



T.C.
SIVAS CUMHURİYET ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

TEHDİT İSTİHBARATI
SİSTEMLERİ
(THREAT INTELLIGENCE
SYSTEMS)

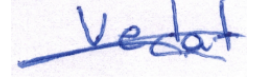
VEDAT ÖNAL
LİSANS BİTİRME PROJESİ

Haziran-2022
SİVAS

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

İmza



VEDAT ÖNAL
Tarih: 24/06/2022

ÖZET

TEHDİT İSTİHBARATI SİSTEMLERİ

VEDAT ÖNAL

Danışman: Dr. Öğr. Üyesi Halil ARSLAN

Günümüz dünyasında yaşam koşullarını kolaylaştıran ve bilgilere hızlı bir şekilde ulaşım sağlayan internet ağıımız bir yandan bizlere fayda sağlarken bir yandan ise çalıştığımız kurum ve kuruluşlara farkında olmadığımız çeşitli tehditler oluşturuyor. Bu projede kurum ve kuruluşları hedef alan tehditlerin öncesinde hazırlanması gereken durumlar ve senaryolar tehdit anındaki (olay anı) çalışanların yapması gerekenleri ve tehdit sonrasında kurum ve kuruluşların atması gereken adımları detaylı bir şekilde araştırılmıştır. Ayrıca tehdit için kullanılan popüler platformlar ve araçlar (tools) detaylı incelemeye çalışılmış ve nitelikleri bakımından karşılaştırılarak kendi sınıfından tablolar hazırlanmıştır.

Anahtar Kelimeler: Source, Analysis, Apt, MISP, STIX/TAXII

İÇİNDEKİLER

ÖZET	iv
İÇİNDEKİLER	v
KISALTMALAR	viii
1. GİRİŞ	1
2. SİBER TEHDİT İSTİHBARATI	4
2.1. Tehdit İstihbaratı Nedir?	4
2.2. Tehdit İstihbaratı Neden Önemlidir?	4
2.3. Tehdit İstihbaratının Faydaları Nelerdir?	4
2.4. Tehdit İstihbarat Yaşam Döngüsü Nedir?	5
2.4.1. Direction (Yönlendirme).....	6
2.4.2. Collection (Toplamak)	6
2.4.3. Processing (İşleme).....	7
2.4.4. Analysis (Analiz)	7
2.4.5. Dissemination (Yaygınlaştırma)	8
2.4.6. Feedback (Geri Bildirim).....	8
2.5. Tehdit İstihbarat Türleri	9
2.5.1. Stratejik Tehdit İstihbaratı	9
2.5.1.1. Stratejik Tehdit İstihbaratının Kaynakları	9
2.5.2. Taktik Tehdit İstihbaratı	10
2.5.2.1. Taktik Tehdit İstihbaratının Kaynakları	11
2.5.2.2. Tehdit Aktör TTPS'yi Ayırt Etme.....	12
2.5.3. Operasyonel Tehdit İstihbaratı	13
2.5.3.1. Operasyonel Tehdit İstihbaratının Kaynakları.....	14
2.5.3.2. Operasyonel Tehdit İstihbaratını Toplamanın Engelleri	15
2.5.4. Özet	15
2.6. Tehdit İstihbarat Akışı Nedir	16

3. TEHDİT İSTİHBARAT PLATFORMLAR	17
3.1. Kaynaklar (Sources)	18
3.1.1. AbuseIPDB	18
3.1.2. APT Groups and Operations / Apt Grupları ve İşlemler	19
3.1.3. DigitalSide Thread-Intel	19
3.1.4. Disposable Email Domains / Tek Kullanımlık E-posta Alanları.....	19
3.1.5. ExoneraTor	19
3.1.6. FireHOL IP List	19
3.2. Formatlar (Formats).....	20
3.2.1. STIX/TAXII.....	20
3.2.2. Cybox.....	21
3.2.3. MAEC.....	21
3.2.4. VERIS Framework	22
3.3. Çerçeveler ve Platformlar (Frameworks and Platforms)	22
3.3.1. Abuse.IO	22
3.3.2. Collective Intelligence Framework (CIF).....	24
3.3.3. MISP Threat Sharing	26
3.3.4. YETI - Your Everyday Threat Intelligence	27
3.3.5. Cuckoo Sandbox	28
3.3.6. Stoq – Analysis Simplified	30
3.3.7. Forager	31
3.4. Araçlar (Tools).....	32
3.4.1. AIEngine.....	32
3.4.2. FENRIR	32
3.4.3. GOSINT.....	33
3.4.4. Libtaxii	33
3.4.5. Cuckoo Sandbox	33
3.4.6. LOKI.....	34
3.5. Araştırma, Standartlar ve Kitaplar (Research, Standards & Books).....	34
3.5.1. APT & Cyber Criminal Campaign Collection	34
3.5.2. ATT&CK	34
3.5.3. Siber Tehdit İstihbaratı İçin Kesin Kılavuz	35
3.5.4. Tehdit İstihbarat: Toplama, Analiz, Değerlendirme	35

4. TEHDİT İSTİHBARAT PLATFORMLARI KARŞILAŞTIRMA.....	36
4.1. Kaynaklar (Sources)	36
4.2. Formatlar (Formats).....	37
4.3. Çerçeveler ve Platformlar (Frameworks and Platforms)	37
4.4. Araçlar (Tools).....	38
5. SONUÇLAR VE ÖNERİLER.....	39
5.1. Tehdit İstihbarat Kavramları.....	39
5.2. Siber Tehdit İstihbaratı Faydaları Nelerdir?	40
5.3. Siber Bir Tehdittin Öncesi, Saldırı Anı Ve Sonrası.....	41
5.4. Öneriler	42
KAYNAKLAR	43

KISALTMALAR

Kısaltmalar

API : Application Programming Interface / Uygulama Programlama Arayüzü
APT : Advanced Persistent Threat / Gelişmiş Kalıcı Tehdit
BT : Bilişim Teknolojileri
C2 : Command and Control / Komuta ve Kontrol
CAPEC: Common Attack Pattern Enumeration and Classification / Ortak Saldırı Modeli Numaralandırma ve Sınıflandırma
CERT : Computer Emergency Response Team / Bilgisayar Acil Müdahale Ekibi
CIF : Common Industry Format / Ortak Endüstri Format
CISO : Chief Information Security Officer / Bilgi Güvenliği Baş Sorumlusu
CISP : Cyber Security Information Sharing Partnership / Siber Güvenlik Bilgi Paylaşımı Ortaklığı
CSTR : Cyber Security & Technology Risk / Siber Güvenlik ve Teknoloji Riski
CSV : Comma Separated Values
CTI : Cyber Threat Intelligence / Siber Tehdit İstihbarat
CYBOX: Cyber Observable eXpression / Siber Gözlemlenebilir Ekspresyon
DBIR : Data Breach Investigations Report / Veri İhlali Araştırmaları Raporu
DDOS : Distributed Denial of Service / Servis Dışı Bırakma Saldırıları
DEVSECOPS: Development, Security ve Operations / Geliştirme, güvenlik ve Operasyonlar
DNS : Domain Name Server / Alan Adı Sunucusu
FQDN : Fully Qualified Domain Name / Tam Nitelikli Alan Adı
HTTP : Hyper Text Transfer Protocol / Üst Metin Transfer Protokolü
HUMINT: Human Intelligence / İnsanı İstihbarat
IOC : Indicator Of Compromise / Uzlaşma Göstergeleri
IP : Internet Protocol / İnternet Protokol
IPS : Intrusion Prevention System / İzinsiz Giriş Önleme Sistemi
IPV4 : Internet Protocol Version 4/ İnternet Protokol Versiyon 4
ISACS : Information Sharing and Analysis Centers / Bilgi Paylaşım ve Analiz Merkezleri
JSON : JavaScript Object Notation / JavaScript Nesnesi Gösterimi
MAEC: Malware Attribute Enumeration and Characterization / Kötü Amaçlı Yazılım Özniteliği Numaralandırma ve Karakterizasyon
MD5 : Message-Digest algorithm 5
MISP : Malware Information Sharing Platform / Kötü Amaçlı Yazılım Bilgi Paylaşım Platformu
MITM : Man in the Middle / Ortadaki Adam saldırıları
MWR : Morale, Welfare and Recreation
NIDS : Network Intrusion Detection System / Ağ Saldırı Tespit Sistemi
NLP : Natural Language Processing / Doğal Dil İşleme
OSINT: Open-source intelligence / Açık Kaynak İstihbarat
PDF : Portable Document Format / Taşınabilir Doküman Format
PII : Personally Identifiable Information / Kişisel Olarak Tanımlanabilir Bilgiler
SAAS : Software as a Service
SHA1 : Secure Hash Algorithm 1
SHA256: Secure Hash Algorithm 256
SIEM : Security Information and Event Management / Güvenlik Bilgileri ve Olay Yönetimi

SOC : Security Operations Center / Güvenlik Operasyon Merkezi
SSL : Secure Socket Layer / Güvenli Giriş Katmanı
STIX : Structured Threat Information eXpression
TAXII : Trusted Automated eXchange of Indicator Information
TIP : Threat Intelligence Platform / Tehdit İstihbarat Platformu
TLS : Transport Layer Security / Güvenli Giriş Katmanı
TOR : The Onion Router
TTP : Tactics, Techniques and Procedures / Taktikler, Teknikler ve Prosedürler
URL : Uniform Resource Locator / Tekdüzen Kaynak Bulucu
VPN : Virtual Private Network
XML : Extensible Markup Language

1. GİRİŞ

İstihbarat toplama geçmişten günümüze kadar devam eden saldırılara ve tehditlere önceden haberdar olmak için ortaya çıkan bir sistemdir. Günümüzde bu sistemle siber alanda da karşılaşırız. Siber saldırılar, bilgisayar sistemlerini hedef alarak bu sistemlerdeki zafiyetleri kullanıp insanlara kurum ve kuruluşlara zarar vermesini amaçlayan aktivitelerdir. Bu saldırılar doğrudan sistemleri hedef alan planlı organize karmaşık ve gün geçtikçe daha da çok çağa ayak uyum sağlayan bir saldırı türü/türleri haline gelmiştir. Bu saldırıların türleri günümüzde daha çok malware (kötü amaçlı yazılım), phishing (kimlik avı saldırısı) veya DDoS varyasyonları karşımıza çıkıyor.

Hızla büyüyen gelişen ve karmaşık hale gelen saldırıların gerçekleşmeden önce gerekli önlemlerin alınabilmesi amacıyla tehdide yönelik istihbarat bilgilerinin toplanması ve bunların analiz edilerek anlamlandırılması ve gerçekleşmesi halinde ise tespit edilmesi için önemli rol oynar. Gartner tarafından siber tehdit istihbarat meselesini şöyle tanımlar;

“Mevcut veya ortaya çıkan bir tehdit hakkında kapsam, mekanizmalar, göstergeler, çıkarımlar ve eyleme geçirilebilir tavsiyeler dahil olmak üzere kanıta dayalı bilgi”

Siber savunma sistemleri günümüzde genellikle siber saldırıları algılama veya tanıma ve bunlara karşı önlemleri alan sistemler olarak geliştirilmiştir ve geliştirmeye devam edilmektedir. Örneğin bir sistemi hedef alan saldırılar için saldırı tespit etme sistemi, saldırı önleme sistemi ve bunları engellemek üzerine yapılan geliştirmişlerdir. Bu tür geliştirilen sistemler genellikle statik ve dinamik yapılara sahip olsa da, özellikle bu sistemleri yöneten kişinin bilgisi veya kişilerinin bilgileri kadar bir kabiliyete sahip olan sistemlerdir.

Hedef sistemleri gerçekleşen siber saldırıların tespit ve önlenmesi önemli olduğu kadar öncesinden de gerekli önlemlerin alınması önemlidir. Özellikle hangi türden veya herhangi bir saldırı gerçekleşmeden önce gerekli istihbarat bilgilerinin elde edilmesi ve o saldırının vereceği zararın daha gerçekleşmeden bertaraf (ortadan kaldırmak) etmeyi sağlamada kilit rol oynar. Bunların birlikte mevcut sistemlere gerçekleşmesi olasılığı büyük ihtimal olan saldırı senaryolarını ele alarak daha önceden önlenabilir.

Dünyada ilk basit virüslerden gerçekleşen siber saldırılar günümüzde çok sayıda ve farklı türlerde tehditleri barındıran ve gittikçe daha fazla karmaşık hale gelmiştir.

Örneği APT saldırısı kendi içinde oltalama (Phishing), kötücül yazılım (Malware), arka kapı (backdoor), DNS yönlendirme (DNS orientation) vs. gibi farklı türde tehditleri içeren tek bir saldırı türüdür. Saldırıların bu şekilde farklı olmasının ana sebebi, klasik yanlarını bilen saldırı türlerinin savunma sistemleri tarafından kolayca tespit edilmesi ve engellenmesidir. Bu yüzden saldırılar gittikçe daha fazla karmaşık hale getiriyorlar, başka ifadeyle çağa uyum sağlayan mekanizmalardır. Tabii ki böyle durumda mevcut siber savunma sistemi doğal olarak saldırılarını tespit ve bertaraf etmekte kendini zorlayacaktır.

Nasıl ki Hacktivistlerin hedef sistemlerindeki zafiyetleri keşif yaparak ve mevcut zafiyete uygun saldırı için kendilerini geliştirmesi ve bununla beraber zafiyetleri kullanan saldırı çeşitleri ve sayıların artmasına sebep olup, aynı durumda siber güvenlik uzmanlarında bu geliştirilmiş saldırı mekanizmalara karşısın sürekli kendilerini güncel tutmaları, ortaya çıkan bu saldırıların analiz etmeleri ve bunlardan haberdar olmaları uzun zaman alabilmektedir. Yeni çıkan bir saldırının uzun zaman sonrasında siber güvenlik uzmanları tarafından belirlenip ona karşı bir savunma mekanizmasının geliştirilmesi sürecine kadar geçen zaman zarfında kurum bu saldırıya maruz kalmış, kurumdaki kritik bilgiler sızdırılmış, kurum tamamen tehdit altında kalmış olabilmektedir.

