Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Twitter Tweetleri Üzerinden Açık Kaynak İstihbaratı Tabanlı Yarı-Otomatik Siber Güvenlik Modeli

Ali EKŞİM [a,b*], İrem CİVELEK [b]

[a] *TÜBİTAK BİLGEM UEKAE, PK 74, 41470 Gebze, Kocaeli, TÜRKİYE*

[b] *MSÜ, Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul, TÜRKİYE*

** Sorumlu yazarın e-posta adresi: ali.eksim@tubitak.gov.tr*

ÖZET

Açık kaynak istihbaratı (Open Source Intelligence, OSINT), kamuya açık bilgilerin sistematik olarak toplanması, işlenmesi ve analiz edilmesi sonucu elde edilen bilgiden istihbarat üretme disiplinidir. Açık kaynak istihbaratı çıkarmak stratejik bir zekâ olarak görülmektedir. Siber saldırılar için açık kaynak istihbaratı çıkarmak, saldırıların önlenmesi için yeni bir zekâ seviyesi oluşturacaktır. Sosyal medya, istihbarat için hızlı ve etkili bir kaynak oluşturmaktadır. Yapılan araştırmalar sıfırıncı gün (zero-day) atakların, saldırı gerçekleşmeden ya da henüz çok yayılmadan sosyal medya üzerinden tespit edilebildiğini göstermektedir. Bu nedenle OSINT tabanlı saldırı önleme sistemlerinin, siber ataklara karşı etkili bir önleme sağlayacağı düşünülmektedir. Bu çalışmada OSINT tabanlı saldırı tespit çalışmaları ile ilgili literatür taraması yapılmış aynı zamanda sosyal medya üzerinden saldırı istihbaratı sağlandığı anda devreye giren yarı-otomatik OSINT tabanlı saldırı önleme modeli önerilmiştir. Bu model, tweetler içerisinden istihbarat dataların çıkartılabildiği durumunda (BlackIP, virüs imzası vb.) sisteme otomatik eklenmesini, çıkartılamadığı durumlarda saldırıyı analiz edecek uzmana en kısa sürede maksimum bilgi sağlayacak şekilde oluşturulmuştur.

Anahtar Kelimeler: *Açık Kaynak İstihbaratı, Güvenlik, OSINT, Saldırı Tespiti, Siber Savunma*

Cyber Security Model Based on Open Source Intelligence via Twitter Tweets

ABSTRACT

Open Source Intelligence (OSINT) is a system of intelligence generation from information gathered by systematic collection, processing and analysis of publicly available information. Open source intelligence is seen as a strategic intelligence. Open source intelligence for cyber attacks will create a new level of intelligence to prevent attacks. Social media is a fast and effective resource for intelligence. Research shows that zero-day attacks can be detected through social media without attack or spread. Therefore, it is thought that OSINT-based intrusion prevention systems will provide effective prevention against cyber attacks. In this study, a literature review about OSINT-based intrusion detection studies and a semi-automatic OSINT-based intrusion prevention model that was

Geliş:06/12/2018, Düzeltme:15/01/2019, Kabul: 17/01/2019

introduced when attack intelligence was provided through social media was proposed. This model is created in such a way that the intelligence data can be automatically added to the system (BlackIP, virus signature, etc.) from within the tweets, and to provide maximum information as soon as possible to the expert to analyze the attack.

Keywords: *Open Source Intelligence, Security, OSINT, Attack Detection, Cyber Defense*

I. GİRİŞ

Açık kaynak istihbaratı (Open Source Intelligence, OSINT), kamuya açık bilgilerin sistematik olarak toplanması, işlenmesi ve analiz edilmesi sonucu elde edilen bilgiden istihbarat üretme disiplinidir [1] ve hükümetlerin doğrudan kontrolü olmayan açık kaynaklı bilgiyi içermektedir. Dergi, gazete, broşür, ansiklopedi, haber siteleri, sosyal ağlar, bloglar vb. kaynaklar açık kaynak istihbaratı oluşturmaktadır. Burada herhangi gizli bir bilgiye ulaşma için çaba sarf etme söz konusu değildir. Bu nedenle bilgiye ulaşmak kısmen maliyetsizdir. OSINT'in en büyük avantajları genel olarak güncel ve herkesle paylaşılabilir bilgilerin uzman maliyeti gerektirmeden elde edilmesi ve sınırsız potansiyele sahip olmasıdır [2].

