



# **SOME ve SOC AÇIK KAYNAK ÇÖZÜMLER**

**Yazar:** Samet Sazak – Uygur Köroğlu

**Baskı:** 2018

# İÇİNDEKİLER

Cyber Security Operation Center (C-SOC) Nedir?.....	3
1- MISP (Zararlı yazılım bilgi paylaşma platformu) .....	5
2- The Hive Projesi .....	6
The Hive; İş Birliği Yapmak:.....	6
The Hive; Detaylandırma .....	7
The Hive; Analiz.....	7
3- Yeti Projesi.....	8
Yeti Kullanım Alanları .....	9
4- Fame-FIR Framework .....	10
Fame Tehdit İstihbaratından Yararlanmak.....	11
FIR (Fast Incident Response) Projesi .....	12
5- Cortex Projesi .....	13
6- GOSINT Framework.....	14
7- Collective Intelligence Framework.....	15
8- Cyphon Projesi .....	16
Cyphon Çalışma Mimarisi .....	16
Cylops Arayüzü.....	17
9- RTIR Projesi (Request Tracker).....	18
RT; Email Entegrasyonu: .....	18
RT; Özel Çalışma Alanları: .....	19
10- Apache Metron .....	20
Metron'a ait bazı özellikler: .....	21
Metron Dashboard .....	21
Metron Mimarisi .....	22

## Cyber Security Operation Center (C-SOC) Nedir?

Güvenlik operasyonları merkezi (SOC), bir kuruluşun güvenlik durumunu sürekli olarak izlemek, analiz etmek ve geliştirmekle sorumlu bilgi güvenliği ekibidir. SOC ekibinin amacı, teknolojik çözümleri ve güçlü bir süreç yönetimi kullanarak siber güvenlik vakalarını tespit etmek, analiz etmek ve bunlara tepki vermektir. Güvenlik operasyon merkezlerinde genellikle siber güvenlik analistleri, mühendisleri ve oluşan tüm süreçleri denetleyen yöneticiler bulunur. SOC personeli, güvenlik sorunlarının keşfedildiğinde hızla ele alınmasını sağlamak için organize bir şekilde olay müdahale (incident response) ekipleriyle yakın çalışırlar.

SOC analistleri, artmakta olan siber güvenlik tehditleri, sürekli uyarı yorgunluğu ve SOC'leri yetersiz bırakan endüstriyel sorunlar sebebiyle sürekli olarak yıpranmaktadır. Hem rutin hem de karmaşık görevlerin otomasyonu, hem analistin zamanını artırmakta hem de olaya müdahale sürecini hızlandırmaktadır. Her geçen gün saldırganlar daha hızlı ve daha güçlü hale geldiğinden, siber güvenlik sektörünün liderleri "otomasyonunun" günümüzün siber tehdit ortamında bir zorunluluk olduğunu anlamaktadır.

Etkili bir siber güvenlik operasyon merkezi (C-SOC) oluşturmak için kaynaklar iletişimini "geliştiren" ve "verimliliği" artıracak şekilde organize etmeyi gerektirmektedir. SOC'nin üç temel işlevini organize etmek için gerekli üç etken: insan, süreç ve teknolojidir.

### İnsan:

Birçok organizasyon, mevcut güvenlik işlevlerini gerçekleştiren çalışanlara ve ilgilenen diğer kişilere resmi eğitim programları sağlayarak, kendi SOC'lerini kendi kaynakları ile kurmayı tercih etmektedir. Diğerleri kurum içi ve dışı kaynakların karma bir karışımını yapmaktadır. Sizin için en doğru seçenek; mevcut kurum içi kaynaklara, bütçenize ve karşılaştığınız tehditlerin aciliyetine bağlı olmaktadır. Güçlü bir güvenlik operasyonları ekibi oluşturmaya başlamak için mevcut personelinizin envanterini çıkartmak önemlidir. Sorulması gereken bazı iyi sorular şunlardır:

- Kurum içerisinde siber güvenlik amaçlı çalışanlar kimlerdir?
- Bilgi teknolojileri alanından kimseler güvenlik amaçlı çalışmaya hazır mıdır?
- Siber güvenlik amaçlı dışarıdan insan kaynağı ihtiyacı var mıdır?
- Kurum içerisinde kaç kişi (diğer çalışanlara göre) SOC ekibinin bir parçası olacak organizasyonda bulunmuştur?
- İşe alma planı ve bütçesi nedir?
- Yıllık toplam siber güvenlik bütçesi nedir? SOC'nin uygulanmasını desteklemek için BT veya diğer departmanlardan daha fazla bütçe çekebilir miyiz?
- Güvenlik ağı noktaları bizi ne kadar etkilemektedir ve onlara yönelik olarak SOC'yi ne kadar erken inşa edebiliriz?

Bu temel sorular güçlü bir SOC oluşturmak için insan kaynağını anlamak açısından yardımcı olabilmektedir.

## [SOME ve SOC EKİPLERİ İÇİN AÇIK KAYNAK ÇÖZÜMLER]

### Süreç:

Bir SOC oluşturulmadan önce, genellikle güvenlik işleri, darmadağın haldedir ve elden ele iletilen işlerdir. Kimin hangi işle uğraştığı, sorunların nasıl çözüldüğü ve belgelendiği düzenli bir süreç içerisinde geçmemektedir. Daha resmi ve merkezileştirilmiş bir organizasyon oluşturmaya başlarken, mevcut prosedürlere şu şekilde sorular sorarak değerlendirmek iyi bir fikir olmaktadır:

- Siber tehditleri kim izliyor?
- Siber güvenlik olaylarını atayan çalışanlar kimlerdir?
- Siber güvenlik olaylarını düzeltmekten kim sorumludur?
- Mevcut işlemler belgelenmiş midir?

Bu soruların yanıtları, işlerin nerede durduğunu bilmenize yardımcı olabilir, böylece güvenlik operasyonlarını optimize etmek için bir plan oluşturabilirsiniz. Bir SOC ile süreçteki her adımın daha büyük bir stratejinin parçası olmasını sağlayarak, işlem başladığından itibaren olay yönetimi iş akışları oluşturulmalıdır. İş akışları, her bir takım üyesinin rolü ve sorumlulukları etrafında netlik sunmaya yardımcı olur, böylece hiçbir taş devrilmez.

### Teknoloji:

Birçok kurum ağlarında görünürlük stratejisini ve olaylara tepkisini destekleyecek, bütçesine uyan teknoloji araçları istemektedir. Kuruluşunuz için seçtiğiniz teknolojilerin aşağıdakilere uyması gerekmektedir:

- İçinde bulunduğunuz ortam (bulut(cloud), kurum içi (dedicated) veya ikisi birlikte) nedir?
- Karşılaştığınız siber tehdit türleri (kötü amaçlı yazılım, kimlik avı, vb.) nelerdir?
- Uyumluluğun yerine getirilmesi için zorunlu olduğunuz şartlar (HIPAA, SOC2, ISO 27001 vb) nelerdir?

SOC'nizin teknolojisi geliştirildiğinde, kapsama alanında herhangi bir boşluk bulunup bulunmadığını veya zaten sahip olduğunuz araçlarla işlevsellikte çakıştığını da belirleme fırsatı bulabilirsiniz. Örneğin, güvenlik izlemesi yapan üç araç olabilir, ancak hiçbirisi zararlı yazılımlara karşı koruma sağlamaz. Bu tarz durumları tespit etmeniz oldukça önemli olmaktadır.

