Fırat Üniversitesi Fen. Bil. Dergisi
34(2), 89-94, 2022

Araştırma Makalesi

EDR Ürünleri Kullanılarak Uç Nokta Görünürlüğünün Sağlanması

Kevser Mehveş DAĞCI[1*], Şengül DOĞAN[2], Türker TUNCER[3]

[1] Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Merkez, Elazığ, Türkiye
[2] Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği, Merkez, Elazığ, Türkiye
[3] Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği, Merkez, Elazığ, Türkiye
[*1] dagcikevser@gmail.com, [2] sdogan@firat.edu.tr, [3] turkertuncer@firat.edu.tr

(Geliş/Received: 30/04/2022; Kabul/Accepted: 07/09/2022)

Öz: Günümüzde büyük kurum ve kuruluşlara yapılan siber saldırılar gün geçtikçe artmaktadır. Meydana gelen siber saldırılar sonucunda; kurumlar maddi ve itibar kaybı gibi büyük kayıplar yaşamaktadırlar. Siber saldırıların geç tespiti, analistlerin yetkinliği ve verilerin ayrıştırılma sürecinde yaşanan aksaklıklar saldırıların zarar boyutunu arttırmaktadır. Bu sebepten dolayı meydana gelen saldırıların erken tespiti önem arz etmektedir. Bilgi güvenliğine aykırı durumların yaşanmaması ve saldırıların erken tespit edilebilmesi için kapsamlı yapılara ihtiyaç duyulmuştur. Bu ihtiyaç doğrultusunda uç nokta saldırı tespit sistemleri geliştirilmiştir. Bu çalışmada yaygın olarak kullanılan uç nokta (endpoint) tespiti ve cevaplama (response) yazılımlarının kullanım alanlarına ve özelliklerine yer verilmiştir. Sonuç olarak uç nokta tespiti ve cevaplama sistemlerinin (Endpoint Detection and Response –EDR–) görünürlüğünün artırılmasının sağlayacağı avantajlar sunulmuştur.

Anahtar kelimeler: Uç nokta güvenliği, Uç nokta ajanları, Çoklu müdahale işlemleri, Olay müdahale, Uç nokta analizi

Providing EndPoint Visibility using EDR Products

Abstract: Today, cyber-attacks on large institutions and organizations are increasing day by day. As a result of cyber-attacks; Institutions experience great losses such as financial and reputational loss. The late detection of cyber-attacks, the competence of analysts and the disruptions in the data separation process increase the damage size of the attacks. For this reason, early detection of attacks is important. Comprehensive structures were needed to prevent situations against information security and to detect attacks early. In line with this need, endpoint intrusion detection systems have been developed. In this study, the usage areas and features of the commonly used endpoint detection and response software are given. As a result, the advantages of increasing the visibility of endpoint detection and response systems (Endpoint Detection and Response -EDR-) are presented.

Key words: Endpoint Security, Endpoint Agent, Multiple intervention operation Incident response, Endpoint analysis

1. Giriş

Günümüzde teknolojinin ilerlemesi ve gelişmesine bağlı olarak büyük ve kurumsal şirketlerce uç nokta sistemlerin güvenliğinin sağlanması çok önemli bir konu haline gelmiştir [1]. Özellikle uzaktan çalışmanın daha da yaygın hale gelmesi ile birlikte uç nokta güvenliği siber saldırılar için daha büyük önem kazanmaktadır. Saldırı yöntemleri gittikçe değişmekte ve uç nokta güvenliğine yönelik tehdit ve saldırılar daha yeni, yakalanması zor bir hal almaktadır [2]. Bir uç sisteminin güçlü yönlerinden biri, artık bir IP adresi alınabildiği dünyanın herhangi bir yerinde bir uç noktayı konuşlandırabilmektir. Bu güç, güvenlik açısından da bir zayıflık teşkil etmektedir. Güvenlik araştırmacıları ve mühendisler bu saldırıların önüne geçmek için son nokta korumasına yönelik uç nokta tespit müdahale ürünleri geliştirmektedirler. Herhangi bir veri bir saldırgan tarafından yerel olarak ya da uzaktan erişilirse veya değiştirilirse etkisi çok yüksek olabilir [3]. Uç nokta güvenliği, ağ üzerinde bulunan tüm varlıkları güvence altına almak için tasarlanmış birçok farklı donanım sistemini, yazılım programını ve diğer araçları kapsayabilen bir terimdir.

