KOTTO BİLİŞİM A.Ş.

KAMU SİBER GÜVENLİK DÜZENLEMELERİ UYUM KİTAPÇIĞI

www.kottoas.com

Günümüzde artış gösteren **14 siber saldırı**

KOTTO
BİLİŞİM A.Ş.

KOTTO BİLİŞİM A.Ş.

GÜNCEL MEVZUAT HAKKINDA BİLGİLENDİRME

5 Temmuz 2019'da Cumhurbaşkanlığı tarafından yayınlanan, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde kurumlar tarafından alınması gereken önlemler açıkça göstermektedir ki günümüzde bilgi güvenliği ve mahremiyeti, tamamen milli bir konu haline gelmiştir.

Her bir kurumun kendi üretmiş olduğu verilerin tamamını merkezî sistemlerde toplayabilmesi ve erişim olanaklarını sağlayarak denetim altında tutabilmesi gerekmektedir.

5651 sayılı kanun, kamu kurumları, özel şirketler ve kullanıcılar için bir öneri niteliği taşımamakta ve aynı zamanda internet üzerinden işlenen bilişim suçlarının önemli ölçüde önüne geçilmekle beraber kullanıcıların internet üzerinden aldatılmalarını ve kötü amaçlı içeriklerden korunması da amaçlanmaktadır.

2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile hayata geçirilen, Siber Güvenlik Kurulu, e-Devlet uygulamalarının güvenli olarak ortak kullanılabilmesi amacıyla Kamu Sanal Ağı (KamuNet)'nın kurulmasına karar vermiştir.

Kurumlar içerisinde 2019/12 sayılı Genelge'de bahsedildiği üzere veri sızmasını sağlayan yurtdışı kaynaklı veri transfer uygulamaları, kurumsal olmayan mesajlaşma ve iletişim uygulamaları, yurtdışında veri saklayan ofis belgeleri düzenlemeye ilişkin uygulamalar, kurumsal olmayan e-posta platformlarına erişimler kısıtlanmalıdır.

11. Kalkınma Planı, 3 boyutlu yazıcılardan sosyal medya ve e-ticaret platformlarına kadar teknolojinin merkezinde olduğu birçok yeni alana dair politika önerileri sunmakta, siber güvenlik ve veri mahremiyetiyle ilgili önemli hususlara da ulusal savunmanın bir parçası olarak dikkat çekmektedir. (Teknik altyapı, kurumsal kapasite ve beşeri sermaye.)

6698 sayılı Kişisel Verilerin Korunması Kanununun (KVKK) amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

10 Mart – 7 Nisan 2015 arasında yapılan toplantılar ile Türkiye'nin siber güvenlik boyutunda güçlü ve zayıf yönlerinden hareketle stratejik amaçları ve gerçekleştirmesi gereken eylemler belirlenmiştir. Tüm bu çalışmalar kapsamında üretilen bilginin toplanması, incelenmesi ve değerlendirilmesi sonucunda "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır.


6698 KVKK
• Veriket
• BiSoft DD
• Limrad NAC
• Kotto
• Standardizasyon Hizmeti
• Talia Stamp
CB 2019-12
• DivvyDrive
• LogSign
• Limrad NAC
• Limrad MDM
• Talia Stamp
• Veriket
• BiSoft DD
• Trapmine
• Milat
(Ulak Haberleşme)
• Kron PAM
KOTTO
BİLİŞİM A.Ş.
KAMUNET
• Kotto ISO 27001
Danışmanlık Hizmeti
• Picus
• Limrad MDM
• Limrad Radius
• Milat
(Ulak Haberleşme)
• Roksit
• Trapmine
• Limrad NAC
5651 İnternet
• Kotto BGYS Eğitimi
• LogSign
• Kron OTP
• Olta.La
• Talia Stamp
• Limrad MDM
• Limrad Radius
• Turk Trust SSL
• Milat
(Ulak Haberleşme)

KOTTO BİLİŞİM A.Ş.

Güvenli Bulut ve Veri Transferi Çözümü

DivvyDrive

DIVVY DRIVE

Dosyalarınız Güvende

Cihazlarınızın başına ne gelirse gelsin, DivvyDrive'da depolanan dosyalarınız güvendedir.

Veri Şifreleme

Dosyalarınız DivvyDrive'da özel kripto algoritmaları ile şifrelenerek saklanır.

Güçlü Arama

DivvyDrive dosyalarınıza daha hızlı erişmenizi sağlar. Anahtar kelimeyle içerik arayabilirsiniz.

Paylaşım

Dosyalarınızı istediğiniz kişilerle paylaşabilir ve düzenleyebilirsiniz.

Virüslere Karşı Koruma

DivvyDrive tüm verileri parçalayarak depoladığı için hiçbir virüs aktif hale gelemez.

7/24 Erişim

Verilerinize erişmek herhangi bir bilgisayardan DivvyDrive ile tüm verileriniz elinizin altında.

Kolay ve Güvenli Bulut Depolama

DivvyDrive, bulunduğunuz her yerde. Evinizde, iş yerinizde ve hareket halindeyken yanınızda. Siz neredeyseniz, dosyalarınız da tam orada. Harekete ve paylaşmaya hazır.

- Tek Kullanımlık Dosya Yükleme ve İndirme
- SSL Sertifikası ile Bağlantı ve Sürekli Şifreli Koruma
- Sınırsız Bant Genişliği
- Güçlü ve Hızlı İçerik Araması ve Zengin İçerik Önizleme

LimRAD AUTH PLATFORM

Ağ Erişim Güvenliği Çözümü
LimRAD NAC

NAC, network için basit ve etkili bir güvenlik çözümüdür. Erişim denetimi ile yetkili olmayan kullanıcıların ağ üzerinde bulunmaları engellenir. NAC teknolojisinin kullandığı 802.1x çözümü kötü niyetli insanlar tarafından artık kolay bir şekilde atlatılabilmektedir. Bu nedenle günümüzde 802.1x çözümüne ek yetenekler gerekmektedir. Örneğin ARP zehirlenmesi, Switch Port VLAN değiştirme gibi tehlikelere karşı ek özellikler eklenmelidir. NAC kullanımının amacı güvenlik kriterlerine uyan ve ağa giriş için onay verilmiş kullanıcıları ve cihazları ağa almaktır.

NAC İle Kazanılacak Bazı Yetenekler

- Sistem güvenliğini sorgular ve sıkılaştırma sağlar. Örneğin Antivirüs güncel değilse ağa bağlanılamaz.
- Kullanıcı yetkilendirmesini denetler ve varlık erişim kontrollerini yapar.
- Hem kullanıcı bazlı hem de cihaz bazlı yetki ve erişim denetimi sağlar.
- Kullanıcı ve cihazdan bağımsız olarak ağların kendi güvenlik denetlemesini yapar.
- Sıfırıncı Gün (Zero-Day) saldırılarına karşı etkili bir önlemdir.
- Zararlı kullanıcı veya cihazlardan oluşacak problemleri kaynağında engeller.
- Kötü niyetli yazılımların erişim ve yayılmasını engeller.
- Ağda hangi cihaz var, ağa kim dâhil gibi bilgilere bakarak ağ yönetimini etkinleştirir.

