

— UÇ NOKTA GÜVENLİĞİ VE TEHDİT BİLDİRİMİ

MartaSecurity – Marta Tehdit Bildirim Sistemi

Sunucularınızdaki şüpheli hareketi görün, haberdar olun, tek konsoldan müdahale edin

MartaSecurity; Windows ve Linux sunucu ile istemcilere kurulan bir ajan ve çok kiracılı merkezi web konsolundan oluşur. Active Directory ve Windows güvenlik olaylarını, Sysmon ve Sigma kurallarıyla zenginleştirilmiş tespitleri ve Linux sistem günlüklerini izleyerek önemli olaylarda e-posta ve SMS ile bildirim gönderir. Envanter, yama, aygıt kısıtlama, sertleştirme ve denetimli uzak erişim aynı konsoldan yönetilir.

ÖNE ÇIKANLAR

01

Katmanlı tehdit tespiti

Windows güvenlik olayları, Sysmon telemetrisi ve Hayabusa Sigma kuralları birlikte değerlendirilir; kaba kuvvet, kimlik bilgisi çalma girişimi, log silme gibi olaylar önem derecesiyle alarma döndürür.

02

E-posta ve SMS bildirimi

Yüksek ve kritik alarmlar müşteri bazlı alıcılara e-posta ve SMS ile iletilir; sessiz saatler, kategori filtresi, özet ve sabah raporları politikayla ayarlanır.

03

Çok kiracılı merkezi konsol

Tek konsolda birden çok müşteri; her müşterinin ajanları, grupları, politikaları ve alarmları izole görünür. Müşteri kullanıcıları yalnızca kendi verisini görür.

04

Denetimli uzak erişim

Uç noktaya tarayıcıdan RDP veya SSH ile bağlanma; ajan üzerinden dışa doğru tünel, RDP oturum kaydı ve dışa aktarılabilir erişim günlüğü.

KİMLER İÇİN

Birden çok müşterinin sunucularını tek konsoldan izleyen yönetilen hizmet sağlayıcılar (MSP)

Active Directory ortamında kaba kuvvet, yetki yükseltme ve log silme girişimlerinden anında haberdar olmak isteyen BT ekipleri

Ayrı bir SOC ekibi olmadan e-posta ve SMS ile güvenlik alarmı almak isteyen KOBİ'ler ve kamu kurumları

USB ve çevre birimi kullanımını kısıtlamak, yama durumunu takip etmek isteyen kurumlar

Sunuculara uzak erişimi kayıt altına almak ve erişim günlüğü tutmak zorunda olan ekipler

Özellikler 109 ÖZELLİK

Aşağıdaki liste ürünün mevcut sürümünde çalışan özellikleri modül modül gösterir.

Windows ve Active Directory tehdit tespiti 13

- Güvenlik, Sistem, Uygulama ve PowerShell günlüklerinin 5 dakikada bir taranması
- Etki alanı denetleyicisinde Directory Service günlüğü ve Kerberos olaylarının eklenmesi
- Mesai dışı ve hafta sonu etkileşimli/RDP oturum açma alarmı
- Kaba kuvvet tespiti: kullanıcı başına 10 dakikada 5 başarısız oturum açma veya Kerberos ön doğrulama hatası
- Hesap kilitlenmesi (kritik) ve kilit açma alarmı
- Domain Admins, Administrators gibi ayrıcalıklı gruplara üye ekleme/çıkarma alarmı
- Başka kullanıcının, özellikle yönetici/servis hesabının şifresinin sıfırlanması
- Kullanıcı oluşturma/silme, etki alanı politikası değişikliği
- Güvenlik günlüğünün silinmesi ve denetim politikası değişikliği (kritik)
- AD nesnesi değişikliği ve silinmesi
- Yeni servis kurulumu ve açık kimlik bilgisiyle oturum açma alarmı
- Komut satırı göstergeleriyle şüpheli PowerShell, cmd, mshta, rundll32 vb. süreç başlatma
- Paylaşımda 5 dakikada 50 dosya veya 5 klasör silinmesinde toplu silme alarmı (kritik)