Bu meseleyle ortaya çıkan tehditlerin istihbarat bilgileri çerçevesinde tespit edilmesi, bu saldırılar üzerinden siber güvenlik uzmanları gereken siber savunma mekanizmaların geliştirilmesi süreci büyük önem taşımaktadır.

Siber tehdit istihbaratı (CTI) her ne kadar önemli bir konu olsa da özellikle farklı ortamdaki verilerin toplanması gerekse de onların analiz edilmesi klasik analitik kısımdaki süreçleri zordur. Siber tehdit istihbaratında bilgi kaynağı olarak sıklıkla tercih edilen internet dünyası, yapısal ve yapısal olmayan pek çok verileri barındırmaktadır.

İnternet üzerinde formlar, bloglar, sosyal medyalar, raporlar, araştırmalar gibi çeşitli platformlarda yazılan metinler önemli varlıklardır. Keşfedilen yeni bir zafiyeti kullanarak gerçekleştirilecek yeni bir saldırının ortaya çıkması durumunda, bu saldırı ile ilgili çeşitli bilgileri bu tür platformlardan diğer kullanıcıların bilgisine sunulabilmektedir. Dolayısıyla sürekli gelişen ve büyüyen dinamik bir yapı olan platformların incelenerek yeni zafiyetlerin tespitinin sağlanması siber güvenlik uzmanlarına önemli bir avantaj sağlayacaktır. Özellikle internetin karanlık tarafı Dark Web, Darknet ve Deep Web olan platformlarda kötü niyetli (hacker) gruplarının fikir

alışverişinde bulunduğu forumlar ve bloglar kullandıkları mekanizmaları öğrenmek için önemli şekilde takip edilmesi gereken platformlardır.

Siber tehdit istihbaratının genel amacı, sisteme gerçekleşen saldırıyı hızlı bir şekilde tespit ederek siber güvenlik uzmanlarının bu tehditlerden haberdar olmasını olabildiğince erken süreye çekmek olsa da bu yeni tehditlerin analiz edilerek bir sonraki saldırının hangi özellikleri barındırabileceğinin tahmin edilmesini sağlamak da önemli bir unsurdur. Bu amaçla, tahmin edici (predictive) sistemleri geliştirilmek gereklidir.

2. SİBER TEHDİT İSTİHBARATI

2.1. Tehdit İstihbaratı Nedir?

Tehdit istihbaratı, bir kuruluş tarafından geçmiş, şimdiki veya ortaya çıkan tehditleri daha iyi anlamak için toplanan ve kullanılan siber güvenlik verilerini ifade eder. Bu bilgi, ağıınızda neler olup bittiğine dair bağlam sağlar ve hem potansiyel tehditleri belirlemenize hem de yenilerinin önünde kalmanıza yardımcı olur.

Kapsamlı bir siber güvenlik stratejisinin önemli bir bileşeni, reaktif değil proaktif çalışma yeteneğidir. Tehdit verileri aracılığıyla elde edilen içeriği uygulamak, güvenlik ekiplerinin siber tehditlerini bir adım önünde kalabilmeleri için daha hızlı ve daha bilinçli güvenlik kararları almalarına olanak tanır. [1]

2.2. Tehdit İstihbaratı Neden Önemlidir?

Tehdit görüntüleme sürekli gelişmekte ve daha karmaşık hale gelmektedir. Temel güvenlik önlemleriniz olsa bile, BT ekibinizi şu anki siber tehditlerin mevcut haliyle bilgilendirilmesine genellikle yeterli değildir. Tehdit istihbarat, birçok nedenden ötürü, güvenlik uzmanlarının bir saldırganın düşünce sürecini anlamalarına, motifleri ve saldırı davranışını bir tehditin arkasındaki motifleri ve saldırı sürecini anlamalarına yardımcı olduğu için faydalıdır. Bu bilgi, güvenlik ekiplerinin potansiyel bilgisayar korsanlarının kullandığı taktikleri, teknikleri ve prosedürleri öğrenmelerine yardımcı olur tehdit izlemeyi, tehdit kimliğini ve olayı yanıt süresinin geliştirilmesine yol açar. [1]

2.3. Tehdit İstihbaratının Faydaları Nelerdir?

Siber tehdit istihbaratı, tehditlere bağlam sağlayarak, bir kuruluşun güvenlik yeteneklerini geliştirerek BT operasyonlarını güçlendirmeye yardımcı olur. Tehdit istihbaratının kurumsal kuruluşlara sağladığı avantajlardan yararlanmanın üç yolu şunlardır:

A. Azaltılmış maliyetler (Reduced costs)

Tehdidinin daha yavaş olduğu, daha fazla veri ihlali kuruluşunuza ne kadar fazla zararı olacaktır. Tepki zamanı düşürerek, tehdit istihbaratı, bir veri ihlali ile ilişkili düzenleyici ve yasal ücretleri ortadan kaldırmanıza yardımcı olabilir. Ayrıca, siber tehdit istihbarat, güvenlik ekiplerinin yanlış pozitifleri doğru şekilde tanımlamalarına, gereksiz tehdit yanıtı konusunda zaman ve para tasarrufu sağlar.

B. Gelişmiş Kurul Raporlaması (Enhanced board reporting)

Yaygın bir mücadele birçok BT uzmanları, tahtaya bildirilirken yüzleşir, kullandıkları siber güvenlik çözümlerinin etkinliğini göstermektedir. Tehdit istihbarat, güvenlik ekiplerinin ağ savunmasını görselleştirmeye yardımcı olur. Bu, tüm tarafların hizalanmasını ve bu değerli siber güvenlik uygulamalarının gösterilmesini sağlar.

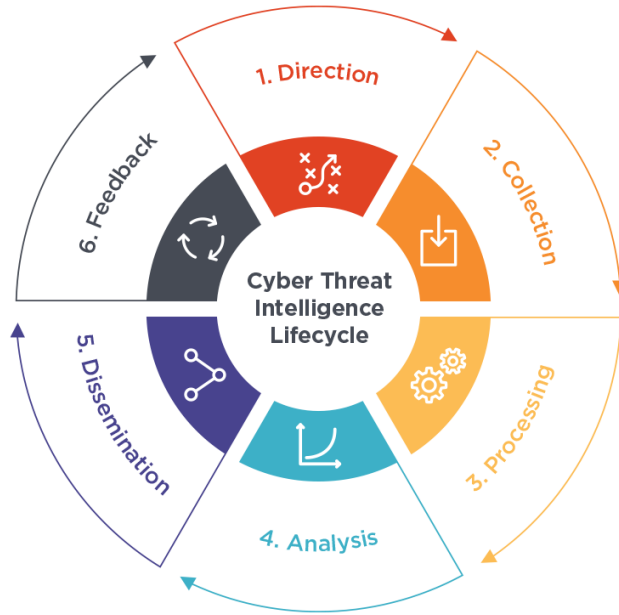
C. Geliştirilmiş Tehdit Sınıflandırması (Improved threat classification)

Tehdit istihbaratını kullanarak, organizasyonlar, hangi güvenlik açıklarının işleriyle en büyük riski oluşturduğunu bilmek için tehditleri ölçekbilir ve değerlendirebilirler. Siber güvenlik duruşunuza devam eden görünürlük ile, tehlikenin öne çıkmasını sağlayarak riski verimli bir şekilde tanımlayabilir ve sınıflandırabilirsiniz. Bu gelişmiş risk yanıtını ve iyileştirilmesine dönüştür. [1]

2.4. Tehdit İstihbarat Yaşam Döngüsü Nedir?

Tüm dolandırıcılık, fiziksel ve siber güvenliği programları için olgun ve sofistike olanlar için temel bir Framework.

Yüksek seviyede, tehdit istihbarat yaşam döngüsü, sonuçları güvence alt olarak çizmek ve verilere dayanarak harekete geçmek için gerekli olan yüksek veri hijyeni standartlarını uygulamak ve uygulamak için temel adımları özetlemektedir. Bu yinelemeli ve uyarlanabilir metodoloji, nihayetinde ham verileri bitmiş istihbarat dönüştüren altı (6) aşamadır (bkz. Şekil 2.1.). [2]



Şekil 2.1. Tehdit istihbarat yaşam döngüsünün altı (6) aşaması

2.4.1. Direction (Yönlendirme)

Tehdit istihbaratı yaşam döngüsü, hangi varlıkların ve iş süreçlerinin korunması gerektiğini belirlemek ve öne çıkarma ve bunların tehlikeye girmesinin sonuçlarını anlamakla başlar. Genellikle Bilgi Güvenliği Baş Sorumlusu (Chief Information Security Officer-CISO) tarafından yönlendirilen bu aşamada, güvenlik ekipleri ayrıca hedeflerine ulaşmak için hangi bilgilere ihtiyaç duyduklarını belirlemeli ve karşılaştıkları belirli zorlukları ele almalıdır.[3]

Bunu etkili bir şekilde yapmak için doğru soruların sorulması gerekir:

- Kuruluş ve sektördeki benzerleri en çok ne tür saldırılara karşı savunmasızdır?
- Hangi kötü niyetli aktörler bu saldırıları başlatıyor ve neden?
- Bir siber analist veya teknik olmayan yönetim kurulu üyesi toplandıktan sonra tehdit istihbaratını kim alacak?
- Siber istihbarat programı paydaşların iş hedeflerini nasıl destekleyecek?

2.4.2. Collection (Toplamak)

Koruma gerektiren kritik varlıklar oluşturulduktan sonra, bu varlıklar için neyin tehdit oluşturduğuna ilişkin veri türleri ve bilgi kaynakları tanımlanmalıdır. Yaygın olarak toplanan tehdit verisi biçimlerine ek olarak, ör. kötü niyetli IP'ler ve etki alanları, kişisel olarak tanımlanabilir bilgiler (Personally Identifiable Information- PII) gibi güvenlik açığı verileri, haberleri, sosyal medya kaynaklarından gelen bilgiler dikkate alınabilir. [3]

Birinci aşamada özetlenen gereksinimleri karşılamak için ihtiyaç duyulan ham veriler hem dahili hem de harici çeşitli kaynaklardan elde edilebilir:

- Ağ ve Güvenlik Duvarı olay günlükleri (Network and firewall event logs)
- Endüstri Tehdit Verileri Yayınları (Industry threat data feeds)
- Siber Güvenlik Satıcıları (Cybersecurity vendors)
- İç ve dış kötü amaçlı yazılım analizi (Internal and external malware analysis)
- Haberler ve Bloglar (News and blogs)
- Bilgi Paylaşımı Toplulukları (Information sharing communities)

- Konu Uzman Raporlama (Subject matter expert reporting)
- Karanlık Web Forumları (Dark web forums)

2.4.3. Processing (İşleme)

Toplamaktan sonra, yanlış pozitifliği ve fazlalıkları ortadan kaldırmak için ham tehdit verilerinin organize edilmesi ve temizlenmesi ve kullanılabilir bir formata çevrilmesi gerekir. Veri işleme ayrıca şifreleme, doğruluk ve alaka düzeyi ile sıralama ve yabancı dillerden çeviri de içerebilir.

Daha küçük dijital ayak izleri olan örgütler bile, insanların manuel olarak işlenmesi, otomasyonun özellikle tehdit yaşam döngüsünün bu zaman tüketen aşaması için özellikle önemli hale getirilmesi için günlük olarak çok fazla veri topluyor. [3]

Bunu etkili bir şekilde yapmak için doğru soruların sorulması gerekir:

- Mevcut iç ve dış kör noktalarınız nerede?
- Hangi teknik ve otomatik toplama tekniklerini kullanabilirsiniz?
- Dark web deki siber suç forumlarına ve kapalı kaynaklara ne kadar iyi sızabilirsiniz?

2.4.4. Analysis (Analiz)

Bu aşamasının temel amacı, potansiyel güvenlik sorunlarını tanımlamak ve yönlendirme fazında belirtilen ihtiyaçlara dayanarak işlem yapılabilir görüşler geliştirmektir. Veriler, karar vericiler tarafından tüketilecek raporlar ve değerlendirmelerde paketlenmiştir. Genellikle PowerPoint sunumları, notlar, tehdit listeleri veya canlı yayınlar tehdit istihbaratının potansiyel bir tehdit destekleme kontrollerini ve kaynakların dağılımını ayarlamak gibi kararları bilgilendirmek için tehdit istihbaratının küratörlüğüne sahiptir. Analiz bağlam sallaştırma bilgi tehdit olur. [3]

Bunu etkili bir şekilde yapmak için doğru soruların sorulması gerekir:

- Hangi tür varlıklar, süreçler ve personel risk altındadır?
- Tehdit istihbaratı ekibim için operasyonel verimliliği nasıl artıracak?
- Başka hangi sistem ve uygulamalar fayda sağlayabilir?

2.4.5. Dissemination (Yayınlaştırma)

Çoğu kuruluş, kurumsal riski yönetmek için siber tehdit istihbaratına güvenen çok sayıda ekibe sahiptir. İstihbarat aktarmanın en anlaşılır ve eyleme geçirilebilir yollarını belirlerken her ekibin özel operasyonel ihtiyaçları ve uzmanlık düzeyi dikkate alınmalıdır. Güvenlik ekipleri en çok kötü amaçlı yazılım (malware) bulguları ve yüksek riskli IP adresleri gibi teknik bilgilerle ilgilenirken, yönetici ekipler siber tehditlerin iş riskini, sorumluluğunu ve kârını nasıl etkilediğini anlamak ister.

Güvenlik derecelendirme platformları gibi araçlar, bilgileri birden çok son kullanıcıya uygun bir biçimde ve bir zaman çizelgesinde sunar. Teknik ekipler, günlük görevlerini yerine getirmelerine yardımcı olmak için en güncel veri akışlarına erişebilirlik, güvenlik liderleri, yönetim kurulu ile periyodik toplantılar için olağan anlarda üst düzey yönetim kurulu özet raporları alabilir.[3]

Bunu etkili bir şekilde yapmak için doğru soruların sorulması gerekir:

- Hangi paydaşlar, tamamlanmış tehdit istihbaratı raporlamasından yararlanır?
- İstihbaratı sunmanın en iyi yolu nedir ve hangi teslimat sıklığında?