Yazılım Tabanlı Ağ Çözümü

Maya SD-WAN

Hibrit WAN, coğrafik olarak ayrılmış iki farklı WAN üzerinden gönderilen trafiğin tek bir merkezde toplanmasıdır.

Hibrit WAN, geleneksel WAN mimarisiyle ortaya çıkan sorunları çözdüğü için 5G hızlarında çok önemlidir.

Trafiği doğrudan internete yönlendirerek, trafik bir veri merkezinden geçtiğinde meydana gelebilecek ekstra atlama ve gecikmeyi ortadan kaldırabilmektedir.

Hibrit bir WAN'ın diğer bir faydası da kullanıcıların gerçek zamanlı izlemeyi kullanarak veri merkezine en iyi yolun hangisi olduğuna karar vermelerine izin vermesidir.

Geleneksel WAN optimizasyon teknikleri simetrik olduğundan, hibrit WAN geleneksel WAN mimarisinden daha iyi bir seçenek olarak kabul edilir. Hibrit WAN ile hem MPLS bağlantısını hem de internet bağlantısını kullanarak asimetrik optimizasyon tekniklerini de kullanabilirsiniz.

Ayrıca, Hibrit WAN bağlantının gerçek zamanlı gecikme süresini izler veya bağlantı üzerinden gerçekleşen hataların sayısına dayalı olarak trafik için en iyi yolun hangisi olduğuna karar verir.

Sonuç olarak, hibrit WAN kullanımının, azaltılmış WAN maliyetleri dahil olmak üzere WAN trafiğinin ve cihazlarının basitleştirilmiş ve iyileştirilmiş yönetim orkestrasyonu, geliştirilmiş ve birleştirilmiş görünürlük ve izleme trafiği ve daha iyi güvenlik gibi bir dizi avantajları vardır.

5G HAZIR MAYA (MİLAT AĞ YÖNETİM VE ANALİZ SİSTEMİ) ÜRÜN AİLESİ

- Geniş alan ve yerel alan ağa yönelik yönetim ve analiz çözümleri
- Milat yazılım tanımlı kontrolcü (SDN Controller)
- CPE (Müşteri Uç Ekipmanı) üzerinde sanal fonksiyonlar
- Trafik politikaları yönetimi
- Geniş alan ve yerel alan ağı izleme ve yönetimi
- Sanal ve fiziksel (VNF/PNF) ağ fonksiyonlarının kolaylıkla entegre edilebildiği bir platform
- Ağ altyapılarında tam monitör, kontrol ve yönetim imkanı
- Artırılmış, özgün siber güvenlik tedbirleri

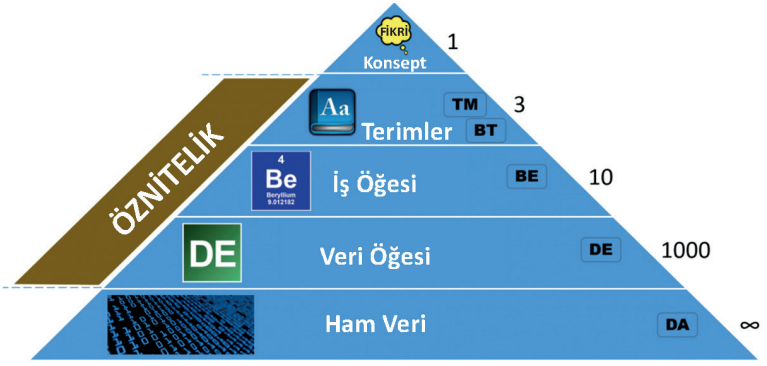
Veri Sözlüğü Çözümü

BiSoft Data Dictionary

Günümüzde Kurum/Organizasyonların tamamı verdiği hizmetleri ve kurumsal süreçlerini yönetebilmek için veri üreten, toplayan ve başka sistemlerle bu verileri paylaşan bilgi sistemleri kullanmaktadır. Ancak çoğu zaman kurumların sahip olduğu verilerin tiplerinde bir standart yoktur. Verilerin nasıl saklanacağı ve ne anlama geleceği gibi konular yazılım geliştiricilerin inisiyatifine kalmaktadır. Bunun sonucu olarak hem kurumsal hafıza oluşturulamamakta hem de sistemler arası veri paylaşımında ve entegrasyonda sorunlar yaşanmaktadır. BDD Kurumlara ait tüm uygulama, servis, platform ve altyapı katmanlarında kullanılacak olan verilerin belirlenen standarda uygun şekilde oluşturulması ve yönetilmesini sağlamakta, terminoloji birliği oluşturarak paydaş ekosistemi ve entegrasyon kabiliyetlerini yükseltme ve kurumsal hafıza oluşturulma amacını taşımaktadır. Bu amaçla Veri Sözlüğü projelerinde rehber olarak belirlenen ISO11179 standardına uyulmakta ve bir bütünlük sağlanması amaçlanmaktadır.

Veri Sözlüğünün Sağladığı Faydalar

- Kurumlardaki uygulama/sistemler tarafından üretilen verilerin Veri Sözlüğü'ne uygunluğu.
- Verilerin tanımlanması ve merkezi kaydedilmesi ile kurumsal hafızanın kişilerden bağımsız hale getirilmesi.
- Verilere hızlı ve güvenli erişimin sağlanması.
- Veri kalitesinin artması. (Kişisel verilerin azaltılması gibi) Veri analizlerinin daha kolay ve verimli yapılabilmesi.



- Veri kullanımında tutarlılık sağlanması.
- Gereksiz veri tanımlarının azalması ya da ortadan kalkması.

Olay Kayıtları Toplama, İzleme ve Yönetimi (SIEM)

Logsign

Logsign, belirlenen bir network üzerinde raporlamayı arzu ettiğiniz faaliyetlere ait log 'ların yönetilebildiği ileri seviye SIEM güvenlik çözümüdür. Kurumlara gelişmiş görsellik ve ağlarını daha iyi anlama imkanı sunar.

Veri güvenliği yönetimi kapsamında hassas ve ileri düzey öneme sahip olan veri güvenliği log yönetimini yapabilen, bu yönetimi sağlamak için belirlediğiniz veri kaynaklarında toparlanan verileri güvenli ve yönetilebilir bir ortamda toparlayan, sistem yöneticileri için bu verileri anlamlandıran teknolojidir.

Ayrıca gelişmiş tehdit analizi yaklaşımı ve ileri seviye korelasyon yetenekleri ile de tehditleri çok daha kolay fark etmenizi ve önlem almanızı sağlar. Sektör lideri güvenlik ürünleri ile aralarındaki senkronizasyon sayesinde herhangi bir tehdit algılandığında güvenlik ürünlerinin otomatik olarak aksiyon almasını tetikleyebilir.