Açık kaynak istihbaratı çıkarma, devlet ve kurumlar için bir stratejik zekâ seviyesi olarak görülmektedir [3]. Bu kaynaklara sosyal ağların da eklenmesi, açık kaynak istihbaratında yeni seviye oluşmasını sağlamıştır. Sosyal medya üzerinden birçok kötü niyetli grubun tespit edilmesi bu sayede gerçekleştirilmiştir.

Açık kaynak istihbaratı, siber saldırılar için kullanıldığında hackerları, siber saldırı planlarını, saldırıların etkileyeceği sistemleri, saldırının nasıl yapılacağı gibi bilgileri ortaya çıkarma özelliğine sahiptir. 2016 yılında nesnelerin İnterneti (Internet of Things, IOT) cihazlardaki bir açıklık kullanılarak gerçekleştirilen Dağıtık Hizmet Reddi (Distributed Denial of Service, DDoS) saldırısında, yapılacak saldırının önceden tahmin edilebileceğini gösteren bazı sinyaller keşfedilmiştir. Anna Sapienza`nın çalışması [4] hackerların bir saldırı gerçekleştirmeden önce darkweb forumları ya da Twitter gibi sosyal ağlarda hazırlık yaptıklarını göstermiştir ve DDoS saldırıların tahmin edilebileceğini kanıtlamıştır. Darkweb forum sitelerinden elde edilen istihbarat ile erken uyarı sistemi oluşturmuş ve %84'luk başarı ile alarm üreten bir sistem geliştirmiştir.

Siber güvenlik için açık kaynak istihbarat kaynaklar resmi ve resmi olmayan kaynaklar olarak iki bölüme ayrılabilir. Resmi kaynaklar; ulusal güvenlik açıkları veritabanı (National Vulnerabilities Database, NDV) ve ortak güvenlik açıkları veritabanı (Common Vulnerabilities Database, CVD) gibi açıklık veri tabanları, White IP listeleri, Black IP listeleri, virüs imza veri tabanları vb. kaynaklardır. Resmi olmayan kaynaklar ise Twitter, uzman blogları, güvenlik şirketi icra kurulu başkanlarının hesapları, haber siteleri vb. kaynaklardır. Ağustos 2016'da gerçekleşen Ulusal Güvenlik Teşkilatı (National Security Agency, NSA) araçlarının sızdırılmasında kullanılan açıklığın NDV veri tabanına eklenmeden 9 gün öncesinde Twitter üzerinden 2 hesapta paylaşıldığı tespit edilmiştir [5]. Siber saldırılarda zaman vektörü oldukça önemlidir. Hasar meydana geldikten sonra elde edilen bilgi yararsız olmaktadır. Bu nedenle saldırı öncesinde yapılacak saldırı hakkında minimum sürede maksimum bilgi sahibi olmak saldırının etkilerini azaltmak hatta yok etmek için zaman tasarrufu sağlayacaktır. Bu nedenle sosyal ağların bilgi edinmedeki hızı özellikle sıfırıncı gün (zero-day) ataklara karşı büyük bir

avantaj oluşturmaktadır. R. Campiolo ve arkadaşlarının çalışmasında [6] her gün bilgisayar güvenliği ile ilgili Twitter üzerinden %60 oranında önemli bilgi toplanıldığı ve bu bilginin %43'nün geleneksel medyadan daha hızlı elde edildiği doğrulanmıştır.

2010 yılında İran`ın nükleer santrallerini hedef alan Stuxnet solucanı nükleer santrale zarar verecek kadar etkili olmuş ve kısa bir süre içerisinde hızla yayılarak tüm dünyada etkisini göstermiştir [7]. Bu kadar hızlı yayılan ve kritik altyapıları hedef alan sistemlere karşı Seokcheol Lee çalışmasında açık kaynak istihbaratı tabanlı tehdit ve açıklık tespiti için bir yapı önermiştir [8]. Bu çalışmada sosyal medyadan ve farklı kaynaklardan edinilen istihbarat bilgileri toplanılarak kritik yapıları etkileyen tehdit ve açıklık istihbaratı çıkartılmıştır.

