aa teknoloji

Binalyze DFIR

Adli Bilişim Destekli Otomatik Siber Soruşturma Platformu

Binalyze DFIR; uç nokta, bulut ve hibrit ortamlarda uzaktan kanıt toplama, adli analiz ve otomatik soruşturma yetenekleriyle SOC ekiplerinin alarmların arkasındaki gerçeğe dakikalar içinde ulaşmasını sağlar. AA Teknoloji, Binalyze'ın yetkili iş ortağı olarak platformun mevcut Wazuh, CrowdStrike ve SOC altyapılarıyla entegrasyonunu tasarlar; POC, kurulum, eğitim ve teknik destek süreçlerini tek elden yürütür.

Günümüz SOC Ekiplerinin Karşılaştığı Zorluklar

EDR, XDR ve SIEM sistemleri alarmı üretir; ancak olayın kök nedenini, etkilenen sistemleri ve saldırının kapsamını anlamak için çoğu zaman ek kanıt gerekir. Dağıtık yapılarda bu kanıtların uç nokta ve bulut ortamlarından manuel toplanması soruşturmayı uzatır ve analistin zamanını asıl analiz yerine veri toplamaya ayırmasına neden olur.

⚠ Hangi Ekiplere Hitap Eder?

- Alarmın gerçek bir olaya işaret edip etmediğini hızlıca doğrulamak isteyen SOC ekiplerine
- Manuel kanıt toplama nedeniyle yavaşlayan olay müdahale ve DFIR ekiplerine
- Uç nokta ve bulut kanıtlarını aynı soruşturma altında birleştirmek isteyen analistlere
- Soruşturma ve raporlama sürecini daha izlenebilir hale getirmek isteyen kurumlara

Temel İlkeler

Görünürlük
Uç nokta, bulut ve uygulamalardan adli düzeyde kanıt toplama

Hız
Alarmdan soruşturmaya hızlı geçiş

Bütünlük
Kanıt ve bulguları tek yerde toplama

Analiz
DRONE motoru ile otomatik adli analiz ve önceliklendirme

Teknik Özellikler

Kanıt Toplama Modülleri
- Acquisition: Hedefli veya tam adli kanıt toplama
- Hunt: YARA, Sigma ve osquery ile tehdit avı
- Compare: Baseline karşılaştırma ve anomali tespiti
- InterACT: Gerçek zamanlı komut çalıştırma ve müdahale

Bulut ve Genişletilmiş Yetenekler
- Tornado: Microsoft 365 ve Google Workspace kanıt toplama
- Magellan: Tam metin arama ve eKeşif
- Fleet AI: Doğal dil ile YARA, Sigma, osquery kuralı üretimi
- Outpost: Uzak ve internete kapalı ortam desteği

Platform Desteği
- Windows, Linux, macOS uç nokta desteği
- ESXi sanallaştırma ortamı desteği
- On-premise veya SaaS kurulum seçenekleri
- Active Directory, 2FA ve LDAP desteği

Entegrasyonlar
- Wazuh, CrowdStrike, Splunk
- Microsoft Sentinel ve Cortex XSOAR
- ServiceNow, Okta, Slack
- Cisco, Sumo Logic, Elasticsearch Logstash Kibana

Binalyze DFIR Nasıl Çalışır?

Binalyze DFIR, bir güvenlik alarmından sonra ihtiyaç duyulan adli kanıtları uzaktan toplar, analiz eder ve bulguları aynı soruşturma altında birleştirir. Böylece analist, farklı araçlar arasında veri aramak yerine olayın gerçekten ne olduğunu ve ne kadar yayıldığını anlamaya odaklanabilir.

Çalışma Akışı

1. Kanıt Toplama
- Uç noktalardan canlı durum ve geçmişe dönük veriler toplanır.
- Bulut kanıtları alınır.
- Hedefli veya kapsamlı adli veri toplama gerçekleştirilir.
- Toplanan veriler tehdit istihbaratı ve tespit kurallarıyla zenginleştirilir.

→

2. Analiz ve Önceliklendirme
- DRONE motoru adli kanıtları otomatik analiz eder.
- YARA, Sigma ve osquery kurallarıyla tehdit avı yapılır.
- Baseline karşılaştırmasıyla anormal değişiklikler tespit edilir.
- Kritik bulgular önceliklendirilir, gürültü filtrelenir.

→

3. Soruşturma ve Raporlama
- Tüm kanıt ve bulgular merkezi hub'da birleştirilir.
- Zaman çizelgesi ve vaka yönetimi oluşturulur.
- Soruşturma çıktıları raporlanır.

Örnek Kullanım Senaryosu

Wazuh, CrowdStrike veya başka bir SIEM/EDR üzerinde şüpheli bir alarm oluştuğunda Binalyze DFIR ilgili sistemden adli kanıtları toplamak ve olayı doğrulamak için kullanılabilir. Alarmdan DFIR soruşturmasına geçiş aynı akış içinde yürütülür.

Avantajlar

DRONE Otomatik Analiz
Adli kanıtları yerleşik analizörler ve tespit kurallarıyla otomatik işler; kritik bulguları önceliklendirir ve soruşturma süresini önemli ölçüde kısaltır.

Merkezi Soruşturma Hub'ı
Kanıtları, bulguları, notları ve zaman çizelgelerini tek alanda toplar; ekip iş birliğini ve vaka yönetimini kolaylaştırır.

Fleet AI (Yapay Zekâ Destekli Soruşturma)
Doğal dil komutlarını YARA, Sigma ve osquery kurallarına dönüştürür; soruşturma iş akışlarını hızlandırır ve analistlerin kritik kararlara odaklanmasını sağlar.

Mevcut SOC ile Birlikte Kullanım
Wazuh ve CrowdStrike alarmlarını adli soruşturma süreciyle tamamlayabilir.

aa teknoloji

AA Teknoloji, Anadolu Ajansı iştiraki olarak medya teknolojileri, siber güvenlik ve açık kaynak çözümleri alanlarında hizmet sunan bir teknoloji şirketidir. SOC hizmetleri, sızma testi, SIEM/EDR, tehdit istihbaratı ve medya altyapısı çözümlerini kurulum, entegrasyon ve 7/24 yerel teknik destekle birlikte sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.