- Ağ Cihazları
- İşletim Sistemleri
- Güvenlik Ürünleri
- Veri Tabanları
- Uygulama Sunucuları
- Zafiyetler / Tehditler
- Kullanıcı Davranışları
- Vekil (Proxy) Sistemler
- E-Posta Sunucuları
- Uç Nokta Güvenliği
- Güvenlik Duvarları
- Ağ Erişim Kontrol (NAC Saldırı Tespit (IPS)
- Tehdit İstihbaratı
- Sensörler

- Tarama ve Soruşturma
- Alarm ve Korelasyonlar
- Veri Görselleştirme
- Raporlama
- Uyum Denetimleri
- Gösterge Panoları
- Vaka ve Müdahale
- Farkındalık

LimRAD AUTH PLATFORM

Mobil Cihaz Yönetim Çözümü
LimRAD MDM EDM

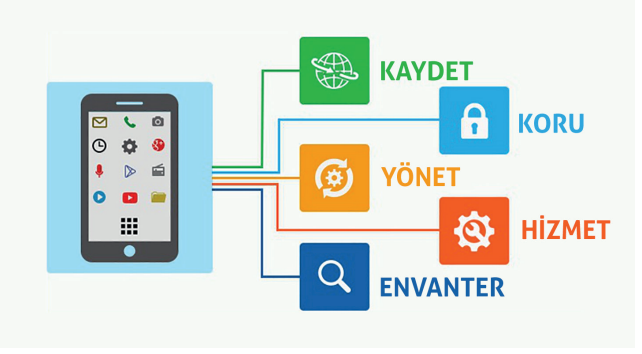
Mobil Cihaz Yönetimi (MDM, Mobile Device Management) bir kısaltma olup, işletmelerin varlık ve taşınabilir bilgi güvenliği için kullandığı en güncel teknolojidir. MDM, dağıtım, güvenceye alma, izleme ve entegrasyon işlemlerinin yapıldığı idari alandır ve işletmelere temel olarak, iş yerlerindeki mobil aygıtların (akıllı telefon, tablet vb.) merkezden ve uzaktan yönetimine dair hizmetler sunar. Aşağıdaki işlev sayesinde, kullanıcıların çalışmalarını kesintiye uğratmadan, kablosuz bağlantı yoluyla mobil cihazlar hızlı ve etkin bir şekilde yönetilebilir ve uzak destek verilebilir.

- **Güvenlik Yönetimi:**
Mobil cihazın çalınması veya kaybedilmesi halinde, güvenlik önlemi olarak tüm kurumsal veriler uzaktan kaldırılabilir ve silinebilir.

- **Politika Yönetimi:**
Kurumsal verileri (kamerayı kapatmak, ekran görüntüsü aldırmamak, ekran kilidi ve parola kilidini zorunlu kılmak, bir hesaptan başka hesaba e-posta yönlendirmesini engellemek vb. yoluyla) güvence altına almak amacıyla işletmelere yönelik bilgi güvenliği kısıtlamaları mobil cihazlara otomatik olarak dağıtır.

- **Yazılım Dağıtımı:**
İşletmelerin, uyguladıkları bilgi güvenliği politikasını esas alarak, kurulum için gerekli uygulamaları mobil cihazlara dağıtmasına olanak sağlar ve tekil kurulum yapma zorluğundan kurtarır.

- **Envanter Yönetimi:**
Cihazdaki yazılım ve donanım verilerini düzenli olarak toplar ve kullanıcıların uygulamaları nasıl kullandıklarını izler.



LimRAD Auth Platform herhangi bir açık kaynak kod kullanılmadan yeniden kodlanmış geliştirilmiştir. Her bir modülü yeniden endüstri standartlarına göre yorumlanarak hazırlanmıştır. Lisanslama adedine göre ölçeklenebilir multithreading mimarisi sayesinde donanım kaynak kullanımını kendisi belirler. Erişimin yapıldığı erişim cihazı, zaman, cihaz türü, lokasyon, kullanıcı adı gibi bilgiler ile doğrulama sırasında kullanıcılar ayrıştırılabilir ve buna göre yetkilendirme yapılabilir. Çoklu donanım üreticisi desteği sayesinde (Multi-Vendor) donanım marka bağımlılıklarınızı ortadan kaldırır. Endüstri standardı çalışan tüm üreticiler ile birlikte çalışabilir.

Çalışırken arttırılabilir kapasite özelliği sayesinde tek bir sanal cihaz (Virtual Appliance) üzerinde 1.000.000 cihaza kadar eş zamanlı yönetim yapılabilir.

KOTTO BİLİŞİM A.Ş.

Ayrıcalıklı Hesap Yönetimi Çözümü

Single Connect PAM

IKron

Ayrıcalıklı hesap yönetimi (PAM, privileged account management) siber güvenlik konusundaki en önemli kontrol hedeflerinden biri olarak ortaya çıkmış ve hızlıca genel kabul görmüştür. Siber suçluların, kritik varlıklara sınırsız erişim elde etmek için ilk hedefleri ayrıcalıklı hesapları (admin, root, sys vb.) bulmak ve bunlardan yararlanmaktır.

Peki ayrıcalıklı hesap nedir?

Ayrıcalıklı bir hesap, sıradan kullanıcılardan daha fazla ayrıcalığa sahip olan bir kullanıcı hesabıdır. Ayrıcalıklı hesaplar, örneğin, yazılımı yükleyebilir veya kaldırabilir, işletim sistemini yükseltebilir veya sistem veya uygulama yapılandırmalarını değiştirebilir. Standart kullanıcılar için normal olarak erişilemeyen dosyalara da erişebilirler.

Etki Alanı Yönetim Hesapları (Domain Admins), Yerel Yönetim Hesapları (Local Admins), Güçlü Kullanıcı Hesapları (Power Users), Hizmet Hesapları (Servis Accounts), Uygulama Hesapları (Application Admins), bir veya daha fazla sistemde yönetici ayrıcalıkları verilen kimlik bilgileri olarak adlandırılır ve gelişmiş/yüksek otorite ile, bu kimlik bilgilerinin ele geçirilmesi veya istismar edilmesi her kuruluş için en kötü durum senaryosudur.

Bu kimlik bilgilerine erişimi olan bir saldırgan güvenilir bir kullanıcı olarak görünür ve aylarca işlem kayıtlarında algılanamayabilir. Ayrıca yetkili hesapların kötüye kullanımı ile içeriden yapılan saldırılar çok daha fazla zarar verebilir.

PAM bu sorunu nasıl çözer?

PAM çözümleri, kapsamlı bir işlevsellik seti sunar, kolay kullanım ve kurulum ile mevcut güvenlik ekosistemine hızlıca entegre olur.