Uç nokta güvenliği sağlamaya yönelik geliştirilen bu sistemler, uç nokta verilerinin sürekli olarak izlenmesi ve toplanmasını, kural tabanlı olarak otomatik yanıt ve analiz özelliklerini birleştiren çözümlerdir. Böylece uç noktalar üzerindeki görünürlük artmıştır [4].

Tüm uç nokta algılama ve yanıtlama sistemleri aynı şekilde çalışmaz ve aynı yetenek çeşitliliğine sahip değildir. Bununla birlikte, tüm uç nokta algılama ve müdahale araçları, aynı amaç için aynı temel işlevleri yerine getirir. Siber güvenlik dünyası çok geniş ve uçsuz bir alandır. Bu alan içerisinde her probleme yönelik her gün yeni çalışmalar yapılmakta ve ürünler geliştirilmektedir. Bu çalışma ile dünya üzerinde yaygın olarak kullanılan

[*] Sorumlu yazar: dagcikevser@gmail.com. Yazarların ORCID Numarası: [1] 0000-0003-2429-486X, [2] 0000-0001-9677-5684, [3] 0000-0002-1425-4664

bir EDR ürünü üzerinden uç noktalardaki görünürlüğünün sağlanma adımları açıklanmıştır. Herhangi bir güvenlik ihlaline karşı zaman kaybetmeden, birden fazla makine üzerinde daha hızlı ve efektif çözümler üretilebileceğine yönelik çalışmalar yapılmıştır. Ayrıca, bu çalışma büyük organizasyonlar görev yapan siber güvenlik ve adli bilişim mühendisleri için iyi bir el kitabı özelliği taşımaktadır.

2. Vmware Carbon Black Uç Nokta Tespiti ve Cevaplama

Carbon Black (Bit9 ve Bit9+ Carbon Black), Massachusetts merkezli bir siber güvenlik şirketidir. Şirket, zararlı davranışları tespit etmek ve kötü amaçlı dosyaların bir kuruluşa saldırmasını önlemeye yardımcı olmak için tasarlanmış uç nokta güvenlik hizmeti sağlamaktadır. 2019 Ekim ayında şirket, VMware tarafından satın alınmıştır [5].
Carbon Black EDR ürünü ile uç nokta görünürlüğünü ve güvenliğini sağlamaya yönelik olarak, ajan kurulan bilgisayarlar üzerinde meydana gelen kötücül davranışları analiz edebilir, çalıştırılan ve silinen zararlı dosyaları tespit edilerek incelenmektedir.

2.1. Uç Nokta Güvenliği Riskleri

Son noktada ihlallerle en iyi nasıl başa çıkılacağına karar vermek için öncelikle bunların oluşturduğu gerçek riskleri anlamak önemlidir. İlk olarak korumasız cihazlar, uzaktaki çalışanlar tarafından veya bir BYOD anlaşmasının parçası olarak kullanılanlar olma eğilimindedir. Bu kısmen güncel olmayan antivirüs veya İnternet güvenlik yazılımı nedeniyle daha düşük bir güvenliğe sahip oldukları anlamına gelir. Ek olarak, sahte veya lisanssız çözümler çalıştırabilecekleri veya güvenilmeyen bir ağdan çalıştıkları için daha yüksek bir riske sahiptirler [6]. Uç nokta görünürlüğü sağlanması ile tehdit avı ve olay tepki süresi azalarak saldırı önleme becerileri artmaktadır [7]. Uzaktan çalışan kullanıcı bilgisayarlarında olası veri sızıntısını engellemek amaçlı uç nokta seviyesinde veri sızıntısını önlemeye yönelik güvenlik önlemleri alınmalıdır [8].