2.4.6. Feedback (Geri Bildirim)

Bu aşama, son kullanıcıların aşağıdaki tehdit döngüsünü yönlendirme fırsatı verdiği için ilk yönlendirme fazlasıyla yakından ilişkilidir. Tüm takımlardan devam eden geri bildirimler, istihbarat ihtiyaçlarının karşılanmasını sağlar ve güvenlik liderlerinin kaydırma önceliklerine cevaben ayarlamalar yapmalarını sağlar. Periyodik ekip anketleri, iç iş birliği platformları ile devam eden bir iletişim kanalı ile desteklenmelidir. Amaç, tehdit toplama işlemini sürekli olarak daraltmaktır, böylece ilgili ve doğru bilgi, mümkün olduğunca çabuk ihtiyaç duyanlara iletilebilir. [3]

Bunu etkili bir şekilde yapmak için doğru soruların sorulması gerekir:

- Sonuç olarak, bitmiş tehdit ne kadar değerli? Ne kadar eyleme geçirilebilir ve kuruluşunuzun bilinçli güvenlik kararları almasını sağlıyor mu?
- Ve son olarak hem bitmiş tehdit hem de kuruluşunuzun istihbarat döngüsünü iyileştirme açısından ileriye dönük olarak nasıl geliştirebilirsiniz?

2.5. Tehdit İstihbarat Türleri

Tehdit istihbarat üç benzersiz kategoriye ayrılabilir:

- ✓ Stratejik (Strategic)
- ✓ Taktik (Tactical)
- ✓ Operasyonel (Operational)

Bu sınıflandırmaların her biri, verilerin toplanması ve sunumunda devam eden girişimlerle nasıl ilişkili olduğu konusunda belirli bir role hizmet eder. [4]

Üç tür tehdit istihbaratının her birine daha yakından bakalım:

2.5.1. Stratejik tehdit istihbaratı (Strategic threat intelligence)

Basit bir ifadeyle, stratejik tehdit istihbaratı, bir kuruluşun tehdit ortamının kuşbakışı bir görünümüdür. Belirli aktörler, göstergeler veya saldırılarla ilgilenmez, bunun yerine üst düzey stratejilerin iş kararlarının daha geniş etkisini anlamalarına yardımcı olmayı amaçlar.

Hedef kitlenin öncelikle üst düzey ve yönetim kurulu düzeyinde olduğu düşünüldüğünde, stratejik tehdit istihbaratı neredeyse tamamen teknik değildir. Bunun yerine, risk puanları ve belirli bir eylem veya kararın olası sonuçları gibi faktörleri, örneğin bir dış pazara girme veya ideolojik bir pozisyon alma gibi faktörleri kapsar.

Belirli, üst düzey kararları bildirmek için kullanıldığından, stratejik tehdit istihbaratı genellikle devam eden bir girişimden ziyade talep üzerine toplanır ve çoğunlukla bir rapor veya briefing olarak sunulur. [4]

2.5.1.1 Stratejik tehdit istihbaratının kaynakları

Diğer istihbarat kategorilerinin aksine, stratejik tehdit istihbarat kaynaklarının çoğu açık kaynaktır, yani isteyen herkes tarafından serbestçe erişilebilir. Yaygın örnekler şunları içerir:

- Ulus devletlerden ve diğer çıkar gruplarından gelen politika belgeleri
- Yerel ve ulusal medya
- Sektöre ve konuya özel yayınlar
- İlgilenilen kişilerden yorumlar, çevrimiçi etkinlikler ve makaleler
- Güvenlik kuruluşları tarafından üretilen ücretsiz içerik (ör. teknik incelemeler, araştırma raporları vb.)

Stratejik kaynakların erişilebilirliği muazzam bir pozitif olabilirken, aynı zamanda iki ucu keskin bir kılıç olabilir, çünkü analistler değerli iç görüleri belirlemek için büyük miktarlarda ham veriyi manuel olarak işlenmelidir. Daha da kötüsü, en değerli içgörüler genellikle yabancı dil kaynaklarında "gizlenir / hidden" ve bu da analistleri çeviriye daha da fazla zaman ayırmaya zorlar.

Neyse ki, analistler doğru araçlarla silahlandırılıyor, bu zorluklar büyük ölçüde atlatılabilir. Güçlü tehdit istihbarat çözümleri, ilgili bilgileri gerçek zamanlı olarak belirleyerek ve yerel olmayan sonuçları otomatik olarak çevirerek çok sayıda kaynağı otomatik olarak tarayabilir. [5]

2.5.2. Taktik tehdit istihbaratı (Tactical threat intelligence)

Taktiksel tehdit istihbaratı, tehdit aktörleri tarafından hedeflerine ulaşmak için (örneğin, ağları tehlikeye atmak, verileri sızdırmak vb.) savunucuların kuruluşlarının nasıl saldırıya uğrama olasılığının olduğunu anlamalarına yardımcı olmayı amaçlamaktadır, böylece uygun algılama ve azaltma mekanizmalarının var olup olmadığını veya uygulamalarının gerekip gerekmediğini belirleyebilirler.

Neredeyse tamamen teknik olmayan stratejik tehdit istihbaratının aksine, taktik tehdit istihbaratı ağırlıklı olarak teknik bir izleyici kitlesine yöneliktir ve genellikle bazı teknik bağlamları içerir. Özellikle, taktik tehdit istihbaratı, sistem mimarları, yöneticiler ve güvenlik personeli gibi bir organizasyonun savunmasıyla doğrudan ilgili personel tarafından tüketilir, ancak daha üst düzey güvenlik karar vermede de rol oynar.

Tehdit aktörü TTB'leri her zaman değiştiğinden, taktik tehdit istihbaratı genellikle istek üzerine değil, normal istihbarat operasyonları sırasında toplanır. [4]

2.5.2.1. Taktik tehdit istihbaratının kaynakları

Tipik organizasyon için, güvenlik satıcıları ve diğer endüstri oyuncuları tarafından üretilen raporlar, en kolay erişilebilir bunlar taktiksel tehdit istihbarat kaynağıdır. Çoğu durumda, bu raporlar belirli bir tehdit grubuna veya saldırı kampanyasına odaklanır ve aşağıdaki gibi kilit taktik bilgiler sağlar:

- Hedeflenen yerler ve endüstriler
- İstihdam edilen saldırı vektörleri (örneğin, spear phishing, sql injection vb.)
- Kullanılan araçlar ve teknik altyapı

Bazı durumlarda, endüstri-maceralı (industry-vetted) raporlar, Siber Güvenlik Bilgisi Paylaşım Ortaklığı (Cybersecurity Information Sharing Partnership - CISP) gibi istihbarat paylaşım girişimleriyle elde edilebilir.

Bu raporlar son derece değerli olabilse de geniş bir izleyici kitlesi için üretilirler ve sonuç olarak yalnızca küçük bir kısmı herhangi bir belirli kuruluşla alakalı olacaktır. Bu nedenle, endüstri raporları en iyi ihtimalle eksik bir taktik tehdit istihbaratı kaynağıdır.

Daha kapsamlı ve güvenilir bir taktik tehdit istihbaratı akışı, aşağıdaki kaynaklardan herhangi birini veya tümünü içerebilen aktif bir toplama süreci gerektirir:

- Açık kaynak (Open Source)
- Honeypot lar ve karanlık ağlar (Honeypots and darknets)
- Telemetri verileri (Telemetry data)
- Tarama ve gezinme (Scanning and crawling)
- Kötü amaçlı yazılım analizi (Malware analysis)
- Kapalı kaynak (Closed source)
- İnsan ilişkileri (Human relationships)

Taktiksel tehdit istihbaratı için kurum içi bir toplama yeteneği oluşturmak mümkün olsa da bunu yapmak maliyetli olabilir ve çeşitli özel araçlar ve beceriler gerektirir. Çoğu kuruluş için, özel güvenlik sağlayıcılarından taktik tehdit istihbaratı satın almak daha gerçekçi bir tekliftir. [6]

2.5.2.2. Tehdit aktör TTPS'yi ayırt etme (Discerning threat actor TTPs)

Taktik tehdit istihbarat dört kategoriye girer:

1. Saldırı vektörleri (Attack Vectors)

Endüstrisindeki veya konumundaki organizasyonları hedeflemek için tehdit aktörleri ne tür saldırılardır? Örneğin, hedeflenmiş spear phishing kampanyalarını kullanarak kimlik bilgilerini toplayabilirler veya belgelenmiş güvenlik açıklarını, ayrıcalıklarını arttırmak için kullanabilirler.

Hangi saldırı vektörlerinin sizinki gibi organizasyonlara karşı kullanıldığı anlaşılıyor, çünkü savunucuların zamanlarını ve kaynaklarını etkili bir şekilde öncelik vermelerini sağlar.

Diğer önemli sorular şunlardır:

- Hedefleri nasıl seçiyorlar?
- Özel güvenlik açıklarını sömürüyorlar mı?
- Hedef ağlardaki lateral ve / veya artan ayrıcalıkları nasıl hareket ediyorlar?
- Hedefleri nelerdir ve hangi varlık classlarını hedefliyorlar?
- Gözlenebilir davranış kalıpları var mı?

2. Araçlar (Tools)

Herhangi biri, eğer varsa, operasyonları boyunca (örneğin, hedef ağları tehlikeye atmak, artmak, ayrıcalıkları tehlikeye atmak veya verileri tehlikeye atmak için) tehdit aktörleridir. Bu tür bilgiler genellikle başarılı veya başarısız saldırıların mortem sonrası analizlerinden gelir ve ideal olarak kullanılan spesifik kötü amaçlı yazılımların veya kullanılmış kitlerin ayrıntılarını içerir.

Yürüyüş siparişleri ile savunucuları sağlamanın yanı sıra, bu tür bilgi aynı zamanda bir tehdit grubunun beceri ve finansman seviyesine ilişkin iç görüş sağlayabilir.

3. Altyapı (Infrastructure)

Kullandıkları araçlara ek olarak, tehdit aktörleri tarafından kullanılan daha geniş altyapının anlaşılmasına da yardımcı olur. Çoğu durumda bu, saldırının veri sızdırma kısmıyla ilgilidir, çünkü bu genellikle güvenliği ihlal edilmiş bir ağ içindeki bir nokta ile harici bir komuta ve kontrol (command and control - C2) sunucusu arasındaki iletişime dayanır.

C2 sunucularının belirli IP adreslerini belirlemek daha çok teknik tehdit istihbaratının alanı olsa da taktik tehdit istihbaratı daha çok örneğin HTTP veya DNS gibi kullanılan iletişim tekniklerine odaklanacaktır.

Bu iletişimlerin nasıl yürütüldüğünü anlamak, savunucuların, mevcut durumdaki bir ağ tarafından algılanıp engellenmeyeceğini veya daha fazla kontrol yapılması gerekip gerekmediğini belirlemelerini sağlar.

4. Adli Kaçınma Stratejileri (Forensic Avoidance Strategies)

Son olarak, tehdit aktörleri araçlarının ve eylemlerinin tespit edilmesini önlemek için hangi teknikleri kullanıyor? Gelişmiş tehdit grupları, tespiti geciktirmek veya önlemek için çeşitli stratejiler kullanacak ve olay müdahale analistleri gibi cephe

savunucularının hangi tekniklerin yaygın olarak kullanıldığını anlamaları için para ödüyor. [6]

2.5.3. Operasyonel Tehdit İstihbaratı (Operational Threat Intelligence)

Operasyonel tehdit istihbaratı, belirli saldırılar veya kampanyalarla ilgilidir. Savunucuların belirli bir saldırının doğasını, amacını ve zamanlamasını anlamalarına yardımcı olur ve ayrıca sorumlu grupların doğası ve karmaşıklığı hakkında fikir verir. Ancak çoğu durumda, yalnızca kısmi bağlam elde edilebilir.

Birçok yönden gerçek operasyonel tehdit istihbaratı, güvenliğin en önemli ayağı ve savunuculara önleyici olarak kontrolleri yerleştirme ve saldırıları gerçekleştirmeden önce engelleme fırsatı sunar. Kısmi istihbarat bile yaklaşmakta olan saldırılar hakkında önemli bilgiler sağlayabilir. Örneğin, olası saldırı yollarını istismar edilmeden önce vurgulayarak.

Operasyonel tehdit istihbaratı, neredeyse tamamen teknik bir kitleye (ör. güvenlik operasyonları personeli ve yöneticileri) yöneliktir, bu nedenle kaçınılmaz olarak teknik bağlamı içerir.[4]

2.5.3.1. Operasyonel tehdit istihbaratının kaynakları

Operasyonel tehdit istihbaratının belirli saldırı planları ile ilgili olduğu için, onu elde etmenin sadece iki yolu vardır:

- İnsan kaynaklarını aktif bir tehdit grubunda yetiştirmek, büyük olasılıkla işe alım veya infiltrasyon yoluyla
- Bir tehdit grubunun iletişimini önlemek veya başka bir şekilde ödün vermek

Şaşırtıcı olmayan bir şekilde, daha sonra, dört birincil tehdit istihbarat kategorisinin, operasyonel tehdit istihbaratının kapalı kaynaklardan gelmesi muhtemeldir. Bazı gruplar açık kanalları (örneğin, sosyal medya, açık IRC kanalları vb.) Kullanarak iletişim kurarken, çoğu daha gizli bir yaklaşım sağlar.

En yaygın kaynaklardan bazıları şunlardır:

- İnternet sohbet odaları (hem açık hem de özel) çoğu zaman IRC sunucularında barındırıldı
- Sosyal medya (Facebook, Instagram, Twitter vs.)