- Kuruluştaki tüm ayrıcalıklı kullanıcı ve uygulama hesaplarını keşfeder.
- Kullanıcılara yalnızca yetkilendirildikleri sistemler için ayrıcalıklar verir.
- Ayrıcalıklı kullanıcılar için yerel / doğrudan sistem şifrelerini ortadan kaldırır.
- Ayrıcalıklı erişim elde etmek için özel iş akışları/iş emirleri ve onay süreçleri oluşturur.
- Yalnızca ihtiyaç duyulduğunda erişimi verir ve erişimi sona erdiğinde erişimi iptal eder.
- Check-in ve check-out işlevselliği ile bir e-kasada ayrıcalıklı kimlik bilgileri güvenli bir şekilde saklanır.
- Şifreleri sürekli ve düzenli (otomatik) olarak değiştirir.
- Farklı bir dizi heterojen sistem üzerinden erişimi merkezi olarak yönetmeyi sağlar.
- Denetim ve adli durumlar için ayrıcalıklı oturum etkinliğini kayıt eder ve delil izleme imkanı sunar.
- Uç noktalar üzerinde gerektiği kadar yetki ilkeleri uygular ve yetkileri sınırlar.

Kron

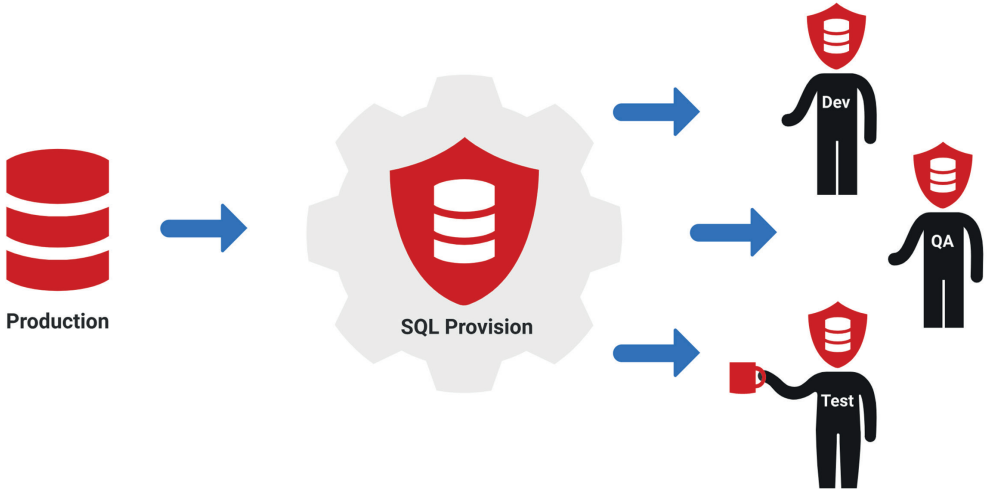
Veri Maskeleme Çözümü
Data Masking

Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemlere veri maskelemesi denilmektedir. KRON Single Connect Veritabanı Maskeleme ürünü ile bütün veriler KVKK ve GDPR uyumlu olarak güvende kalabilir.

Single Connect™: Veritabanı Maskeleme

Dinamik veri maskeleme özelliği sayesinde, geliştirici ve veritabanı yöneticileri ile danışmanların kullandıkları TOAD, Navicat, SQL*Plus, SQL Developer gibi istemcilerin veri tabanlarına yaptıkları erişimlerde, yapılan tüm sorgulamalar, belirlenebilen ve özelleştirilebilen maskeleme kurallarına uygun bir şekilde, gerçek zamanlı olarak dinamik maskelenebilmektedir.

Dinamik veri maskelemede (DDM); redaksiyon– karıştırm – geçersizleştime – bulanıklaştırma – simgeleştirme, yerine geçme gibi maskeleme metodları desteklenmektedir.



KOTTO BİLİŞİM A.Ş.

Güvenlik Otomasyon Yazılım Çözümü

SOAR

atarlabs

SOAR çok farklı kaynaklardan gönderilen güvenlik verilerinin toplanarak düzenlenmesini standardizasyonunu ve otomasyonunu sağlamak için ortaya konmuş bir sistemler bütünüdür.

Sürekli artan tehditlere karşı ağda toplanan verilerin artması sonucunda elde edilen farklı ve büyük verilerin düzenlenmesi ve raporlanması zorlaşmaktadır. SOAR Veri çeşitliliğinin ve miktarının artması karşısında tehdit müdahale yeteneklerinin artmasını sağlamakta ve iş süreçlerini kolaylaştırmaktadır. 10 ve daha fazla elemanın çalıştığı NOC ve SOC ekiplerinin SIEM yanında SOAR da kullanma gerekliliği de ortaya çıkmaktadır. SOAR kavramı içinde öne çıkan iki önemli tanım otomasyon ve orkestrasyondur. Otomasyon uzmanın elle yapacağı işlemlerin otomasyon ortamında hızlıca ve hatasız yapılması, orkestrasyon ise farklı güvenlik uygulama ve servislerinin birlikte çalıştırılması ve birbirine entegre edilmesidir. Saldırılar daha karmaşık hale geldikçe tehdit istihbaratında hızlanmak gerekecektir. Daha hızlı öğrenme ve daha hızlı cevap süreleri elde etmenin yolu SOAR dan geçmektedir. SOAR şüpheli davranışların algılanmasını kolaylaştırmakta ve cevap verme süresini azaltmaktadır. Veri kaynaklarından gelen bilgileri birleştirerek işlemlerin etkinliğini ve verimliliği arttırmakta ve cevapları otomatikleştirmektedir. Sonuç olarak SIEM olayların analizini yapıp sonuçları söylerken SOAR olayları anlayıp karşı hamle yapmaktadır.

ATAR (Automated Threat Analysis and Response), tek bir siber güvenlik çözümüyle farklı ürünler kullanan kurumların da etkili sonuçlar elde etmesini sağlayan bir SOC ve siber güvenlik ROBOTU çözümüdür.

ATAR siber güvenlik robotu siber saldırıların hızına ve hacmine yetişemeyen kurumlara destek olur. Öğretilen saldırı reflekslerini otomatik olarak işletir. Böylece ATAR bir güvenlik operasyon merkezi(SOC) içerisinde sık tekrarlanan işlemleri bir insana uzmana gerek kalmadan işletebilir. Toplam alarm işleme yükünün %40'lık bölümü otomatik olarak (robotla) karşılanırken, ATAR'ın sağladığı vaka inceleme ve yanıtlama imkanları operasyon merkezi uzmanlarının 20 kat daha hızlı analiz ve çözümleme yapmasına imkan sağlıyor.