Hackerlar açıklık bulmak, açıklığı yaymak ve hedef belirlemek için sosyal medyayı sıklıkla kullanmaktadırlar [3]. Aynı zamanda güvenlik şirketlerinin icra kurulu başkanları uğramış oldukları saldırıları sosyal medya üzerinden takipçilerine duyurabilmektedir.

Saldırı örnekleri ve yapılan çalışmalar göstermiştirki siber saldırıların önlenmesi için OSINT tabanlı kaynaklara ihtiyaç vardır. Siber saldırılar için sosyal medya açık kaynak istihbaratına dayalı güvenlik önlemlerinin oluşturulması, saldırıların engellenmesi için yeni bir seviye oluşturacaktır. Özellikle zero-day ataklara karşı önemli bir güç elde edilecektir. Fakat internet üzerindeki kaynakların fazlalığı ve bu kaynakların insanlar tarafından tek tek elde edilmesi ve takip edilmesinin zorluğu nedeniyle otomatik analiz sistemlerine ihtiyaç duyulmaktadır. Önerilen yarı-otomatik model ile sistem, kaynaklardan otomatik çıkarımlarda bulunarak analistlerin yükünü bir nebze azaltmaktadır. Aynı zamanda analiste en kısa sürede maksimum bilgiyi sağlayarak analiste zaman kazandırmaktadır.

Bu makalenin ikinci bölümünde sosyal medyayı istihbarat kaynağı olarak kullanılmasına dair literatür araştırması yapılmış, üçüncü bölümünde önerilen yarı otomatik OSINT tabanlı saldırı önleme modeli bileşenleri açıklanmış, dördüncü bölümde modelin çalışması açıklanmış ve beşinci bölümde sonuç ve tartışmalardan bahsedilmiştir. Bu çalışmanın bazı kısımları UAS 2018`de sunulmuştur [17].

II. İLGİLİ ÇALIŞMALAR

Literatürde siber saldırılar için istihbarat kaynağı olarak haber sitelerini, uzman bloglarını, darkweb forum sitelerini ve sosyal medyayı kullanan çalışmalar bulunmaktadır. Bu çalışmaların birçoğu sınıflandırma ve makine öğrenme metotlarını kullanarak çıkarımlar yapan ve erken uyarı mekanizmalarına sahip çalışmalardır. Uyarılar, olası saldırın değerlendirmesi adına bir analist ya da uzmana bildirilmektedir.

OwlSight [9] birden fazla istihbarat kaynağından büyük hacimde veri toplayıp bunları analiz eden bir sistemdir. Günlük 107'den fazla kötü amaçlı yazılımın ne zaman ortaya çıktığını, ne kadar yayıldığını, ait olduğu aile sınıfını ortaya çıkartan ve bu verileri görselleştirerek düşük yanlış alarm sayısına sahip gerçek zamanlı bir uyarı sistemi oluşturmaktadır.

CyberTwitter [10] siber güvenlik ile en yüksek alakaya sahip tweetleri saklayan, analiz eden ve saldırı potansiyeli olan analiz sonuçlarına göre uyarı veren bir sistemdir. NDV, CVE, Microsoft ve Adobe resmi güvenlik bildirilerinden elde edilen güvenlik ile ilgili kelimeler ile eğitilmiş bir sistem ile Twitter üzerinden siber güvenlik ile alakalı tweetleri tespit edip uyarı oluşturan bir sisteme sahiptir.

Tehlike göstergeleri (Indicator of Compromise, IOC) [11] blog, forum, tweet gibi kaynaklarından elde ettiği yapılandırılmamış verilere doğal dil işleme (Natural Language Processing, NLP) teknikleri uygulanmıştır. Bu teknik ile verilerden kötü amaçlı yazılım imzası, botnet IP'leri gibi bilgilerin çıkarımı yapılarak saldırı önleme sistemlerine otomatik girdi oluşturulur.