- Hem açık hem de karanlık web (dark web)'de barındırılan kamu ve özel (Public and private) forumlar

Daha az karmaşık tehdit grupları, özellikle ideolojik motivasyonlara sahip olanlar, planlarını nispeten korunmasız kanallarla tartışmak için içeriktir, daha ciddi ceza operasyonlarının önlem alma olasılığı daha yüksektir. Bu bizi önemli bir noktaya getirir: Operasyonel tehdit istihbaratı, belirli bireylerin ve grupların faaliyet ve iletişimiyle ilgili olduğu için, koleksiyonu bir dizi yasal (legal) ve etik (ethical) husus ortaya çıkarır.

2.5.3.2. Operasyonel tehdit istihbaratını toplamanın engelleri

Operasyonel tehdit istihbaratının toplanması ve analiz edilmesi durumunda, tehdit analistlerinin dört birincil engelle karşılaşması muhtemeldir:

Erişim (Access): Çoğu tehdit grubu, planlarını tartışırken en azından bazı önlemleri alır ve gizliliği korumak için ellerinden geleni yapar. Sadece dikkate alınacak etik ve yasal etkiler yok, ancak çoğu durumda bir grubun iletişimine erişmek mümkün olmayacağını kabul etmek de önemlidir.

Dil (Language): Benzer bir notta, birçok ciddi tehdit grubu İngilizce olmayan ülkelerde bulunur ve ana dillerini kullanarak iletişim kurar. Bu operasyonel tehdit istihbarat ortaya çıkarma masrafına ekleyebilir, ancak bu engel, kaydedilmiş geleceğe dahil olan bir doğal dil işleme (natural language processing - NLP) motorunun kullanılmasıyla üstesinden gelinebilir.

Çok fazla gürültü (Too Much Noise): Sohbet Odaları ve Sosyal Medya gibi birçok ortak operasyonel tehdit istihbarat kaynağı doğal olarak yüksek hacimli, el ile izleme yapılmaz. Bir kez daha, güçlü tehdit istihbarat çözümlerine dahil olan teknoloji bu engellemeye yardımcı olur.

İşlevsizlik taktikleri (Obfuscation Tactics): Zaten belirttiğimiz gibi, birçok tehdit grubu, niyetlerini meraklı gözlerden gizlemek için büyük uzunluklara gider. Ortak İşlevsizlik Taktikleri, hedef isimler ve / veya saldırı türlerinin yerine özel kodların kullanımını ve bireysel takma adların düzenli değişimini içerir. [7]

2.5.4. Özet

Type	Tagline	Half life of utility (for good guys and bad guys)	Focus	Built on the analysis of	Output data types
Strategic	Who? Why?	Long (multiyear)	Non-technical	Big campaigns, groups, multi victim intrusions (and operational intel)	Long form writing about: victimology, YoY methodology, mapping intrusions and campaigns to conflicts, events and geopolitical pressures
Operational	How? Where?	Medium (one year plus)	Mixed (both really)	Whole malware families, threat groups, human behavior analysis (and tactical intel)	Short form writing, bulleted lists, about: persistence and comms techniques, victims, group profiles, family profiles, TTP descriptions, triggers, patterns, and methodology rules
Tactical	What?	Short (months)	Technical	Security events, individual malware samples, phishing emails, attacker infrastructure	Atomic and machine-readable indicators such as IPs, domains, IOCs, "signatures"

Şekil 2.2. Tehdit istihbarat türlerinin karşılaştırması

2.6. Tehdit İstihbarat Akışı Nedir?

Tehdit istihbaratı beslemeleri (Feeds) ve kaynakları (sources), tehditler ve kötü aktörler hakkında sürekli olarak eyleme geçirilebilir bilgi akışlarıdır. Tehdit istihbaratı analistleri, olağan dışı etkinlik ve kötü amaçlı etki alanları ve çeşitli kaynaklardan IP adresleri gibi IoC ler hakkında güvenlik verileri toplar. Feed'ler yalnızca tehditlerle ilgili ham verilerdir; bir analist, raporlar oluşturmak için onlardan istihbarat alır.

Tehdit Verilerinin Toplanması için TTP (Taktikler, Teknikler ve Prosedürler)

1. Açık Kaynak İstihbaratı (OSINT) ile Veri Toplama

Buna Arama Motorları, Web Hizmetleri, Web Sitesi Ayak İzi, E-postalar, Whois Araması, DNS Sorgulaması ve Araçlar (Tools), Çerçeveler (Framework), Komut Dosyaları (Scripts) kullanılarak OSINT çalışmasının Otomatikleştirilmesi gibi açık kaynaklar aracılığıyla veri toplama dahildir. [15]

2. İnsan İstihbarat Yoluyla Veri Toplama (HUMINT)

Bu süreç, İnsan Temelli Sosyal Mühendislik Teknikleri, Mülakat, Sorgulama ve Sosyal Mühendislik Araçları aracılığıyla veri toplamayı içerir.

3. Siber Karşı İstihbarat (CCI) Yoluyla Veri Toplama

Bu adımda Honeypots, Pasif DNS İzleme, Rakiplerin Altyapısını Döndürmek, Malware Sinkholes ve YARA kuralları aracılığıyla tehdit verileri toplanır.

4. Uzlaşma Göstergeleri (IoC ler) aracılığıyla Veri Toplama

Dahili kaynaklardan, harici kaynaklardan dijital kanıt verileri toplama ve özel tehdit IOC leri oluşturma.

5. Kötü Amaçlı Yazılım (Malware) Analizi Yoluyla Veri Toplama

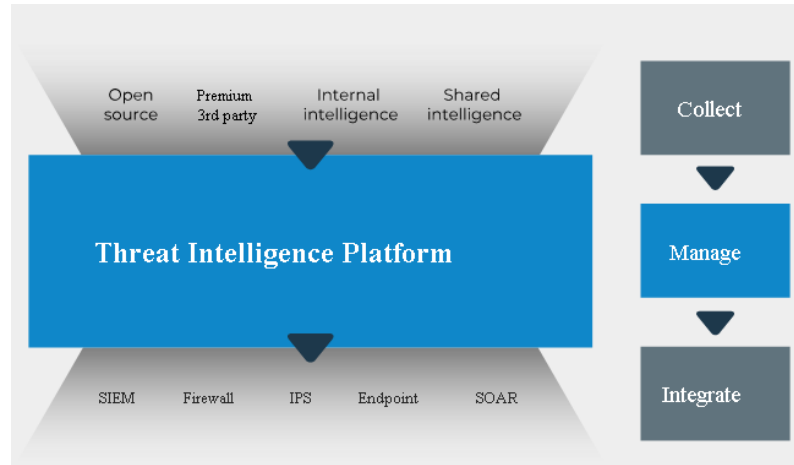
Kötü amaçlı yazılım analizi, kötü amaçlı yazılım örneğinin kaynağını ve etkisini ve analiz araçlarını dağıtarak nasıl çalıştığını anlama sürecidir. Kötü amaçlı yazılım birden çok şekilde çalışır ve güvenli olmayan cihazlar hakkında kullanıcının bilgisi olmadan bilgi toplar.

3. TEHDİT İSTİHBARAT PLATFORMLARI

Günümüzün siber güvenlik ortamı, büyük miktarda veri, analist eksikliği ve giderek daha karmaşık hale gelen düşmanca saldırılarla ilgili birkaç yaygın sorunla işaretlenmiştir. Mevcut güvenlik altyapıları, bu bilgileri yönetmek için birçok araç sunar, ancak bunlar arasında çok az entegrasyon vardır. Bu sistemleri yönetmek için sinir bozucu miktarda mühendislik çabası ve zaten sınırlı olan kaynakların ve zamanın kaçınılmaz israfı anlamına gelir.

Bu sorunlarla mücadele etmek için birçok şirket bir Tehdit İstihbarat Platformu (TIP - Threat Intelligence Platform) uygulamayı tercih ediyor. Tehdit İstihbarat Platformları, siber tehdit istihbaratının ve aktörler, olaylar, imzalar, bültenler ve TTB'ler gibi ilişkili varlıkların yönetimini kolaylaştırmak için bir SaaS veya şirket içi çözüm olarak dağıtılabilir. Dört temel işlevi yerine getirme yeteneği ile tanımlanır:

- I. Birden fazla kaynaktan istihbarat toplama
- II. Verilerin iyileştirilmesi, normalleştirilmesi, zenginleştirilmesi ve risk puanlaması
- III. Mevcut güvenlik sistemleri ile entegrasyonlar
- IV. Tehdit istihbaratının analizi ve paylaşımı



Şekil 3.1. Tehdit istihbarat platformları verileri geçişi

Bu yapıda “tehdit” ile “istihbarat” kavramları daha önceden detaylı incelemiştir. Şimdi ise bunların yanına “Platform” kavramı ilave yapacağız.

Platform, mevcut araçlar ve ürünlerle bütünleşen, analistlerin geleneksel olarak yaptığı işlerin çoğunu otomatikleştiren ve basitleştiren bir tehdit istihbaratı yönetim sistemi sunan paketlenmiş bir ürün.

Tehdit istihbarat platformu bir kuruluş içinde üç ekip ile daha çok yararlıdır.

Bunlar:

- I. Güvenlik Operasyon Merkezi (SOC - Security Operations Center) Ekipleri
- II. Tehdit İstihbarat (Threat Intelligence) Ekipleri
- III. Yönetim ve Yönetici (Management and Executive) Ekipleri

Ve Olası güvenlik ürünü entegrasyonları arasında API, SIEM, Endpoint, IPS ve Firewall bulunur. [8]

3.1. Kaynaklar (Sources)

Çeşitli kaynaklardan bilgi toplamak, güçlü bir güvenlik altyapısına sahip olmak için kritik bir bileşendir. Bunlar desteklenen kaynaklar;

- Open Source (Açık Kaynak)
- Third Party Paid (Üçüncü Taraf Ücretli)
- Government (Devlet)
- Trusted Sharing Communities (ISACs - Bilgi Paylaşımı ve Analiz Merkezleri).
- Dahili (Internal)

Aşağıdaki kaynakların toplamak için tehditlerle ilgili (umarız) güncel bilgileri elde etmek için listeler ve/veya API'ler sağlar. Gerçek tehdit istihbaratı oluşturmak için belirli bir miktarda (Domain/Etki Alanı veya Business spesifik/İşletmeye özel) gereklidir. [9]

3.1.1. AbuseIPDB

Bilgisayar korsanlarının, spam göndericilerin ve internetteki kötü niyetli etkinliklerin yayılmasıyla mücadeleye yardımcı olmaya adanmış bir projedir. Görevi, web yöneticilerine, sistem yöneticilerine ve diğer ilgili taraflara çevrimiçi kötü amaçlı etkinliklerle ilişkilendirilmiş IP adreslerini bildirmeleri ve bulmaları için merkezi bir kara liste sağlayarak Web'i daha güvenli hale getirmeye yardımcı olmaktır. [10]

AbuseIPDB, python programlama dili ile kişiselleştirebilirsiniz. [16]

3.1.2. APT groups and operations / APT grupları ve işlemler

APT grupları, operasyonları ve taktikleri hakkında bilgi ve istihbarat içeren bir elektronik tablo. [10]

Yıla göre sıralanan APT ile ilgili çeşitli halka açık kaynakların derlemesi ile oluşan repository (depo). [17]

3.1.3. DigitalSide thread-intel

Çoğunlukla kötü amaçlı yazılım analizine dayanarak ve URL'ler, IP'ler ve alanları tehlikeye atan açık kaynaklı siber tehdit istihbarat göstergeleri kümelerini içerir. Bu projenin amacı, SOC / CSTR / CERT / individuals (Bireyler) tarafından minimum ehlekti (çapa) ile kullanılmak üzere alaka firmalarını avlamak, analiz etmek, toplamak ve paylaşmak için yeni yollar geliştirmek ve test etmektir. Raporlar üç yolla paylaşılır: STIX2, CSV ve MISP feed (besleme). Raporlar, projenin GIT deposunda da yayınlanmaktadır. (NOT: Formatlar kısımdan STIX2, CSV ve MISP'ları detaylı inceleyiciyiz.) [10] [18]

3.1.4. Disposable Email Domains / Tek Kullanımlık E-posta Alanları

Genel olarak spam / taciz hizmetleri için kullanılan anonim veya tek kullanımlık e-posta alanları koleksiyonu. Birçok farklı programlama dillerden kullanmak mümkündür. (Python, PHP, Ruby, Node Js ve C#) [10] [19]

3.1.5. ExoneraTor

Tor ağının bir parçası olan bir IP adresi veritabanını korur. Belirli bir tarihte belirli bir IP adresinde çalışan bir TOR rölesi olup olmadığını soruyu cevaplar. Röleler İnternet'e Tor ağına kayıt olmaktan daha farklı bir IP adresi kullanırsanız, röle başına birden fazla IP adresi saklayabilir. [10]

3.1.6. FireHOL IP List

400'den fazla kamuya açık olan IP feeds (beslemeleri), evrimlerini, Geo haritasını, IP lerin yaşını, tutma politikasını, çakışmalarını belgelemek için analiz etti. Site siber suça (saldırıları / attacks, suiistimal / abuse, kötü amaçlı yazılım / malware) odaklanmaktadır. [10] [20]

Yukarıda anlatmaya çalıştığım kaynakların sadece altısı bunlar gibi onlarcası veya yüzlercesi mevcuttur.

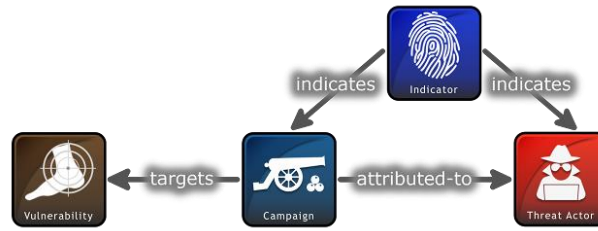
3.2. Formatlar (Formats)

Tehdit İstihbaratını paylaşmak için standartlaştırılmış biçimler (çoğunlukla IOC ler) kullanır. Bunlar çeşitli kaynaklardan toplanan büyük miktar veriler farklı formatlardan toplanması. [8] [11]

- STIX/TAXII
- JSON and XML
- Email
- CSV, TXT, PDF, Microsoft Word document vb. çeşitli formatlardadır.