Tekrarlanan İşlem Otomasyonu
- Senaryo odaklı otomasyon
- Karmaşık mantık bileşen desteği
- 90+ Platform için Bağlantı Desteği
- Tam veya Yarım Otomatikleştirme

Analist Verimini Artırma
- Bütünleşik inceleme arayüzü
- İşbölümcü çalışma ortamı
- Tek tıklamayla delil topla ve işle
- Delil saklama / arşivleme

Güvenlik Operasyon Merkezi
- SOC işlemlerinden ölçüm toplama
- Servis seviyesi anlaşma ölçümü
- İşyükü izleme
- Raporlama ve Tablolama
- İş/İşlem tasarrufu

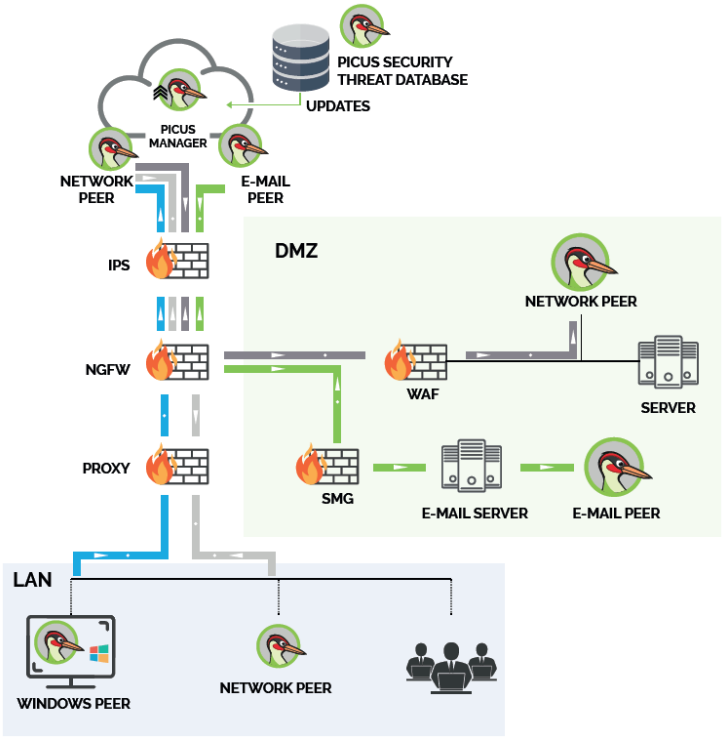
KOTTO BİLİŞİM A.Ş.

PICUS

Sızma Testi Simülasyon Çözümü

Her geçen gün kurumların en büyük tehdidi haline gelen siber saldırılar için yerli girişimci Picus harekete geçti. Kurumların siber güvenlik açıklarını test eden ürünümüz, bu alanda ihracata başlayan ilk çözüm oldu.
Picus ile birçok kurumun uzun sürede tespit edebildiği güvenlik açıklarını, çok daha kısa sürede ortaya çıkarmaya yardımcı oluyoruz. Sürekli güvenlik denetimi yaklaşımını geliştirerek, şirketlerin sahip olduğu teknolojiyle kurumların bu tehditlere ne ölçüde hazır olduklarını ve ellerindeki mevcut güvenlik yatırımıyla bu saldırılardan korunmak için yapmaları gerekenleri raporluyoruz.

- **Yükle ve Yaygınlaştır**
- Yazılım seti birkaç saat içinde kurulabilir ve hemen çalışmaya başlayarak kritik sonuçlar üretir.
- **İlk Durum Değerlendirmesi**
- Güvenlik açıklarını ve zafiyetleri tespit ederek gerçek zamanlı eylemler için rehberlik eder.
- **Ölçüm ve Görselleştirme**
- Elde edilen sonuçları gerçek zamanlı olarak raporlar, tablolar ve objektif kıyaslamalar yapmaya olanak tanır.
- **Yatıştırma ve Hafifletme**
- Ürün ve üreticiye özel tespit edilmiş olan zafiyetlere yönelik iyileştirme önerileri ve acil eylem planları hazırlar.



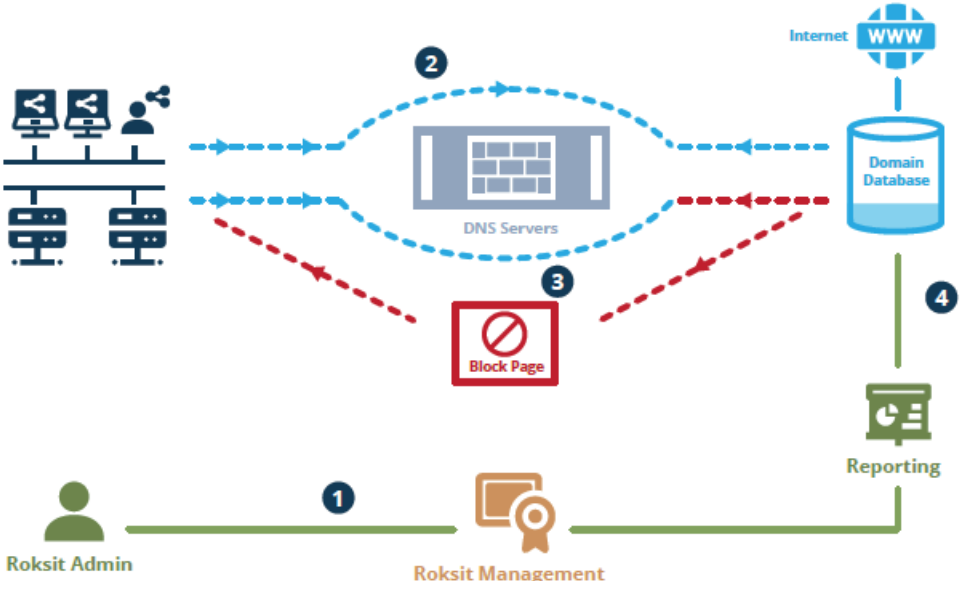
Saldırganlar tarafından kullanılan 2 bin 400'den fazla atak tekniğine Picus Security Labs tarafından her ay 200 farklı tehdidin eklendiği ve testlerin günlük olarak sürekli yapılabildiği bir yapı, kurumların siber saldırılara hazırlık seviyesinin arttırılmasını sağlıyor.

Alan Adı Güvenlik Duvarı Çözümü
(DNS Firewall)

Roksit, DNS trafiğini inceleyip analiz eder ve sınıflandırır. DNS trafiği üzerinde yapılan analizler sonucunda Malware, C&C Botnet, Ransomware, Phishing vb. zararlı ağ trafiğini tespit ederek istenmeyen trafiği engeller. Bu sayede etkin bir koruma sağlar. Roksit, Yapay Zeka tekniklerinin kullanıldığı yüksek başarılı gelişmiş sınıflandırma mekanizması ile kapsamlı bir domain kategorizasyonu veri tabanına sahiptir. Roksit DNS güvenlik duvarı, kullanıcıların DNS trafiğini analiz ederek web güvenliği ve uygulama kontrolü sağlayan etkili/– gelişmiş Bulut Tabanlı bir Siber Güvenlik Hizmetidir. Gelişmiş ve esnek raporlama özelliği sayesinde ağ yöneticilerine gerekli aksiyonları alabilmeleri için anlamlı bilgiler sunar.

Katma Değerli Çözümler:

- 360 Derece DNS Güvenliği
- Botnet C&C Koruması
- Zararlı Yazılım Bulaşmış Cihaz ve Dosya Tespiti
- Ransomware Koruma
- Bulut Tabanlı Güvenlik Çözümü
- Reklamsız İçerik



Nasıl Çalışır?