Bu çalışmada Twitter üzerinden istihbarat elde etmeye yoğunlaşılmasının nedeni, Twitter'daki her bir tweetin az sayıda karakter ile sınırlandırılmış olması sebebi ile bilginin özünü taşımasıdır. Haber siteleri ve uzman blogları analiz için büyük bir hacme sahip olması nedeni ile zaman kaybı yaratmaktadır. Bu sitelerdeki kelimelerin birbirleri ile bağlantılarının çıkarılması sınıflandırılması ve analiste sunulması tweetlerin analiz edilmesine oranla çok daha uzun sürecektir.

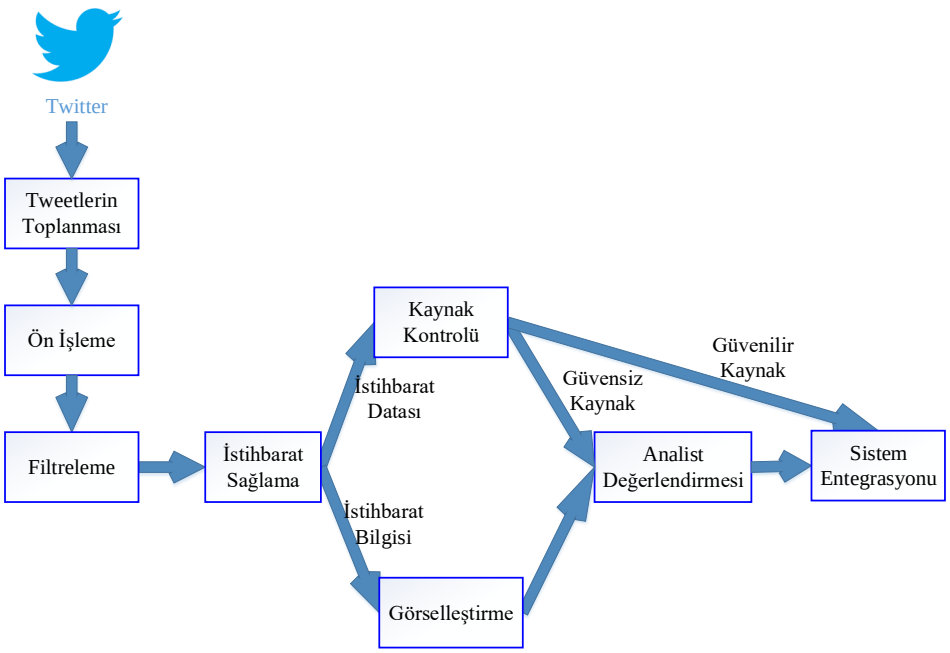
Her gün Twitter üzerinden atılan tweet sayısı 500 milyona ulaşmaktadır [12]. Fakat atılan her tweet güvenlik ile alakalı olmayacaktır. Bu nedenle analiz için siber güvenlik ile alakalı tweetlerin tespit edildikten sonra analize sokulması gerekmektedir. Literatürde siber güvenlik ile alakalı tweetlerin elde edilmesi için yapılmış çalışmalar bulunmaktadır.

Yiğit Erkal ve arkadaşlarının çalışmasında [13] siber güvenlik ile alakalı kelimelerin frekansları ölçülmüştür. Bu çalışmada Naive Bayes sınıflandırıcı ile bir tweetin siber güvenlik ile alakalı olup olmadığına göre sınıflandırılması yapılmıştır. Kullanılan yapı tweetlerin sınıflandırılmasında %70 oranında başarı sağlanmıştır.

Spitters ise çalışmasında [14] tek kelime yerine kelime kalıplarını kullanarak tweetlerin tehdit içerip içermediğini tespit etmeye çalışmıştır. Kullanılan filtrelerde makine öğrenmesi metotları kullanarak sistemin tehdit içeren kelime ve kelime gruplarını öğrenmesi sağlanmıştır.