Bu blog yazısında, Olay Müdahale sürecinizi iyileştirmenize ve siber saldırılar karşısında SOC ekiplerinin tepki ve otomasyon ihtiyaçlarına yardımcı olacak açık kaynak kodlu veya ücretsiz kullanılabilecek araçları tanıtmaya çalışacağız.

## 1- MISP (Zararlı yazılım bilgi paylaşma platformu)

MISP (Zararlı yazılım bilgi paylaşım platformu) siber tehdit istihbaratının paylaşımına yardımcı olan ücretsiz ve açık kaynaklı bir yazılımdır.

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.

### OSINT - CVE-2015-2545: overview of current threats

The screenshot displays the MISP Threat Sharing interface. On the left, a table lists event details for CVE-2015-2545, including Event ID (3865), Julid (57480963-76dc-4272-8116-4ea302de0b81), Org (CIRCL), Owner org (CIRCL), Contributors (CIRCL), Email (alexandre.dulaunoy@circl.lu), Tags (tip:white, circl-osint-feed, Type:OSINT, estimative-language:likelihood-probability-very-likely), Date (2016-05-25), Threat Level (Medium), Analysis (Completed), Distribution (All communities), Info (OSINT - CVE-2015-2545: overview of current threats), Published (Yes), and Sightings (0). Below this table is a list of events with columns for Expanded, Events, Tag, and Action. The first event has a tag 'estimative-language:likelihood-probability-almost-no-chance' and the second has 'estimative-language:likelihood-probability-very-unlikely'. On the right, a 'Related Event' section shows a list of related events with dates and counts. Below this, a network diagram shows connections between various entities, including 'webcancheck.myfw.us', 'be35b7882469ae4d9de233f75e7beb7211f9dc2c878694479a3e5872a4e78542', and 'reg.finet.org'.

Bu platform kurum ve kuruluşların zararlı yazılım tehdit göstergeleri (IOC) hakkında bilgi paylaşımlarını sağlar. MISP kullanıcıları, zararlı yazılımlar (malware) veya tehditler hakkındaki "iş birliğine" 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 gönderebilmektedir. MISP platformunun temel hedefi tehdit bilgilerini açığa çıkarmayı, olgunlaştırabilmeyi ve istismar edilmesini önleyen sorunsuz bir operasyon sağlayan sağlam bir platform olmaktır.

Web sayfası: <http://www.misp-project.org/>

Github: <https://github.com/MISP>

Topluluk: <http://www.misp-project.org/communities/>

## 2- The Hive Projesi

The Hive, açık kaynak kodlu, siber olay müdahale ekiplerinin işlerini hızlıca halledebilmesi için tasarlanmış, ölçeklenebilir ve ücretsiz bir olay müdahale platformudur.

Bir siber vakayı araştırırken takım çalışması kullanmak, olay müdahale işlerinin kalitesini büyük ölçüde artırmaktadır. TheHive'in tasarımcıları, takımların birlikte çalışmasına ve zamanında soruşturma yapabilmesi için iş birliği yapmalarına odaklanan ayrıntılı bir analiz ve SOC düzenleme platformudur. Her bir soruşturma süreci, bir veya daha fazla göreve bölünebilen bir olaylara (case) karşılık gelir. Bu görevler güvenlik operasyon analistlere atanır ve daha sonra bunları eş zamanlı olarak araştırmaları istenir.

TheHive ayrıca, analistlerin vakalar oluşturmalarına ve e-posta veya SIEM gibi farklı kaynaklardan uyarılar göndermesine olanak tanıyan bir Python API istemcisine sahiptir. TheHive Project tarafından yapılan ek yardımcı araçlar toplu analiz yapabilmek için bir otomasyon aracı olan Cortex ve bir tehdit istihbaratı besleme (feed) toplayıcısı olan Hippocampe aracını geliştirmektedirler.

### The Hive; İş Birliği Yapmak:

İş birliği TheHive'in kalbindedir. Birden fazla analist aynı anda aynı vakayı çalıştırabilir. Örneğin, bir analist zararlı yazılım analizini ele alabilirken, bir başkası IOC'ler ile çalışabilmektedir. Örneğin bir Komuta&Kontrol sunucusu ekip arkadaşlarınca eklendikten hemen sonra etkinliğin proxy logları üzerinde çalışılabilir. TheHive'in canlı akışını kullanarak, herkes gerçek zamanlı olarak platformda neler olduğunu gözlemleyebilmektedir.

The screenshot displays the TheHive web interface. The top navigation bar includes links for 'New Case', 'My tasks', 'Waiting tasks', 'Alerts', and 'Statistics'. A search bar is present on the right. The main content area shows a 'List of cases (11 of 26)' with a table of cases. The table has columns for 'Title', 'Severity', 'Tasks', 'Observables', 'Assignee', and 'Date'. The first case is '#19 - [MISP] #3150 OSINT - Sofacy's 'Komplex' OS X Trojan by Palo Alto networks'. The right sidebar shows a detailed view of a case, including a 'test case' section with a 'status: Resolved' and a 'summary: blah'. The sidebar also shows a list of alerts and updates.

(Olayların bulunduğu bir listeden oluşan ekran görüntüsü)

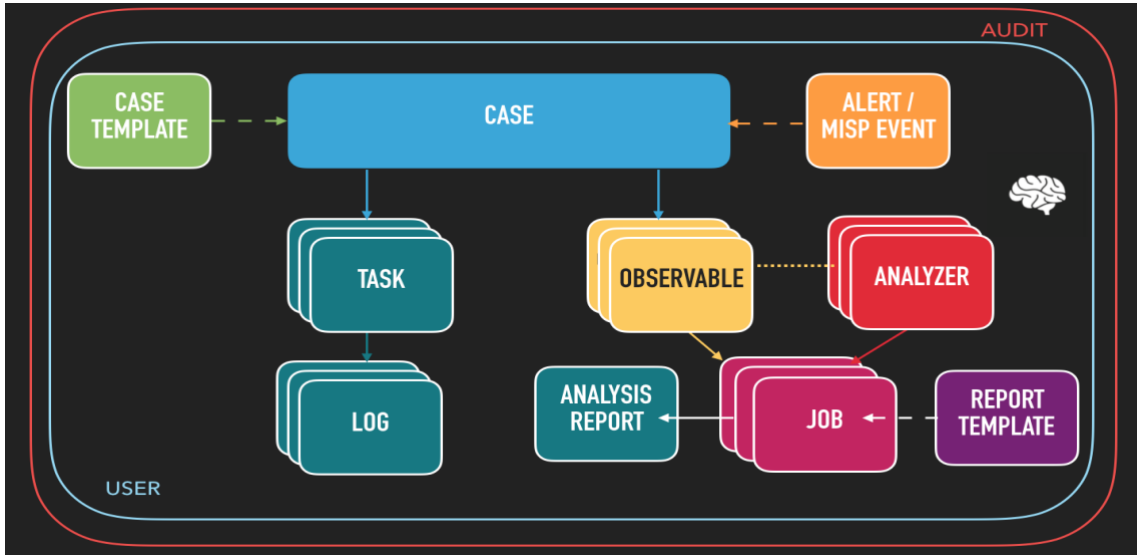
## The Hive; Detaylandırma

TheHive projesinde her soruşturma bir olaya karşılık gelir. Durumlar, MISP (Malware Information Sharing Platform) olaylarından, SIEM uyarılarından, e-posta raporlarından ve diğer kayda değer herhangi bir güvenlik olayından oluşturulabilir.

