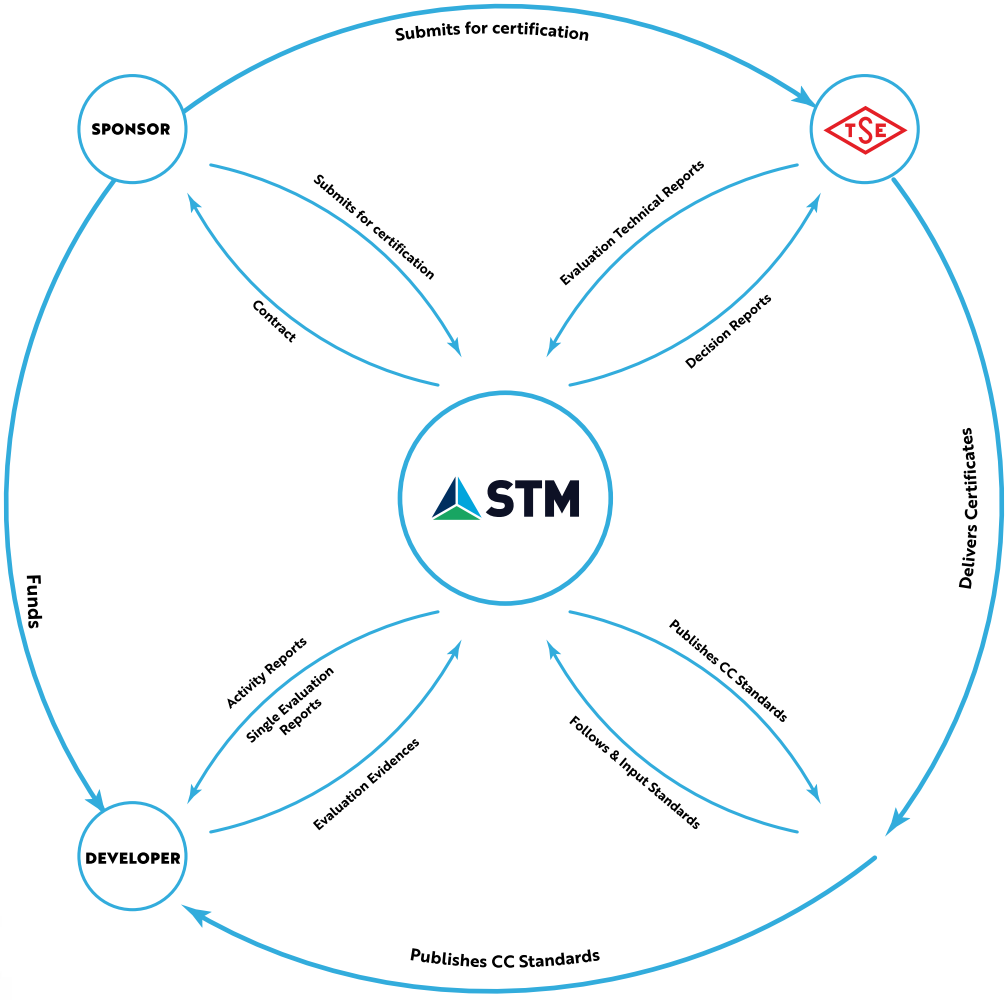
ALC: Ürün Geliştirme Yaşam Döngüsü
- Geliştirme süreçlerinin değerlendirilmesi
- Ar-Ge sahası fiziksel güvenlik önlemlerinin değerlendirilmesi
- Konfigürasyon yönetiminin değerlendirilmesi
- Geliştirmede kullanılan araçların değerlendirilmesi

AGD: Kullanıcı Dokümantasyonu
- Kullanım, kurulum, teslim ve bakım kılavuzlarının değerlendirilmesi