III. MODEL BİLEŞENLERİ

Önerilen model, "Tweetlerin toplanması", "Filtreleme", "Ön işleme", "Yapılandırma", "Kaynak kontrolü", "Görselleştirme", "Analist değerlendirmesi", "Sistem entegrasyonu" olmak üzere 8 bölümden oluşmaktadır. Önerilen modele göre sistemin çalışma mekanizması görsel olarak Şekil 1'de gösterilmiştir.



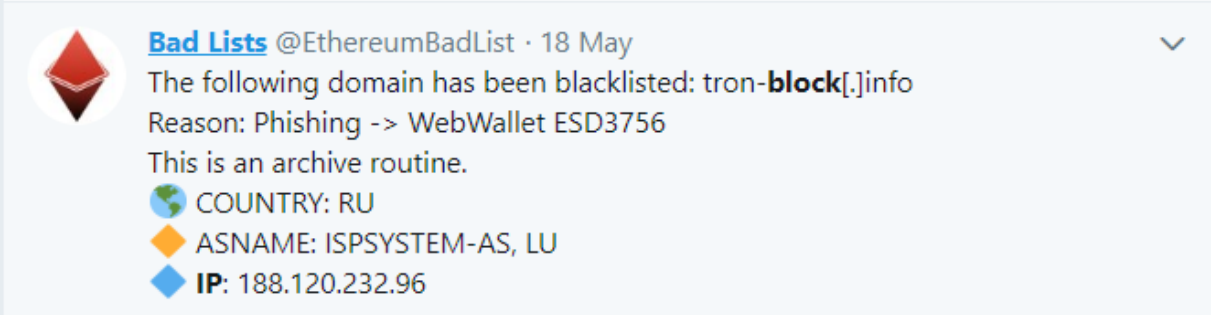
Şekil 1. *Sistemin Çalışma Mekanizması*

A. TWEETLERİN TOPLANMASI

Veri madenciliği metotları kullanılarak siber güvenlik ile alakalı kelimeler çıkartılır. NLP tekniklerinden Word gram sınıflandırma ile siber güvenlikle alakalı tweetlerde geçen kelimelerin frekanslarına göre sınıflandırma işlemi yapılır.

Sınıflandırma sonucu elde edilen siber saldırı ile ilgili kelimeler Twitter üzerinden gerçek zamanlı tweet elde etmek için kullanılır. Tweepy [15] Twitter'dan veri çekmek için Twitter'ın kendi uygulama programlama arayüzlerini (Application Programming Interface, API) kullanan bir pyhton kütüphanesidir. Tweepy kütüphanesi kullanılarak siber saldırı ile ilgili olması beklenen tweetler toplanır. Tweepy kullanılarak elde edilen tweet örnekleri Şekil 2 ve Şekil 3`te gösterilmiştir.

Şekil 2. *Tweet Örneği*



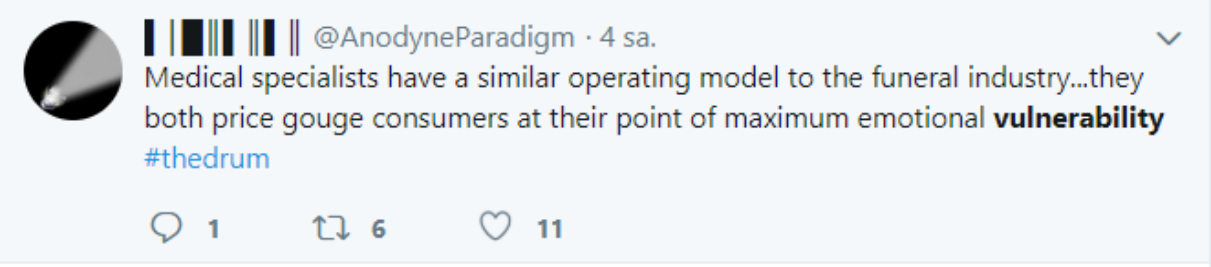
Şekil 3. *Tweet Örneği*

B. ÖN İŞLEME

Ön işleme adımı tweet metninin filtrelemeye uygun hale getirilmesi için uygulanan yöntemleri içermektedir. Filtreleme işleme yalnızca tweet metnine göre yapılacaktır. Bu nedenle retweet sayısı, beğeni sayısı, tweet sahibi gibi ögeler çıkartılarak yalnız tweet metni elde edilir. Twitter içerisinde kullanılan özel karakterler (#, ; vb.) çıkartılır ve metinin tüm harfleri küçük harfe dönüştürülerek filtrelemeye hazır metin oluşturulur.