Her vaka bir veya daha fazla göreve ayrılabilir. Analistler, vaka oluşturulduğunda aynı görevleri eklemek yerine, TheHive'in şablon motorunu kullanarak onları bir kez ve herkes için oluşturabilirler. Durum şablonları, takımın etkinliğini artırmak, önemli zaman alan soruşturmanın tipini belirlemek ve sıkıcı görevleri otomatikleştirmek için metrikleri belirli vaka türleriyle ilişkilendirmek için kullanılabilir. Her görev belirli bir analiste atanabilir.

Ekip üyeleri bir görevin başkalarının onlara atanmasını beklemeden de işlem yapabilmektedir. Görevler, analistlerin, görevin ne olduğunu, sonuçlar, kanıtlar veya kayda değer dosyaları eklemeleri gibi bir olayı tanımlamak için katkıda bulunabilecek çok sayıda çalışma içerebilmektedir. Bunların dışında kayıtlar, zengin bir metin editörü veya Markdown kullanılarak yazılabilmektedir ve bu durum yazı işleri için oldukça avantajlıdır.

## The Hive; Analiz



TheHive'in Python API istemcisi TheHive4py sayesinde, SIEM uyarıları, kimlik avı ve diğer şüpheli e-postalar ve bunun gibi diğer güvenlik olaylarını eklemek mümkün olmaktadır. Bütün uyarıları ana panelde güncellenmiş olarak görüntülenebilmektedir.

Web sitesi: <https://thehive-project.org/>

Github: <https://github.com/CERT-BDF/TheHive>

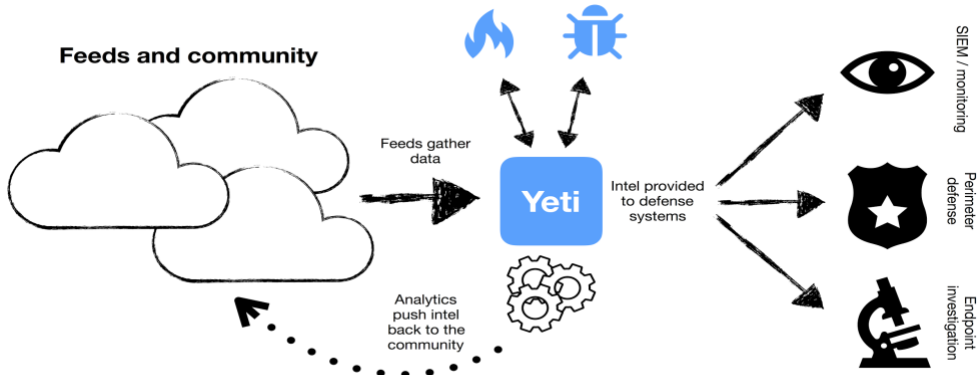
Topluluk: <https://groups.google.com/a/thehive-project.org/forum/#!forum/users>

### 3- Yeti Projesi



Yeti, tehdit göstergelerini (indicator of compromise), teknik, taktik ve prosedürler (TTP) hakkındaki bilgileri tek birleşik bir depoda organize etmeyi amaçlayan bir platformdur. Yeti, tehdit göstergelerini (IOC) otomatik olarak zenginleştirebilme 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. Bir

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 işleyebilmektedir. 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.





## [SOME ve SOC EKİPLERİ İÇİN AÇIK KAYNAK ÇÖZÜMLER]

Yeti üzerine eklenen tüm bu verileri hızlıca listeyelebilir, 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 tehdit istihbaratını SIEM gibi yazılımlar üzerine aktarmakla uğraşmaktan kurtarmaktadır.

### Yeti Kullanım Alanları

Örneğin zararlı yazılımları tespit edebilmek için bir sandbox sisteminiz var ve yeni bir bankacılık zararlısı tespit ettiniz. Bu zararlı yazılım çaldığı verileri depolamak için kullanıcının "Roaming" dizininde başka bir alt dizin kullandığını anladınız. Bunu belgelemek istersiniz, böylece başka bir analist bu davranışı gördüğünde bunun bir bankaları hedefleyen bir zararlı yazılım davranışı olduğunu kolayca anlayabilmektedir.

The screenshot shows the 'New Malware' form in the YETI application. The form is located at `localhost:5000/entity/new/malware`. The interface includes a navigation bar with 'YETI', 'Observables', 'Indicators', 'Entities', 'New', and 'Investigations'. The 'New' dropdown is active. The form fields are: 'Name' (Dridex), 'Family' (Banker), 'Tags that will link to this entity' (dridex), 'Bind to entities' (empty), and 'Aliases' (empty). The 'Description' field is a rich text editor with a toolbar and a placeholder text: 'Short description for the **Dridex** malware. You can use markdown here.' The bottom right corner shows 'Autosaved: 10:55 am', 'lines: 1', 'words: 11', and '0:72'. A 'Save' button is at the bottom left.

Web sitesi: <https://yeti-platform.github.io/yeti-ecosystem>

Github: <https://github.com/yeti-platform/yeti>

Topluluk: <https://yeti-platform.github.io/community>

## 4- Fame-FIR Framework

FAME, uçtan uca (end-to-end) analizi hızlandırmak ve otomatikleştirmek için mümkün olduğunca çok bilgi kullanan ve zararlı yazılımlar ile ilgili dosyaların analizini kolaylaştırmak amacı ile geliştirilmiş açık kaynak zararlı yazılım analiz platformudur.

Fame projesi, zararlı yazılım analizi alanında uğraşan ekiplerin ana problemlerini çözmek üzerine tasarlanmıştır.

Bir zararlı yazılım analizini tamamlamak oldukça fazla zaman almaktadır, örneğin spam emailler ile dağıtılan bir bankacılık zararlısını ele aldığımızda analist bu zararlı yazılımı dağıtılan spam mailler sayesinde tanımış bile olsa kimin ve nasıl hedef aldığını öğrenmek için elde edilen örneği sanal bir makineye yüklemesi, analiz sonucunu beklemesi, belleğin imajını alması ve bu belleğin analizini yapması, tersine mühendislik gibi oldukça zorlu süreçleri tamamlaması gerekmektedir. Ayrıca her analist farklı sorunları farklı bir şekilde çözebilir.

Fame, bir framework olarak bu sorunları ele almaktadır ve çözüm oluşturulmuş modülleri zincir gibi kullanarak uçtan uca analiz yapmaktadır. Örneğin, bir analist bir zararlı yazılım örneği gönderecek, birkaç dakika bekleyecek ve FAME malware ailesini tanımlayacak, yapılandırmasını çıkartacak ve malware'in kuruluşunu nasıl hedeflediğini tespit edebilecektir.

Fame, modüller olarak Python sınıflarını (class) kullanmaktadır. Bu yönden de oldukça avantajlı, kolay yazılabilir ve anlaşılabilir bir Syntax'e sahiptir.

```
from fame.core.module import ProcessingModule

class DummyModule(ProcessingModule):
    name = "dummy"
    description = "Does nothing. Give me something useful to do!"

    def each(self, target):
        # Do something usefull

    return True
```

## [SOME ve SOC EKİPLERİ İÇİN AÇIK KAYNAK ÇÖZÜMLER]

**Office Macros**  
Detailed Results

- Auto\_Open: Runs when the Excel Workbook is opened
- Base64 Strings: Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
- Hex Strings: Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
- Shell: May run an executable file or a system command
- Invoke-Expression: May run PowerShell commands
- Lib: May run code from a DLL
- cmd.exe: Executable file name

**MACROS**

```
Attribute VB_Name = "ThisWorkbook"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True

Attribute VB_Name = "Sheet1"
Attribute VB_Base = "0{00020820-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
```

## Fame Tehdit İstihbaratından Yararlanmak

Fame üzerindeki tehdit istihbaratı modülleri, analizinizi tehdit istihbaratı platformlarınızdaki etiketler ve göstergelerle zenginleştirmek için FAME tarafından otomatik olarak kullanılmaktadır.

