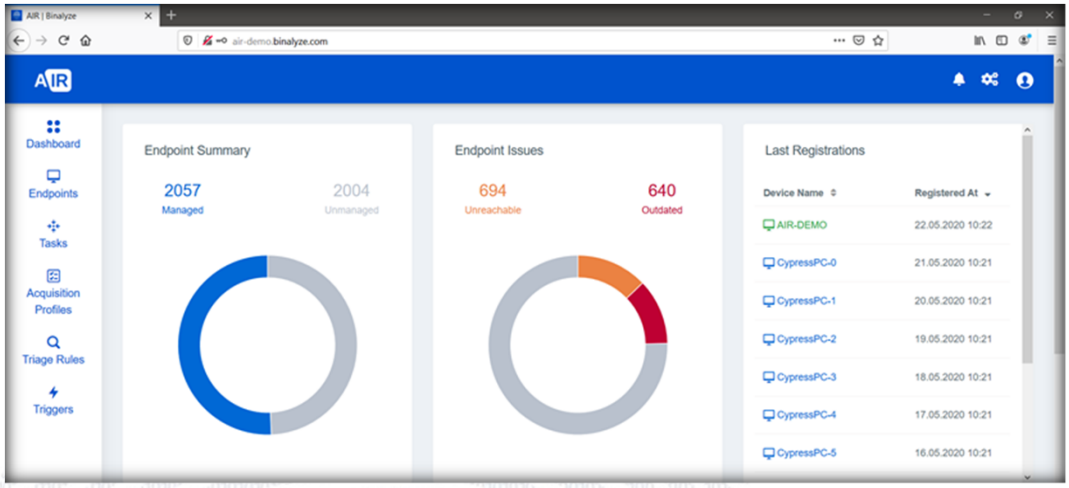
DIFOSE



b!nalyze
1100100011001 101001

AIR Automated Incident Response

OTOMATİK OLAY MÜDAHALE

Vakit kaybetmeksizin gerçek zamanlı olarak siber olaylara müdahale imkanı sağlayan AIR, mevcut SIEM/SOAR ürünleriyle entegre bir şekilde otomatik olarak bulguları toplar. Manuel, otomatik olarak ve zamanlanmış bulgu toplama seçenekleriyle esneklik sağlar.

NASIL ÇALIŞIR?

İstemci-sunucu teknolojisiyle çalışan AIR kontrol konsolunun yönetim bilgisayarına, pasif agent'ın ise ağdaki uç noktalara yüklenmesi yeterlidir. Geri kalan tüm işi AIR sizin için yapacaktır. Siber olay sırasında veya sonrasında, kontrol konsolu vasıtasıyla AIR agent oluşturulacak toplama profillerine göre, 130'dan fazla farklı veri arasından istediklerinizi sizin için toplayıp, ağ üzerinde veya yerel diskinizde depolayıp, HTML olarak size raporlayacaktır.

TONLARCA BULGU

AIR siber olayın çözümüne yönelik kritik verileri ağ üzerinden manuel veya otomatik olarak toplar. Toplanan veriler;

- Sistem bilgisi
- RAM İmajı
- PageFile
- CSV formatında MFT
- Olay Günlükleri
- Registry Hive
- Geri Dönüşüm Kutusu Bilgileri
- Prefetch Dosyaları
- WMI Script
- Route &ARP & TCP & UDP Tabloları
- Ağ Adaptörleri ve Ağ Paylaşımları
- Hibernation Dosya Bilgisi
- Birim bilgisi
- Sistem Geri Yükleme Noktaları
- Bilininen uygulamalara ait bulgular

Toplamda 130'dan fazla veri, bulgu ve delil...

www.difose.com.tr info@difose.com.tr /difose

Automated Incident Response (AIR), müşteri lokasyonunda (on-premise) kurulan ve istemci-sunucu (Client-Server) mimarisinde çalışan bir siber olay müdahalesi otomasyon çözümüdür. AIR 3'üncü parti uygulamalar ile servisler vasıtasıyla haberleşecek şekilde tasarlanmıştır. Bu sayede yeni çözümlerle entegre olması ve kabiliyetlerinin hızlı bir şekilde başka uygulamalar vasıtasıyla kullanılması mümkün hale gelmektedir.