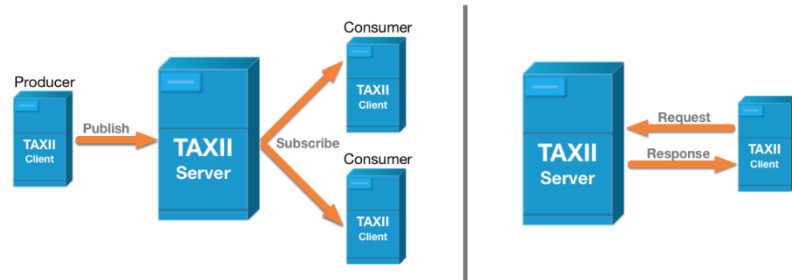
3.2.1. STIX/TAXII

STIX, siber tehdit bilgilerinin temsili için standart bir dile sahip olduğu bir dildir. TAXII 'ya benzer şekilde, bir paylaşım programı veya aracı değildir, ancak programları veya araçları destekleyen bir bileşendir. [8][11]



Şekil 3.2. STIX ilişkisi Örnek

Bazen STIX yapılarıyla karışıklığa neden olan şeylerden biri, olay veya gösterge kullanılıp kullanılmayacağıdır. Daha fazla analiz veya takip için bir geçmişi sağlamayı hedefliyorsanız, bir olay oluşturmamız gerekir. Aramak için bir öge listesi oluşturmak istiyorsanız, bir gösterge yapısı kullanın.



Şekil 3.3. TAXII Collections

TAXII, organizasyonlar, ürünler ve hizmetler arasında işlem yapılabilir tehdit bilgilerinin paylaşılmasını sağlayan bir dizi hizmet ve mesaj değişimini tanımlar. TAXII, bir bilgi paylaşım programı değildir ve güven anlaşmalarını tanımlamaz. Aksine, organizasyonların ortaklarıyla bilgi paylaşımlarına yardımcı olmak için siber tehdit bilgilerini değiştirmek için bir dizi özelliktir. [21]

TAXII, aşağıdaki üç paylaşım modeline sahiptir:

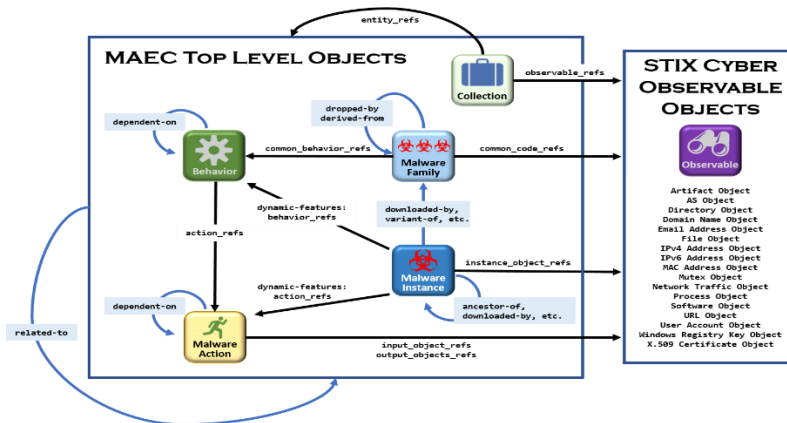
- Hub and Spoke: Bir merkezi temizleme merkezi
- Kaynak (Source) / Abone (Subscriber): Bir kuruluş tek bilgi kaynağıdır
- Peer-to-Peer: Birden fazla organizasyon bilgilerini paylaşıyor

3.2.2. Cybox

Siber gözlemlenebilir ekspresyon (Cybox - Cyber Observable eXpression) dili, konuşlandırılmış alet ve işlemlerin tutarlılığını, verimliliğini ve birlikte çalışmasını sağlayan işletme siber güvenliğinin operasyonel alanları arasında ve bunların yanı sıra, genel durumsal farkındalığı arttıran işletme siber güvenliğinin operasyonel alanları arasında siber gözlemlenmelerini temsil etmek için ortak bir yapı sağlar. Detaylı otomatikleştirilebilir paylaşım, eşleme, algılama ve analiz sezgiselliği potansiyeli. [8] [11]

3.2.3. MAEC

Kötü amaçlı yazılım niteliği numaralandırması ve karakterizasyonu (MAEC - Malware Attribute Enumeration and Characterization) projeleri, davranış, eserler ve saldırı kalıpları gibi niteliklere dayanarak, kötü amaçlı yazılımlar hakkında yapılandırılmış bilgileri paylaşmak için standart bir dil oluşturmayı amaçlamaktadır. [8][11][22]



Şekil 3.4. MAEC top level object

3.2.4. VERIS Framework

Etkinlik kaydı ve olay paylaşımı için kelime hazinesi (Veris - Vocabulary for Event Recording and Incident Sharing), güvenlik olaylarını yapılandırılmış ve tekrarlanabilir bir şekilde tanımlamak için ortak bir dil sağlamak için tasarlanmış bir dizi metrik. Veris, güvenlik endüstrisindeki en kritik ve ısrarcı zorluklardan birine bir cevaptır- kalite bilgisi eksikliği. Yapılandırılmış bir format vermenin yanı sıra, Veris, Verizon Veri İhlali Araştırmaları Raporunda (DBIR- Data Breach Investigations Report) ihlalleri hakkında rapor vermek için topluluktan veri toplar ve bu veri tabanı çevrimiçi olarak VCDB.org'da yayınlar. [8][11][23]

Yukarıda anlatmaya çalıştığım format türlerin sadece dörttü bunlar gibi onlarcası veya yüzlercesi mevcuttur.

3.3. Çerçeveler ve Platformlar (Frameworks and Platforms)

Tehdit istihbaratının toplanması, analiz edilmesi, oluşturulması ve paylaşılması için çerçeveler, platformlar ve hizmetler. [12]

3.3.1. Abuse.IO

AbuseIO, (kötüye kullanım/suiistimal) raporları almak, işlemek, ilişkilendirmek ve ağınızdaki suiistimal vakaları ile ilgili belirli bilgileri içeren bildirimleri oluşturmak ve göndermek için kullanılabilecek, açık kaynak kodlu ve ücretsiz bir araç setidir. AbuseIO'nun amacı, suiistimal süreçlerini otomatikleştirmek ve geliştirmektir. [12]

```
abuseio@ar3:/opt/abuseio$ php artisan user:list
```

ID	Account	User	First Name	Last Name	Roles
1	Default	admin@isp.local	System	Admin	System Administrator
2	Default	user@isp.local	Elizabeth	Smith	Abusedesk User
3	Customer Internet	admin@isp2.local	Warren	King	System Administrator
4	Customer Internet	user@isp2.local	Sophie	Davidson	Abusedesk User
5	Business Internet	admin@isp3.local	Richard	Paterson	System Administrator

```
abuseio@ar3:/opt/abuseio$ php artisan ticket:list
```

Id	Ip	Domain	Class id	Type id
1	172.16.10.13		BOTNET_INFECTION	ABUSE
2	fdf1:cb9d:f59e:19b0:0:45:0:22		BOTNET_INFECTION	ABUSE
3	10.0.2.150		COMPROMISED_SERVER	ABUSE
4	fdf1:cb9d:f59e:19b0:0:33:4f		COMPROMISED_SERVER	ABUSE

Şekil 3.5. Sistemdeki kullanan veriler

Abuse.IO ana özellikleri:

- Abuse mesajlarını alıp abuse raporlarına otomatik olarak parse etmek ve mail yoluyla iletmek (bir posta sunucusu işleyicisi, örn. Postfix aracılığıyla).

- Karmaşıklığı azaltmak için zaten açık bir durumda olan raporları birleştirilebilir.
- Abuse türlerini sınıflandırmak ve belirli vakalarda özel eylemler oluşturabilir.
- IPAM sisteminizi kolayca entegre edilebilir.
- Case(olay) başına otomatik bildirimler ayarlanabilir.
- Olayları yanıtlama, kapatma veya not ekleme, organize olmalarını sağlamaktadır.

[New event](#) [CSV Export](#)

Show entries
Search:

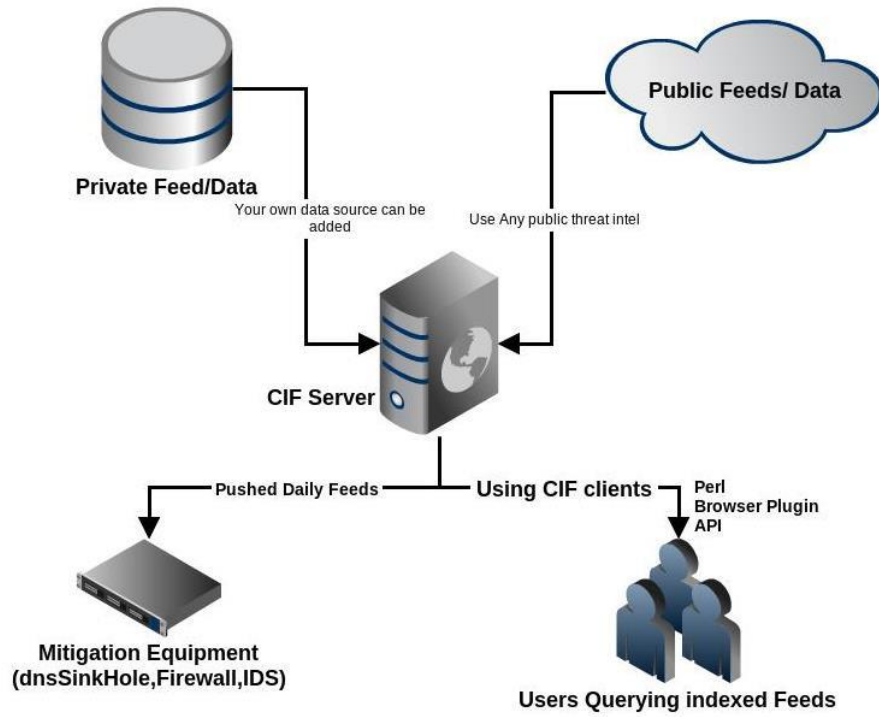
Ticket Id	IP	Domain	Type	Classification	Events	Notes	Status
3	10.0.2.150		Abuse	Compromised server	1	0	Open
9	10.0.2.100		Abuse	Copyright Infringement	1	0	Open
37	10.0.2.23	nacions.com	Abuse	Compromised website	3	0	Open
38	10.0.2.26		Abuse	Phishing website	2	0	Open
48	10.0.2.2		Abuse	Compromised website	1	0	Open

Şekil 3.6. Arama portalı

Abuse.IO içerisinde bulunan parserlar ve kaynakları [24]

- Any RFC compliant ARF formatted message
- Any RFC compliant FBL Messages (Feedback Loop)
- Any DNS based RBL
- Shadowserver
- SpamCop
- IP Echelon
- fail2ban reporting service
- Junk Email Filter
- Google Safe Browsing reports for ASN's
- Project Honey Pot
- Clean MX
- Cyscon / C-SIRT
- Netcraft
- SpamExperts
- USGO-Abuse
- Microsoft SNDS
- Abuse-IX
- Woody
- Webiron
- Copyright Compliance
- Cegtek
- Juno

3.3.2. Collective Intelligence Framework (CIF)



Şekil 3.7. Collective Intelligence ilişkisi

CIF, bir siber tehdit istihbarat yönetim sistemidir. CIF, birçok kaynaktan gelen bilinen zararlı yazılım tehdit göstergelerini (IOC) birleştirmenize ve bu bilgileri tanımlamanızı ve algılamanızı sağlamaktadır. CIF te depolanan en yaygın tehdit göstergeleri türleri, zararlı etkinlikle ilişkili olduğu gözlenen IP adresleri, FQDN leri (Fully Qualified Domain Name) ve URL'lerdir. CIF, çeşitli tehdit verilerini herhangi bir kaynaktan alabilmektedir. Framework'ün çalışma mantığı şu şekildedir. [12][25]

- Herhangi bir kaynaktan veri alma.
- Bu veriyi kaydetme ve reputation (itibar)'a göre değerlendirme.
- Sorgular aracılığıyla tekrar veriye erişim ve dışarı aktarma.

CIF Nasıl Çalışır?

- Parse (Ayrıştırma Süreci)

CIF, aynı tipteki birçok farklı veri kaynağından veri toplamayı destekler; örneğin, zararlı domainlerin veri setleri veya feedlerini (beslemeleri) toplayabilir. Her benzer veri setini kaynak veya güvenilirlik oranı gibi farklı niteliklerle işaret edilebilmektedir.

➤ Normalize (Normalleştirme)

Tehdit istihbaratı veri setleri genellikle aralarında ince farklara sahiptir. CIF, diğer uygulamalarda veya süreçlerde tehdit istihbaratından yararlanırken size öngörülebilir bir deneyim sunan bu veri kümelerini normalleştirmektedir.

➤ Post Process

CIF, tek bir tehdit istihbaratından ek istihbarat elde eden birçok işlemciye sahiptir. Basit bir örnek, bir domain ve bir IP adresinin CIF içine alınan bir URL'den türetilmesidir.

➤ Store (Depolama)

CIF, milyonlarca tehdit istihbarat verilerini depolamak için son derece optimize edilmiş bir veritabanı şemasına sahiptir. CIF v2, Elasticsearch kullanmaktadır.

➤ Query (Sorgu)

CIF bir web tarayıcısı, yerel istemci veya doğrudan API kullanılarak sorgula olabilmektedir. CIF, milyonlarca kayıt veritabanına karşı sorgulama yapmak için son derece optimize edilmiş bir veri tabanı şemasına sahiptir.

➤ Share (Paylaşma)

CIF kullanıcıları, grupları ve API anahtarlarını destekler. Her tehdit istihbaratı verisi, belirli bir kullanıcı grubuyla paylaşılacak üzere etiketlenebilir. Bu, tehdit istihbaratının federasyonlar arasında paylaşılmasına izin vermektedir.