Örneğin,

Observables		
Network & Host		
VALUE	SOURCES	TAGS
http://api.ipify.org/	cuckoo	downloader   hancitor   ipcheck
http://gunomehad.com/is5/gate.php	cuckoo	Hancitor C&C
http://Zx2strategies.com/wp-content/plugins/wpshore-breadcrumb/pm.dll	cuckoo	Pony delivery

Send to Yeti | Fame | Threat Intelligence Data | Both | Threat Intelligence Indicators

Olay müdahale ekiplerinin zararlı yazılım analizi kısmında işlerini kolaylaştırmak için oluşturulan FAME, "FIR" adında bir olay yönetim (incident managment) platformuna da sahiptir.

## FIR (Fast Incident Response) Projesi

FIR

New event

Dashboard

Incidents

Events

Stats

search...

Incident Leader None Plan None Severity 1 Category Phishing Status Closed Detection CERT B/L Demo BusinessLine 1

Currently logged in as dev [logout] [Admin]

### Incident / Phishing / test

Opened on Jan. 15, 2015, 5:47 p.m. by dev

DESCRIPTION

phishing copying our brand website on http://evilwebsite.com/evilurl  
detected by one of our clients

TO-DO LIST

Action	Accountable	
Contact registrar	CERT	
+ Add To-Do Item		

CORRELATED ARTIFACTS

Type	Values
Hostnames	evilwebsite.com (2) ✕

RELATED FILES

Date	File	Description	
Feb. 5, 2015, 5:20 p.m.	MongoHub.zip		
Feb. 5, 2015, 5:50 p.m.	YARA_User_s_Manual_1.6__1_.pdf	yara	

Browse... Upload files Download archive

ATTRIBUTES

Name	Value	
loss	2784	✕

+ Add attribute

Comments (3)

Artifacts (2)

		Comment	Action
2015-02-09 14:32	dev	new test	Monitor ✕
2015-01-30 19:10	dev	Changed "status" from "Closed" to "Open"; Changed "is_starred" from "True" to "False";	Info ✕
2015-01-15 17:47	dev	Incident opened	Opened ✕

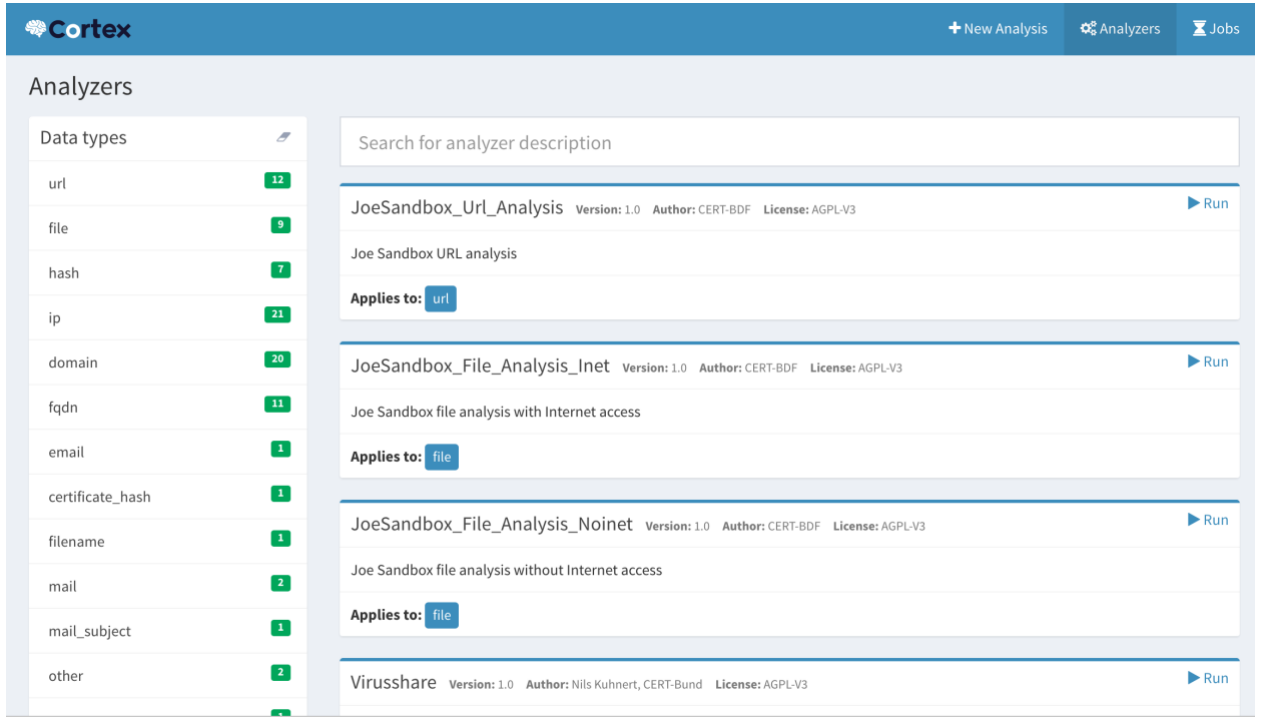
+ Add Comment Edit Open Block Incident followup Alert Takedown

## 5- Cortex Projesi

Cortex, tehdit istihbaratı ve olay müdahale alanında SOC ekiplerinin sık karşılaştığı bir sorunu çözmek amaçlı geliştirilmiştir. Bu sorun toplanan tehdit göstergelerinin tek bir araç kullanarak ve sorgulanarak nasıl analiz edileceğidir.

TheHive Projesi tarafından açık kaynak kodlu ve ücretsiz bir yazılım olan Cortex bu amaçla oluşturulmuştur. IP, e-posta adresleri, URL'ler, alan adları, dosyalar veya dosya özetleri gibi göstergeler, bir web arayüzü kullanılarak tek tek veya toplu modda analiz edilebilir. Analistler, Cortex REST API sayesinde bu işlemleri otomatikleştirebilirler. Cortex Scala'da yazılmıştır. Bootstrap ile birlikte AngularJS kullanmaktadır.

Cortex'in sunduğu avantajlardan biri, bir analiz işlemi için bir servis veya bir araç kullanmak istediğiniz de her seferinde tekerleği yeniden icat etmek zorunda kalmamanızdır.