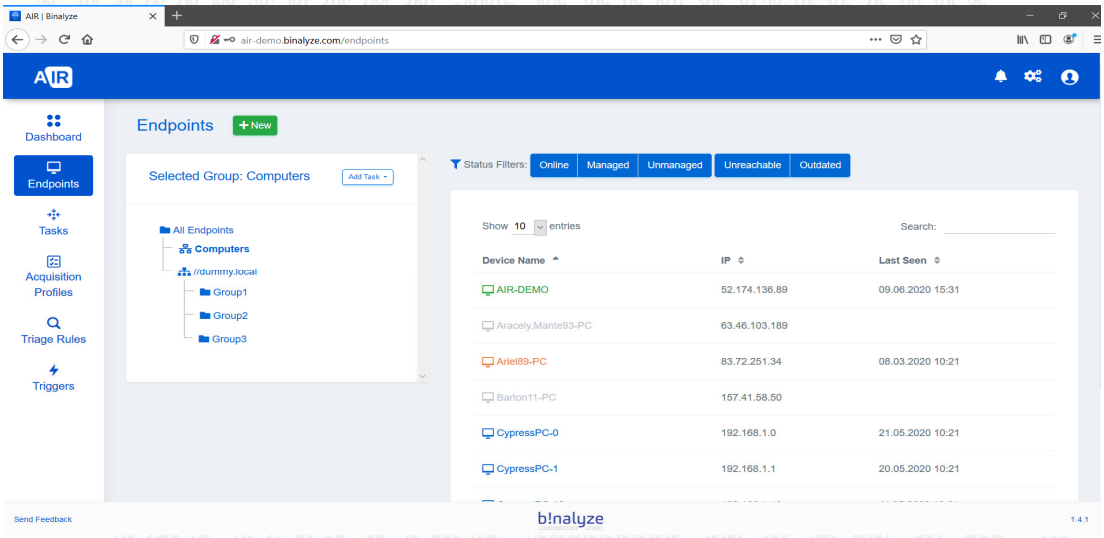
Ek olarak, AIR içerisinde gerçekleştirilen tüm faaliyetlerin de Syslog destekli SIEM gibi sistemlere feed edilebilmesi sağlanabilmektedir. Aşağıda sıralanan iki ana bileşenden oluşmaktadır.

- **AIR Yönetim Konsolu**

  Web tabanlı çalışan bir arayüz ile kurum içerisinde ağa bağlı herhangi bir cihazdan erişilebilen bir yönetim arabirimidir. Çoklu kullanıcı ve Active Directory kullanıcılarını destekler. Backend tarafında NodeJS, MongoDB, NATS teknolojileri kullanılmakta olup, frontend tarafında ise Vue.js kullanılmaktadır.

- **AIR Uç Nokta Agent**

  Uç noktadan yönetim konsoluna tek yönlü bağlanacak şekilde tasarlanan bileşendir. Konsol tarafından iletilen görevleri icra ederek yine konsola sonucunu bildirir. Pasif olarak tasarlanması sebebiyle uç noktada kaynak tüketimine yol açmaz.



AIR Özellikler

- Uzaktan Toplama
- Zamanlanmış Toplama
- Kullanıcı Dostu
- YARA+ ile Triage
- Profil toplama
- SIEM/SOAR ile Tetikleme
- Aktif Dizin Entegrasyonu
- HTML Raporlama
- Tam Otomatik Delil Toplama
- SPLUNK Desteği
- Kriptolama Tespiti
- SHA256 Desteği
- Zaman Damgası