Sysmon ve Sigma tabanlı gelişmiş tespit 8

- Microsoft Sysmon'un otomatik kurulumu ve hazır yapılandırma ile beslenmesi
- LSASS belleğine erişim ile kimlik bilgisi çalma girişimi alarmı (kritik)
- Süreç enjeksiyonu (uzak iş parçacığı) ve süreç kurcalama tespiti
- Word, Excel, Outlook gibi Office uygulamalarından kabuk başlatılması
- Geçici klasörlere şüpheli dosya bırakılması ve kabuklardan başarısız DNS sorguları
- Hayabusa ile Sigma kurallarının olay günlükleri üzerinde 30 dakikada bir çalıştırılması
- Sigma eşleşmelerinde kural adı, önem derecesi ve MITRE ATT&CK taktik bilgisi

- Bilinen güvenlik yazılımları ve sistem hesapları için gürültü azaltma filtreleri

Süreç bütünlüğü ve dosya bütünlüğü 5

- Çalışan her süreç için dijital imza durumu, yayıncı ve SHA-256 değeri
- Aynı yoldaki dosyanın hash değeri değiştiğinde veya Microsoft imzası kaybolduğunda 'ikili dosya kurcalandı' alarmı
- Geçici/kullanıcı klasörlerinden uzun süre çalışan imzasız süreç alarmı
- Dosya bütünlüğü izleme: hosts dosyası, Başlangıç klasörleri ve Run/RunOnce kayıt anahtarları
- Bütünlük değişikliklerinde eklendi/silindi/değiştirdi ayrımıyla alarm

Linux izleme 7

- systemd servisi olarak çalışan Linux ajanı
- SSH başarısız doğrulama, geçersiz kullanıcı ve root oturumu alarmları
- sudo kullanımı ve başarısız sudo denemeleri
- Yerel hesap ve grup değişiklikleri, paket yöneticisi işlemleri
- systemd servis hataları, bellek yetersizliği (OOM) ve çökme olayları
- Süreç ve kurulu paket envanteri, kurulu ağ bağlantıları ve ARP tablosu
- 23 hazır Linux politika şablonu (SSH, sudo, hesap, paket, kararlılık)

Bildirim ve raporlama 11

- Yüksek ve kritik alarmlarda e-posta bildirimi; müşteri, sunucu ve IP bilgisiyle HTML tablo
- Yüksek ve kritik alarmlarda müşterinin telefon listesine SMS
- SMS sağlayıcıları: SanalSantral, Netgsm, İletiMerkezi, Teknomart; test gönderimi
- Müşteri kendi SMTP ve SMS sağlayıcısını tanımlayabilir
- Merkezi mail aktarımı: ajan+kategori başına 15 dakika bekleme ile tekrar eden maillerin önlenmesi
- Kategori, minimum önem derecesi ve sessiz saat filtreleri (sessiz saatte yalnız kritik)
- Saatlik, 4 saatlik, günlük veya haftalık alarm özeti

- Sabah raporları: Sysmon özeti, güvenlik olay sayaçları, paylaşımında dosya silme raporu
- Filo raporu: çevrimiçi/çevrimdışı, sürüm ve işletim sistemi dağılımı, alarm dağılımı, eksik yama sıralaması
- Filo raporunun CSV olarak dışa aktarımı ve yazdırma
- Alarm listesi: önem derecesi ve zaman aralığına göre filtre, alarm detayında olay alanları

Envanter ve görünürlük 12

- Çalışan süreçler (15 dakikada bir) ve anlık çekme
- Kurulu programlar
- Donanım: üretici, model, seri no, işlemci, bellek, diskler, BIOS, son açılış
- Servisler ve zamanlanmış görevler (Microsoft dışı görevler önde)
- Oturum açma geçmişi: kullanıcı, oturum tipi, kaynak IP
- USB depolama geçmişi: aygıt adı, seri no, son bağlanma
- Yerel kullanıcılar; yönetici ve süresi dolmayan şifre işaretleri
- PowerShell komut geçmişi (ScriptBlock kayıtları)
- Ağ: SMB oturumları, TCP bağlantıları ve süreç, dinleyen portlar ve süreç eşlemesi, ARP tablosu
- CPU, bellek ve disk kullanım trend grafikleri
- Sunucu tipi (DC, üye sunucu, istemci) ve rol tespiti: AD DS, DNS, DHCP, IIS, Hyper-V, RDS, SQL, dosya/yazdırma sunucusu
- Yedekleme ve antivirüs ürünlerinin tespiti (Veeam, Acronis, Backup Exec, Defender, McAfee, Sophos)