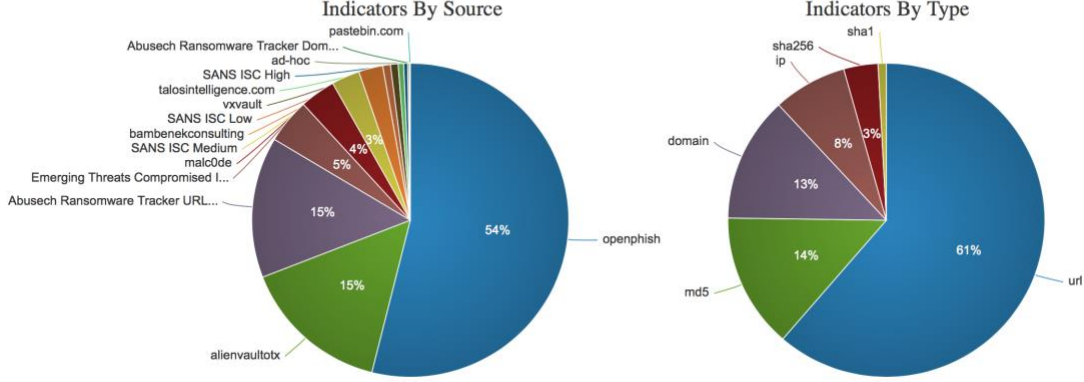


Web sitesi: <https://github.com/CERT-BDF/Cortex>

## 6- GOSINT Framework

### Indicator Metrics

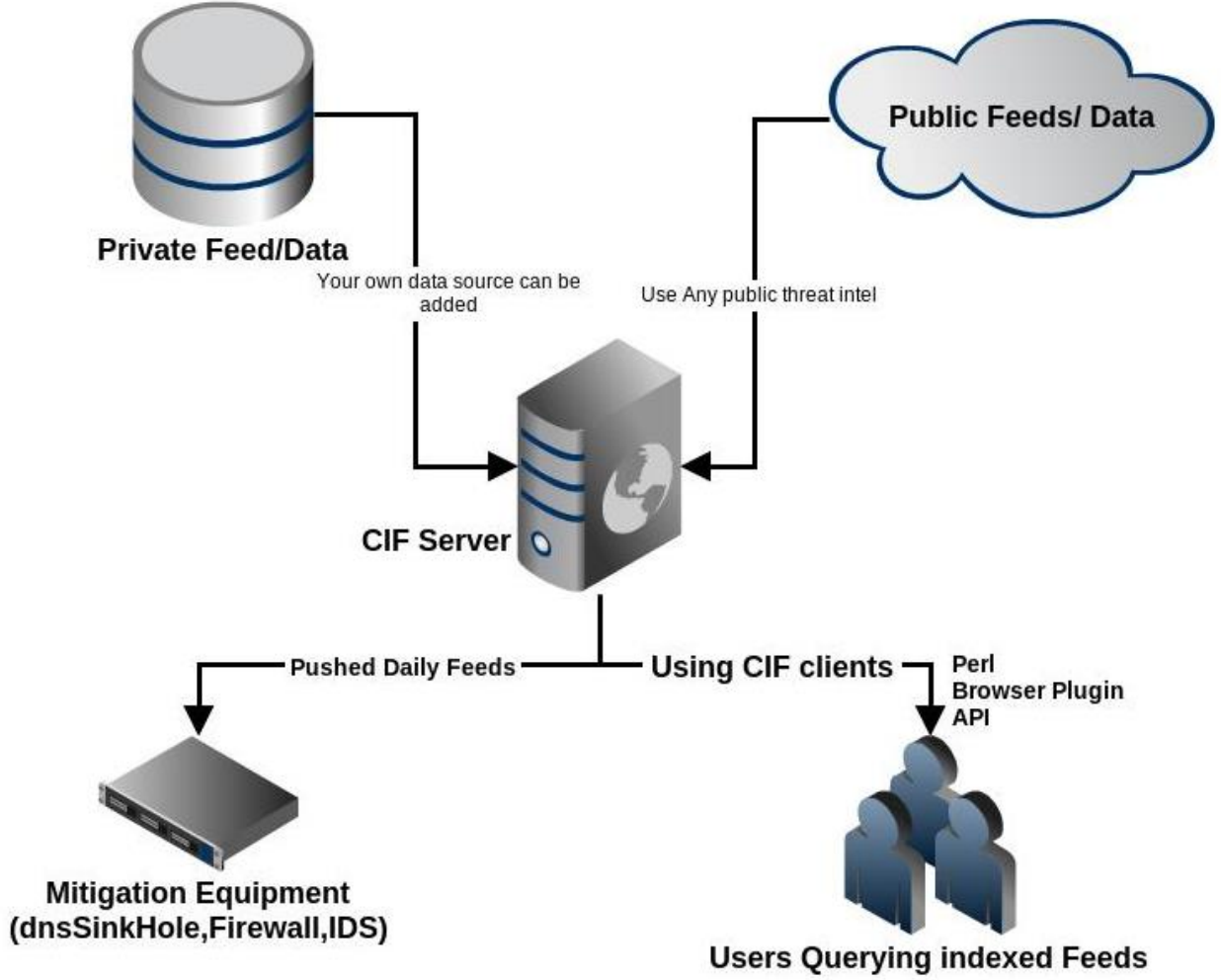
View a breakdown of the indicators currently loaded into GOSINT below.



Yazımızda da bahsettiğimiz gibi internet üzerinde halihazırda çok fazla açık kaynak tehdit istihbarat aracı bulunmaktadır. Ancak bu konu hakkında yararlı bilgi bulmak, toplamak ve filtrelemek için kolay bir yol bulunmamaktadır. GOSINT, bir güvenlik analistinin yapılandırılmamış tehdit istihbaratını toplamasına ve standartlaştırmasına olanak tanımaktadır.

GOSINT'i tehdit göstergeleri için bir transfer istasyonu olarak düşünebilirsiniz. Yazılım, tehdit istihbaratı analistlerine bir göstergenin izleme değerinde olup olmadığını veya reddedilmesi gerektiğini değerlendirmesine izin verir. Bu karar verme aşaması, herhangi bir tehdit göstergesini yönetmede çok önemlidir. Hem bir insan analisti hem de GOSINT'in kendisi tarafından tetkik edilmesi, göstergelerin tehdit algılama etkinliğini artırır. Ekleyebileceğiniz gösterge kaynakları sayısında da bir sınır bulunmamaktadır.

## 7- Collective Intelligence Framework



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 etkinliklerle ilişkili olduğu gözlenen IP adresleri, FQDN'leri ve URL'lerdir.

CIF, çeşitli tehdit verilerini herhangi bir kaynaktan alabilmektedir.

Framework'ün çalışma mantığı şu şekildedir.

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

Web sitesi: <http://csirtgadgets.org/>

Github: <https://github.com/csirtgadgets/massive-octo-spice>

## 8- Cyphon Projesi

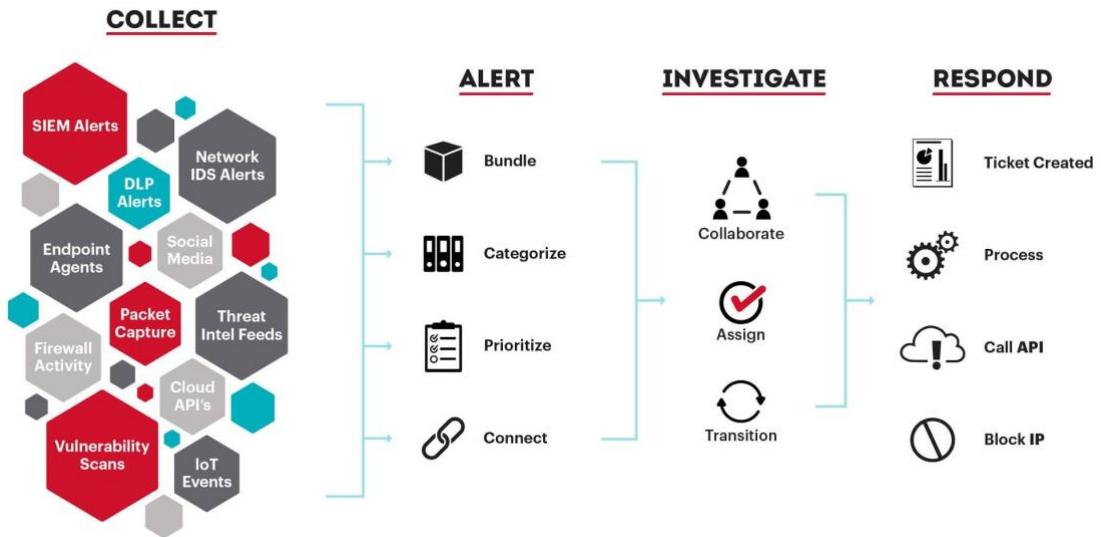
Cyphon, çok sayıda ilgili görevi tek bir platformda hızlandırarak olay müdahale (incident response) sorunlarını ortadan kaldırıyor. Analitik iş akışı için veri toplama, uyarıları paketleme ve önceliklendirme işlerini ve analistlerinizi olayları araştırmak ve belgelemek için yetkilendirmek için kapsamlı bir çözüm sunmak için olayları alır, işler ve süreçlere ayırır.

