

Tehdit İstihbaratı

Siber Güvenlikte Tehdit İstihbaratı Nedir ?

Tehdit istihbaratı kısaca kurumlara ve kuruluşlara siber dünya üzerinden herhangi bir şekilde tehdit olabilecek unsurların saptanması ve bu unsurlara karşı önlem alınmasıdır.

Tespit edilmek istenen unsurlar arasında potansiyel saldırganların motivasyonları metotları ve amaçları vardır.Siber tehdit istihbaratının yararları arasında veri sızıntılarını önlemek, kurum ve kuruluşların daha güvenilir olmasına yardımcı olmak, finansal maaliyetlerden tasarruf sağlamak ve itibar kaybını önlemektir.



Peki Siber Tehdit İstihbaratı Neden Önemlidir ?

Tehdit istihbaratı çözümleri var olan veya oluşmakta olan tehdit faktörlerini depolar.Ardından bu veri, analiz edilir ve filtrelenir bu sayede bu veriler otomatize güvenlik araçları tarafından kullanılabilir. Bu tür bir güvenlik önleminin amaçları arasında kurum ve kuruluşları “zero day” exploitleri ve APT(Advanced Persistent Threat) hakkında bilgilendirmek ve bu tür saldırılardan nasıl korunacağını göstermektir.

IoC (Indicators of Compromise) : IoC ‘ ler sisteme izinsiz erişim veya saldırganların sistemdeki gerçekleştirdiği aktiviteler,veri ihlalleri gibi veri parçacıklarını kapsarlar.

IoC Çeşitleri

IoC'ler tehditleri aşağıdaki kategorilerde incelenebilir.

- 1-Virüs İmzaları.
- 2-Saldırgan IP adresleri.
- 3-Zararlı yazılım(malware) dosyaları.
- 4- Botnet kontrol sunucuları.

IoC ler tanımlandıktan sonra gelecekteki saldırı vektörleri tanımlanıp, bu saldırılara karşı önceden önlem almak mümkün olur.

Açık Kaynaklı Tehdit İstihbaratı Yayınları(Feeds)

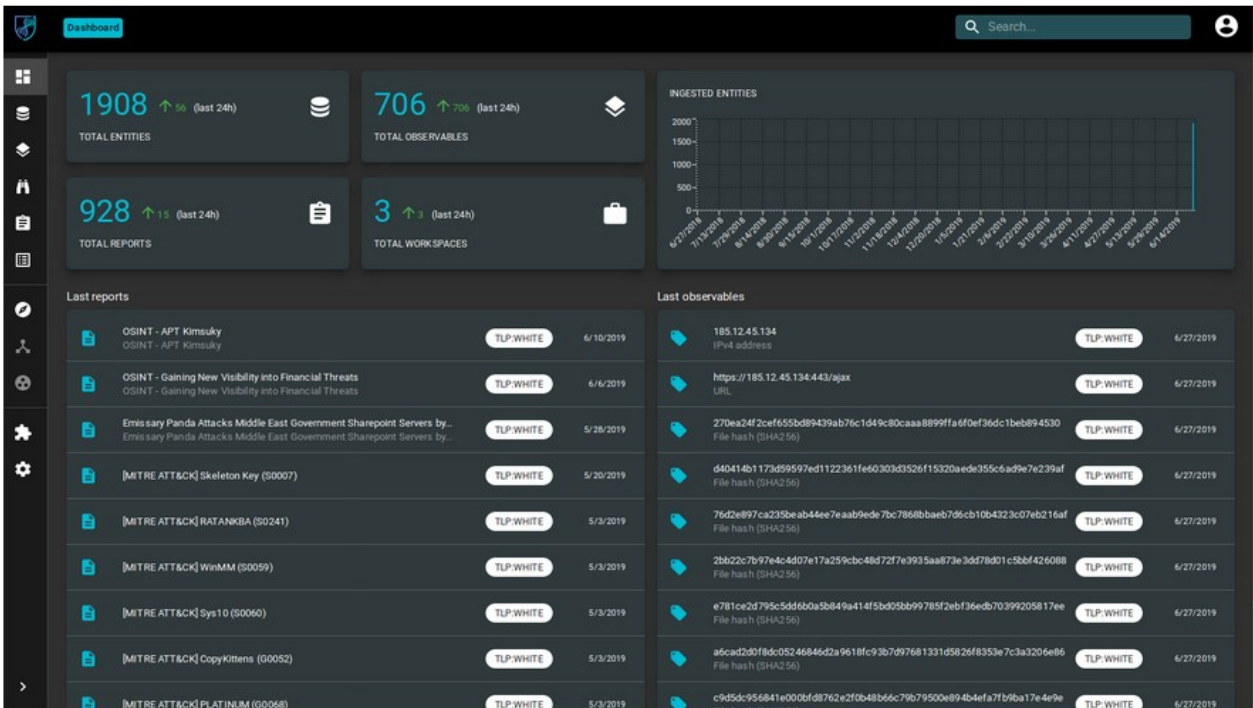
- #abuse.ch: Ransomware Tracker
Ransomware Tracker fidye saldırılarına yönelik verileri toplayan bir yayın. Siber güvenlik ekipleri bu yayının sayesinde saldırının kaynağı olan IP adreslerini görebilir ve bu IP adreslerine kurum içinden erişimi engelleyebilirler.
- VirusTotal : Üzerinde onlarca virüs tarayıcısı, karalisteye alma servisleri bulunduran bir servis.
- Department of Homeland Security : Automated Indicator Sharing
- FBI: InfraGard Portal
- SANS: Internet Storm Center.
- Cisco:Talos Intelligence.
- Google: Safe Browsing
Safe browsing servisi tehlikeli web sitelerini indeksler ve bu tür web sitelerini güvenlik farkındalığı oluşturmak amacıyla paylaşır. Hergün binlerce zararlı site tespit eder.