Uç nokta yönetimi ve müdahale 11

- Bekleyen Windows güncellemelerini tarama ve tümünü yükleme; yüklü KB listesi
- Uzaktan program kurma (Chocolatey paketi veya MSI adresi) ve kaldırma
- Aygıt kısıtları: USB depolama, CD/DVD, Bluetooth, web kamerası, USB ses, USB yazıcı engelleme/izin
- Servis başlatma, durdurma ve yeniden başlatma
- Kapatma, yeniden başlatma, oturum kapatma ve bekleyen işlemi iptal
- Oturumdaki kullanıcıya ekranda mesaj gönderme
- SYSTEM yetkisiyle PowerShell betiği çalıştırma; yalnız üst yönetici, geçmişli kayıtlı
- Komut kuyruğu: envanter, ağ görüntüsü, denetim politikası uygulama, Sysmon kurulumu
- Komut geçmişi ve ajan servis loglarının canlı izlenmesi

- Gruba toplu komut gönderme
- Ajanı devre dışı bırakma ve uzaktan tam kaldırma

Sertleştirme ve denetim politikası 9

- Denetim politikalarının otomatik açılması (Türkçe Windows uyumlu)
- PowerShell ScriptBlock ve modül kaydı, komut satırı denetimi, dosya paylaşımı denetimi
- Salt-okunur sertleştirme denetimi: şifre politikası, eski/PNE hesaplar, krbtgt yaşı, RDP NLA, log boyutları
- 90 gündür oturum açmamış hesapları devre dışı bırakma (izin listesiyle)
- 'Şifre süresi dolmasın' işaretini kaldırma (izin listesiyle)
- Hesap işlemlerinde önceki durum yedeği (CSV) ve geri alma betiği
- Şifre politikası sıkılaştırma (en az 14 karakter, kilitleme, geçmiş)
- AD Geri Dönüşüm Kutusu, LDAP tanı kaydı, RDP NLA zorunluluğu
- Simple TCP servisini kapatma ve olay günlüğü boyutlarını büyütme

Politika yönetimi ve alarm susturma 8

- Merkezi politikaların ajana otomatik dağıtımı
- Politikaların gruba veya ajana çoklu atanması
- Sürükle-bırak öncelik sırası ve hangi ayarın hangi politikadan geldiğini gösteren çıkışma görünümü
- 101 hazır şablon: tespit, mail, loglama, Sysmon, Hayabusa, envanter, mesai, özet, rol, sessizlik, güncelleme, Linux
- Ajan sayfasında amaç odaklı politika sihirbazı
- Ajana etki eden tüm politika ve susturma kurallarının tek ekranda görünümü
- Alarm imzasıyla susturma; ajan, grup, müşteri veya genel kapsam
- Susturma öncesi son 30 günde eşleşecek alarmların önizlemesi

Uzak erişim ve oturum denetimi 6

- Windows uç noktalara tarayıcıdan RDP, Linux uç noktalara SSH ve VNC
- Bağlantı ajanın dışa doğru şifreli tüneli üzerinden; uç noktada port açmaya gerek yok
- Oturum başına 90 dakika üst sınır
- RDP ve VNC oturum kaydı (tuş vuruşları hariç), kaydın indirilmesi

- Uzak Erişim günlüğü: operatör, makine, müşteri, protokol, süre, durum; CSV dışı aktarım
- Gömülü RustDesk ile gözetimsiz uzak masaüstü; operatör için önceden yapılandırılmış istemci indirme