Birçok işletme, ağlarını gözetlemek için e-postalara güvenmektedir. Cyphon, e-posta, günlük mesajları, API'ler, sosyal medya ve daha pek çok şeyi içeren çeşitli kaynaklardan ayrıntılı bilgi toplayarak veri yönetimindeki boşlukları kapatır. Analistlere, tüm bu veri kaynaklarına bir platform aracılığıyla tam erişim sağlayarak, Cyphon, veri kapsamını en üst düzeye çıkarırken ağları izlemek için gereken süreyi ve enerjiyi en aza indirmektedir.

Uyarılar tetiklendiğinde, analistler olayı doğrudan Cyphon aracılığıyla inceleyebilir. Karşılaşılan aktivitenin türünü, coğrafik kökenini ve kritiklik seviyesini hızlı bir şekilde görebilirler. Bir düğmeyi tıklayarak olayla ilgili günlükleri bulmak için verilere derinlemesine dalebilirler. Bu, bir uyarıyı araştırmak için gereken zamanı ve çabayı azaltır, böylece analistler daha verimli çalışabilir ve olaylar daha çabuk giderilebilir.

Cyphon, başka bir SIEM veya veri toplama aracın daha fazla özellik sunmaktadır. İş akışınızı düzene sokmak için diğer API'lerle bütünleşen hepsi bir arada bir olay yönetimi çözümüdür. Cyphon, analistlerin ekip üyeleri ile sorunları paylaşmalarına ve analiz sonuçlarına uyarı eklemelerine olanak tanır. Bu, operasyon merkezimize veya güvenlik görevlilerine tam şeffaflık sağlarken, aynı zamanda kuruluşunuz için değerli bir bilgi tabanı oluşturur.

## Cyphon Çalışma Mimarisi



Kuruluşlarınızın Cyphon'dan en iyi şekilde yararlanmasına yardımcı olmak için, uyarıları yönetmek için bir kullanıcı arabirimi olan Cyclops geliştirilmiştir. Cyclops, Cyphon uyarılarını kolayca görüntülemenizi, atamanızı ve araştırmanızı sağlar. Verilerinize "göz" sağlar, sorunlara hızlı ve etkili bir şekilde yanıt vermenizi sağlar.



## Cyphons Arayüzü

The screenshot displays the Cyphon Alerts dashboard. On the left, there are filters for Level (Critical, High, Medium, Low, Info), Status (New, Busy, Done), Source (All), Time (Any), and Assigned (All). The main area shows a list of alerts with columns for Level, Status, Source, Time, and Details. The details column includes the alert title, source, level, status, assigned person, outcome, and incidents. On the right, there is a detailed view of a specific alert (Alert 3) showing its title, details, locations, and analysis.

Level	Status	Source	Time	Details
Critical	New	dss.ids	03/15/2017 01:20 PM	POLICY-OTHER Adobe ColdFusion admin API ac...
High	Busy	dss.ids	03/15/2017 01:20 PM	SERVER-WEBAPP WebTester install2.php arbitra...
Medium	Done	dss.ids	03/15/2017 01:20 PM	MALWARE-CNC Win.Trojan.Dexter variant o...
Low	New	dss.ids	03/15/2017 01:20 PM	MALWARE-CNC Win.Trojan.Dexter CasinoLo...
Info	Busy	dss.ids	03/15/2017 01:19 PM	SERVER-WEBAPP Drupal RESTWS restws_page...
	Done	dss.ids	03/15/2017 11:25 AM	POLICY-OTHER Adobe ColdFusion admin AP...
	New	dss.ids	03/15/2017 11:25 AM	SERVER-WEBAPP WebTester install2.php ar...
	Busy	dss.ids	03/15/2017 11:25 AM	MALWARE-CNC Win.Trojan.Dexter variant o...
	Done	dss.ids	03/15/2017 11:25 AM	MALWARE-CNC Win.Trojan.Dexter CasinoLo...
	New	dss.ids	03/15/2017 11:25 AM	SERVER-WEBAPP Drupal RESTWS restws_page...
	Busy	smokey.mail	02/26/2017 08:34 AM	[**SMOKEY**][CRIT-310] Up2Date prefetch failed
	Done	smokey.mail	02/21/2017 11:44 AM	[**SMOKEY**][CRIT-861] Advanced Threat Prot...
	New	smokey.mail	02/21/2017 11:14 AM	[**SMOKEY**][CRIT-861] Advanced Threat Prot...
	Busy	smokey.mail	02/21/2017 10:37 AM	[**SMOKEY**][CRIT-861] Advanced Threat Prot...
	Done	smokey.mail	02/21/2017 10:02 AM	[**SMOKEY**][CRIT-861] Advanced Threat Prot...
	New	smokey.mail	02/21/2017 09:15 AM	[**SMOKEY**][CRIT-861] Advanced Threat Prot...
	Busy	dss.ids	01/04/2017 11:55 AM	MALWARE-CNC Torpig bot sinkhole server DNS lookup

Cyphon birkaç açık kaynak projesinin yardımıyla çalışır. Cyphon'u çalıştırmak için tüm bağımlılıklarını yüklemeniz gerekir. Bu işlemi, bir uygulamayı bir mikro hizmet kümesi olarak kolayca dağıtmanıza olanak tanıyan Docker kullanılarak basitleştirilmiştir.

Cyphon'u hem geliştirme hem de üretim ortamlarında çalıştırmak için Docker Oluşturma dosyaları seti hazır olarak bulunmaktadır. Bu, Cyphon'u ve kullandığı diğer hizmetleri hızlı bir şekilde kurmanıza ve çalıştırmanıza izin verir.

Web Sayfası: <https://www.cyphon.io/>

Github: <https://github.com/dunbarcyber>

## 9- RTIR Projesi (Request Tracker)

Her büyüklüğe ait kuruluşlar, müşteri isteklerini, iç proje görevlerini ve her türlü iş akışını izlemek ve yönetmek için Request Tracker kullanabilir. Özel ticket süresi, sorunsuz e-posta entegrasyonu, yapılandırılabilir otomasyon ve detaylı izinler ve roller ile RT, müşterilerinizin, personelinizin ve sizin ihtiyaçlarınıza cevap verir.

RT, birçok popüler mobil cihaz da dahil olmak üzere, herhangi bir modern tarayıcı ile çalışan bir sunucu tarafında, veritabanı destekli bir web uygulamasıdır. E-posta arayüzü, Outlook'tan Apple Mail'e, Thunderbird'den Gmail'e ve Mutt'e kadar herhangi bir posta istemcisiyle çalışır. Sunucu tarafında RT, Unix benzeri veya Linux işletim sistemi, SQL veritabanı, web sunucusu ve Perl gerektirir.