OPENCTI

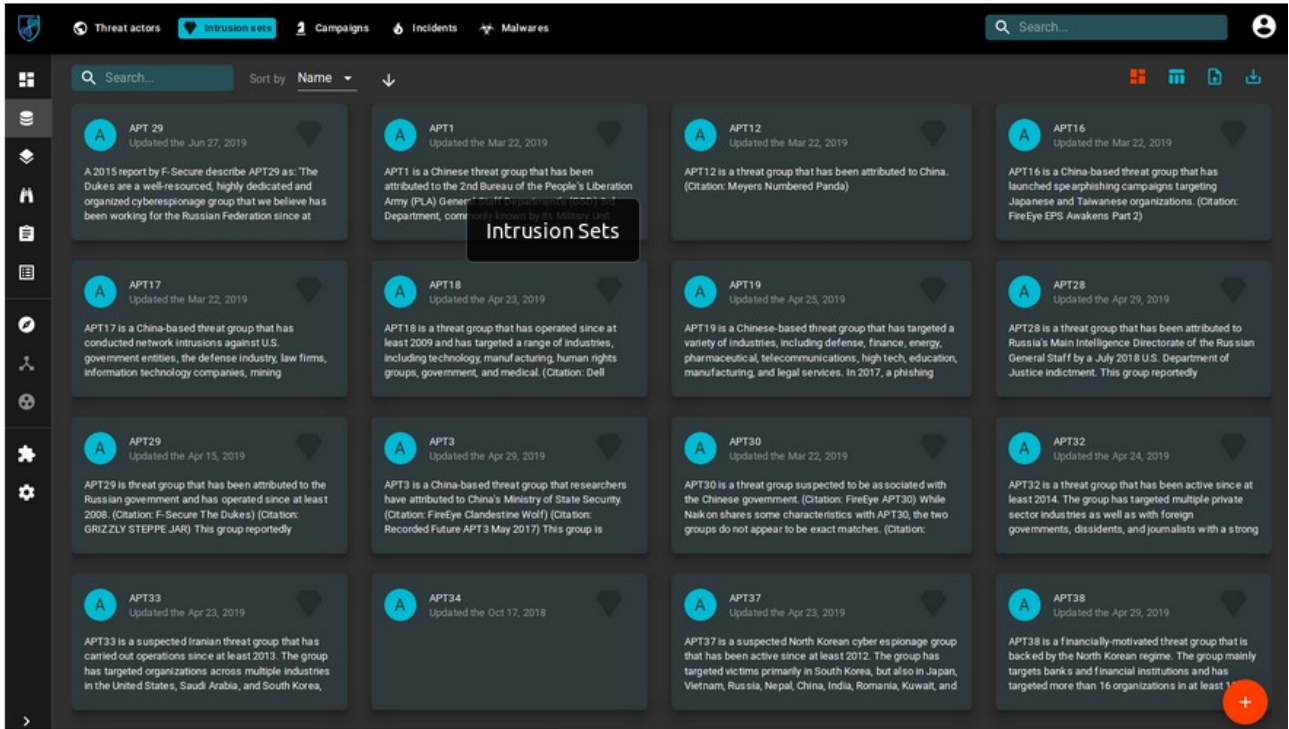
OpenCTI kurumlara ve kuruluşlara siber tehdit istihbaratı verilerini yönetmesine olanak veren açık kaynak kodlu bir araç. Verileri teknik ya da teknik olmayan şekilde belirli bir düzene ve yapıya göre sıralama,görselleştirme ve organize etme özelliklerine sahip.



