SCADAfence
GLOBAL VAD

OTD BİLİŞİM

Beyaz Kağıt

DENİZCİLİK
& KONTROL SİSTEMLERİ
SİBER GÜVENLİK SUÇLARI

2022

Hack The Port Tanıtım

Hack The Port 2022, ABD Siber Komutanlığı, NSA ve Maryland İnovasyon ve Güvenlik Enstitüsü (MISI) tarafından desteklenen ve Amerika Birleşik Devletleri'ndeki işlevsel bir deniz limanının güvenliğini tehlikeye atmak için gerçek dünya girişimini simüle eden bir yarışmadır. Yarışma, Mart 2022'de Florida'da gerçekleşti.

Yarışma organizatörleri, " Red Teams" kırmızı takımları Limanı Hacklemeye, yani limanın teknolojik altyapısının güvenliğini ciddi şekilde tehlikeye atmaya ve "Blue Teams" mavi takımları savunuculuk yapmaya davet etti. Yarışma, gerçek dünyadaki bir endüstriyel limanın tüm yönlerini ve olası risklerini kapsayan altı senaryoyu içeriyordu.

Kırmızı ekiplerin, gerçek dünyadaki tehdit aktörlerinin ağları ihlal etme girişimlerinde kullanacakları kimlik avı, metasploit, DDOS saldırıları ve diğerleri dahil olmak üzere herhangi bir yolu kullanmalarına izin verildi. Mavi takımın görevi saldırıları tespit etmek ve saldırganları durdurmaktı. Bu teknik inceleme de, alıştırmanın bulgularını ve sonuçlarının özeti ve SCADAfence'in limanı saldırılara karşı başarıyla savunmadaki başarısını detayları bulunuyor.

Yönetici Özeti

SCADAfence Platformu, Hack The Port yarışmasında, kurgusal porta yönelik en fazla saldırıyı başarılı bir şekilde tespit edip önlerken en az yanlış alarm sonuçlarla tüm rakiplerini geride bıraktı.

SCADAfence Platformu, kritik sistemleri tehlikeye atmak için DCSync, Log4J, kendinden imzalı metasploitler, Mimikatz indirme, RDP saldırıları ve domain denetleyicilerini hackleme gibi çeşitli teknikler kullandıkları için kırmızı ekipleri yakaladı.

Gerçek dünyada, bu tür saldırılar tespit edilmezse bir limanın kapanmasına ve ekipmanda büyük hasara, kritik sistemlerin kesintiye uğramasına ve hatta fiziksel yaralanmalara neden olabilir.

SCADAfence Platformunu Kurma

Tehdit aktörlerinin limana saldırmasını tespit etmek ve önlemek için ilk adım, SCADAfence Platformunu çalışır duruma getirerek liman ağlarını güvence altına almaktı.

Hack The Port etkinliği başlamadan önce SCADAfence ekibi kurulum paketini etkinlik organizatörlerine gönderdi. Organizatörler SCADAfence Platformunu kendi başlarına sorunsuz bir şekilde kurabildiler ve kutudan çıktığı gibi çalıştı. SCADAfence ekibinin ek yapılandırma yapmasına veya destek vermesine ihtiyaç duyulmadı.

SCADAfence Platformunun mega fabrikaya veya Hack The Port gibi liman işletmesi ağına kurulması arasında herhangi bir fark olmadan 10 dakikada tamamlanır. 10 dakika sonunda, SCADAfence Platformu çalışmaya başlamış ve limanı koruyordu.