### RT; Email Entegrasyonu:

The screenshot displays the RT web interface for updating ticket #5. The top navigation bar includes links for Home, Search, Assets, Tools, and a user login status (Logged in as watson). The main header shows the ticket title 'Update ticket #5 (Need some help)' and a search bar. Below the header, there are tabs for Display, History, Basics, People, Dates, Links, Jumbo, Reminders, and Actions. The 'Message' section on the left contains fields for 'One-time Cc:', 'One-time Bcc:', 'Subject:', and 'Message:'. The 'Ticket and Transaction' section on the right includes fields for 'Update Type:', 'Status:', 'Owner:', and 'Worked:'. A large red box in the center contains the text 'Can you send a screenshot of the error you are seeing?'. Below this, there is an 'Attach:' section with a 'Drop files here or click to attach' prompt. At the bottom, there are links for 'Include attachments:' and 'Update Ticket'.

- Request Tracker, anahtar e-posta adreslerine gönderilen tüm e-postaları alır ve yönetir: örneğin, support @, sales @, helpdesk @, security @.
- Dahili ekipler, aynı ticket üzerinde harici müşteriler ve ekip üyeleri ile birlikte iletişim kurabilir.
- Otomatik cevaplar için şablonları ve her cevapla yararlı bağlantılar göndermek üzere sayfalarınızı ve diğer bilgiler de dahil olmak üzere markalı, stilli HTML e-postaları göndermek için diğer tüm yazışmaları özelleştirebilirsiniz.
- Personel, ticket cevaplarını e-posta yoluyla yönetebilir veya RT'nin tam web arayüzünü kullanabilir.
- E-posta ile gönderilen yanıtları ve yorumları ve ilgili tüm aktiviteleri kontrol edebilirsiniz.

## RT; Özel Çalışma Alanları:

Home Search Articles Assets Tools Admin Logged in as root RT for aperturescience42.local BEST PRACTICAL

**Modify scrip #12** New ticket in General Search...

Scripts Basics Applies to

**Basics**

Description: On Resolve Notify Requestors

Condition: On Resolve

Action: Notify Requestors

Template: Resolved in HTML

Applies to: Global

☒ Enabled (Unchecking this box disables this scrip)

Reset Save Changes

**User Defined conditions and results**

(Use these fields when you choose "User Defined" for a condition or action)

Custom condition:

Custom action preparation code:

Custom action commit code:

RT'nin yaşam döngüsü, ticket durumlarınızı ve işlemlerinizi içeren kişiselleştirilebilir iş akışları oluşturmanıza olanak tanır. Ticket'larda yapılan her işlem otomatik olarak yapılandırılmış script'leri tetikler. Her bir script'teki koşullar ve işlemler, bir ticket üzerinde önemli güncellemeler yapıldığında, RT ya da diğer sistemlerdeki olayları otomatik hale getirmenizi sağlar.

SLA aracı gibi gelişmiş özellikleri, her bir ticket üzerindeki son tarih gibi anahtar değerleri otomatik olarak ayarlar; böylece bir yanıtız kalmazsınız. Rt-crontool programı, ticket güncellemelerini otomatik olarak gerçekleştirir veya ticketlar boşta kaldığında bildirim göndermek için zamanlanmış işleri çalıştırabilir.

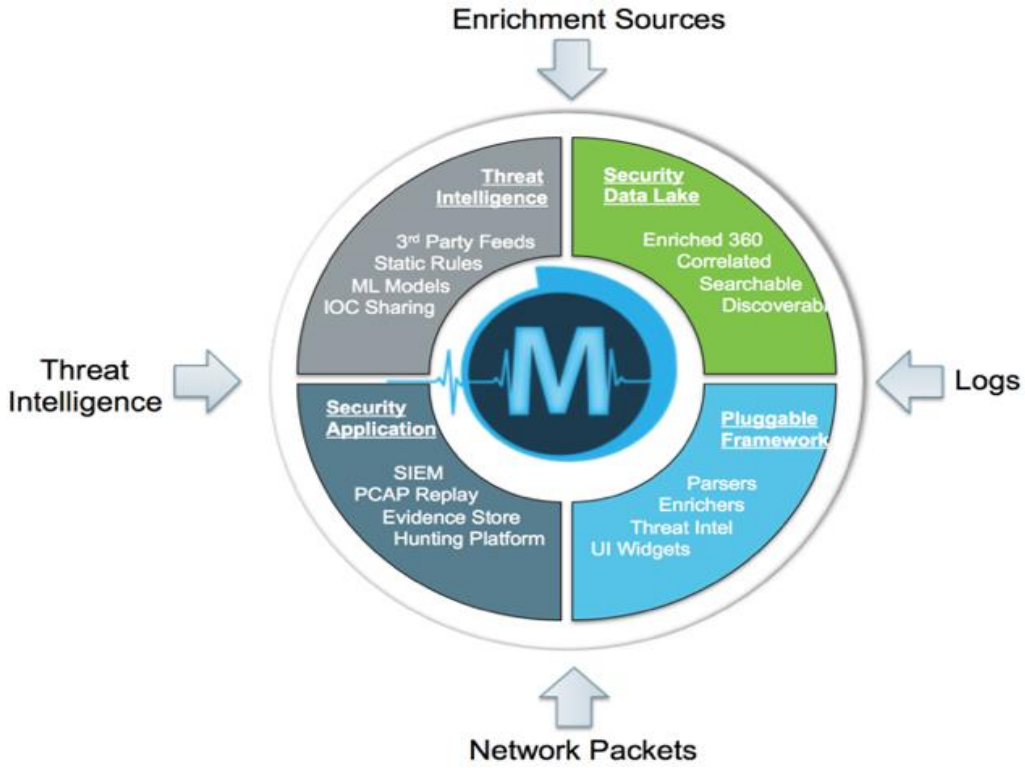
Web Sayfası: <https://bestpractical.com/request-tracker>

Github: <https://github.com/bestpractical>

## 10- Apache Metron

Apache Metron, on yıl süren büyük veri bilgisini ve akışlı analitik deneyimini, güvenlik ekiplerinin kullanacağı seçilmiş bir teknoloji paketi halinde kapsayan, yenilik için oluşturulmuş bir araçtır. Siber güvenlik platformu için temel altyapıyı oluşturmakla ilgili tekrarlanabilir veri mühendisliği problemleri hakkında kaynak harcamaya gerek kalmadan, gerçek zamanlı profil oluşturma ve istatistiksel analiz için makine öğrenimini hızlı bir şekilde kullanabilmek için bir platform sağlar.

Apache Metron, eski adıyla OpenSOC, tehdit izleme ve analizi için merkezi bir araç sunmak için çeşitli açık kaynaklı büyük veri teknolojilerini birleştirir. Metron, güvenlik telemetrisine tek bir platformda en güncel tehdit istihbarat bilgilerini uygularken log toplama, full packet capture, indeksleme, depolama, gelişmiş davranış analizi ve veri zenginleştirme yetenekleri sunar.



Apache Storm, Apache HBase ve Apache Kafka'nın üzerine kurulan Metron, full packet capture da dahil olmak üzere herhangi bir telemetri kaynağını ölçeklendirebilir, normalleştirebilir ve dönüştürebilir.