Opencti platformunu açtığımızda karşımıza dashboard çıkıyor.
Dashboard:



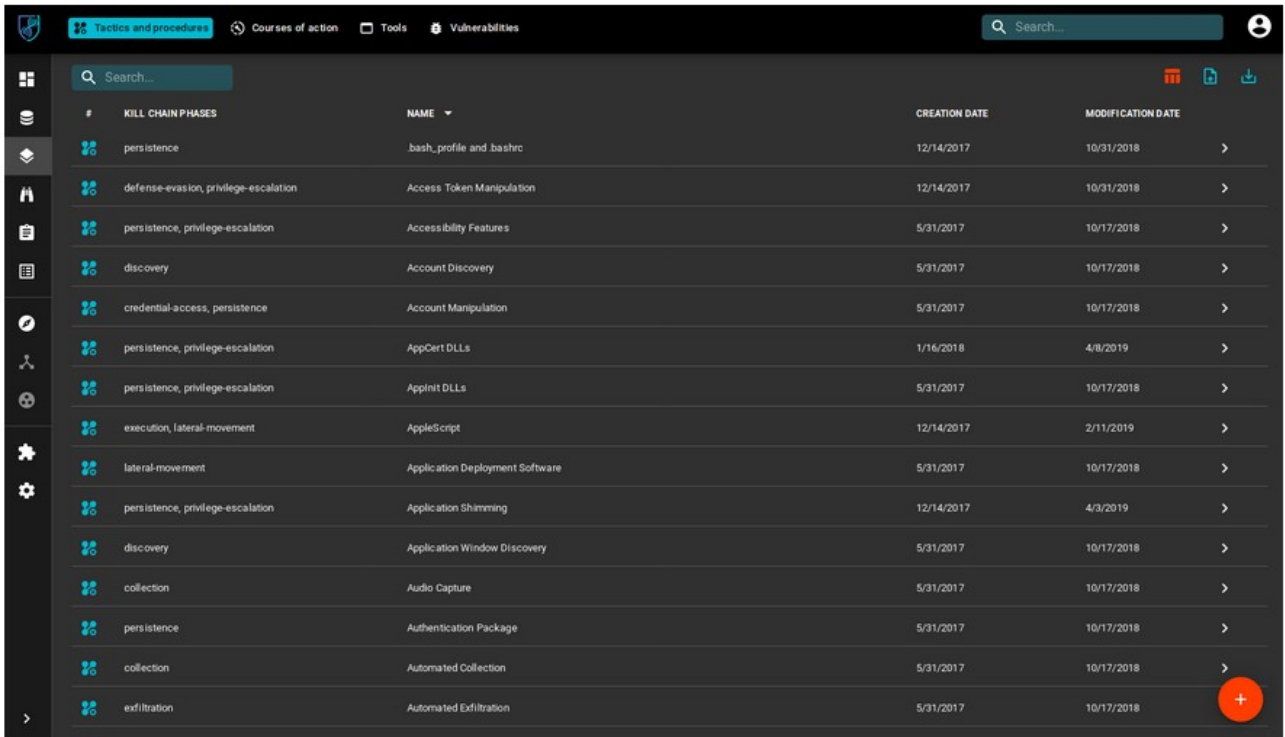
Threats:Bu servis ile tehdit faktörleri hakkında bilgi alabiliyoruz. Resimde APT(Advanced Persistent Threat) tehditleri hakkında bilgiler bulunmakta.



The screenshot displays the 'Threat actors' section of a security dashboard. It features a grid of 16 APT (Advanced Persistent Threat) threat groups. Each entry includes a circular icon with a letter 'A', the APT name (e.g., APT 29, APT1, APT12), an update date, and a brief description of the group's activities and targets. A central overlay labeled 'Intrusion Sets' is visible. The dashboard includes a search bar at the top and a sidebar with navigation icons.

APT Name	Updated	Description
APT 29	Updated the Jun 27, 2019	A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2007.'
APT1	Updated the Mar 22, 2019	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department, commonly known as the 2nd Department, commonly known as the 2nd Department.
APT12	Updated the Mar 22, 2019	APT12 is a threat group that has been attributed to China. (Citation: Meyers Numbered Panda)
APT16	Updated the Mar 22, 2019	APT16 is a China-based threat group that has launched spearfishing campaigns targeting Japanese and Taiwanese organizations. (Citation: FireEye EPS Awakens Part 2)
APT17	Updated the Mar 22, 2019	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining.
APT18	Updated the Apr 23, 2019	APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical. (Citation: Dell)
APT19	Updated the Apr 25, 2019	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing.
APT28	Updated the Apr 29, 2019	APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly
APT29	Updated the Apr 15, 2019	APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. (Citation: F-Secure The Dukes) (Citation: GRIZZLY STEPPE JAR) This group reportedly
APT3	Updated the Apr 29, 2019	APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. (Citation: FireEye Clandestine Wolf) (Citation: Recorded Future APT3 May 2017) This group is
APT30	Updated the Mar 22, 2019	APT30 is a threat group suspected to be as associated with the Chinese government. (Citation: FireEye APT30) While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches. (Citation:)
APT32	Updated the Apr 24, 2019	APT32 is a threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as with foreign governments, dissidents, and journalists with a strong
APT33	Updated the Apr 23, 2019	APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea.
APT34	Updated the Oct 17, 2018	
APT37	Updated the Apr 23, 2019	APT37 is a suspected North Korean cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and
APT38	Updated the Apr 29, 2019	APT38 is a financially-motivated threat group that is backed by the North Korean regime. The group mainly targets banks and financial institutions and has targeted more than 16 organizations in at least 11