Roksit DNS Firewall kullanmaya başlamak için "management.roksit.com" web adresinden kayıt işlemi gerçekleştirilir. Kayıt işlemi sonrasında güvenlik politikası oluşturulur ve uygulanır. DNS yönlendirilmesi ile kullanılmaya başlanır. Kullanıcı internet trafiği(DNS) Roksit' e ulaşır. Domain adresinin kategorisine göre yanıt dönülür. Zararlı internet trafiği oluşturulduğunda, güvenlik politikanıza göre Roksit "Engellendi" sayfası dönecektir. Tüm internet(DNS) trafiği gerçek zamanlı kayıt edilerek hızlı ve esnek raporlar sunar.

olta.la

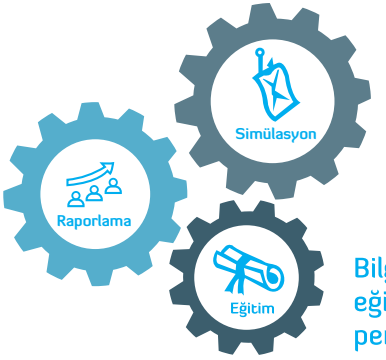
Siber Güvenlik Farkındalık Çözümü

Olta.la, personel farkındalığını en üst düzeye çıkarmak için oltalama saldırılarını simüle etmenizi ve personelinizi bilgisayar başında eğitmenizi sağlar.

Personeliniz, Sizin Güvenliğiniz

Siber güvenlik tarihi boyunca, endüstri sürekli gelişen teknoloji altyapısından ve çevrelerden kaynaklanan tehditlere odaklandı. Yeni yatırımlara rağmen, yeni güvenlik olaylarının sayısı artmaya devam ediyor. Olta.la, makineler yerine siber güvenliğin en zayıf halkası olan insan savunmasını güçlendiriyor.

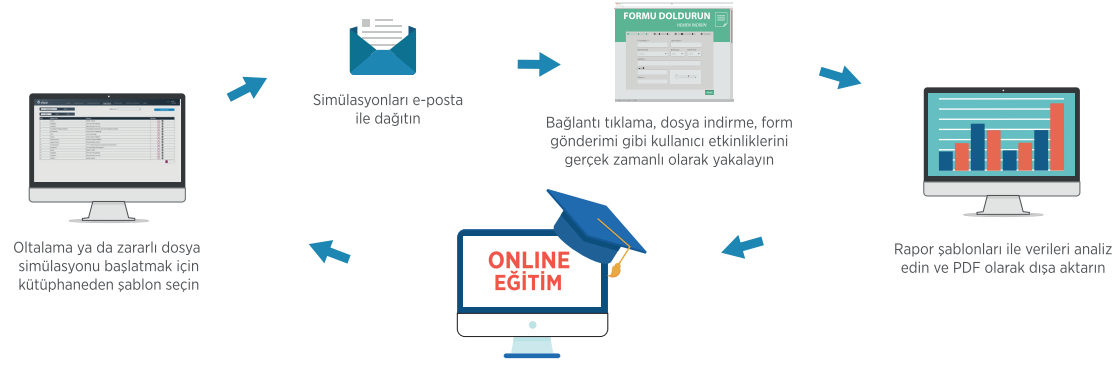
Oltalama ve Eğitim sonuçlarınızı grafiksel ve detaylı bir şekilde raporlayabilirsiniz.



Zengin ve güncel oltalama şablonları ile personelinizi oltalama saldırılarına karşı test edebilir

Bilgisayar başında eğitim alt yapısı ile personelinizi eğitebilir

Olta.la nasıl çalışır?



KOTTO BİLİŞİM A.Ş.

Tek Seferlik Güvenli Parola Çözümü (OTP)

EPSILON GRUP

Bankacılık ve e-ticaret gibi sektörler başta olmak üzere iş dünyasında son kullanıcıların kullanım güvenliği çok büyük önem taşımaktadır. Özellikle kişisel bilgi kullanımı ve finansal işlemler söz konusu olduğunda markalar güvenliği artırıcı ekstra önlemler almak konusunda hassasiyet göstermektedirler. Yaygın olarak kullanılan OTP (Tek Seferlik Parola) bu önlemlerin işlevsel olanları arasında genel kabul görmüştür.

Kritik Kurumsal Verilere Yetkisiz Erişime Karşı Koruma

Multi-factor authentication, sıradan bir kimlik doğrulama işlemine (Single Factor Authentication) bir katman daha ekleyerek verilerinize veya sanal çalışma ortamınıza erişimi daha güvenli hale getiren güçlü bir kimlik doğrulama mekanizmasıdır. Multi-factor authentication ile izinsiz erişimler engellenir. Siber saldırılara karşı kendinizi hedef olmaktan korursunuz. Sisteminizi, kolayca ulaşılabilir olmaktan çıkarırsınız.

Güvenliği Artırın Maliyetleri Düşürün.

Manuel kullanıcı yönetimi hataya açık olduğu gibi emek isteyen yoğun bir iştir. Yerleştirme ve kapanış süreçlerini otomatikleştirerek; rolü, departmanı ve diğer niteliklerini temel alarak insanın katılımını azaltabilir ve erişim denetimini düzene sokabilirsiniz.

Kritik Sistem Erişimini Koruma

Günümüzde her kuruluş, kullanıcı kimliğini etkin bir şekilde doğrulamak ve güvenli erişimi sağlamak için yaşanan karmaşık zorluklarla karşı karşıyadır. İşletmelerde dağıtılan işgücü; web, mobil ve bulut ağlarına, uygulamalara, rekabet avantajı ve operasyonel verimlilik sağlayan kaynaklara her zaman ve her yerden erişime uygunluk istemektedir. Aynı zamanda, kuruluşlar güvenlik ihlallerini önlemek, sürekli uyumu sürdürmek ve marka itibarını korumak için dinamik bir gelişme içerisindedirler.

Epsilon OTP, eksiksiz ve esnek bir şekilde endüstri lideri güvenlik çözümleri sunar. Tamamıyla entegre edilmiş kimlik doğrulama platformumuz ve yenilikçi cihazlarımız, kullanıcılara yüksek değerli varlıkları basit ve sezgisel olarak korumakla kalmayıp aynı zamanda müşteriye değer katmaktadır.

KOTTO BİLİŞİM A.Ş.

e-Noter Güvenli Zaman Damgası Çözümü (TTS)

TaliaStamp

Elektronik ortamdaki dökümanlarınızı, damgaladığı zamanı ve o damgalandığı tarihten itibaren değiştirilmediğini gösterir. Aynı zamanda resmi delil olarak kullanabilirsiniz...

Her Zaman Orjinal

TaliaStamp'le damgalanan dosyaların orijinal içerikleri kurum içerisinde kalır ve orjinal hali korunur.