➤ Produce

CIF, depolanan tehdit istihbaratından yeni veri kümeleri oluşturulmasını destekler. Bu veri setleri, tür veya güvenilirlik ile oluşturulabilir. CIF ayrıca feed oluşturma sürecinde whitelisting desteklemektedir.

3.3.3. MISP Threat Sharing



Şekil 3.8. MISP Threat Sharing logosu

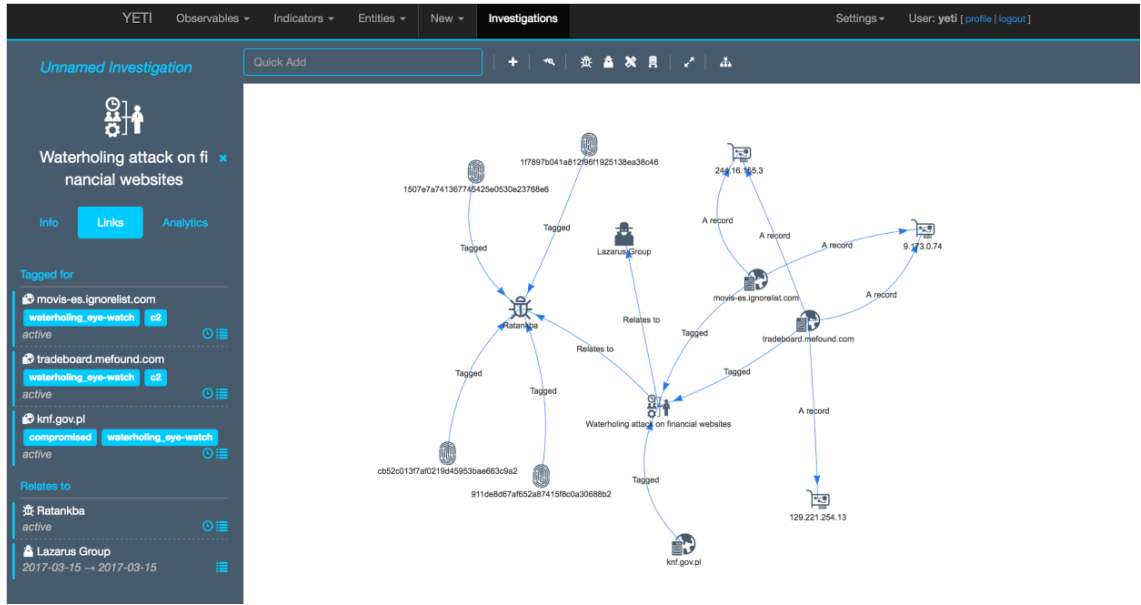
MISP (Zararlı Yazılım Bilgi Paylaşım Platformu) siber tehdit istihbaratının paylaşımına yardımcı olan ücretsiz ve açık kaynak kodlu bir projedir.

MISP, hedeflenen saldırıların, mali dolandırıcılık bilgilerinin, güvenlik açıklarının veya terörle mücadele bilgilerinin ele geçirilmesi ve toplanması, paylaşılması, depolanması ve ilişkilendirilmesi için oluşturulmuş bir siber tehdit istihbaratı platformudur.

MISP platformu kurum ve kuruluşların zararlı yazılım tehdit göstergeleri (malware IOC leri) hakkında bilgi paylaşımlarını sağlar. Kullanıcılar, zararlı yazılımlar (malware) veya tehditler hakkındaki "işbirliğine" dayalı bilgiden yararlanırlar. Bu güvenilir platformun amacı, hedeflenen saldırılara karşı kullanılan karşı önlemlerin geliştirilmesine yardımcı olmak ve önleyici eylemler oluşturmaktır.

MISP, bir web arayüzü (analistler veya olay müdahale ekipleri için) üzerinden kullanılabilir. Bir REST API üzerinden de tehdit göstergelerini (IOCs) alıp gönderilebilmektedir. MISP platformunun temel hedefi tehdit bilgilerini açığa çıkarmayı, olgunlaştırabilmeyi ve istismar edilmesini önleyen sorunsuz bir operasyon sağlayan sağlam bir platform olmaktır. [12][26]

3.3.4. YETI - Your Everyday Threat Intelligence



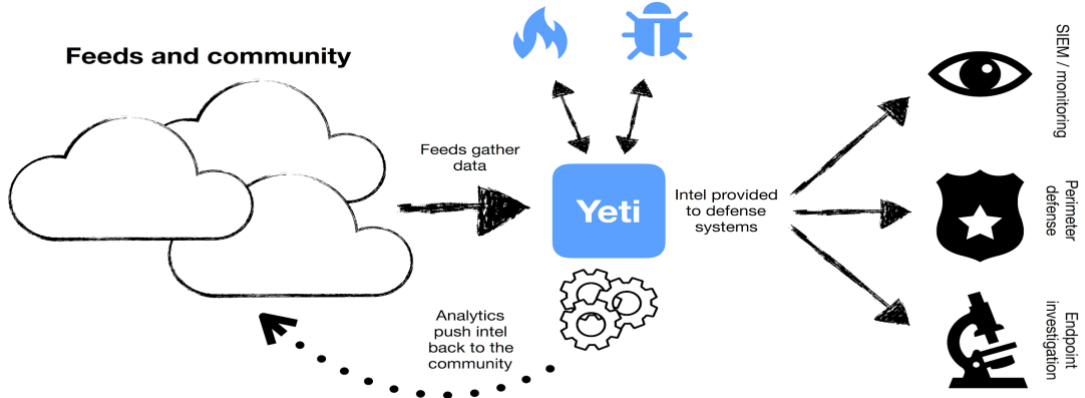
Şekil 3.9. YETI dashboard

Yeti, tehdit gösterilerini (indicator of compromise) ve bu göstergelerin teknik, taktik ve prosedürleri (TTP) hakkındaki bilgileri tek bir depoda organize etmeyi amaçlayan bir platformdur.

Yeti, tehdit göstergelerini (IOC) otomatik olarak zenginleştirilme özelliğine sahiptir. Örneğin domain alanlarını çözmek, IP adreslerini coğrafi konumlara ayırmak gibi. Yeti kullanıcıların rahat bir ortamda çalışabilmesi için “Bootstrap” tabanlı bir kullanıcı arayüzü sunmaktadır. Bir web API arabirimi üzerinden diğer araçlarla entegre edilebilmekte ve kullanılabilir. [12]

Yeti, çok çeşitli kaynaklardan örneğin yazımızda bahsettiğimiz zararlı yazılım bilgi paylaşım platformu olan MISP üzerinden zararlı yazılımlara ait göstergeler, XML özetleri, JSON verileri toplayabilir ve işlenebilir. Sorguları otomatik hale getirebilir ve olay müdahale ekiplerinin işlerine yardımcı olabilmektedir. Yeti, yakın zamanda piyasaya sürülen ve tehdit istihbarat yönetimini kolaylaştırmayı amaçlayan birçok araçtan biridir. Beslemeler ile verilerini derlemenize ve zenginleştirmenize yarayacak çok geniş bir araç kombinasyonuna sahiptir.

Yeti üzerine eklenen tüm bu verileri hızlıca listeleyebilir, analiz edebilir, ilişkilendirebilir ve dışa aktarım sağlayabilirsiniz. Örneğin bu veriler SIEM gibi ürünlere meşhur formatlarda aktarılabilir ve entegrasyon sağlanabilir. Bu sayede yapılan analizler sonucu bulunan tüm bulguları SIEM gibi yazılımlar üzerine aktarmak ile uğraşmaktan kurtarmaktadır. [12]



Şekil 3.10. YETI işleme akışı


3.3.5. Cuckoo Sandbox



Şekil 3.11. Cuckoo Sandbox logosu

Cuckoo Sandbox, şüpheli dosyaların analizini otomatikleştirmek için kullanabileceğiniz açık kaynaklı bir yazılımdır. Bunu yalıtılmış bir ortamda çalışırken, "zararlı işlemlerin davranışlarını" izleyen özel bileşenlerden yararlanmaktadır.

Şüpheli herhangi bir dosyayı birkaç dakika içinde sandbox ortamına yükledikten sonra Cuckoo bu dosyayı gerçekçi ancak yalıtılmış bir ortamda yürütür daha sonra size bu dosyanın davranışını özetleyen ayrıntılı bir rapor sunmaktadır. [12]



Info	File	Signatures	Screenshots	Static	Dropped	Network	Behavior
Category	Started On	Completed On	Duration	Cuckoo Version			
FILE	2013-01-26 23:50:42	2013-01-26 23:53:10	148 seconds	0.5			
File Details <small>file indicators</small>							
File name	eFeb717fdbb98d8043eb4c51254d9b74						
File size	93696 bytes						
File type	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed						
CRC32	83427ED8						
MD5	eFeb717fdbb98d8043eb4c51254d9b74						
SHA1	2644a7c50aa3cd36be0dd219efe531ed72ae514						
SHA256	8dafb21e7d106a6c98f745f30c2577ee7b0984ec7ba2c4107f7ddcd0d127bafe						
SHA512	097e682a4723c6e72caaac01e49711b21e8091cd0cab90a192aa233ba9e0eF3c4468951f4f53fa1b6543d55395c6e6859c2a6b121d697cc74889d570d623273						
Ssdeep	3lone						
PEID Signatures	None matched						
Yara Signatures							
Antivirus	38/42 collapse						

Şekil 3.12. Cuckoo Sandbox arayüzü

Analiz:

Windows, Linux, Mac OS X ve Android sanal ortamlarında zararlı web sitelerinin yanı sıra birçok farklı zararlı dosyayı (çalıştırılabilir dosyalar, ofis belgeleri, pdf dosyaları, e-postalar vb.) analiz etmenizi sağlamaktadır.

- API çağrılarını ve dosyanın genel davranışını izleyebilir hale getirmekte ve bunu herhangi bir kişi tarafından anlaşılabilir olan üst düzey bilgi ve imzalara dönüştürülmektedir.
- SSL / TLS ile şifrelenmiş olsa bile ağ trafiğini analiz edebilmenizi, yerel ağ yönlendirme desteğiyle, tüm trafiği kesebilir, InetSIM veya ağ arabirimi veya VPN aracılığıyla yönlendirebilirsiniz.
- Enfekte edilmiş sanallaştırılmış sistemin gelişmiş bellek analizini, Volatility ile birlikte YARA'yı kullanarak bir process memory parçacığı üzerinde çalışabilmektedir.

Cuckoo'nun açık kaynak niteliği ve kapsamlı modüler tasarımı sayesinde analiz ortamının, analiz sonuçlarının işlenmesinin ve raporlama aşamasının herhangi bir yönünü özelleştirebilirsiniz. Cuckoo, sandbox'ı istediğiniz framework'e istediğiniz şekilde, istediğiniz formata lisanslama gereklilikleri olmadan kolayca entegre etmek için tüm gereksinimleri sağlar.

Raporlama:

Cuckoo, Zararlı yazılım izleme sonuçları ve davranışlarının ayrıntılı açıklamalarını içeren büyük log dosyaları (örnek olarak ortalama 6 MB, ancak 100 MB'ye ulaşılabilir) oluşturur. Cuckoo kullanarak topladığımız veriler şunları içerir:

- API logları
- Network (Ağ) Logları
- Drop edilen dosyalar hakkında statik veriler
- Ekran görüntüleri
- Sistem manipülasyonu: Dosyalar / Kayıt / Mutex ler / Hizmetler
- Başlangıç processleri ve örneklerle ilişkileri

Bu bilgilerle, örnekleri davranışlarına göre sınıflandırmak mümkündür. Zararlı yazılım tanımlamaları oluşturmak ve zararlı yazılım bulaşmalarının çoğunu düzenlemek için de yeterli bilgi sağlamaktadır. [27]

3.3.6. stoQ – Analysis simplified



Şekil 3.13. stoQ logosu

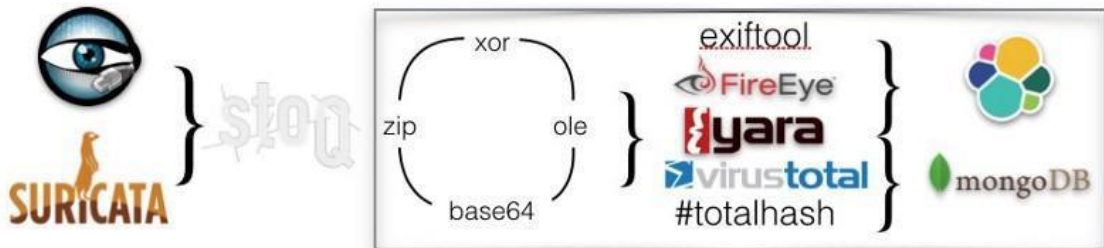
StoQ, bir analistin yapması gereken daha sıradan ve tekrar eden görevleri basitleştirmeye yardımcı olan bir otomasyon framework'üdür. Analistlerin ve DevSecOps takımlarının farklı veri kaynaklarından, veritabanlarından, decoder/encoderlardan ve diğer birçok görevden hızla geçiş yapmalarına olanak tanır. stoQ, bireysel güvenlik araştırmacıları için yeterince kullanışlıdır. Ayrıca kurumsal hazır ve ölçeklenebilir olacak şekilde tasarlanmıştır. [12]

➤ StoQ Nasıl Çalışır?

Temel olarak stoQ, bir analistin iş akışının (workflow) ortasında olacak şekilde yapılandırılmıştır.

➤ Ingestion Aşaması

stoQ verileri tek tek dosyalardan alabilir, yeni dosyaların olduğu bir diziyi izleyebilir, bir veritabanından veya bir API'den alabilir. Bu ölçekte stoQ'nun son derece güçlü olduğu yer burasıdır. HTTP veya e-posta gibi tehdit vektörlerinden dosya ayıklamak, otomatik zenginleştirme ve işleme için stoQ'a gönderilebilir. Suricata veya Bro dan dosya ayıklamanın işlemiyle birlikte stoQ'un bu dosyaları işlemesi için ayarlanabilmektedir. Tüm yürütülebilir dosyaları, PDF'leri veya Office Belgelerini gönderebilir daha yüksek riskli dosya türlerini otomatik olarak analiz etmeyi sağlar.



