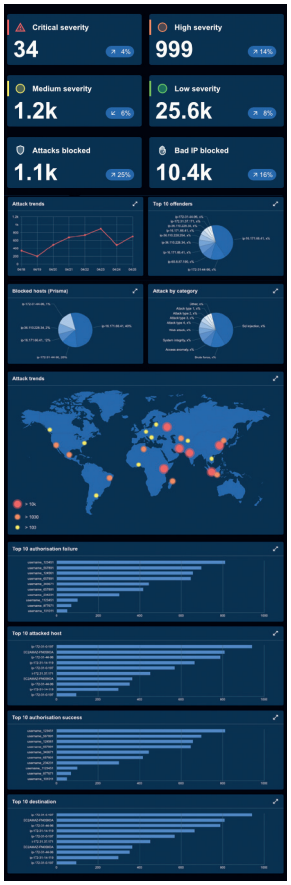
Temel Ürün Özellikleri

Proaktif Gözetim Önleme

- Bilgi toplama araçlarını engeller
- Bağlantı noktası taramasını engeller
- Güvenlik açığı taramasını durdurur
- Saldırı öncesi teknikleri belirler ve engeller

Tahmine Dayalı Tehdit İstihbaratı

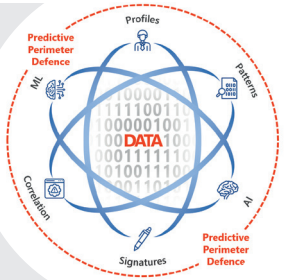
- Gerçek zamanlı tehdit istihbaratı akışı
- Kötü amaçlı yazılım imzalarını engeller
- Kötü amaçlı URL'leri engeller komuta ve kontrol, vb.)
- İtibar puanlamasını kullanarak kötü amaçlı IP'yi engeller



Tam XDR Özellikleri

- Merkezi EDR, IDS, IPS ve SIEM
- Tüm günlüklerin gerçek zamanlı korelasyonu
- Çekirdek düzeyinde izleme
- Dosya bütünlüğü izleme
- Anormal davranışlar için Hesap Ele Geçirme ve Kullanıcı Profili Oluşturucu

Otomatik Siber Güvenlik İstihbarat Uygulaması (ACSIA) Genişletilmiş Tespit ve Yanıt (XDR) Plus



Temel Operasyonel Özellikler

1 Basit kurulum
Linux Mac ve Windows uç noktalarını destekler.

2 Ortamlar
Fiziksel, sanal ve kapsayıcı devreye alımlarla şirket içi ve bulut altyapısı için kullanılabilir.

3 Kesinlik
Tahmine dayalı, proaktif ve XDR özellikleri genelinde konsolidasyon ve günlükler, adli düzeyde doğruluk sağlayan tehdit korelasyonunda büyük iyileştirmeler sağlar.

4 Clients
İstemci aracısı ile ve aracısız istemci modunda kullanılabilir.

5 İyileştirme
Web ve mobil cihazlarda yapay zeka ve makine öğrenimi kullanarak tek tıkla düzeltme.

6 Ayak İzi
Çok az yer kaplar - 100 sunucuyu izlemek için tipik bir ACSIA sunucu platformu:

- *2 CPU İşlemci*
- *8GB Hafıza*
- *100GB Depolama*

(İzlenecek daha büyük ortamlar için boyutu ölçeklendirmeniz yeterlidir.)

İletişim ve Demo Talebi için **General Global**

+90 312 911 59 30

generalglobal.com.tr

ACSIA
XDR PLUS

Dectar'dan ACSIA XDR Plus, Genişletilmiş Tespit ve Yanıt. Güçlü bir tehdide sahip (XDR) çözümü sağlayan istihbarat yeteneğidir. gerçek zamanlı tahmine dayalı, proaktif ve iyileştirilmiş siber savunma koruması.

ANAHTAR

FAYDALAR

Çalıştırması basit - "Uyarı Yorgunluğunu" azaltan mükemmel doğrulukla

Heterojen - Linux ile Kubernetes'te fiziksel, sanal veya kapsayıcılı sunucuları ve masaüstlerini izler, Mac ve Windows desteği tek platform

Otomasyon - Ayarlanabilir seviyeler otomasyon

Uygun fiyatlı - piyasadaki en iyi yatırım getirisi

"Sizi bulamazlarsa size saldıramazlar."