3. Uç Nokta Tespiti Ve Cevaplama (Endpoint Detection And Response)

Uç nokta güvenliği sağlama çözümü (EDR), güvenlik ekiplerine uç noktaları sürekli olarak izleme ve olaylara anında müdahele için merkezi bir platform sağlamaktadır. Olayların nereden yayıldığı, nasıl ilerlediği ve kaynağını bulup çözümlendirme gibi kritik soruların cevabını "Incident Investigation" yaparken bulabilmemize olanak tanımaktadır. EDR ürünleriyle, kısa süre içerisinde tehdit edilen ya da saldırıya uğrayan makineyi tespit etme, önlem alma ve iyileştirme gibi çözümler sağlanabilmektedir.
EDR platformları, meydana gelebilecek zararlı aktiviteleri daha öncesinden tespit edilmesine olanak sağlayan ve sürekli izleme özelliğine sahip uç nokta ajanlarından oluşmaktadır. EDR araçları, kuruluştaki her ana bilgisayarda sistem günlüklerini toplar [9]. Bu ajanlar sayesinde, sistemler üzerinde görünürlük arttırılır ve anlık müdahale işlemleri gerçekleştirilerek olayın zarar boyutu minimum seviyeye indirilmektedir.
EDR sistemleri, zararlı yazılımlara karşı kullanılan en önemli sistemlerden birisidir. Bununla birlikte, kötü amaçlı yazılım tespiti, özellikle yeni çıkan zero day attacks (sıfırıncı gün saldırısı) gibi kötü amaçlı yazılımların tespiti artık inanılmaz derecede zor ve giderek daha karmaşık hale gelmiştir. Bu tür saldırıların tespiti için davranışsal analiz, zeki sistemler, trafik analizi gibi yöntemler kullanılmaktadır. Ancak, bu önlemler ve gelişmiş yöntemler dahi, tüm zararlı yazılımların engellenmesini sağlayamamaktadır. SANS Enstitüsünün raporuna göre, siber saldırıların % 50'den azının antivirüs yazılımı tarafından tespit edildiği sonucuna varmıştır [6].
Antivirüs yazılımlarının aksine, EDR platformları yeni tehditleri tespit etmek için virüs imzalarına güvenmez. Bunun yerine EDR araçları, kötü niyetli siber aktörlerin varlığını tespit etmek için uzlaşma göstergeleri (IOC), saldırı göstergeleri (IOA) veya anormal süreç davranışlarını proaktif olarak arama yaparak tespit etmektedirler. Eski anti-virüs araçlarını atlatan, tehdit avlama olarak da bilinen tehditleri proaktif olarak aramak, tehdit aktörlerinin bir ağda tespit edilmeden kalma sürelerini azaltacaktır. Tehdit avcılığı, bir analistin bakmak için siber tehdit istihbarat yayınlarını kullanarak yeni tehditlere ayak uydurmasını gerektirir [11].
Bir kuruluşu hedef alabilecek yeni ortaya çıkan tehditler için uç nokta tespiti ve yanıtı araçları, kötü amaçlı yazılımların davranış analizine ve kötü niyetli kullanıcı etkinliğine dayalı olarak analistler tarafından oluşturulan önceden belirlenmiş bir dizi kuralı kullanarak kötü niyetli faaliyetlere tepki verebilir [11].

4. EDR Ürünleri Çalışma Metodolojisi

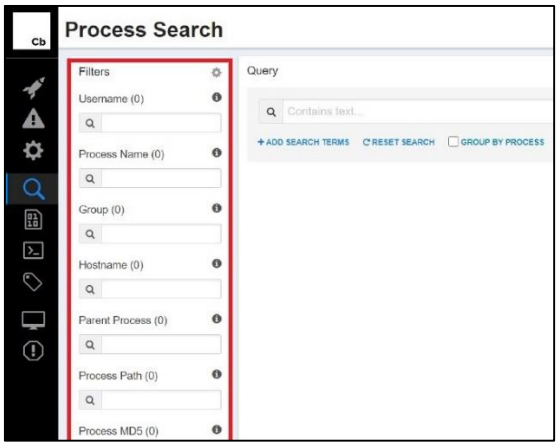
EDR, son kullanıcı sistemleri üzerindeki ağ olaylarını ve kullanıcı aktivitelerini sürekli olarak izlemek için kullanılmaktadır. EDR üzerinde tespit edilen veriler merkezi bir veri tabanına kaydedilir. EDR araçları ile geçmiş bir olayı araştırmak ve tanımlamak için veriler analiz edilebilir veya benzer tehditleri aramak ve bunlara karşı önlem almak için kullanılabilmektedir. Herhangi bir tehdit unsuru oluşması durumunda, EDR aracı son kullanıcıyı uyarabilir ve bloklama işlemi gerçekleştirebilir. EDR ürünleri ile bir veya birden fazla makine üzerinde işlemler gerçekleştirebilmektedir [12].
EDR sisteminin tüm uç noktalarda çalışabilmesi için, izleme yapılacak sistemlere EDR ajanlarının yüklenmesi gerekmektedir. Bu yükleme genellikle uç noktaya dağıtılan bir yazılım paketi biçimindedir. EDR ajanları sistemler üzerinde tek tek kurulabildiği gibi toplu olarak da kurulabilmektedir. Toplu kurulum için kuruluş içerisinde kullanılan Active Directory yönetim yazılımları gibi çözümler kullanılmaktadır.