Şekil 3.14. stoQ iş akışı

➤ Zenginleştirme

XOR encoded içeriği otomatik olarak işleme özelliği veya base64 decode etmek için dekode eklentileri bulundurur. Arşivleri açma ve PDF belgelerini sadeleştirme gibi görevleri otomatikleştirilir. Carver eklentileri, Word Belgelerinde gömülü olan shell

kodu veya flash dosyaları gibi gizli yükleri ayıklamak için kullanılır. Bu zenginleştirilmiş nesneler daha sonra ek işleme için stoQ framework'üne geri gönderilir.

➤ İşleme

Bu süreç, stoQ'nun betiklerle (exiftool, TRiD, Yara, vb.) ve API'lerle (FireEye, VirusTotal, ThreatCrowd, vb.) Etkileşime girmesine ve nesnelerimizle ilgili daha fazla veri almasına izin verir.

➤ Export

StoQ bir nesneyi alıp, zenginleştirdikten ve işledikten sonra, sonuçlar depolama için bir Bağlayıcı (connector) eklentisine gönderilir. Bu, normal bir metin dosyası veya veri tabanı kadar basit veya birden fazla veri merkezine yayılmış birden fazla veri tabanı gibi karmaşık bir yapı olabilir.

Bu verileri ElasticSearch veya Splunk gibi bir şeyle kullanmak, stoQ'dan geçen nesneler için bize çok zengin bir meta veri kaynağı sağlayabilmektedir. Büyük ve ayrıntılı veri kümesi, çevrenizdeki daha büyük eğilimleri ve anomalileri bulmak için kullanılabilir. stoQ, bu meta verilerin tümü için sorguları ve uyarıları düzenlemenizi sağlar.

Artık kuruluşunuzdaki tüm yara isabetlerini arayabilir veya işlenmiş tüm dosya adlarını listeleyebilirsiniz.[28]

3.3.7. Forager



Şekil 3.15. Forager logosu

Tüm tehdit istihbaratı verilerini almak, saklamak ve düzenlemek için daha kolay bir yol olup olmadığını hiç merak ettiniz mi? Tüm tehdit istihbarat uygulamalarının "trilyonlarca veri noktasını korele eden" bir veri tabanı gerektirmediğini ve bunun yerine basit TXT dosyaları ile, diğer yayınlardan, PDF tehdit raporlarından veya diğer verilerden tehdit verilerini çekebilen basit bir araca ihtiyacınız varsa. Önceden

yapılandırılmış 15 tehdit beslemesiyle Forager açık kaynak bir çözüm oluşturuyor. [12][29]

Özellikler:

- Modüler feed fonksiyonlarını kullanarak URL lerden tehdit verilerini alma
- Domain, md5, sha1, sha256, IPv4 ve YARA göstergelerini ayıklama
- Mevcut intel setini tek bir IP ile veya bir IOC dosyasıyla arama
- Carbon Black tarafından kullanılması için JSON feed leri üretme
- Carbon Black için Basit HTTP JSON besleme sunucusu sağlama

Yukarıda anlatmaya çalıştığım çerçeveler ve platformlardan sadece yedisi bunlar gibi onlarcası veya yüzlercesi mevcuttur.

3.4. Araçlar (Tools)

Tehdit istihbaratının ayrıştırılması, yaratılması ve düzenlenmesi için her türlü araç. Çoğunlukla IOC tabanlı. [13]

3.4.1. AEngine

Aengine, herhangi bir insan müdahalesi olmadan öğrenme yeteneklerine sahip bir sonraki nesil etkileşimli veya programlanabilir. Python, Ruby, Java ve LUA paket denetim motorudur, NIDS (Network Intrusion Detection System - Ağ Saldırı Algılama Sistemi) İşlevselliği, DNS Domain sınıflandırması, ağ kolektörü, ağ adli tıp ve diğerleri. [13][30]

3.4.2. FENRIR

Florian Roth tarafından oluşturulan üç araçtan biridir. Fenrir, basit bir IOC (Indicator of Compromise) tarayıcı bash betiğidir. Aşağıdaki Uzlaşma Göstergeleri (IOC ler) için Linux/Unix/OSX sistemlerinin taramasına izin verir: [13]

- Hashes
MD5, SHA1 ve SHA256 (MD5SUM, SHA1SUM, SHA -A 256) kullanarak
- File Names (Dosya adlar)
String - tam yolun alt dizesinin kontrol edilmesi, örn. "/var/temp/p.exe" in "temp / p.exe"
- Strings

Dosyalarda GREP

- C2 Server

'lsf -i ' ve 'lsf -i -i' çıktısında C2 sunucu string'lerini kontrol etme

Florian Roth tarafından oluşturulan diğer araçlar ise; LOKI ve THOR (ücretsiz versiyon THOR Live)'dir.[31]

3.4.3. GOSINT

GOSINT çerçevesi (framework), yüksek kaliteli indicators of compromise (IOC ler) toplamak, işlemek ve ihraç etmek için kullanılan bir projedir. GOSINT, bir güvenlik analistinin yapılandırılmış ve yapılandırılmamış tehdit istihbaratını toplamasına ve standartlaştırmasına olanak tanır. Güvenlik operasyonlarına tehdit istihbaratı (threat intelligence) uygulamak, uyarı verilerini ek güven, bağlam ve birlikte olma ile zenginleştirir. Bu, benzer veya özdeş kötü niyetli davranış göstergelerini belirlemek için üçüncü taraflardan güvenlik olayı verilerine araştırma uyguladığınız anlamına gelir. Çerçeve (framework), Go'da bir JavaScript (frontend) ile yazılmıştır. [13][32]

3.4.4. Libtaxii

Bir Python Kütüphanesi Güvenilir Otomatik Gösterge Bilgisi Değişimi (TAXII™ - Trusted Automated eXchange of Indicator Information) v1.x Mesajları ve Taxii Services'i çağırıyor. [13][33]

3.4.5. Cuckoo Sandbox

Cuckoo Sandbox, otomatik bir dinamik malware (kötü amaçlı yazılım) analiz sistemidir. En iyi bilinen açık kaynaklı kötü amaçlı yazılım analiz sanal alanları etrafında ve araştırmacılar, CERT / SOC takımları ve dünyanın dört bir yanındaki tehdit istihbarat ekipleri tarafından sıkça konumlandırılmıştır. Birçok kuruluş için Cuckoo Sandbox, potansiyel kötü amaçlı yazılım örnekleri için bir ilk bakış açısı sağlar.

Cuckoo sandbox'tan keşfedilen davranışlara dayanan YARA kuralları oluşturmanıza olanak sağlar. Bu ortam malware (kötü amaçlı yazılım) yürütüldüğü için, çalışma zamanı string'leri ve beğenileri gibi belirli davranışlar hakkında kurallar oluşturabilirsiniz. [13][27]

3.4.6. LOKI

Florian Roth tarafından oluşturulan üç araçtan biridir. LOKI oluşturulan (created)/yazılmış (written) ücretsiz açık kaynaklı bir IOC (Indicator of Compromise) tarayıcısıdır. GitHub sayfasına göre, tespit 4 yöntemeye dayanmaktadır: [13]

1. File Name IOC Check - Dosya Adı IOC Kontrolü
2. Yara Rule Check (we are here) - Yara Kural Kontrolü (Biz Burdayız)
3. Hash Check - Hash kontrolü
4. C2 Back Connect Check - C2 arka bağlantı kontrolü

LOKI hem Windows hem de Linux sistemlerinde kullanılabilir. Windows kullanıcıları ikili dosyayı hem 32 bit hemde 64 bit sistemlerde çalışacak. Linux kullanıcıları LOKI dosyasını indirmek için aynı bağlantıyı kullanabilir. [34]

Yukarıda anlatmaya çalıştığım araçlar sadece altısı bunlar gibi onlarcası veya yüzlercesi mevcuttur.

3.5. Araştırma, Standartlar ve Kitaplar (Research, Standards & Books)

Tehdit istihbaratıyla ilgili her türlü okuma materyaller.

3.5.1. APT & Cyber Criminal Campaign Collection

Kapsamlı (tarihi) kampanya koleksiyonu. Girişler çeşitli kaynaklardan gelir. [14][35]

3.5.2. ATT&CK

Rakip Taktikler, Teknikler ve Ortak Bilgi (ATT&CK™), bir düşmanın bir kurumsal ağ içinde faaliyet gösterirken gerçekleştirebileceği eylemleri tanımlayan bir model ve çerçevedir. ATT&CK, bir ağa izinsiz giriş sırasında hangi eylemlerin görülebileceği konusunda daha fazla farkındalık sağlayan erişim sonrası teknikler için sürekli büyüyen ortak bir referanstır. [14]

MITRE nin CAPEC, STIX ve MAEC gibi ilgili yapılarla entegrasyon üzerinde aktif olarak çalışmaktadır. [36]

3.5.3. Siber Tehdit İstihbaratı İçin Kesin Kılavuz

Siber tehdit istihbaratının unsurlarını açıklar ve çeşitli insan ve teknoloji tüketicileri tarafından nasıl toplandığını, analiz edildiğini ve kullanıldığını tartışır. Ayrıca istihbaratın taktik, operasyonel ve stratejik düzeylerde siber güvenliği nasıl iyileştirebileceğini ve saldırıları daha erken durdurmasına, savunmanızı geliştirmenize ve tipik Dummies tarzında üst düzey yönetimle siber güvenlik sorunları hakkında daha verimli konuşmasına nasıl yardımcı olabileceğini inceler. [14][37]

3.5.4. Tehdit İstihbarat: Toplama, Analiz, Değerlendirme

MWR Info Security tarafından hazırlanan bu rapor, stratejik, taktiksel ve operasyonel varyasyonlar dahil olmak üzere birkaç farklı türde tehdit istihbaratını açıkça tanımlamaktadır. Ayrıca tehdit istihbaratının gereksinimleri ortaya çıkarma, toplama, analiz etme, üretme ve değerlendirme süreçlerini tartışır. Ayrıca, MWR Info Security tarafından tanımlanan tehdit istihbaratı türlerinin her biri için bazı hızlı kazanımlar ve bir olgunluk modeli de dahildir. [14][38]

Yukarıda anlatmaya çalıştığım araştırma, standartlar ve kitaplar sadece dört tanesi bunlar gibi onlarcası veya yüzlercesi mevcuttur.

4. Tehdit İstihbarat Platformları Karşılaştırma

Günümüzde tehdit istihbarat platformlarının birden fazla yazılım ve bu yazılımların özellikleri bakımından birbirinden farklılıkları vardır. Bu özellikleri kıyaslama yapmak için 3. Bölümde detaylı şekilde incelediğimiz yazılımları alt başlıkları ile ayrı ayrı tablolarıyla kıyaslamaya çalıştım.

4.1. Kaynaklar (Sources)

	Açık kaynak	Programlanabilir	Feed	Operasyonel	Taktiksel	Malware	Anonimlik
AbuseIPDB	✓	✓					
APT Groups and Operations	✓			✓	✓		
DigitalSide Thread-Intel	✓		✓			✓	
Disposable Email Domains		✓					✓
ExoneraTor							✓
FireHOL IP List			✓			✓	

Şekil 4.1. Tehdit istihbarat kaynakların karşılaştırması

Çeşitli kaynaklardan bilgi toplamak kullanılan araçlarını özelliklerini kıyaslaması için yukarıda oluşturulan bazı niteliklerde farklılıklar olduğunu göstermektedir. Açık kaynaklı olanlar içerikleri kamuya paylaşarak yeni amaçlara uygun biçimde değişiklikler yapılabilir. Programlanabilir nitelik uygun programlama dillerinde herhangi birinden özelleştirme yapılabilir. Feed (besleme) kendisinde bulunan kaynakların dışında farklı kaynaklardan destekleyerek kaynak havuzunu büyütebiliriz. Malware (kötü amaçlı yazılımlar) yazılımları destekleyerek özel verileri kaynak havuzuna yüklenebilir.

4.2. Formatlar (Formats)

	Dil mi?	Programları veya araçları destekleme	P2P	Operasyonellik	Tutarlılık & verimlilik	Malware
STIX	✓					
TAXII		✓	✓			
Cybox	✓			✓	✓	
MAEC	✓					✓
VERIS Framework	✓					

Şekil 4.2. Tehdit istihbarat formatların karşılaştırması

Bunlar çeşitli kaynaklardan toplanan büyük miktar verileri paylaşma veya taşıma işlevi için kullanan formatların özelliklerini kıyaslaması için yukarıda oluşturulan bazı niteliklerin farklılıklar olduğunu göstermektedir. İlk nitelik işaretli olanlar standart bir dile sahip olduğunu göstermektedir. P2P ise birden fazla ağ bilgilerini paylaşma özelliğine sahiptir.

4.3. Çerçeveler ve Platformlar (Frameworks and Platforms)

	Otomasyon	Açık kaynak	IOC	Yönetim sistemi	Veri toplama	TTP	YARA	Elastic Search
Abuse.IO	✓	✓						
CIF			✓	✓	✓			✓
MISP		✓	✓		✓			
YETI			✓			✓		
Cuckoo Sandbox		✓					✓	
stoQ	✓							✓
Forager					✓		✓	

Şekil 4.3. Tehdit istihbarat Çerçeveler ve platformların karşılaştırması

Toplanan verileri analiz edilmesini ve paylaşılmasını kolaylaştırmasını sağlayan framework'lar ve bazı platformların özelliklerini kıyaslaması için yukarıda oluşturulan bazı niteliklerin farklılar olduğunu göstermektedir. Otomasyon nitelikli işaretli olanlar bazı süreçleri seri şekilde otomatik gerçekleştiriyor. Açık kaynaklı olanlar içerikleri kamuya paylaşılan ve yeni amaçlara uygun biçimde değişiklikler yapılabilir. IOC işaretliler daha önce de meydana gelen güvenlik ihlallerine ilişkili kanıtlar eşleştirmesi. YARA kurallı işaretliler dosyaları ve programları malware olup olmadığını kontrol etme özelliklerine sahip olduğunu belirtmektedirler.