Bir demo ayarlamak için beni tarayın

ACSIA XDR Plus Tahmine Dayalı / Proaktif / Reaktif Siber Savunma Sistemi	Siber Saldırı Türleri	Siber Saldırı Metodolojileri
• Kötü Amaçlı URL Engelleme • Kötü Amaçlı IP Engelleme • Anonim erişimi Engelleme • Kötü Amaçlı Yazılım kaynaklarını engelleme	1. Öngörülü Koruyucu Kalkan	• Anonim Ağ Saldırıları • Komuta ve Kontrol • Fidye Yazılımı Saldırıları
• Özel ACSIA Algoritmaları • Saldırgan Takım Tespiti • Modeller ve Teknik Tespiti • Korelasyon ve ML/AI	2. Bilgi Toplama ve Keşif	• Parmak İzi • Port Tarama • Güvenlik Açığı Taraması
• Özel ACSIA Algoritmaları • Saldırgan Araç Tespiti • Çekirdek Seviyesi Analizi • Model ve Teknik Tespiti • Korelasyon ve Makine Öğrenimi	3. Men-In-The-Middle	• Oturum Ele Geçirme • DNS/IP Sahtekarlığı • Ağ Algılama
• Özel Algoritmalar • Kullanıcı Profili Oluşturucu • Kalıp Tespiti • İlişki ve ML/AI	4. Şifre Saldırıları	• Kaba Kuvvet Saldırıları • Sözlük Saldırısı • Sosyal Mühendislik
• Özel ACSIA Algoritmaları • Kullanıcı Profili Oluşturucu • Kalıplar ve Teknik Tespiti • Çekirdek Seviyesi Analizi • Korelasyon ve ML/AI	5. Drive-By-Saldırı	• Kod Enjeksiyonu • Iframe Yönlendirmesi • Kötü Amaçlı Yazılım Enjeksiyonu
• Veritabanı Manipülasyonu • Veritabanı Dökümü • Veritabanı Uzlaşması	6. SQL Enjeksiyon Tehdidi	• Veritabanı Manipülasyonu • Veritabanı Dökümü • Veritabanı Uzlaşması
• Özel Algoritmalar • İlişki ve Makine Öğrenimi • Saldırgan Araç Tespiti • Kalıp ve Teknik Tespiti	7. Malware	• Balina Kimlik Avı • Mızraklı Saldırı • Pharming
• Özel ACSIA Algoritmaları • Çekirdek Seviyesi Analizi • Korelasyon ve ML/AI	8. Fidye Yazılım Saldırısı	• Kötü Amaçlı Yazılım • Veri Şifreleme • Aldatma
• Özel ACSIA Algoritmaları • Çekirdek Seviyesi Analizi • Korelasyon ve ML/AI	9. Dinleme Saldırıları	• Koklama • Gözetleme • Trafik Kaçırma
• Özel Algoritmalar • Kullanıcı Profili Oluşturucu • Saldırgan Araç Tespiti • Kalıplar ve Teknik Tespiti • Çekirdek Düzeyinde Analiz • İlişki ve Makine Öğrenimi/Yapay Zeka	10. Yapay Zeka Destekli Saldırılar	• AI/ML ile BotNet • Düşman ML/AI • Sosyal Mühendislik
• Özel Algoritmalar • Saldırgan Araç Tespiti • Model ve Teknik Tespiti • Korelasyon ve Makine Öğrenimi	11. Siteler Arası Komut Dosyası Çalıştırma (XSS)	• Kötü Amaçlı Komut Dosyası Enjeksiyonu • Kötü Amaçlı Kod Enjeksiyonu • Kontrol Atlama

Tahmine Dayalı ve Proaktif ASCIA XDR Plus Siber Savunma
Reaktif ASCIA Siber Savunma
Kombine Proaktif/Reaktif ASCIA Siber Savunmaları