Şekil 1 EDR Ürünü Çalışma Yapısı

Adım 1: Uç nokta cihazlara ajan yazılımı dağıtımı gerçekleştirilir. Bunun için öncelikli olarak uç nokta sistem üzerine yüklenen dosya çalıştırılarak veri akışı sağlayacak bir ajan kurulur. Yüklenen ajan, bilgisayarı izler ve tüm aktiviteleri kaydeder.
Adım 2: Kullanıcı ve varlık davranışı analizi (UEBA), kullanıcıların normal davranışlarını dikkate alan bir tür siber güvenlik sürecidir. Buna karşılık, bu "normal" kalıplardan sapmalar olduğunda herhangi bir anormal davranışı veya durumu tespit ederler. Örneğin bir kullanıcı her gün düzenli olarak 20 MB dosya indiriyorsa ancak aniden gigabaytlarca dosya indirirse, sistem bu anormalliği algılayarak hemen uyarabilir. EDR ürün yapısında da bu özellikler etkinleştirilmiştir. EDR ajanında aktif olan bu özellik ile kullanıcı davranışı analiz edilmektedir.
Adım 3: EDR uç noktadaki etkinlikleri sürekli olarak izler ve analiz eder. Bilgileri bir bildirim ile uyarı vererek doğrudan bir gösterge panosuna bildirir. Ana sayfada oluşan alarmların göstergeleri yer almaktadır.
Adım 4: EDR uç noktada potansiyel olarak kötü niyetli anormal davranış oluşumunu algılar. Gelişmiş algoritmalar, saldırı sırasında sırayla yürütülen hizmetlerin ve işlemleri adım adım kaydeder.
Adım 5: Olayı başlatan süreci göstermek için bir görselleştirme veya süreç haritası oluşturulur. EDR ajanı bulunan makine üzerinde çalışan işlemlerin (processlerin) çalışma/çalıştırılma zaman çizelgesi bir görselle gösterilmektedir.
Adım 6: Bir güvenlik analisti veya mühendis, ilgili alarmın uyarı mesajını alır.
Adım 7: Süreç analiz edilir ve gerekli çözümler sağlanır.
Bugün piyasada yer alan EDR çözümlerinin temel işlevleri performansları bakımından birbirleriyle benzerlik göstermektedir. Satıcılar arasındaki en büyük fark, bilgileri görsel olarak nasıl sundukları ve analist için sağlayabildiği kullanım kolaylığıdır.

4.1. İşlem arama

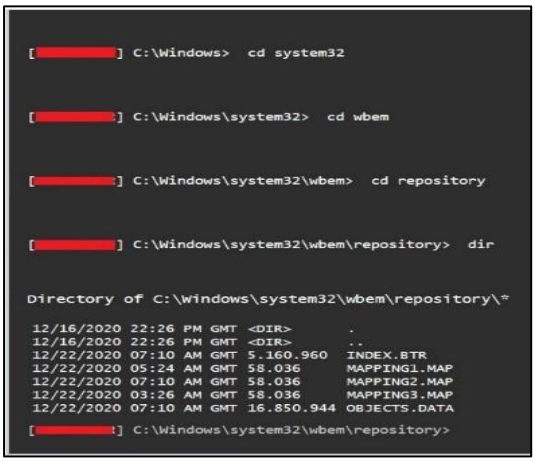
Process Search (işlem arama) işlemi ile sistemler üzerinde meydana gelen tehditlerin kök nedeninin tespiti için, ilgili zararlı aktiviteler tüm uç noktalarda anlık olarak aratılabilmektedir. Örneğin, şüpheli yazılım davranışını bildiren bir alarm veya bir istihbarat raporu alındığında, uç nokta ajanları, sorunları analiz etmek ve çözüm bulmak için verileri otomatik olarak toplamaktadır. Ayrıca şüpheli dosyanın başka hangi makineler üzerinde çalıştığı ve belirlenen zaman dilimi aralığında, şüpheli işlemlerin ve diğer işlemlerin sayıları görüntülenebilmektedir.