Techniques:Bu kısımda herhangi bir saldırı olması durumunda saldırganların kullanabileceği saldırı teknikleri mevcut.Aşağıda bulunan tekniklerden herhangi birisinin kullanımla olduğu tespit edilirse ilgili işlem durdurulabilir.



The screenshot displays the 'Tactics and Procedures' section of a security dashboard. It features a table listing various attack techniques. The table has columns for 'NAME', 'CREATION DATE', and 'MODIFICATION DATE'. A sidebar on the left contains navigation icons, and a search bar is at the top.

NAME	CREATION DATE	MODIFICATION DATE
peristence	12/14/2017	10/31/2018
defense-evasion, privilege-escalation	12/14/2017	10/31/2018
peristence, privilege-escalation	5/31/2017	10/17/2018
discovery	5/31/2017	10/17/2018
credential-access, peristence	5/31/2017	10/17/2018
peristence, privilege-escalation	1/16/2018	4/8/2019
peristence, privilege-escalation	5/31/2017	10/17/2018
execution, lateral-movement	12/14/2017	2/11/2019
lateral-movement	5/31/2017	10/17/2018
peristence, privilege-escalation	12/14/2017	4/3/2019
discovery	5/31/2017	10/17/2018
collection	5/31/2017	10/17/2018
peristence	5/31/2017	10/17/2018
collection	5/31/2017	10/17/2018
exfiltration	5/31/2017	10/17/2018

Reports: Bu sekmede platforma yüklenen bütün raporlar bulunmakta.

#	NAME	AUTHOR	PUBLICATION DATE	STATUS	MARKING
	OSINT - APT Kimsuky	CIRCL	6/10/2019	New	TLP:WHITE
	OSINT - Gaining New Visibility into Financial Threats	CIRCL	6/6/2019	New	TLP:WHITE
	Emissary Panda Attacks Middle East Government Sharepoint Servers by Palo Alto Unit42	CthulhuSPRL.be	5/28/2019	New	TLP:WHITE
	[MITRE ATT&CK] Skeleton Key (S0007)	The MITRE Corporation	5/20/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] RATANKBA (S0241)	The MITRE Corporation	5/3/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] WinMM (S0059)	The MITRE Corporation	5/3/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] Sys10 (S0060)	The MITRE Corporation	5/3/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] Copy Kittens (G0052)	The MITRE Corporation	5/3/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] PLATINUM (G0068)	The MITRE Corporation	5/3/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] CoinTicker (S0369)	The MITRE Corporation	4/29/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] TEMP Voles (G0088)	The MITRE Corporation	4/29/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] H1N1 (S0132)	The MITRE Corporation	4/29/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] APT39 (G0087)	The MITRE Corporation	4/29/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] APT28 (G0007)	The MITRE Corporation	4/29/2019	Analyzed	TLP:WHITE
	[MITRE ATT&CK] Lazarus Group (G0032)	The MITRE Corporation	4/29/2019	Analyzed	TLP:WHITE

Entities: Bu kısımda güncel olarak devam eden saldırılarda risk faktörü oluşabilecek olan kategoriler mevcut. Üniversiteler,Ulaşım vb.

Sector	Updated
Activists	Updated the Jun 26, 2019
Agriculture	Updated the Jun 26, 2019
Arts	Updated the Jun 26, 2019
Aviation	Updated the Jun 26, 2019
Consulting and services	Updated the Jun 26, 2019
Education	Updated the Jun 26, 2019
Electricity	Updated the Jun 26, 2019
Energy	Updated the Jun 26, 2019
Gas	Updated the Jun 26, 2019
Industry	Updated the Jun 26, 2019
Maritime	Updated the Jun 26, 2019
Nuclear	Updated the Jun 26, 2019
Petroleum	Updated the Jun 26, 2019
Rail	Updated the Jun 26, 2019
Transport	Updated the Jun 26, 2019
Universities	Updated the Jun 26, 2019