Çok kiracılı yönetim ve dağıtım 11

- Müşteri bazlı izole ajan, grup, politika ve alarm görünümü
- Üst yönetici ve müşteri kullanıcı rolleri; müşteri kullanıcıları yalnız kendi verisini görür
- Müşteri başına ajan kotası
- Müşteri başına e-posta ve telefon alıcı listesi
- Panel: toplam/çevrimiçi/çevrimdışı ajan, son 24 saat alarmları ve önem dağılımı, müşteri tablosu
- Tek kullanımlık kayıt anahtarı ile tek makine kurulumu
- GPO ile toplu dağıtım için süreli, çok kullanımlık anahtar ve adım adım rehber
- Müşteriye özel Windows ve Linux kurulum dosyası üretimi
- Müşteri self-servis: ajan ekleme, bildirim alıcıları, kendi SMTP/SMS ayarı
- Platform bazında güncel sürüm yönetimi ve filoya güncelleme dağıtımı
- İsteğe bağlı Wazuh: kurulumla Wazuh ajanı kaydı, konsoldan Wazuh paneline erişim

Güvenlik ve işletim 8

- TOTP tabanlı iki adımlı doğrulama (Google Authenticator uyumlu)
- Giriş deneme sınırı ve CSRF koruması
- Son üst yöneticinin silinmesini/devre dışı bırakılmasını engelleme
- Windows'ta ajan sırlarının (SMTP şifresi, API anahtarı) DPAPI ile şifrelenmesi
- Bağlantı kesintisinde ajan tarafı kuyruk: 30 gün / 100.000 kayıt
- SHA-256 doğrulamalı otomatik ajan güncellemesi (Windows MSI, Linux paket)
- Kurulum klasörünün erişim kilidi ve Windows Defender istisnası
- Otomatik veri temizliği: alarm ve ağ/süreç verisi 30 gün, ajan logları 7 gün

Teknik özellikler

Desteklenen uç noktalar

Windows sunucu ve istemci (64-bit; etki alanı denetleyicisi, üye sunucu, iş istasyonu); Linux 64-bit (dpkg/rpm tabanlı dağıtımlar)

Mimari	Uç noktada hizmet olarak çalışan ajan + çok kiracılı merkezi web konsolu; ajan yalnızca dışa doğru bağlantı kurar
Ajan kurulumu	Windows MSI (sessiz kurulum, GPO ile toplu dağıtım), müşteriye özel kurulum dosyası; Linux kurulum betiği (systemd servisi)
Tespit kaynakları	Windows olay günlükleri (5 dakikada bir), Sysmon, Hayabusa Sigma taraması (30 dakikada bir), Linux journald
Bildirim kanalları	E-posta (merkezi veya müşteriye ait SMTP); SMS: SanalSantral, Netgsm, İletiMerkezi, Teknomart
Kimlik doğrulama ve yetki	Kullanıcı adı/şifre, isteğe bağlı TOTP tabanlı MFA, giriş deneme sınırı; üst yönetici ve müşteri rolleri
Veri saklama	Alarm, süreç ve ağ verileri 30 gün; ajan servis logları 7 gün; kaynak grafikleri son 300 ölçüm
Süreklilik ve güncelleme	Bağlantı kesintisinde ajan tarafı kuyruk (30 gün / 100.000 kayıt); SHA-256 doğrulamalı otomatik ajan güncellemesi
Arayüz	Web tarayıcı tabanlı Türkçe konsol

KURULUM VE TESLİM

Merkezi konsol Marta Teknoloji tarafından işletilen çok kiracılı sunucuda hizmet olarak sunulur; uç noktalara Windows MSI veya Linux kurulum betiği ile ajan kurulum, toplu dağıtım GPO ile yapılabilir. Uzak erişim (Guacamole, RustDesk) ve isteğe bağlı Wazuh bileşenleri merkezi sunucu tarafında çalışır.

Demo ve fiyat teklifi için

Ürünü kendi ortamınızda görmek, kapsamı ve fiyatı konuşmak için bize ulaşın.

TELEFON +90 850 441 3 441
+90 324 350 03 50

E-POSTA bilgi@martateknoloji.com.tr

WEB martateknoloji.com.tr

ADRES Mersin Teknopark 35C/B5, Çiftlikköy,
33343 Yenişehir / Mersin
Mersin · İzmir · Londra

© 2026 Marta Teknoloji A.Ş. — Bu broşürdeki bilgiler bilgilendirme amaçlıdır; özellik kapsamı sürüme ve kurulumu göre değişebilir.