4.4. Araçlar (Tools)

	IOC	Program- lanabilir	Saldırı Algılama	Ücretli	YARA Check	Hash Check
AIEngine	✓	✓	✓			
FENRIR	✓			✓		
GOSINT	✓					
Libtaxii						
LOKI	✓				✓	✓

Şekil 4.4. Tehdit istihbarat araçların karşılaştırması

Çoğunlukla IOC tabanlı olan araçların işleri daha seri bir halle gerçekleştirip ayrıştırılması, yaratılması ve düzenlenmesi için her türlü araçların özelliklerini kıyaslama için yukarıdaki tablo oluşturmuştur.

5. SONUÇLAR VE ÖNERİLER

Genel olarak özetleyecek olursak, günümüzde neredeyse sanide bir dünyada farklı yerlerinde çeşitli siber saldırı ve tehditler gerçekleştirmektedir. Bu siber ekosistemi gün geçtikçe hızla büyüyen, gelişen ve daha fazla karmaşık hale gelmekte olan saldırı önceden gerekli önlemleri almak için tüm tehditlere yönelik istihbarat bilgilerinin toplanması ve bunları analiz edilerek sınıflandırılması ve gerçekleşmesi halinde ise tespit edilmesi için önemli rol oynamaktadır.

5.1. Tehdit İstihbarat Kavramları

İstihbarat, ulaşılabilen açık, yarı açık ve gizli kaynaklardan elde edilen bilginin, ulusal güvenliği tehdit edecek unsurlara karşı koruma sağlamak amacıyla yahut politika yapıcılarının, ulus menfaatlerini olumlu şekilde etkileyecek kararların alınması hususunda ihtiyaç duyduğu bilgilerin elde edilip, doğruluğuna göre sınıflandırılması, karşılaştırılması, analiz edilmesi süreci sonucunda ulaşılan bilgidir. Siber istihbarat ise bu sınıflandırılmaların siber uzay üzerinden toplanan istihbarat bilgilerine denilmektedir.

Siber tehdit, kötü niyetli kişi veya oluşumların, kontrol sistemi cihazlarına veya şebekesine yetkisiz erişim teşebbüsünde bulunması, ağ yapısını bozması veya kullanılamaz hale getirmesidir. Siber tehditler çeşitli yerlerden, insanlardan, kurum veya kuruluşlardan kaynaklanabilir. Bu duruma başlıca örnekler:

- Hackerler
- Teröristler
- Ticari rakipler
- Casuslar
- Devletler ve istihbarat kurumları
- Mutsuz çalışanlar
- Organize suç grupları

Yukarıda bahsedilen siber tehdit kaynaklarının, zarar vermek amacıyla gerçekleştirebilirler. Bu tür saldırganlara, kurbanlarına saldırı gerçekleştirirken farklı türlerden çeşitli senaryolar kurabilirler. Siber tehditlere birkaç örnek vermek gerekirse;

- **Malware;** Zararlı yazılım
- **Spyware;** Casus yazılımlar
- **Malvertising;** Reklamlara gömülmüş zararlı yazılımlar

- **Man in the Middle (MiTM);** Ortadaki Adam saldırıları
- **Wiper Attacks;** Bulaştığı sistemde her şeyi geri getirilemeyecek şekilde silen zararlı yazılımlar
- **Distributed Denial of Service (DDoS);** Servis dışı bırakma saldırıları
- **Ransomware;** Fidyeye amaçlı zararlı yazılım
- **Botnet;** Ele geçirilmiş (zombi) bilgisayarlar üzerinden yapılan saldırılar, çoğunlukla DDoS amacıyla kullanılırlar
- **Trojan;** Truva atı denmektedir, bilgisayarın erişimini uzaktan sağlayan zararlı yazılımlardır
- **Phishing;** Oltalama saldırıları
- **Data Breaches;** Veri sızıntıları
- **Worm;** Solucanlar
- **Keylogger;** Klavye işlemlerini Kaydeden zararlı yazılım
- **Backdoor;** Sisteme tekrar (sessizce) erişmeyi sağlayan arka kapı yazılımı
- **Advanced Persistent Threats;** Hedef odaklı saldırılar
- ...

Siber tehdit istihbaratı ise toplanan verilerin analizinden sonra saldırganların düşüncelerini, amaçlarını, motivasyonlarını, yöntem ve metotlarını tespit etmek amacı taşır. Siber tehdit istihbaratı, seviyelerine göre üç gruba ayrılmaktadır. Bunlar; Stratejik istihbarat, Operasyonel istihbarat ve Taktiksel istihbarattır.

5.2. Siber Tehdit İstihbaratı Faydaları Nelerdir?

Ponemon Enstitüsü tarafından 2015 yılının yapılan bir ankete göre; Şirketlerin %40'ında son 24 ayda maddi bir güvenlik ihlali yaşanmıştır ve ihlallerin %80'ninin, tehdit istihbaratı ile engellenebileceği ya da hasarı en aza indirebileceği tespit edilmiştir. Katılımcıların sadece %36'sı şirketlerinin savunmasını güçlü olarak değerlendirmiştir. Katılımcıların neredeyse yarısı bir saldırının sonuçlarını önlemek veya azaltmak için aldıkları istihbarat verilerini artırmaktadır. Bu kurumlar ortalama olarak haftada 16937 alarm almaktadır. Alarmların sadece 3218'i (%19) güvenilir olarak değerlendirilmiştir. Alarmların sadece 705'i (%4) araştırılabilmiştir. Yanlış uyarılara karşılık yılda 1.27 milyon dolar harcadığı belirlenmiştir.

Bu bahsedilen problemler doğru siber tehdit istihbaratı yöntemleri ile minimuma indirgenebilir.

Siber tehdit istihbaratı, olası tehditler hakkında farkındalık kazandırılması amacı taşımaktadır. Kurum içi istenmeyen olaylara gerçekleşmeden önce müdahale edilmesi için gerekli bir alandır. Bu şekilde güvenlik çözümleri en üst seviyeye çıkarılmış ve gerekli önlemler alınmış olur. Siber tehdit istihbaratının faydaları arasında; veri kaybını önleme, veri ihlallerini tespit etme, olay yanıtı, tehdit analizi, veri analizi, tehdit istihbarat paylaşımı sayılabilir.

5.3. Siber Bir Tehdittin Öncesi, Saldırı Anı Ve Sonrası

Siber bir tehdittin olmadan öncesinde yapılabilecek en iyi savunma, tehditlerin gerçekleşmesine izin vermemektir. Bunu yapmak için bazı önemlerin alınması hayati nitelik taşımaktadır. Saldırı gerçekleşmeden önce dikkat edilmesi gereken kritik noktaların BT altyapıları belirli prosedürlere tabi tutulmalıdır. Farklı felaket senaryolarını için plan oluşturulmalıdır. Hangi programlar, sunucular, işlemler, veri tabanları devre dışı kalması halinde yapılan işin devam edilmesine engel oluşturuyorsa, bunlar kritik varlıklardır. Bu varlıkların sistemlerin tanınması ve korumak için gerekli adımların atılmış olması gerekmektedir. Kurumlarda çalışanların olası saldırı anında bilinçli hareket etmeleri için düzenli ve belirli periyotlar ile güncel eğitimler verilmelidir.

Siber bir tehdittin (yani olay) sırasında kurumların yeterli olduğunu düşündüğü tüm önlemleri almış olsa bile, bir siber saldırının gerçekleşmesine engel olamamış olabilir. Bu kritik durumda soğukkanlılıkla uzman ekip ile gerçekleşen olay gerçek bir tehdit mi yoksa kurum içinde yapılan bir işlemin saldırı şeklinde algılanması mı olduğuna cevabın belirlemelidir. Eğer ki kurum dışından gerçek bir tehdit olduğu kesinleşirse daha önce hazırlanan planlardaki adımları devreye sokulur.

Siber bir tehditten sonrasında etkilenen sistemleri izlenmeli ve yaşanan deneyimden çıkarılan olumlu olumsuz davranışlar, kontroller, müdahaleler göz önünde bulundurularak var olan sistem güçlendirilmelidir. Saldırganlar girdikleri sistemlerde arka kapılar (backdoors) bırakmış olabilirler. Bu nedenle etkilenen sistemlerin gözetim altında tutulması ve gerekli testlerin yapılması gerekmektedir.

5.4. Öneriler

Sistemlere veya kurumlara yapan tehdit önceden algılaması için diğer bölümlerde bazı yazılımlar bahsetmeye çalıştım. Yazılımların özelliklerin birbirlerinde bazı noktalarda farklılıkları görünmektedir. Burada zaman açısından oranda zaman kayıp oluşturmaktadır. Bu konuda öneri farklı özelliklerinin ve farklı yapıları birleştirerek daha güçlü tehdit algılama sistemi yapılabilir.

KAYNAKLAR

- [1] Siber tehdit istihbarat nedir - blog rehber
<https://securityscorecard.com/blog/what-is-cyber-threat-intelligence-3-types-and-examples>
- [2] Siber tehdit istihbarat yaşam döngüsü - blog 1
<https://www.flashpoint-intel.com/blog/threat-intelligence-lifecycle/#!>
- [3] Siber tehdit istihbarat yaşam döngüsü - blog 2
<https://securityscorecard.com/blog/threat-intelligence-lifecycle-guide>
- [4] Tehdit istihbarat türleri (The Types of Threat Intelligence) genel anlatım
<https://www.recordedfuture.com/threat-intelligence/>
- [5] Stratejik Tehdit İstihbaratı (Strategic Threat Intelligence) - Kaynak
<https://www.recordedfuture.com/strategic-threat-intelligence/>
- [6] Taktik Tehdit İstihbaratı (Tactical Threat Intelligence) - Kaynak, Tehdit Aktörlerinin TTP'lerini ayırt etme
<https://www.recordedfuture.com/tactical-threat-intelligence/>
- [7] Operasyonel Tehdit İstihbaratı (Operational Threat Intelligence) - Kaynak, Engeller
<https://www.recordedfuture.com/operational-threat-intelligence/>
- [8] Tehdit İstihbarat Platform (Threat Intelligence Platform) – website
<https://www.anomali.com/resources/what-is-a-tip>
- [9] Tehdit İstihbarat Platform (Threat Intelligence Platform) – github
<https://github.com/hslatman/awesome-threat-intelligence#>
- [10] Kaynak
<https://github.com/hslatman/awesome-threat-intelligence#sources>
- [11] Format
<https://github.com/hslatman/awesome-threat-intelligence#formats>
- [12] Çerçeveler ve platformlar
<https://github.com/hslatman/awesome-threat-intelligence#frameworks-and-platforms>
BGA Bilgi Güvenlik A.Ş. – PDF : Açık kaynak kodlu siber tehdit istihbaratı çözümleri.pdf
- [13] Araçlar
<https://github.com/hslatman/awesome-threat-intelligence#tools>
- [14] Araştırma, Standartlar ve Kitaplar
<https://github.com/hslatman/awesome-threat-intelligence#research>
- [15] OSINT Framework yapısı
<https://osintframework.com/>
- [16] AbuseIPDB
<https://www.abuseipdb.com/>
<https://pypi.org/project/abuseipdb/>
- [17] APT Groups and Operations
https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpwaa4O_Son4Gx0Y0IzlcBWMsdvePFX68EKU/pubhtml#
<https://github.com/kbandla/APTnotes>
- [18] DigitalSide Thread-Intel
<https://osint.digitalside.it/>
<https://github.com/davidonzo/Threat-Intel/>
- [19] Disposable Email Domains
<https://github.com/martenson/disposable-email-domains>

- [20] FireHOL IP List
<https://iplists.firehol.org/>
- [21] STIX/TAXII
<https://oasis-open.github.io/cti-documentation/>
- [22] MAEC
<https://maecproject.github.io/>
- [23] VERIS Framework
<http://veriscommunity.net/index.html>
- [24] Abuse.IO
<https://abuse.io/>
<https://github.com/AbuseIO/AbuseIO>
<https://abuse.io/blog/>
www.shadowserver.org
www.spamcop.net
www.ip-echelon.com
www.blocklist.de
www.junkemailfilter.com
safebrowsingalerts.googlelabs.com
www.projecthoneypot.org
<http://www.clean-mx.de>
<https://www.c-sirt.org>
<http://www.netcraft.com/>
<https://www.spamexperts.com>
<https://www.abuseinformationexchange.nl/>
<http://www.woody.ch/>
<https://www.webiron.com/>
<http://www.cegtek.com/>
<http://www.juno.com/>
- [25] CIF
<http://csirtgadgets.org/>
<https://github.com/csirtgadgets/massive-octo-spice>
- [26] MISP Threat Sharing
<http://www.misp-project.org/>
<https://github.com/MISP>
<http://www.misp-project.org/communities/>
- [27] Cuckoo Sandbox
<https://cuckoosandbox.org/>
<https://github.com/cuckoosandbox>
<https://cuckoo.sh/docs/>
- [28] stoQ
<https://stoq.punchcyber.com/>
<https://github.com/PUNCH-Cyber/stoq>
<https://medium.com/stoq>
- [29] Forager
<https://github.com/opensourcesec/Forager>
- [30] AIEngine
<https://bitbucket.org/camp0/aiengine>
- [31] FENRIR
<https://github.com/Neo23x0/Fenrir>

- [32] GOSINT
<https://github.com/ciscocsirt/gosint>
- [33] Libtaxii
<https://github.com/TAXIIPROJECT/libtaxii/>
<https://libtaxii.readthedocs.io/>
<https://taxiiproject.github.io/>
<https://pypi.python.org/pypi/libtaxii/>
- [34] LOKI
<https://github.com/Neo23x0/Loki/releases>
- [35] APT & Cyber Criminal Campaign Collection
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
- [36] ATT&CK
https://attack.mitre.org/wiki/Main_Page
- [37] Siber Tehdit İstihbaratı için kesin Kılavuz
<https://cryptome.org/2015/09/cti-guide.pdf>
- [38] Tehdit İstihbarat: Toplama, Analiz, Değerlendirme
<https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf>