Nebula Siber İstihbarat Servisi

N-SIS

- **Türkiye'ye özel, hızlı ve güvenilir tehdit istihbaratı**
- **USOM entegrasyonu**
- **Homografi/IDN tespiti**
- **STIX desteği**
- **Sahte mobil uygulama tespiti**
- **Dark/Deep Web, Pastebin ve Github veri sızıntısı tespiti**
- **Alan adı ve sosyal medya hesabı kapattırma**
- **Döviz kuru istihbaratı**
- **SSL Sertifika denetimi**
- **IP ve Servis izleme**
- **Zafiyet Tarama**

Siber tehditlerinden sisteminizi ve markalarınızı koruyun!

Verizon 2015 Data Breach Investigations raporuna göre gönderilen oltalama mesajlarının %23'ü kullanıcılar tarafından açılmış ve %11'inin içinde bulunan bağlantılar kullanıcılar tarafından tıklanmış. Yapılan tüm bilgi güvenliği yatırımlarına rağmen internet korsanlarının büyük bir hızla açıp kapattıkları alan adlarını takip edip engellemekte ve kullanıcılarımızın şüpheli e-postaları açmalarını veya e-postalar içerisinde bulunan bağlantıları engellemekte zorlanıyoruz. Her gün kurumlar ve markaları taklit eden kötü amaçlı sahte web siteleri ve mobil uygulamalar ile karşılaşıyoruz. Binlerce kuruma ait veri Internet üzerinde satılıyor veya paylaşıyor. Tüm bunlar olurken internet korsanları her gün sistemimizde zafiyetler aramaya devam ediyor. Nebula Siber İstihbarat Servisi (N-SIS) dış tehditlerden korunmanızı, marka itibarınızı takip etmenizi ve korumanızı, sisteminizdeki kritik değişikliklerden haberdar olmanızı sağlayarak siber dünyada güvende olmanıza yardımcı olur.

N-SIS Temel Özellikleri

Nebula Siber İstihbarat Servisi (N-SIS); tehdit istihbaratı, marka istihbaratı ve sistem istihbaratı olarak üç kategoride siber istihbarat bilgisi sağlar. İstihbarat bilgileri N-SIS portalından, eposta ile ve STIX standardı ile otomatik olarak paylaşılır.

Tehdit istihbaratı: Kurum kullanıcılarının cryptolocker gibi zararlı uygulama ve web sitelerine erişimi engellemek amaçlı tasarlanmış bir güvenlik veri tabanıdır. Tehdit bilgileri (IOC) direkt ürün entegrasyonları ve STIX desteği ile mevcut güvenlik yatırımlarına entegre olabilir.

Marka istihbaratı: Kurumların sahip olduğu marka ve değerlerin kötü amaçlı kullanımlarını tespit etmek üzere tasarlanmıştır. Kurumu taklit ederek bilgi çalmaya çalışan sahte mobil uygulamalar, Dark web'e yüklenen kredi kartı veya kişi bilgileri, yazılımlar, sosyal medyada kurum aleyhine yapılan kampanyalar N-SIS tarafından tespit edilip raporlanabilir. Alan adları, sosyal medya hesapları, mobil uygulamalar N-SIS tarafından kapattırılarak ulaşılamaz hale getirilir.

Sistem istihbaratı: Kurumun sunucularını, IP adreslerini, SSL sertifikalarını ve web yönlendirmelerini düzenli olarak takip eder. Sunucuların DNS-IP değişiklikleri, SSL sertifikalarının güvenlik durumu ve geçerlilik tarihleri, web sunucularının yönlendirme (redirection) işlemleri sürekli izlenir ve otomatik olarak raporlanır.

Tehdit İstihbaratı

Nebula Siber İstihbarat Servisi (N-SIS) bir güvenlik operasyon merkezinin ihtiyaç duyduğu iki ana konuya cevap vermek üzere tasarlandı: Engelleme ve Raporlama. N-SIS kötü kod veya uygulama dağıtan alan adlarını güvenlik üreticilerinden ve kullanıcıların erişmesinden önce öğrenerek güvenlik ürünlerinin engelleme listelerine otomatik olarak yazar. Cryptolocker türevi ataklar bu sayede kullanıcılar kötü bağlantılara erişmeye çalışsa bile engellenmiş olur.

Tehdit istihbaratı verisinin önemli bir bölümü Nebula'ya özgün geliştirilmiş yazılımlar ve Nebula Siber İstihbarat Uzmanlarınca yapılan kontrollerle keşfedilir. Verinin bir bölümü ise açık istihbarat kaynaklarının otomatik olarak okunması ve ayrıştırılması ile elde edilir. Nebula tarafından bulunan ve diğer istihbarat kaynaklarından alınan verilerin bütünleştirilmesinin ardından oluşan tehdit istihbaratı verisi zararlı alan adları, IP adresleri ve zararlı uygulama bilgilerini içerir.

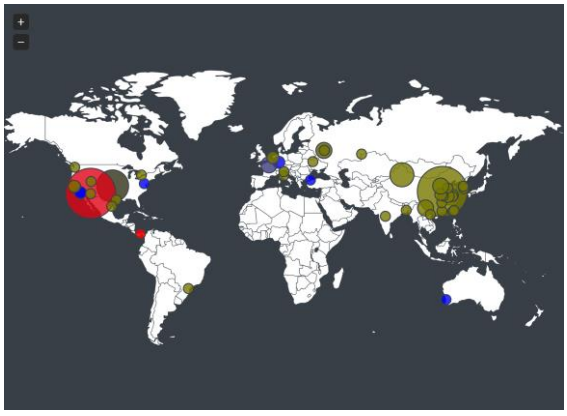
İstihbarat Veri Kalitesi

N-SIS veri tabanında Mart 2020 itibarı ile 340.000'den fazla istihbarat verisi (IOC) bulunmaktadır. Yaklaşık 32.000 kayıt N-SIS'e özeldir ve diğer istihbarat kaynaklarında bulunmamaktadır. Yaklaşık 46.000 kayıt ise diğer istihbarat kaynaklarından önce N-SIS tarafından tespit edilmiştir. Veri kalitesi VirusTotal, WoT ve

McAfee GTI gibi kaynaklara yapılan otomatik sorgular ile denetlenerek ve N-SIS müşterilerine eposta ve N-SIS Web uygulaması ile raporlanır.

		Intel Security (McAfee)		Virus Total		Web of Trust (WoT)	
URL/IP	Kontrol Tarihi	Itibar	Kategori	Itibar	Kategori	Itibar	Kategori
e-borcsorgu_com	2017.04.04-12:28:07.503	Netural (0)	None	0/64		0/0	
fatura-kontor_com	2017.04.04-12:28:07.503	Netural (0)	None	0/64		0/0	
get-bank-cards_market	2017.04.04-12:28:07.503	Netural (0)	None	0/0		0/0	
havayollari_info	2017.04.04-12:28:07.503	Netural (0)	None	0/0		0/0	
hepsiburada_sale	2017.04.04-12:28:07.503	Netural (0)	None	0/0		0/0	
hsbcbank_online	2017.04.04-12:28:07.503	Netural (0)	None	0/64		0/0	
kredinial_net	2017.04.04-12:28:07.503	Netural (0)	None	0/0		0/0	
netfaturaodeme_net	2017.04.04-12:28:07.503	Netural (0)	None	0/0		0/0	

Tehdit istihbaratı verisi N-SIS portalı aracılığı ile detaylı olarak raporlanabilir. Ayrıca güvenlik analistleri portal üzerinde sorgulamalar yaparak araştırmaları için veri üretebilir



Ürün Entegrasyonları

Nebula Siber İstihbarat Servisi (N-SIS) tarafından sağlanan zararlı alan adları, IP adresleri ve dosya bilgileri, bilgi güvenliği ürünlerine sağlanan entegrasyonlar ile otomatik olarak engelleme ve analize tabi tutulabilir.