Delil Niteliği

5070 Sayılı Elektronik İmza Kanunu kapsamında belirtilen maddeler gereği herhangi bir uyuşmazlık durumunda delil olarak gösterilebilir.

Tübitak Kamu SM

TÜBİTAK KamuSM sunucuları üzerinden vurulan damgalar yasal geçerli bir şekilde dosyanın değişmediğini ve belli bir tarihte var olduğunu ispatlar.

Çok Düşük Maliyet

Klasik noter ücretleriyle karşılaştırıldığında çok düşük maaliyetlere dosyalarınızı onaylayabilirsiniz.

ÖZELLİKLER

- TaliaStamp'le damgalanan dosyaların orijinal içerikleri kurum içerisinde kalır,
- Ek yazılım kurulumuna ihtiyaç duymaz ve güvenlik zafiyetlerini önler,
- Böylelikle hem NAS/depolama özelliği sunar hem de güvenlik zafiyetleri engellenir,!
- FortiAnalyzer ile entegre çalışabilir.
- Böylelikle FortiAnalyzer'a damgalama desteği sağlar,

Yeni Nesil Uç Nokta Güvenliği Çözümü

TRAPMINE

TRAPMINE, yeni nesil zararlı yazılımları engelleyebilen, gelişmiş kararlı saldırılara (APT) karşı koyabilen yeni nesil bir uç nokta güvenliği çözümüdür.

Geleneksel imza ve sandbox tabanlı değil, tamamen DAVRANIŞSAL ve MAKİNE ÖĞRENİMİ tabanlı, "bütünleşik ve kesin koruma" yöntemlerini izleyerek saldırı ve tehditleri engeller.

İmza ve güncelleştirme gerektirmez, sistem performansına etkisi olmaz, istemci tarafında kaynak tüketimi minimum düzeyde seyreder.

Antivirüs ve diğer geleneksel güvenlik çözümleri,günümüzde tehdit sağlayıcılar tarafından gerçekleştiren modern ve global siber saldırılara karşı kurumsal yapıları korumada artık etkili değildir.

Mevcut güvenlik çözümleri, bilinmeyen zararlı yazılımlara karşı koruma sağlayamaması yanı sıra, antivirüs gibi geleneksel güvenlik çözümleri, saldırganlar için güvenlik çözümünden çok bir saldırı vektörüdür.

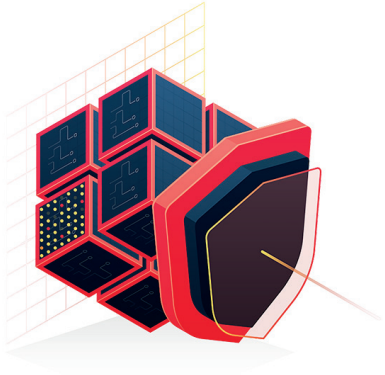
Zararlı yazılımlar, dosyasız zararlı yazılımlar (File-less Malware), fidye yazılımları (Ransomware) ve Process Injection gibi farklı türde zararlı yazılımları engellemek için uç noktalar üzerinde Dynamic Instrumentation(inceleme), Behavioural Analysis(davranışsal analiz) ve Machine Learning (makine öğrenmesi) tabanlı koruma sağlar.

Bu engelleme teknikleri, zararlı yazılımın çalıştırılması anında gerçekleştirilir ve Zero-Day (sıfırıncı gün) saldırıları ve zararlı yazılım tarafından gerçekleştirilen etkinliği tespit etmek için kullanılır.

TRAPMINE, antivirüs çözümlerinden farklı olarak zararlı yazılımları çalışma anında belirler ve engeller, bu sayede klasik güvenlik çözümlerinin aksine, kullanıcı üzerinde meydana gelen performans ve yüksek kaynak tüketimi gibi sorunları ortadan kaldırır.

TRAPMINE, Attack Story Line(saldırı zaman dökümü) özelliği ile birlikte kurumunuzu tehdit altına alan zararlı yazılım veya diğer tehditlerin kaynağı hakkında grafiksel ve istatiksel bilgiler verir. Böylece TRAPMINE, ağınızı hedef alan tehditlerin kaynağını analiz etmenize (Root Cause Analysis) ve gerek duymanız halinde tespit edilen ve tehditlere neden olan kaynaklara müdahale etmenize yardımcı olur.

TRAPMINE + ThreatHunter ile birlikte kurum içerisindeki uç noktaların görünürlüğü ve olaya müdahale (Incident Response) süreçlerini, (detaylı Forensic veri toplama) hızlı ve kolayca gerçekleştirebilme yeteneğine sahiptir.



Yerli Veri Sınıflandırma ve Etiketleme Çözümü

VERİKET

Veriket; Türkiye'nin ilk yerli veri sınıflandırma çözümüdür.

Veriket; hassas verilerinizi belirleme, sınıflandırma ve koruma altına almada, güvenlik politikalarına dayalı bir sistem kurmanızı sağlar.
Günümüzde organizasyonlar çok hızlı bir şekilde veri üretmektedir ve bu verilerin korunması da aynı oranda zorlaşmaktadır. Bununla birlikte çalışanlarınızı verilere hızlı, kolay ve güvenle erişebilmesi ve gerektiğinde aynı şekilde paylaşabilmesi gerekmektedir.
Regulasyonlara Uyum

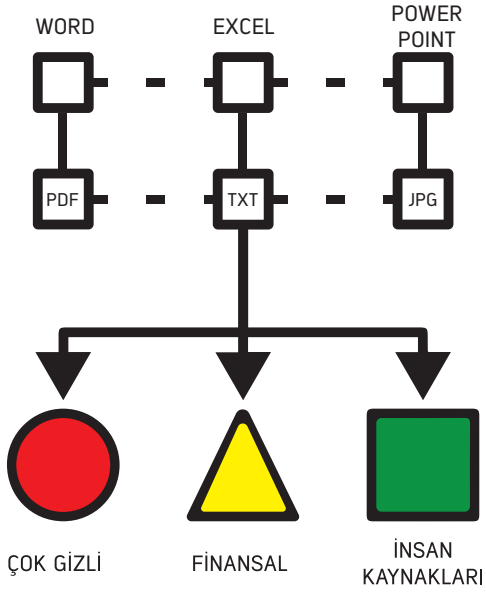
ISO 27001, 6698 Sayılı Kişisel Verilerin Korunumu Kanunu(GDPR), SOC, PCI-DSS, COBIT, ITIL, ILTA, ISF, NIS 800-53/CSF vb. yasal uyumlulukların ve standartların karşılanabilmesine imkan tanır.

Belirleme
Varlığını ve değerini bilmediğiniz verileri koruyamazsınız. Veriket ile yapılandırılmamış verilerinizi manuel ya da otomatik olarak belirleyebilirsiniz.