Şekil 2 Aktivite Sorgulama Arayüzü

4.2. Canlı İşlem

Canlı işlem (Live Response), Carbon Black (CB) Response sensörüne bağlı herhangi bir makineye doğrudan erişim için bir komut satırı ara yüzü açar. Live Response işlemi ile adli bilişim mühendisleri, güvenlik analistleri uzaktan canlı araştırmalar gerçekleştirebilir, devam eden saldırılara müdahale edebilir ve uç nokta tehditlerini anında düzeltebilmektedir. Örneğin, sensör bulunan bir makinede dizin içeriğini görüntülemesine, işlemleri sonlandırılmasına ya da yönetilen bilgisayarlardan dosya almasına olanak tanımaktadır.



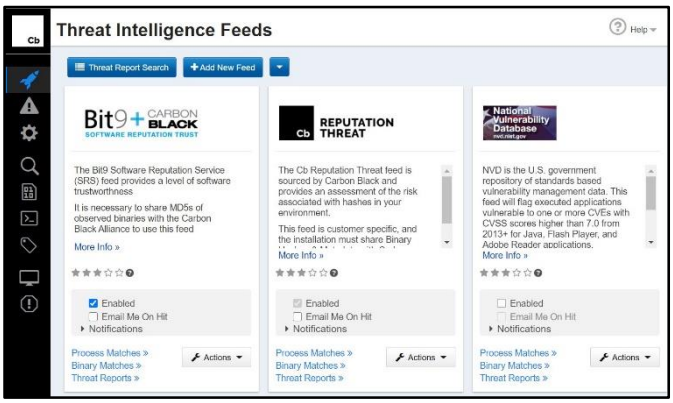
Şekil 3 Canlı sistem Arayüzü

4.3. Tehdit istihbaratı akışları

Tehdit istihbaratı akışları (Threat Intelligence Feeds), bölümü, uç nokta üzerinde yer alan tehditlerin algılanmasını, doğrulanmasını, görünürlüğünü ve analizini geliştirmek için CB sunucusunda etkinleştirilebilen tehdit istihbaratı besleme alanını açıklamaktadır.
Bu beslemeler çeşitli kaynaklardan gelmektedir. Bu kaynaklar:

- Yönetilen güvenlik hizmetleri sağlayıcısı ve bilgi çıkarımı (MSSP / IR) ortakları
- Müşteriler
- Açık kaynak Platformlar

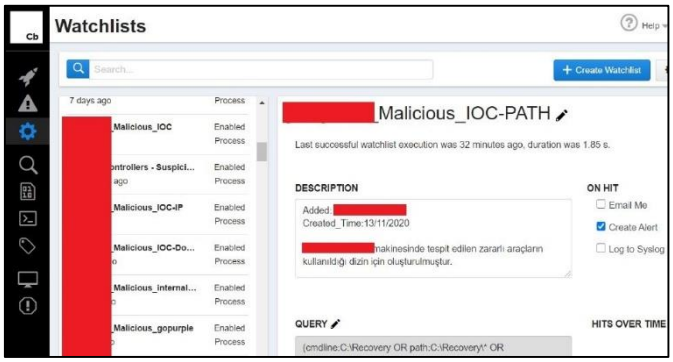
Bu bölüm ile uç nokta için tehdit içerebilecek kurallar seçilerek, uç nokta üzerinde oluşabilecek kötücül bir davranış da alarm üreterek hızlı sonuç alınması sağlanabilmektedir. Threat Intelligence Feeds özelliği ile aynı zamanda kurumlar için önem arz etmeyen beslemeler kapatılabilmektedir.