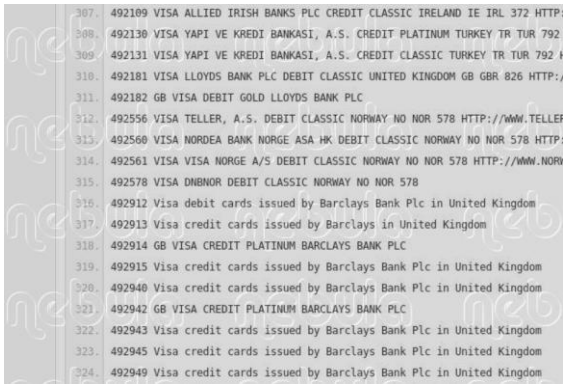
N-SIS tehdit istihbaratı verisi **McAfee Web Gateway**, **Blue Coat Secure Web Gateway**, **McAfee Network Security Platform**, **Palo Alto Networks**, **Fortinet** ve **Sophos** ürünlerine entegre olarak otomatik engelleme sağlanabilir.

McAfee Enterprise Security Manager (McAfee SIEM), **Blue Coat Security Analytics Platform** ve **Carbon Black** entegrasyonları tehdit istihbaratı verisini kullanarak detaylı ve otomatik analiz yapma imkânı sunar.

N-SIS Tehdit istihbaratı verisi **STIX** desteğine sahiptir ve STIX desteği olan her ürüne entegre edilebilir.

Marka İstihbaratı

Internet korsanları yasadışı bilgileri dark web ve deep web adları verilen çeşitli erişim sınırları olan sistemler kullanarak dağıtırlar. N-SIS **dark web** ve **deep web** olarak adlandırılan bu sistemlerde kredi kartı numaraları, eposta adresleri, alan adları, marka ve kişi adları gibi bilgileri otomatik olarak tespit eder ve kuruma otomatik bilgilendirme yapar. Pastebin ve Github gibi pano ve paylaşım portalları N-SIS tarafından tam otomatik olarak izlenir.



Kapattırma/Durdurma

Nebula Siber İstihbarat Servisi tespit edilen sahte alan adlarını, twitter hesaplarını ve mobil uygulamaları tam otomatik ve/veya insan gücü yöntemleri ile durdurabilir, kapattırabilir ve kurumun itibar kaybının önüne geçebilir.

Mobil Uygulama İstihbaratı

Sahte mobil uygulamalar marka haklarını ihlal etmek, müşteri verileri çalmak ve markalar hakkında kara propaganda yapmak için kullanılmaktadır. Kurumların bir mobil uygulamaya sahip olmalarına bakmaksızın marka ve ürünlerini taklit edecek yazılımları tespit etmesi bilgi güvenliği için önem taşır.

Suspicious/Malicious Aplications			
Status	Icon	Application Name	Store
Suspicious		Türksat Frekans	Apple AppStore
Suspicious		Uyduuzay	Apple AppStore
Suspicious		E-Devletim	Google Play Store
Suspicious		Frequencies TurkSat 42	Google Play Store

N-SIS marka ve ürünleri taklit eden veya müşteri verisi çalmak için tasarlanmış mobil uygulamaları **Apple App Store**, **Google Play Store** ve **3. Parti uygulama mağazalarında** yayınlandığı anda tespit eder ve kuruma gerekli bilgilendirmeyi otomatik yapar. Aynı zamanda uygulama dükkanlarından uygulamanın kaldırılması için işlemler başlatılır.

Kurumun resmi uygulama geliştirme hesabı tarafından yayınlanan yeni uygulamalar veya mevcut uygulamaların güncellemeleri de N-SIS tarafından takip edilir ve tespiti halinde gerekli bilgilendirme kuruma otomatik olarak yapılır.

Sosyal Medya İstihbaratı

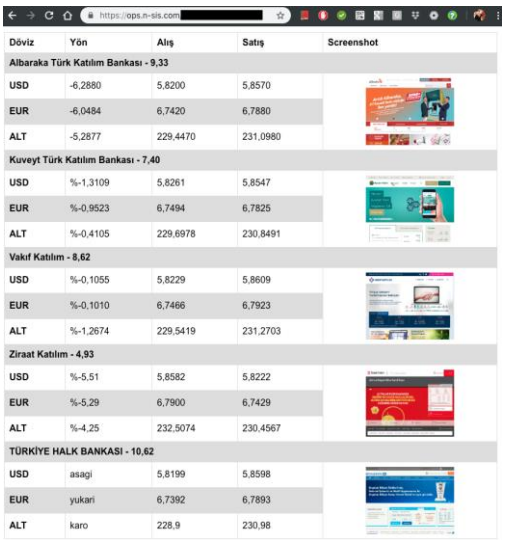
Sahte sosyal medya hesapları ve gönderileri tespit edilerek tuzak kampanyalar hakkında otomatik bilgilendirme sağlanır. Kampanya yürüten sosyal medya hesaplarına API üzerinden tam otomatik yöntemle (bazı sosyal medya ortamlarında insan gücü ile) kapatma talebi iletilir ve kampanya durdurulur.

Veri Sızıntısı İzleme

Kurum personelinin kişisel verilerinin veya şifrelerinin herhangi bir veri sızıntısıyla internet korsanlarının eline geçip geçmediği sürekli olarka izlenir ve tespit edilen sızıntı bilgisi otomatik olarak raporlanır. Kurum personeline ait eposta hesapları ve şifrelerin çalınıp çalınmadığı otomatik olarak izlenir.

Döviz Kuru İstihbaratı

Nebula Siber İstihbarat Servisi, bankanın yayın yaptığı döviz kuru bilgilerini düzenli takip eder. Ayrıca en az 5 diğer bankanın döviz kuru bilgilerini okur, aritmetik ortalamasını alır ve bankanın yayınladığı kur ile karşılaştırır. Beklenmeyen ve olağandışı sapmalar hakkında otomatik uyarı üretilir. Döviz kuru istihbaratı servisinin alt yapısı enerji fiyatları, borsa, faiz oranları gibi özel sistemler ve amaçlar için özelleştirilebilir.



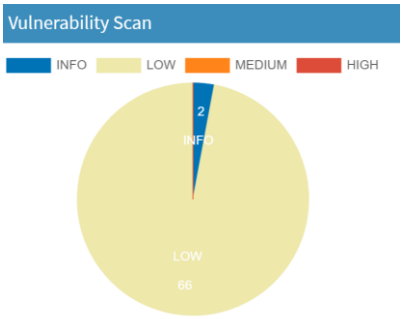
Döviz	Yön	Alış	Satış	Screenshot
Albaraka Türk Katılım Bankası - 9,33				
USD	-6,2880	5,8200	5,8570	
EUR	-6,0484	6,7420	6,7880	
ALT	-5,2877	229,4470	231,0980	
Kuveyt Türk Katılım Bankası - 7,40				
USD	%-1,3109	5,8261	5,8547	
EUR	%-0,9523	6,7494	6,7825	
ALT	%-0,4105	229,6978	230,8491	
Vakıf Katılım - 8,62				
USD	%-0,1055	5,8229	5,8609	
EUR	%-0,1010	6,7466	6,7923	
ALT	%-1,2674	229,5419	231,2703	
Ziraat Katılım - 4,93				
USD	%-5,51	5,8582	5,8222	
EUR	%-5,29	6,7900	6,7429	
ALT	%-4,25	232,5074	230,4567	
TÜRKİYE HALK BANKASI - 10,62				
USD	asagi	5,8199	5,8598	
EUR	yukari	6,7392	6,7893	
ALT	karo	228,9	230,98	

Sistem İstihbaratı

Nebula Siber İstihbarat Servisi (N-SIS) kurumların internet üzerinden erişilebilen IP adreslerini, sunucularını, web hizmetlerini ve SSL sertifikalarını izleyerek zafiyetleri, kontrollü veya kontrolsüz değişiklikleri, erişim problemlerini ve zafiyetleri tespit ederek anında uyarı üretir.

Sistem Zafiyet Tarama

Sisteme kayıt edilen sunucular belirlenen tarih ve saatlerde otomatik olarak zafiyet taramasına tabi tutulur. Bulunan zafiyetler N-SIS portalında listelenir ve raporlanır. Bir önceki taramada bulunmayan yeni zafiyetler için alarmlar üretilebilir.

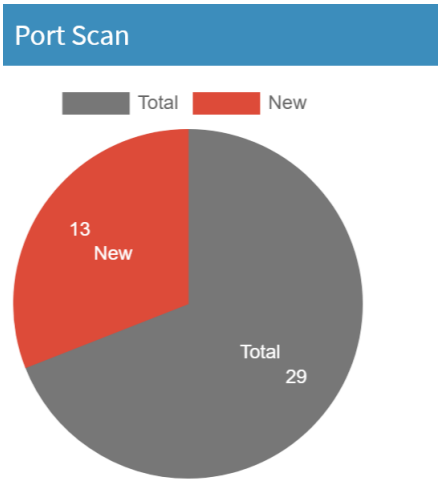


Web Uygulaması Zafiyet Taraması

Web uygulamalarına özel zafiyet taraması önceden belirtilen tarih ve saatte otomatik olarak yapılır. Kullanıcı adı ve şifre ile giriş yapılan web siteleri için otomatik giriş sağlanarak giriş sonrası web sayfaları taranabilir. Tespit edilen açıklıklar N-SIS portalında listelenir ve raporlanır. Bir önceli taramada bulunmayan yeni zafiyetler için alarmlar üretilir.

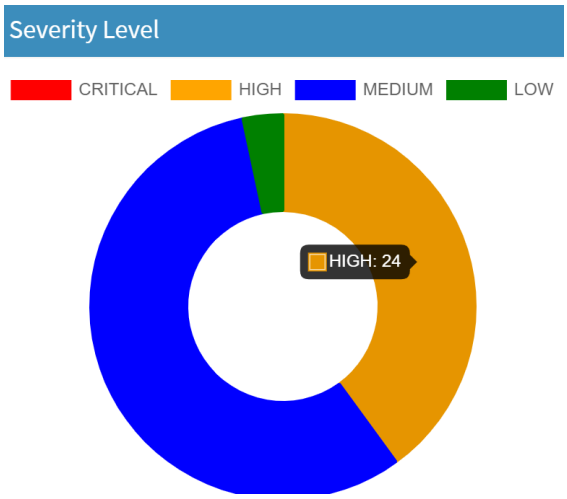
Port Taraması

Takip edilen sunuculara periyodik ve otomatik olarak port taraması yapılabilir. Tarama sonuçları N-SIS portalında raporlanır. Bir önceki taramada bulunmayan, yeni hizmete başlamış portlar tespit edildiğinde sistem yöneticisine alarm gönderilir.



Zafiyet İzleme

N-SIS kullanıcıları bilişim varlıklarının listesini marka ve model olarak hesaplarına kaydeder. Kayıtlı markalar, ürünler ve sürümlerinde tespit edilip duyurulan zafiyetler N-SIS tarafından otomatik olarak öğrenilir ve varlık sahibine riskler alarm olarak gönderilir. N-SIS portalı aracılığı ile zafiyetler hakkında detaylı sorgulamalar yapılabilir ve raporlar alınabilir.



Host Tracker

Sunucu adlarını (örnek: isube.bank.com) sürekli kontrol eden N-SIS sistemlere erişim problemi yaşandığında otomatik bilgilendirme yapar.

Yük dengeleme cihazları, sunucu küme sistemi, sunucu değişikliği gibi kontrollü nedenlerle birlikte DNS sisteminin hack edilmesi, IP adresinin kontrolsüz yönlendirilmesi gibi nedenlerle oluşabilecek IP ve servis etiketi temelli değişiklikler tespit edilir otomatik olarak raporlanır.

Web sunucularının kontrollü ana sayfa yönlendirmeleri (örneğin “geçici olarak bakımdayız” sayfasına yönlendirme) ve kontrolsüz yönlendirme (web hizmetinin ele geçirilerek ana sayfanın değiştirilmesi, htaccess erişimi ile başka bir sayfaya yönlendirme gibi) N-SIS tarafından tespit edilerek kuruma raporlanır.