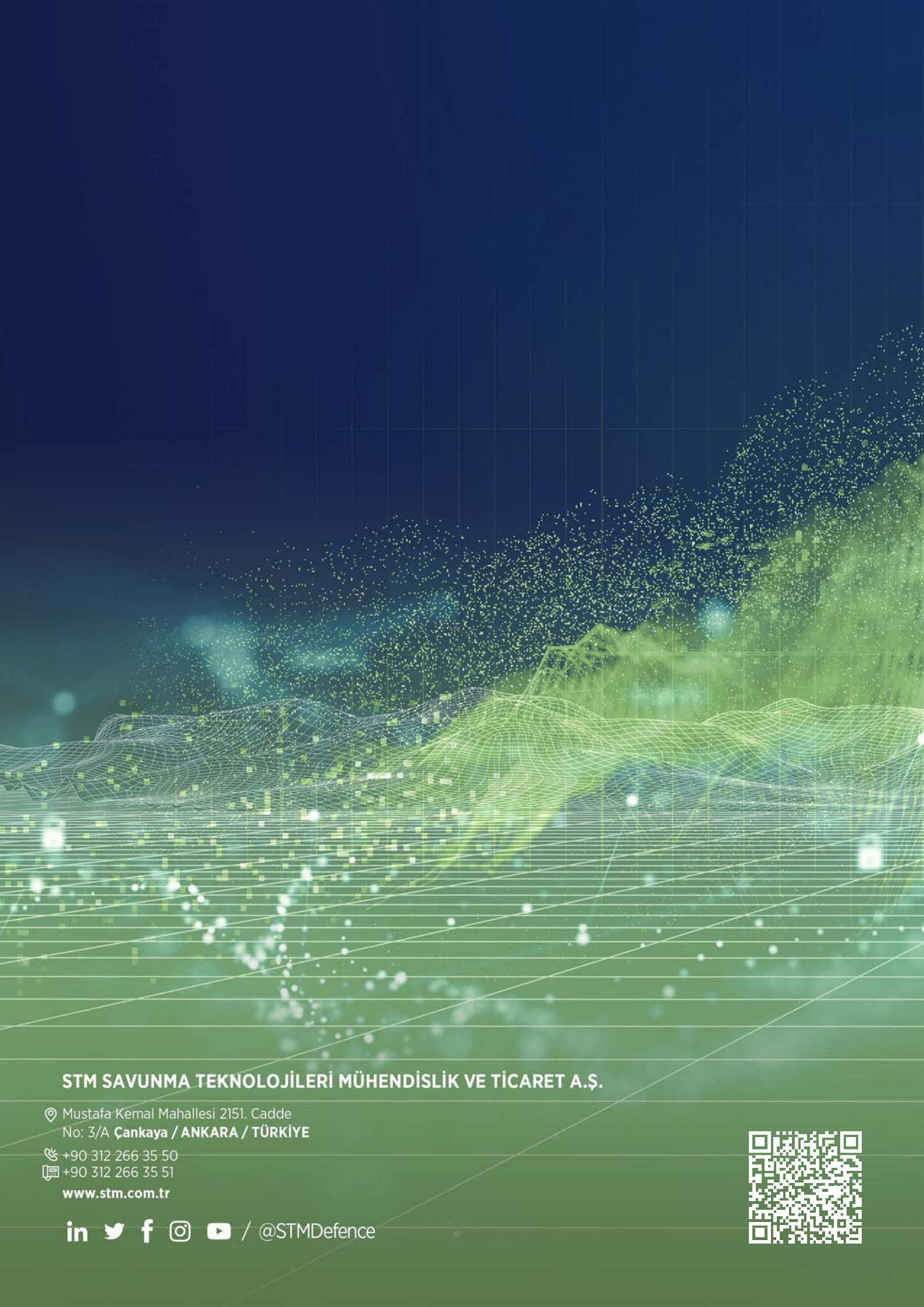
ATE: Test Değerlendirmesi
- Üretici testlerinin değerlendirilmesi, tekrarlanması ve doğrulanması
- Bağımsız fonksiyonel ve güvenlik testlerinin gerçekleştirilmesi

AVA: Açıklık Analizi
- Ürüne yönelik atak potansiyelinin hesaplanması
- Ürüne yönelik açıklık analizinin gerçekleştirilmesi

Ayrıca
- Tüm değerlendirmelerin raporlanması, iyileştirme fırsatlarının belirlenmesi



COMMON CRITERIA CERTIFIED EAL4+



STM SAVUNMA TEKNOLOJİLERİ MÜHENDİSLİK VE TİCARET A.Ş.

Mustafa Kemal Mahallesi 2151. Cadde
No: 3/A **Çankaya / ANKARA / TÜRKİYE**

+90 312 266 35 50
+90 312 266 35 51

www.stm.com.tr

/ @STMDefence