C. FİLTRELEME

Filtreleme için birbiri ile alakalı kelime gruplarının kullanılması tweetin siber saldırı veya güvenlik ile ilgili olma olasılığını arttıracaktır [14]. Buradaki asıl amaç, saldırı ile ilgili maksimum alakaya sahip tweetlerin analiz edilmesini sağlamaktır. Şekil 4'te elde edilen tweet içerisinde vulnerability (açıklık) kelimesi siber saldırı ile ilgili bir kelime olmasına rağmen emotional vulnerability (duygusal hassasiyet) içermesi siber saldırı ile ilgili olmadığını göstermektedir. Filtreleme ile saldırı ile ilgili maksimum alakaya sahip tweetlerin elde edilmesi sağlanmaktadır.



Şekil 4. *Siber Güvenlik ile İlgili Olmayan Tweet Örneği*

D. İSTİHBARAT SAĞLAMA

Yapılandırma aşamasında, IOC [11] entegrasyonu ile yapılandırılmamış tweet metni içerisinden tweetin ne zaman atıldığı, konusu, hedef aldığı sistem, Black IP, yazılım imzası vb. saldırı hakkındaki yapılandırılmış bilgiler çıkartılmaya çalışılır.

Şekil 2 ve Şekil 3'te gösterilen tweetlerden hedef IP, hedef sistem, açıklık türü, yöntem bilgileri gibi istihbarat bilgileri elde edilir.

Şekil 3'de black IP ve black IP listesi olarak verilme nedeni görülmektedir. Sistem tweet üzerinden bu bilgiyi elde edebilirse "blok IP" listesine bu IP'yi otomatik eklemek için kaynağın güvenirliği test eder. Hesabın güvenilir olması durumunda otomatik olarak güvenlik sistemini güncellenir. Hesap güvenilir değil ise analist değerlendirmesi için beklemeye alınır.

E. KAYNAK KONTROLÜ

Kaynak kontrolü sistemin saldırganlar tarafından manipüle edilmesini engellemek amacı ile kullanılmaktadır. Saldırganların doğru olmayan ya da gerçekte var olmayan verileri paylaşmaları, yanıltıcı botlar kullanarak sistemin dengesini bozmalarını engellemek için güvensiz hesaplardan gelen yapılandırılabilir verilerin öncelikle bir analistin değerlendirmesinden geçtikten sonra sisteme eklenmesi sağlanmaktadır.

Tweetin güvenilir bir hesaptan geldiği hesapların farklı hesaplarla bağlantılarına bakılarak çıkartılır. Her bir hesap puan sistemine göre değerlendirildiğinde siber suçlarla bağlantılı hesapların güvenilmez olacağı düşünülmektedir [16]. Güvenilmez, bot olarak tanımlanmış, siber suçlu olarak sınıflandırılmış hesapların güvenirlik puanı düşük olurken güvenlik ile ilgili resmi hesaplar ve bu hesapların bağlantılı olduğu diğer hesaplar yüksek puana sahip olacaktır.

F. GÖRSELLEŞTİRME

Görselleştirme analistin saldırıyı daha iyi analiz edebilmesi için gereklidir. Tweet içerisinden yapıladırılabilmiş veriler metin içeriği, bilginin paylaşıldığı hesap ve güvenirlik puanı, tweetin konusu gibi özellikler ekranda gösterilmektedir. Aynı konu, saldırı cinsi ve hedefe sahip tweetler bir arada gösterilmektedir. Bu sayede analist saldırı veya açıklık hakkında hızlıca ön bilgi sahibi olabilecektir. Şekil 2'deki tweetin örnek görselleştirmesi Şekil 5'te gösterilmiştir.