Sınıflandırma
Belirlemiş olduğunuz verilerinizin yönetilebilmesi için güvenlik stratejileri oluşturmanız ve verilerinizin bu stratejiler doğrultusunda sınıflandırılarak tasniflenmesi gerekmektedir. Veriketin güçlü yönetim paneli ile verilerinizi güvenlik politikalarınız doğrultusunda kolayca tasnifleyebilir ve görsel olarak ayırt edilebilecek şekilde etiketleyebilirsiniz. Bu işlemleri hem epostalarınız üzerinde hem de başta Office dokümanlarınız olmak üzere pdf, txt görsel ve video içerikleriniz üzerinde uygulayabilirsiniz.

Koruma
Veriketin yönetim paneli üzerinde oluşturmuş olduğunuz güvenlik politikaları, otomatik olarak uygulanarak bu kapsamdaki maksimum korumayı sağlar.

Siber Güvenliğe Faydaları
- Kullanıcıları güvenliğin bir parçası haline getirir.
- Kullanıcı farkındalığını arttırır.
- Güvenlik politikalarının etkinliğini arttırır.
- Güvenlik çözümlerine altyapı sunar/yönlendirir.
- İstatistiksel veriler ile güvenlik analizi yapılabilmesine imkan tanır.
- Siber güvenlik yatırımlarınızı sağlıklı olarak planlayabilmenize imkan sunar.
- Regülasyonlara uyumu sağlar.



KOTTO Hukuk, Bilişim ve Süreç Danışmanlığı

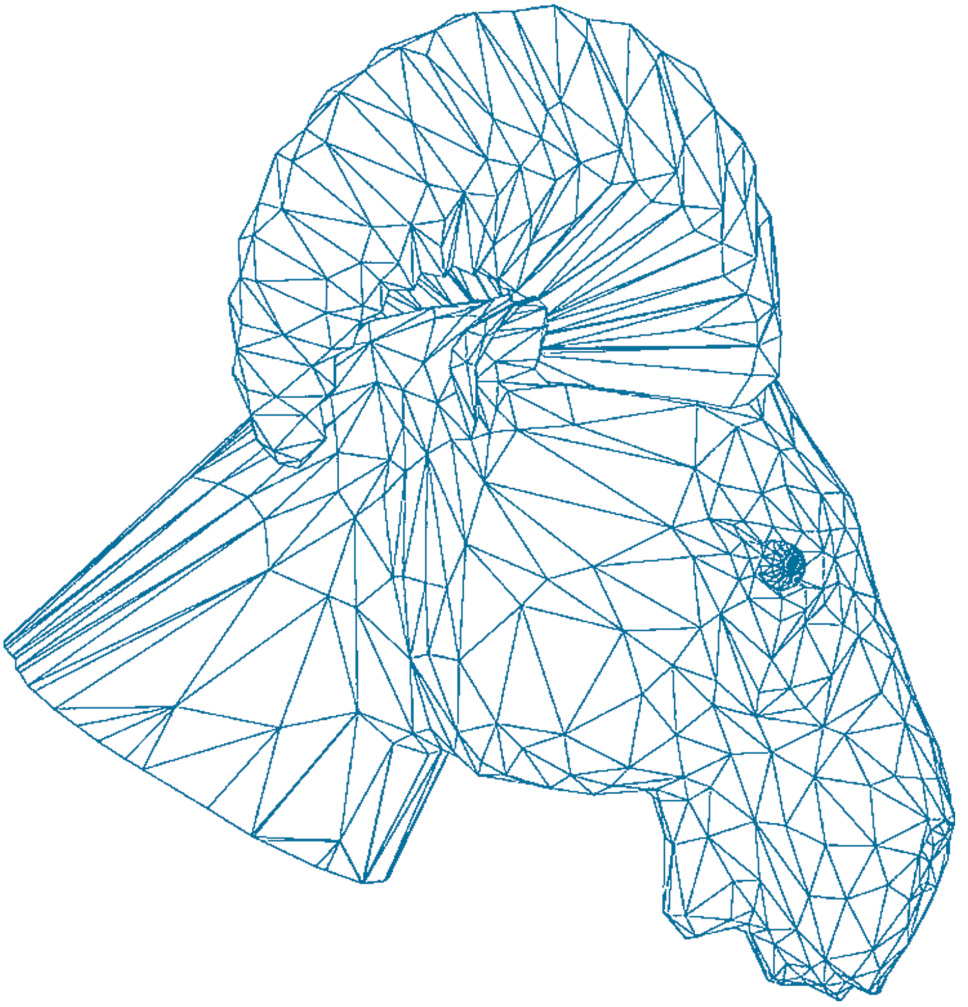
Kurumlara verilecek mevzuata uyum hizmetinin bütüncül bir yaklaşımla ve en iyi bir şekilde sunulması için hukuk, bilişim ve süreç danışmanlığı disiplinlerinin ortak bir çalışma yürütmesi büyük önem arz etmektedir. Gelişen ve genişleyen mevzuata uyum süreci, bu üç disiplinden yalnızca biri ile yürütülemeyecek kadar kapsamlı ve geniş bir alandır.

Bilgi teknolojileri ve güvenliği alanındaki gelişmelerin sadece bir kanuni zorunluluk olarak yorumlanması, uyumluluk sürecinde kritik bir yere sahip olan teknoloji ve süreç danışmanlığı gibi unsurların gerektiği şekilde analiz edilmesini zorlaştıracaktır. Yeni düzenlemelerin, teknoloji hesaba katılmadan uygulanmaya çalışılması hassas kurum ve verilerin korunması için kritik öneme sahip olan şifreleme, tokenizasyon, veri sızıntısı engelleme, veri tabanı güvenliği, zaman damgası ve verileri güvenli silme/yoketme gibi işlemlerin gözden kaçırılmasına neden olacaktır.

Bu düzenlemelerin sadece bilişimsel bir süreç olarak değerlendirildiği bir durumda ise verilecek hizmet DLP, şifreleme, maskeleme gibi güvenlik ürünlerinin sunulmasının ötesine geçemeyecektir. Kanuni yaptırımlar ve önlemler konusunda atılması gereken adımlarla ilgili kurumlara danışmalık hizmetinin en iyi bir şekilde verilebilmesi için hukuki boyutunun göz önüne alınması gerekmektedir.

VERBİS'e kayıt, sözleşmelerin revizyonu, sistem altyapısındaki düzenlemeler gibi çalışmaları kapsayan süreç danışmanlığı ise tanımından da anlaşıldığı üzere hem teknik hem de hukuki alanla birlikte çalışmayı gerektirmektedir.

Bilindiği gibi BT altyapı ve yönetişim kapsamında kullanılan birçok teknoloji bulunmaktadır. Yeni ve mevcut düzenlemeler anlatılan teknolojilerle beraber kullanıldığında daha faydalı, verimli, ölçülebilir, yönetilebilir ve hesap verilebilir olacağı değerlendirilmektedir.



KOTTO
BİLİŞİM A.Ş.

KOTTO BİLİŞİM

Plenty Plaza No: 17 Cevizlidere - Çankaya / ANKARA

Tel: +90 312 472 30 30

info@kottoas.com