Şekil 4 Threat Intellegence Arayüzü

4.4. İzleme listesi

İzleme Listeleri olarak da adlandırılan Watchlists bölümünde, Threat Intellegence alanında yer almayan, çalışılan kuruma özel olarak güvenlik analistlerinin kendi kurallarını oluşturabileceği alan yer almaktadır.
Bu kurallar sayesinde oluşabilecek güvenlik riskleri önceden tespit edilebilmektedir.



Şekil 5 Kural yazma arayüzü

5. Bulgular ve Çıkarımlar

Bu çalışma ile EDR sistemleri detaylı bir şekilde anlatılmış ve bir yazılım üzerinden örneklenmiştir. Siber saldırıların arttığı bu dönemde, kurum ve kuruluşların hem itibar hem de veri güvenliğini korumaya yönelik olarak gerekli yapılandırmaları yapmaları gerekmektedir. Kötücül durumlarla karşı karşıya gelindiğinde gerekli analizlerin zaman kaybetmeden yapılabilmesi için uç noktalarda güvenliğin arttırılması gerekliliği görülmüştür. Uç nokta yazılımları sayesinde birden fazla makine üzerinde zaman kaybetmeden hızlı bir şekilde tespit ve analiz çalışması yapılabildiği bu sayede güvenliğin ve görünürlüğünün arttırdığını göstermiştir.

6. Sonuçlar

Yapılan incelemeler sonucunda uç nokta güvenliğinin sağlanmasının bilgi güvenliğinin sağlanması için çok önemli bir parametredir. Uzaktan çalışmanın artması ve daha da yaygınlaşması ile beraber evden çalışmaya devam eden çalışanlar, siber tehditlere karşı tesis içi çalışanlarla aynı derecede korunmayabilir ve en son güncellemeleri ve güvenlik yamalarını içermeyen cihazları kullanıyor olabilmektedirler. Ek olarak, siber güvenlik çalışanlarının bilgi ve tecrübe eksikliği (insan faktörü) bilgi güvenliğinin sağlanamamasında çok önemli bir faktör olarak görülmektedir. Tüm bu faktörler, kuruluşu ve çalışanlarını siber güvenlik risklerine maruz bırakmaktadır. Bu durum ile siber suçluların kurumsal ağa saldırmak için çalışanı bir basamak olarak kullanabileceği ve çalışanın bilgisayarının kullanılmasını önleyebilmesi için de kullanılan uç noktaların güvenliğinin sağlanmasının gerekli bir hal aldığı görülmüştür.

Elde edilen bulgular sonucunda, kurum ve kuruluşların gerekli yatırımları yaparak uç nokta güvenliğini sağlamaya yönelik çözümler tercih etmesi gerekmektedir.

Kaynaklar

[1] Internet: Intel, https://www.intel.com.tr/content/www/tr/tr/business/enterprise-computers/resources/endpoint-security.html, 05.09.2022.
[2] Internet, Morphisec, https://blog.morphisec.com/endpoint-security-is-harder-than-ever, 05.09.2022
[3] Sivaraman Eswaran, Aruna Srinivasan, Prasad Honnavalli, "A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise", 2021.
[4] Internet: VMware, https://www.vmware.com/topics/glossary/content/endpoint-detection-and-response-edr.html, 05.09.2022.
[5] Internet: VMware Carbon Black, https://en.wikipedia.org/wiki/VMware_Carbon_Black, 05.09.2022.
[6] Patrick J. Walsh, "Network Security", 2009.
[7] Internet: ESET, https://www.eset.com/fileadmin/ESET/TR/Pages/Business/Bundles/ESET_PROTECT_Enterprise__TR_A4.pdf, 05.09.2022.
[8] Internet: Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020): https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf, 05.09.2022.
[9] WU Hassan, A Bates, D Marino, "Tactical Provenance Analysis for Endpoint Detection and Response Systems", 2020.
[10] HV Strong, R Permeh, SJ Oswald, "Endpoınt Detectıon And Response System Wıth Endpoınt - Based Artıfact Storage", 2020.
[11] Terry Liggett, "Evolutıon Of Endpoınt Detectıon And Response Platforms", 2018.
[12] Cezar, A., Cavusoglu, H., & Raghunathan, S. Sourcing, "information security operations: The role of risk interdependency and competitive externality in outsourcing decisions", Production and Operations Management, 2017.