Şekil 5. *Görselleştirilmiş Tweet Örneği*

G. ANALİST DEĞERLENDİRMESİ

Analist değerlendirmesinin iki işlevi bulunmaktadır. Bunlar; "sistemin manipüle edilmesini engellemek için sisteme eklenecek girdilerin kontrol edilmesi" ve "olası saldırı tehditleri için uzmanı bilgilendirmek ve alarm üretmektir". *Güvenilmez hesaptan gelen otomatik istihbarat datası* ve *istihbarat bilgisi* olmak üzere analist değerlendirmesine ihtiyaç duyulan iki tip veri bulunmaktadır. Sistemde oluşturulan bu veri tipleri analist değerlendirmesine sunulmaktadır.

Güvenilmez hesaptan gelen otomatik istihbarat datası: Güvenilmez hesaplardan gelen fakat sistem tarafından otomatik yapılandırılmış bilgiler için analist yalnızca karar verici rolü üstlenecektir. Güvenilmez hesabın sistemi manipüle etmesini engellemek amacı ile hazırlanan girdiler analistin kontrolü sonrası sisteme el ile eklenecektir.

İstihbarat bilgisi: Otomatik istihbarat datası çıkartılamayan tweet için analistin değerlendirmesi beklenmektedir. Saldırının mevcut sistemi etkileyip etkilemeyeceğine karar verip gerekli önlemlerin alınmasını sağlayacak alarm sistemini oluşturmaktadır.

H. SİSTEM ENTEGRASYONU

Değerlendirme sürecinden elde edilen veriler saldırı engelleme sistemlerine girdi olarak verilmektedir. Otomatik çıkartılan Black IP bilgisi, block-IP listesini güncellemektedir ve virüs imzası saldırı önleme sistemlerinin (Intrusion Prevention System, IPS) güncellenmesini sağlamaktadır. Analistin çıkarımları sonucu oluşturulan istihbarat ile gerekli önlemlerin alınması için stratejiler oluşturulur ve buna bağlı olarak sistemin güvenliği için gerekli adımlar işleme konur.

IV. SİSTEMİN ÇALIŞMASI

Veri madenciliği yapılarak elde edilen kelimeler ile Twitter üzerinden gerçek zamanlı tweet toplaması gerçekleştirilir. Elde edilen tweetler ön hazırlıktan geçirilerek filtreleme için uygun hale getirildikten sonra filtreleme basamağına gönderilir. Siber saldırılar ve açıklıklar ile ilgili maksimum alakaya sahip tweetler elde edilir. Elde edilen tweetler istihbarat çıkarılması için IOC sistemine gönderilir. Otomatik çıkarım yapılabilmesi durumunda, sistemin güvenliğinin sağlanması için tweet kaynağının kontrolü gerçekleştirilir. Kaynağın güvenilir olması durumunda elde edilen girdi sisteme entegre edilir. Kaynak güvenilir değil ise analist değerlendirmesi için beklemeye alınır. IOC sisteminden otomatik çıkarım yapılamaması durumunda görselleştirilmiş tweet bilgileri analist değerlendirmesine sunulur. Çıkarımların sonucu güvenlik yapılandırılması gerçekleştirilir.

V. SONUÇ VE DEĞERLENDİRME

Siber saldırılar genellikle hızlı yayılan ve büyük etkilere sahip tehditlerdir. Bu tehditlerin önceden sezilmesi ile saldırıların engellenmesi için savunma yöntemlerinin oluşturulması siber güvenlik için önemli bir adım sağlamaktadır. Twitter; siber saldırıların sezilmesinde, tespit edilmesinde, saldırı hakkında bilgi edinilmesinde hızlı ve etkili bir kaynak olarak kullanılabilmektedir. Twitter'ın tehdit

hakkında özet bilgi içermesi verilerin yapılandırılmasında ve kullanılmasında hız kazandıracaktır. Yapılandırılmamış veriler için ise analist, saldırı hakkında hızlıca ön bilgi sahibi olacak ve saldırının önlenmesinde gerekli adımların atılması için zaman kazanacaktır.