Metron'a verilen veriler, akışa göre coğrafi konum veya varlık tanımlayıcıları gibi değerli bağlamlarla zenginleştirilebilir. Yeni zenginleştirmeler, kesintisiz olarak kullanıcı tanımlı işlevler ve sağlam bir komut dosyası dili ile belirtilebilir. Tehditleri, olay müdahale ve araştırması için yalnızca en büyük tehditlere öncelik verilmesi için kurallar veya makine öğrenmesi modelleri kullanılarak belirlenebilmektedir.

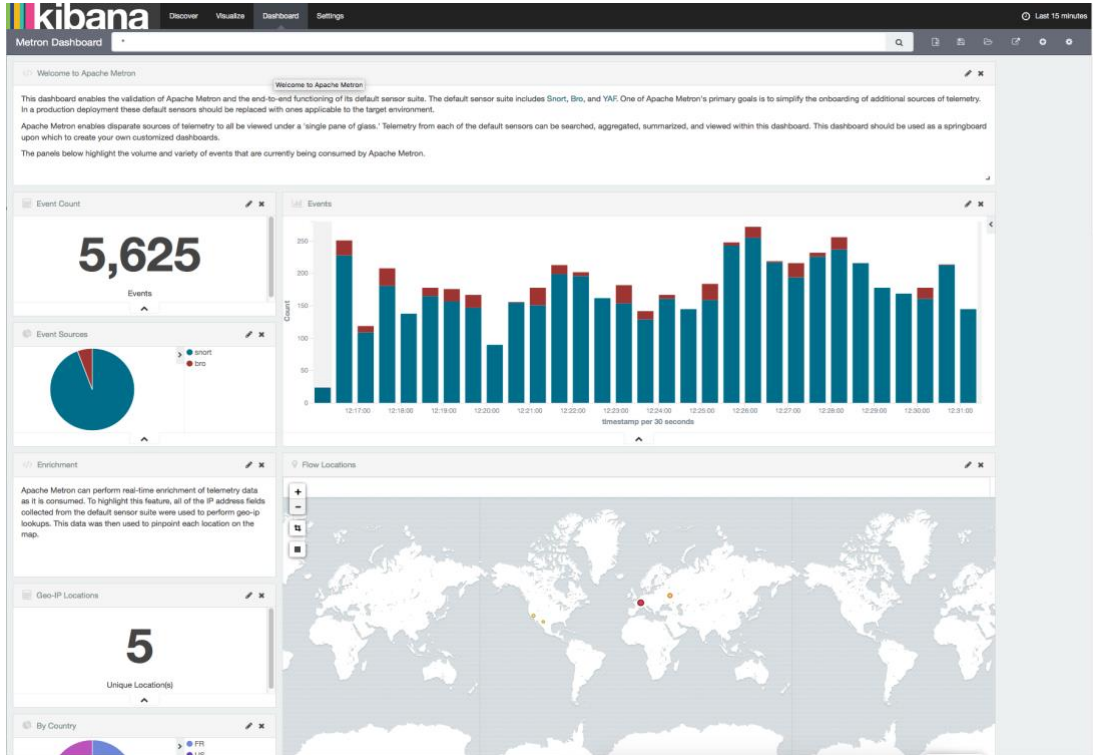
## Metron'a ait bazı özellikler:

- Herhangi bir güvenlik türünde yakalama, saklama ve normalleştirme mekanizması;
- Yüksek oranlarda telemetri;
- Gerçek zamanlı işleme ve zenginleştirme uygulamaları;
- Verimli bilgi depolama;
- Sistemden geçen verilerin merkezi bir görünümünü ve uyarıları sağlayan arabirim
- En büyük veri kümelerinde bile güvenlik analizi yapmak için istatistiksel özet veri yapılarının kullanılması

Apache Metron, ister e-posta hizmeti sağlayıcısı gibi uygulamaya özel ortamlarda olsun isterse Nesnelerin interneti (IoT) gibi platformlarda olsun, kullanıcıların siber güvenlik tehditlerini hızla algılar ve bunlara yanıt vermesini sağlamak için büyük verileri ve makine öğrenmesini kullanır.

Avustralya'nın en büyük telekomünikasyon, medya ve İnternet Hizmet Sağlayıcısı Telstra, anahtar hizmet merkezlerinde kurumsal düzeyde güvenlik operasyon merkezleri (SOC) için Apache Metron kullanmaktadır.

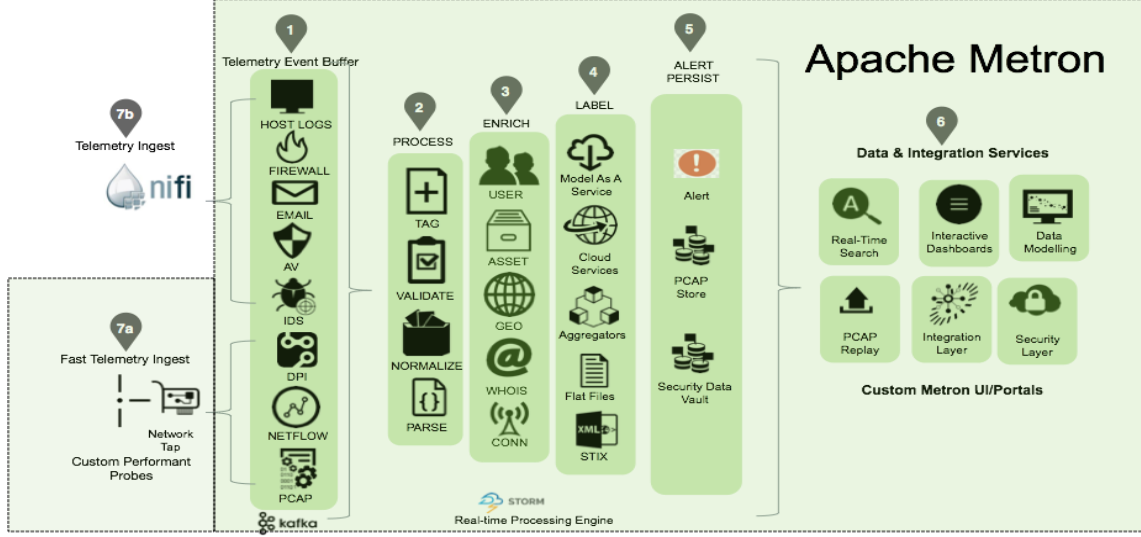
## Metron Dashboard



## [SOME ve SOC EKİPLERİ İÇİN AÇIK KAYNAK ÇÖZÜMLER]

Metron'un varsayılan gösterge tablosu, varsayılan sensör paketiyle Metron'un uçtan uca çalışmasını kolaylıkla doğrulamanıza izin vermek için tasarlanmıştır. Kibana 4'te bulunan yararlı widget'ların bazılarını vurguluyor ve kendi özelleştirilmiş gösterge tablolarınızı oluşturmanız için başlangıç noktası olarak hizmet ediyor.

### Metron Mimarisi



Web Sayfası: <http://metron.apache.org/>

Github Sayfası: <https://github.com/apache/metron>

## BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA’da sürdüren BGA Bilgi Güvenliği’nin ilgi alanlarını “Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri” oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000’den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

## BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.’nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar “Siber Güvenlik Kampları”, “Siber Güvenlik Staj Okulu”, “Siber Güvenlik Ar-Ge Destek Bursu”, “Ethical Hacking yarışmaları” ve “Siber Güvenlik Kütüphanesi” gibi birçok gönüllü faaliyetin destekleyici olmuştur.