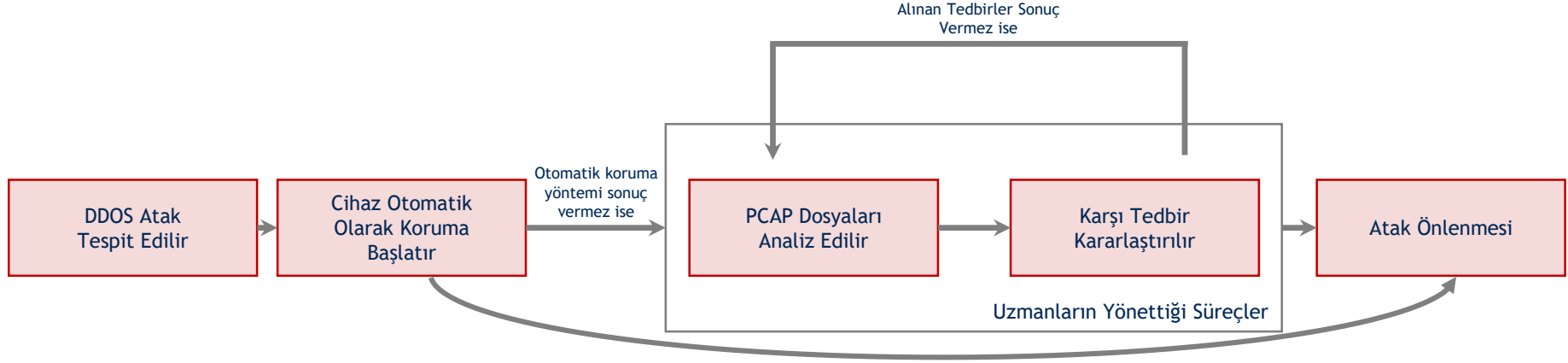




dosTTai (DDOS AI Mitigation Önerisi) Projesi



dosTTai Probleme Genel Bakış



Anormal trafik artışı thresholdları geçtiği takdirde alarm üretilir. Ya da müşteriden haber gelir.

Whitelist ve blacklist IP'lerin kontrolü vb. otomatik koruma tedbirleri bazı durumlarda atığı engelleyemeyebilir.

Ortalama 5K alarm oluşmuştur.

Otomatik koruma sonrası manuel müdahale gereksinim oranı ortalama %10.

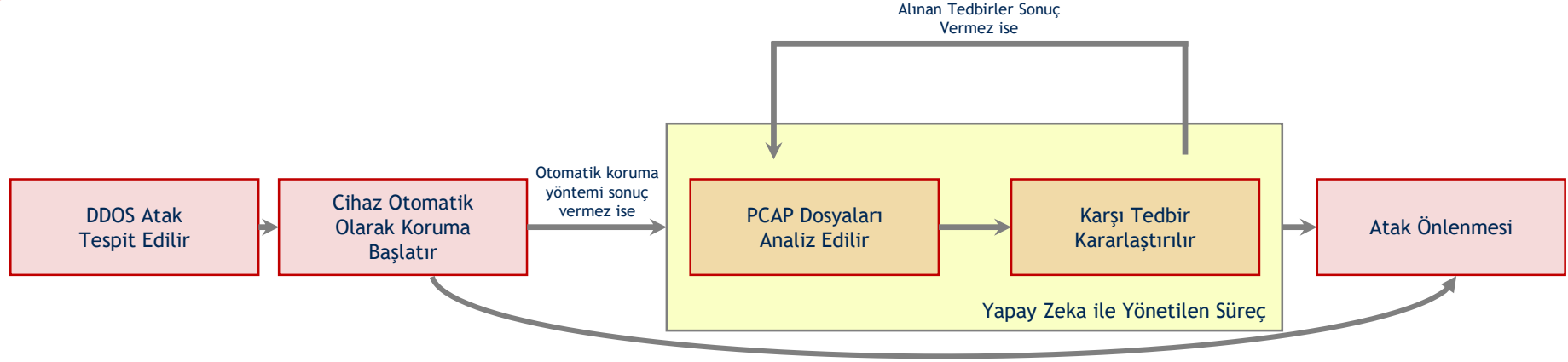
Uzmanlar PCAP dosyalarını (5K network trafiği içeren paketler) yardımcı tool aracılığı ile analiz eder.

Analiz sonucu geçmiş tecrübe ve mitigation ürününün manuelini tarayarak çözüm üretir. Bunlar; belirli bir ip, ülke bloklaya, paket boyutu bloklaya vb. olabilir.