Önerilen model ile otomatik çıkartılan sonuçlar güvenilir bir kaynaktan gelmesi durumunda herhangi bir analist değerlendirmesine ihtiyaç duymadan sisteme eklenerek analistin zaman kaybını engelleyecektir. Kaynağın güvenilir olmaması durumunda analist sonuç çıkarmak için zaman harcamayacak sadece karar verici rolü üstlenecektir. Otomatik yapılandırılamayan veriler için analist, minimum sürede maksimum bilgiye sahip olacaktır. Ek olarak saldırının analiz edilmesi, saldırının önlenmesi için alınacak tedbirlerin belirlenmesi için zaman kazandırılmış olacaktır.

VI. KAYNAKLAR

[1] Department of the Army. (2012, Temmuz). Open-Source Intelligence. Army Techniques Publication. Erişim: https://fas.org/irp/doddir/army/atp2-22-9.pdf.

[2] R. D. Steele, "Open Source Intelligence:What Is It? Why Is It Important to the Military?," *American Intelligence Journal*, vol. 17, no. 1&2, pp. 35-41, 1996.

[3] F. Ansari, M. Akhlaq ve A. Rauf, "Social networks and web security: Implications on open source intelligence," *2nd National Conference on Information Assurance (NCIA)*, Rawalpindi, Pakistan, 2013, ss. 79-82.

[4] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman ve E. Ferrara, "Early warnings of cyber threats in online discussions," *2017 IEEE International Conference on Data Mining Workshops*, New Orleans, LA, A.B.D., 2017, ss. 667-674.

[5] DiSIEM Consortium, "D4.2 OSINT data fusion and analysis architecture," Rap., 2 Mart 2018. Erişim: http://www.disiem-project.eu/wp-content/uploads/2018/03/D4.2.pdf.

[6] R. Campiolo, L. A. F. Santos, D. M. Batista ve M. A. Gerosa "Evaluating the utilization of Twitter messages as a source of security alerts," *The 28th Annual ACM Symposium on Applied Computing*, Coimbra, Portekiz, 2013, pp. 942-943.

[7] P. Mueller ve B. Yedagari, "The Stuxnet Worm," University of Arizona, Rap., 2012. Available:https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf. [Erişildi: 14.01.2019].

[8] S. Lee ve T. Shon, "Open source intelligence base cyber threat inspection framework for critical infrastructures," *2016 Future Technologies Conference (FTC)*, San Francisco, CA, A.B.D., 2016, ss. 1030-1033.

[9] V. S. Carvalho, M. J. Polidoro ve J. P. Magalhaes, "OwlSight: Platform for real-time detection and visualization of cyber threats," *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing*

(HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, A.B.D., 2016, pp. 61-66.

[10] S. Mittal, P. K. Das, V. Mulwady , A. Joshi ve T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM),* San Francisco, CA, 2016, pp. 860-867.

[12] .internetlivestats.com. [Çevrimiçi]. Available: http://www.internetlivestats.com/twitter-statistics/. [Erişildi: 02.12.2018].

[13] Y. Erkal, M. Sezgin ve S. Gündüz, "A new cyber security alert system for Twitter," 2015 IEEE *14th International Conference on Machine Learning and Applications (ICMLA),* Miami, FL, A.B.D., 2015, pp. 766-770.

[14] M. Spitters, P. T. Eendebak, D. T. Worm ve H. Bouma, "Threat detection in tweets with trigger patterns and contextual cues," *2014 IEEE Joint Intelligence and Security Informatics Conference,* Hague, Holland, 2014, pp. 216-219.

[15] tweepy.org. [Çevrimiçi]. Available: http://www.tweepy.org/. [Erişildi: 12.02.2018].

[16] G. Gu, "Machine learning meets social networking security: Detecting and analyzing malicious social networks for fun and profit," *the 5th ACM Workshop on Security and Artificial Intelligence,* Raleigh, North Carolina, A.B.D., 2012, pp. 1-2.

[17] İ. Civelek, M. Kara ve K. Kaya, "Cyber security model via social media with open source intelligence," *2018 1. Uluslararası Akdeniz Sempozyumu,* Mersin, Türkiye, 2018, pp. 52-64.