SSL Tracker

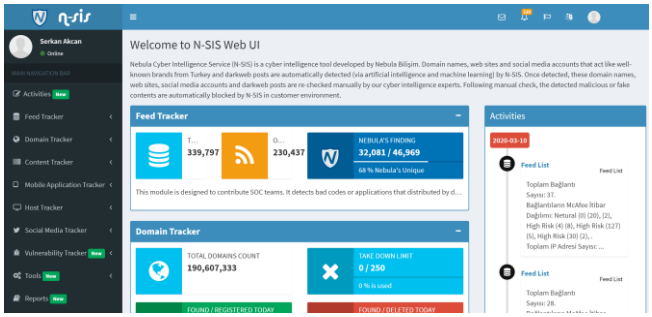
Web sunucular üzerinde hizmet vermekte olan SSL sertifikalarının güvenlik seviyesi ve son kullanım tarihleri N-SIS tarafından düzenli olarak izlenir. Tehdit içeren sertifikalar (örneğin revoke edilmiş olanlar) ve son kullanım tarihi yaklaşan sertifikalar hakkında otomatik uyarılar oluşturulur.

Geçersiz veya geçerli bir sertifikanın değişmesi durumunda N-SIS değişimi tespit edip otomatik uyarı üretir.

HeartBleed, TicketBleed, PoodleSSL ve Lucky13 gibi 20 kadar SSL/TLS zafiyeti otomatik olarak taranır ve tespit edilen zafiyetler otomatik raporlanır.

N-SIS User Portal

Nebula Siber İstihbarat Servisi tespit ettiği tehdit istihbaratı, marka istihbaratı ve sistem istihbaratı bilgilerinin tamamını otomatik olarak e-posta ile iletir. İstihbarat bilgilerinin detayı ve geçmişi ise N-SIS User Portal üzerinden erişilebilir. User Portal üzerinde kuruma ait birden fazla kişi için kullanıcı yaratılabilir ve verilere tüm BT ekibinin erişmesi sağlanabilir.



Lisanslama seçenekleri?

Nebula Siber İstihbarat Servisi yıllık abonelik lisansı ile satılmaktadır. Detaylı bilgi için lütfen bizimle temasa geçiniz.

Nebula Siber İstihbarat Servisi	Temel	Standart	Gelişmiş	Profesyonel
Tehdit İstihbaratı				
2 Günlük Tehdit İstihbaratı	Yok	Var	Var	Var
7 Günlük Tehdit İstihbaratı	Yok	Var	Var	Var
30, 90, 180 Gün ve Sınırsız İstihbarat	Var	Var	Var	Var
Marka İstihbaratı				
Yeni Alan Adı İstihbaratı	Var (3 keyword)	Var (5 keyword)	Var (10 keyword)	Var (25 keyword)
Alan Adı Kapattırma	Yok	Opsiyonel	Opsiyonel	Opsiyonel
Darkweb İstihbaratı	Yok	Var (5 keyword)	Var (10 keyword)	Var (25 keyword)
Apple App Store İstihbaratı	Yok	Var (5 keyword)	Var (10 keyword)	Var (25 keyword)
Google Play Store İstihbaratı	Yok	Var (5 keyword)	Var (10 keyword)	Var (25 keyword)
Facebook İstihbaratı	Yok	Var (1 sayfa)	Var (5 sayfa)	Var (10 sayfa)
Twitter İstihbaratı	Yok	Var (1 hesap)	Var (5 hesap)	Var (10 hesap)
Instagram İstihbaratı	Yok	Var (1 hesap)	Var (5 hesap)	Var (10 hesap)
Sistem İstihbaratı				
Zafiyet ve Port Tarama	Opsiyonel	Opsiyonel	Opsiyonel	Opsiyonel
Sunucu adı izleme	Var (3 Sunucu)	Var (10 Sunucu)	Var (25 Sunucu)	Var (100 Sunucu)
IP izleme	Var	Var	Var	Var
www redirection izleme	Var	Var	Var	Var
Defacement Monitor	Var	Var	Var	Var
SSL Sertifika Güvenlik Kontrolü	Var	Var	Var	Var
SSL Sertifika Expiration Date Kontrolü	Var	Var	Var	Var

Nebula Bilişim Sistemleri Sanayi ve Ticaret Ltd
www.nebulabilisim.com.tr
info@nebulabilisim.com.tr
Tel: 0850 432 86 32