Manuel müdahale süresi ortalama 20-30 dakika sürmektedir.

Alınan aksiyonun sonucunda network trafiği izlenerek atığın önlendiğinden emin olunur.

dosTTai Yapay Zeka Çözüm Önerisi



Anormal trafik artışı thresholdları geçtiği takdirde alarm üretilir. Ya da müşteriden haber gelir.

Whitelist ve blacklist IP'lerin kontrolü vb. otomatik koruma tedbirleri bazı durumlarda atığı engelleyemeyebilir.

Yapay zeka PCAP dosyalarından otomatik yapılan analizleri mitigation ürünün guide'ını, geçmiş aksiyon örnekleri ve uzman direktiflerini göz önünde bulundurarak karşı tedbir önerisi üretir.

Alınan aksiyonun sonucunda network trafiği izlenerek atığın önlendiğinden emin olunur.

Ortalama 5K alarm oluşmuştur.

Otomatik koruma sonrası manuel müdahale gereksinim oranı ortalama %10.

Yapay Zeka ile Karşı Tedbir önerisi 1 dakikadan kısa sürede üretilebiliyor.

dosTTai Uygulaması Ekran Görüntüleri

Dosya Yükleme:

- Kullanıcı paket dosyalarını analiz için sisteme aktarır.

Log Kontrolü:

- Pipeline işlemleri adım adım kaydedilir
- İlerlemeler kolayca takip edilebilir.

Sohbet Geçmişi

- Ekip tarafından geçmişte yapılan analiz ve önerilerin kontrol edilebilmesini sağlar.

Output (Ön İzleme):

- Oluşturulan raporlar listelenir.
- İndirme, silme ve özileme işlemleri yapılabilir.
- Seçili rapor ile mitigation chatbot'u başlatılabilir.

Chatbot:

- Raporlar için otomatik mitigation önerileri üretir.
- Kullanıcının ilave sorularına yanıt vererek aksiyon planı sunar.

The screenshot displays the dosTTai application interface with the following sections:

- File Upload:** A section for uploading files, including a 'Drop File Here' area and a 'Click to Upload' button. Below it, there's a 'Çalışma Modu' (Working Mode) section with 'Tekli PCAP' (Single PCAP) and 'Çoklu PCAP (birleştir)' (Multiple PCAP (merge)) options.
- Log:** A section showing a list of logs with columns for 'Time', 'Source', 'Destination', 'Protocol', 'Action', and 'Status'. It includes a 'Textbox' for filtering and a 'Log' button.
- Outputs:** A section displaying a list of reports under the heading 'Raporlar'. It includes a 'Outputs'u Yenile' (Refresh Outputs) button and a 'Mitigation' button.
- AI Sohbet:** A section for interacting with the AI chatbot, featuring a 'Yeni Sohbet' (New Chat) button and a 'Sohbet Geçmişi (244)' (Chat History) list.
- Chatbot:** A section showing the chatbot's response to a query. It includes a 'Textbox' for input and a 'Gönder' (Send) button.



dosTTai Kazanımlar

1

Müdahele Hızında Artış

- Karşı Tedbir üretim ve öneri adımında Yapay Zeka ile ortalamada 20-30 dakikalık bir kazanım sağlanmıştır.
- Proje canlıya alındıktan sonraki metriklere göre ise ayda ortalama 25, senede ise 300 iş gününe yakın efor kazancı sağlanması öngörülmektedir.

2

Atak Örüntülerinin Çıkarılması

- Atak sırasında farklı trafik paketleri incelenerek ortak örüntülerinin saptanması ve buna göre Karşı Tedbir önerilerinin sunulması sağlanmıştır. (Otomatik müdahale adımı alarm olmayan durumları kapsamamakta.)
- Karşılaşılan durum ve alınan tedbirlerin düzenli raporlanması.

3

Daha Sıkı Koruma Tedbirlerinin Alınmasının Sağlanması

- Personelin manuel müdahale sırasında yapay zeka destekli öneriler ile nokta atışı Karşı Tedbir alması sağlanmıştır.
- Bu sayede normal trafiğin müdahale sırasında en az derecede etkilenmesi amaçlanmıştır.

4

Personel yetkinliğinin artırılması

- Yeni başlayan personelin daha az destek alarak atağa müdahale etmesi beklenmektedir.
- Az bilinen ve kullanılan Karşı Tedbirlerin yapay zeka yardımıyla etkin bir şekilde kullanılması.



Teşekkürler