SCADAfence GLOBAL VAD

OTD BILIŞIM

Saldırı Senaryoları

Liman Vinci

Endüstriyel bir limanın portal vinci, limanın üzerinde duran ve gemilere konteynırları yüklemek ve boşaltmak ve gemi inşası ve onarımında kullanılan motorları ve diğer ağır ekipmanları kurmak için kullanılan büyük bir tavan vincidir. Bu vinçler, özel yazılıma sahip bir bilgisayar aracılığıyla kontrol edilir ve çalıştırılır. Bu saldırı senaryosu, kırmızı ekip katılımcılarından vincin kontrol sistemini ihlal etmeye ve vincin hareketini bozmalarına ve bir geminin motorunu doğrudan okyanusa indirmelerine izin vermek için yeterli erişim elde etmesini istedi.

Su Filtrasyon Sistemi

Büyük bir limandaki su filtreleme sistemi, gemi personeline ve tüm limana temiz su sağlamaktan sorumludur. Bu meydan okumanın amacı, makineleri kontrol eden cihazlara erişerek su filtreleme sistemini sabote etmek ve sistemi suya yanlış oranda katkı maddesi eklemesi için kandırmaktı. Bu zorluğun önemli bir parçası, sistem dedektörlerinin değişiklikleri keşfetmesini engellemekti.

Gemi Bordası Networku

Bu senaryoda kırmızı ekiplerden istenen; limana yanaşmaya çalıştıkları sırada gerçek gemilerin köprü kontrol sistemlerine erişmeleri ve geminin pervanelerini kapatmaları böylece gemiyi engellemeleri yani limanda kilitlenmelerini sağlamalarıydı.

Balast Kontrolü

Bu senaryo da bir geminin köprü üstü kontrol sistemlerine erişim sağlamayı gerektirmekteydi. Bu senaryoda, kırmızı ekipler geminin balast kontrol sistemine erişmeye ve HMI'ların sistemin pompalama yapılmazken bile hatalı olarak su pompaladığını belirtmesini sağlamaya çalıştılar.

Takip Sistemi

Tüm büyük endüstriyel tesisler gibi, Hack The Port'un organizatörleri de limanlarına, gerektiğinde daha sonra incelenmek üzere kaydedilmek üzere dijital görüntüleri kaydeden kameralardan oluşan bir gözetim sistemi yerleştirdiler. Kırmızı ekiplerden bu ağı kapatmaları ve daha sonra tehdit aktörlerini etkileyebilecek hiçbir verinin korunmadığından emin olmaları istendi.

Erişim Kontrol Sistemi

Limanda işçilere verilen güvenlik kimlik kartları, deniz güvenliğinin kritik yönlerinden biridir. Herkesin kısıtlı alanlara uygun erişim seviyesinde yetkiye sahip olmasını sağlamak, ilgili alanların güvenli kalmasına yardımcı olacaktır. Bu senaryoda, kırmızı ekiplerin kapı kontrol sistemlerine ve kart okuyucularına erişmesi ve limana yetkisiz girişlerin yapılmasını sağlamaları gerekiyordu.

SCADAfence GLOBAL VAD

OTD BILIŞIM

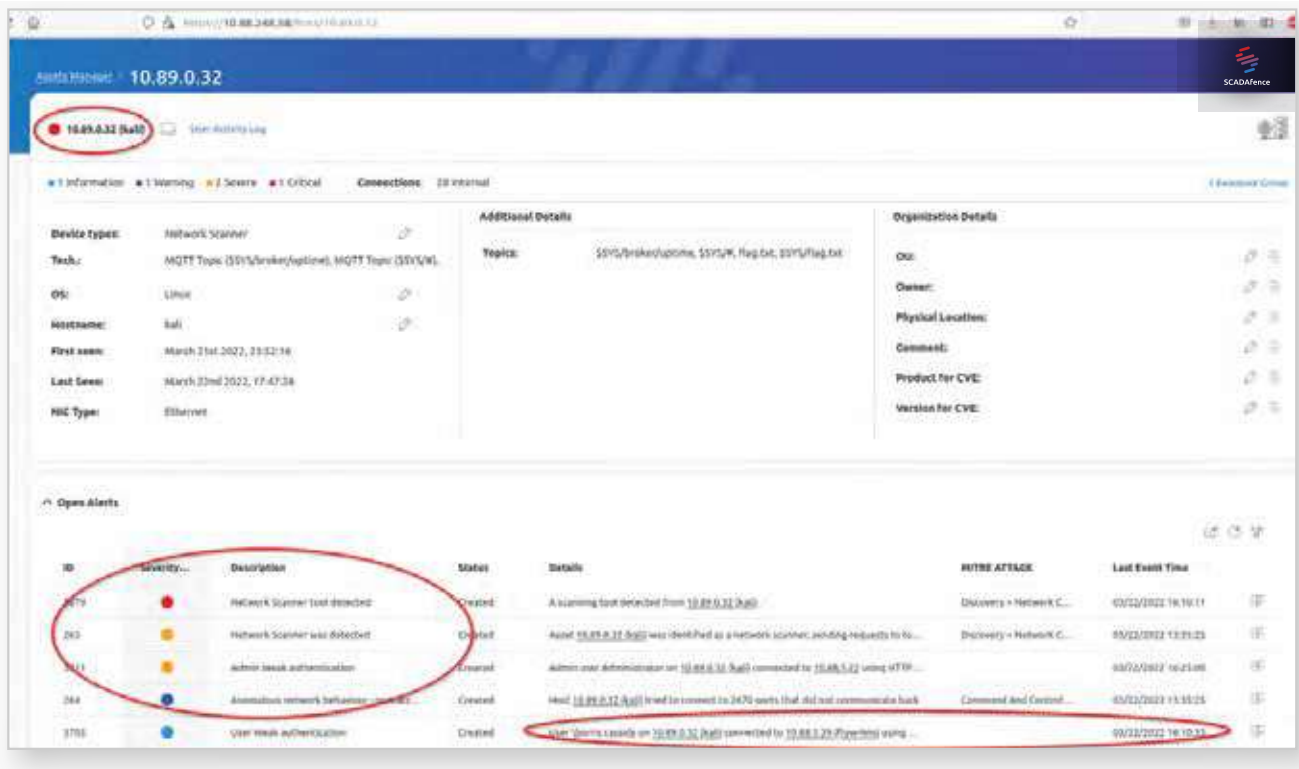
SCADAfence tarafından tespit edilen Kırmızı Ekip Saldırıları

Ağın Taranması

Beklendiği gibi, kırmızı ekipler her senaryoya ağın keşfi ile başladı.1 Bu işlem, Ağa bağlı cihazların bir envanteri, bu cihazlarda çalışan servisler, cihaz tipleri, IP adresleri, açık portlar, üretici isimleri, ve cihazların hangi işletim sistemi yazılımını çalıştırdığı yönündeki bilgileri toplamak için bir tarama ile başlamaktadır. Daha sonra bu bilgileri bilinen güvenlik açıklarıyla bu cihazları ilişkilendirmek için kullandılar ve daha fazla ağ erişimi elde etmek için bulabilecekleri başka bir şey aramaya devam ettiler.

Gerçek Dünya Etkisi:

Bir saldırgan tarafından ana makineden ve ana makineye veri aktarırken eylemlerini ve araçlarını gizlemek için kendinden imzalı (self-signed) Metasploit sertifika kullanılabilir.



Network taraması Host görüntüsü 0.89.0.32

[1] Öldürme zincirinin (kill-chain) ilk adımı tespittir:
- https://collaborate.mitre.org/attackics/index.php/Discovery
- https://attack.mitre.org/tactics/TA0043/
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

SCADAfence GLOBAL VAD

OTD BILIŞIM

Metasploit Sertifika Kullanımı

Rutin bir tarama sırasında, SCADAfence Platformunun tespit ettiği ilk şeylerden biri, DigiCert veya GoDaddy gibi güvenilir bir şirket tarafından imzalanmış bir sertifika yerine Metasploit Framework tarafından imzalanmış bir sertifika olan kendinden imzalı bir (self – signed) Metasploit sertifikasıydı. Bu, ağ üzerinden gönderilen yetkisiz veya kötü amaçlı etkinliği gösterir. Spesifik olarak, [c][d] 10.88.0.252 (NAT) IP adresine sahip bir yönlendirici tarafından verildi.

Gerçek Dünya Etkisi:

Bir Metasploit sertifikası, kendinden imzalı olsa bile, ana makinenin güvenini kazanmak için kullanılabilir. İşaretlenmeden bırakılırsa, tehdit aktörleri ağın daha derinlerine nüfuz edebilir.

Metasploit Sertifika Kullanımını Tespit Etme. Her uyarı, sorunun daha fazla araştırılmasına yardımcı olmak için PCAP dosyasını içerir.

RDP (Uzak Masaüstü Protokolü) Üzerinden Saldırı Girişimi

SCADAfence Platformu, saldırganların FLOW-HMI makinesiyle bağlantı kurmak için 4.700'den fazla kez denediğini tespit etti. Sonunda başarılı bir RDP oturumu oluşturmayı başardılar.

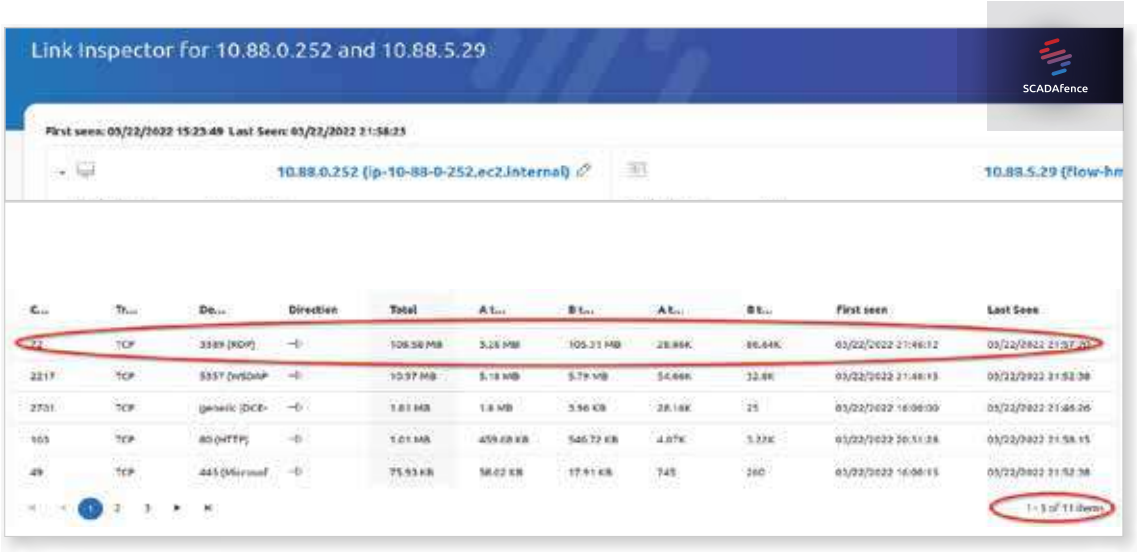
FLOW-HMI ile başarılı bir RDP bağlantısını gösteren bir uyarı

SCADAfence GLOBAL VAD | OTD BILIŞIM

Bilinen kötü niyetli aktörlerden (10.88.0.252, 10.88.0.106) aynı gün gerçekleşen 10.88.5.29'dekii diğer birkaç başarılı RDP oturumunun öncesinde, hedeflenen taramalar veya bruteforce oturum açma girişimleri yapıldı ve yakalandı.

Gerçek Dünya Etkisi:

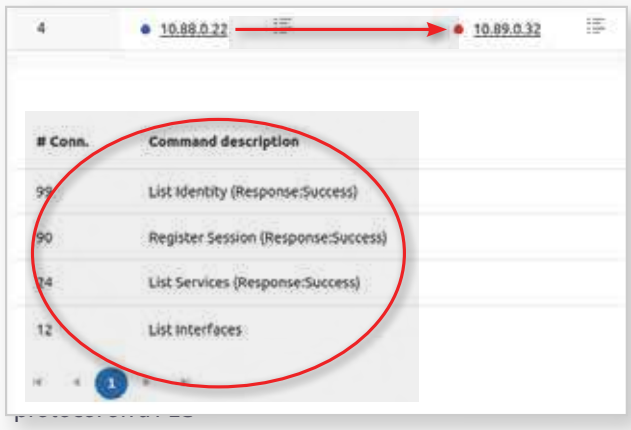
Bir RDP Oturumunu başarıyla başlatan tehdit aktörleri, ana makine üzerinde tam bir kontrole sahiptir ve diğer orijinal oturum açma kimlik bilgilerini, parolaları ve diğer hassas bilgileri çalabilir ve fidye yazılımı saldırıları başlatabilir. Bir HMI'ya bu şekilde erişim, uzak operatörler bu erişimleri fiziksel hasara vermek için kullanabilecekleri için özellikle tehlikelidir.



FLOW-HMI ile başarılı bir RDP bağlantısını gösteren bağlantı denetçisi

Allen-Bradley ENIP Kullanarak Başarılı PLC Taraması

SCADAfence Platformu, başka bir saldırı girişiminde, bir PLC'den ayrıntıları almak için Allen-Bradley'nin ENIP protokolünü kullanmaya çalışan kırmızı takım saldırganlarını yakaladı. SCADAfence Platformu, saldırganların bir cihazın kimliği, model adı, oturum detayları ve PLC'den ek bilgiler gibi detayları başarıyla elde ettiğini tespit edebildi.

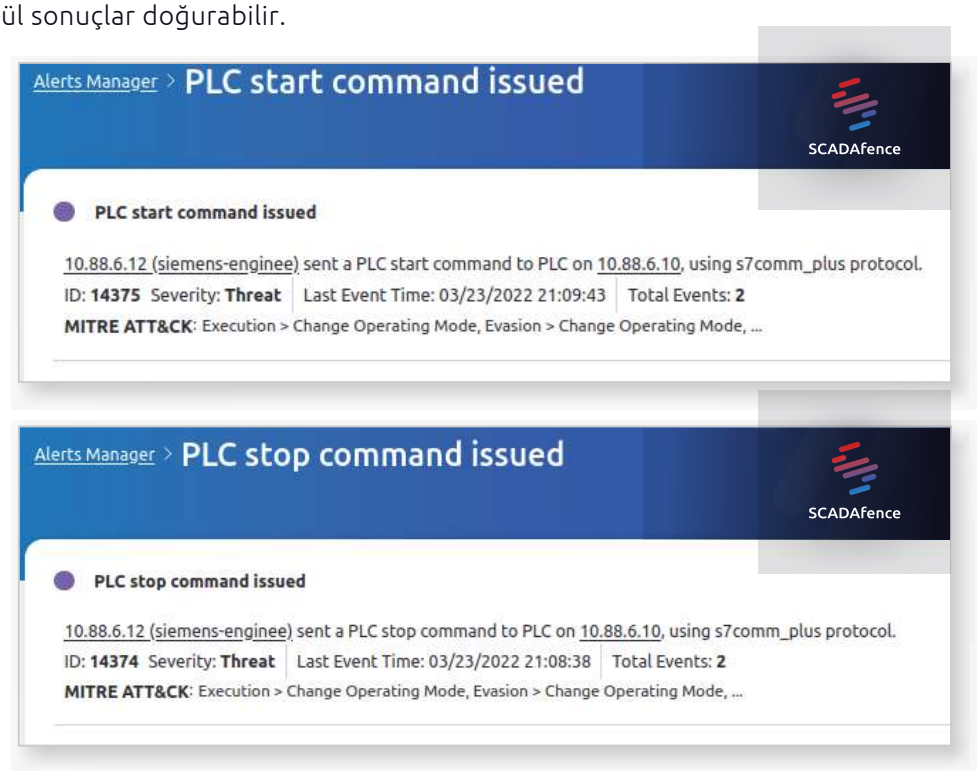


Bir PLC'yi Başlatma ve Durdurma

SCADAfence Platformunun tespit edebildiği en önemli saldırılardan biri, bir PLC'ye gönderilen gerçek başlatma/durdurma komutlarıydı. PLC'ye erişim sağladıktan sonra, tehdit aktörleri, cihazın çalışma modunu değiştirmek için komutlar göndererek güvenliği ihlal edilen cihaza saldırılarını sürdürdüler.

Gerçek Dünya Etkisi:

PLC'ler, fiziksel ekipmanı kontrol etmek veya otomatikleştirmek için kullanılır. Bu erişim seviyesiyle, tehdit aktörleri, bir elektrik şebekesini kapatma, makinelere zarar verme veya bir su kaynağından ödün verme gibi fiziksel saldırıları gerçekleştirmesi için PLC'ye komutlar verebilir ve bunların tümü potansiyel olarak ölümcül sonuçlar doğurabilir.



Mühendislik istasyonu 10.88.6.12, PLC'ye PLC durdurma ve başlatma komutları gönderdi 10.88.6.10

SCADAfence GLOBAL VAD

OTD BILIŞIM

Mimikatz'ı Tehlike Altında Bir Domain Denetleyicisine İndirme

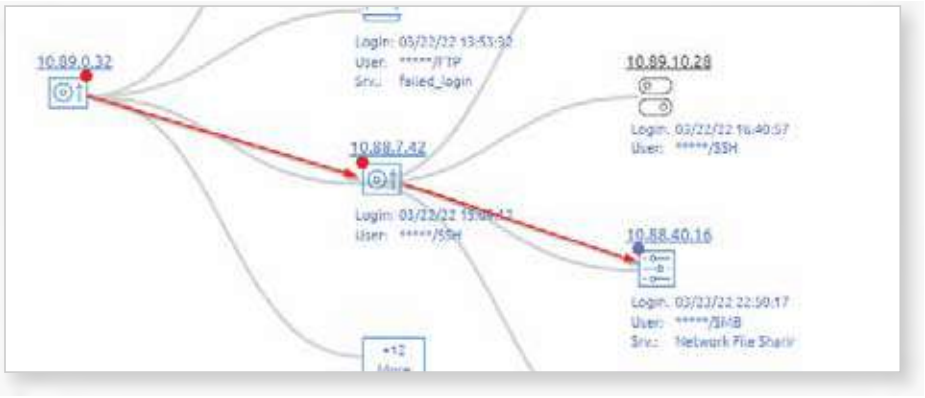
Tehdit aktörlerinin önemli saldırılar başlatmasının önemli bir yolu, önce bir ağda bir yer edinmek, ardından bu giriş noktasını tespit edilmeden çalışabilecekleri ağa daha fazla nüfuz etmek için kullanmaktır. SCADAfence Platformu, bu tekniği kullanan Hack the Port etkinliğinin en önemli saldırılarından birini tespit etti.

Kırmızı Takım'ın ilk ihlali, başlangıç noktası olarak kullandıkları başarılı bir brüte-force saldırısıydı ve ardından, ihlal edilen SSH erişimini kullanarak bir aracı cihaz üzerinden bir domain denetleyicisine eriştiler. Bu noktadan sonra saldırganlar, parolaları ve diğer hassas bilgileri çalmak amacıyla Mimikatz'ı güvenliği ihlal edilmiş bir domain denetleyicisine indirmeye çalıştı. SCADAfence Platformu bu indirmeyi tespit etti.

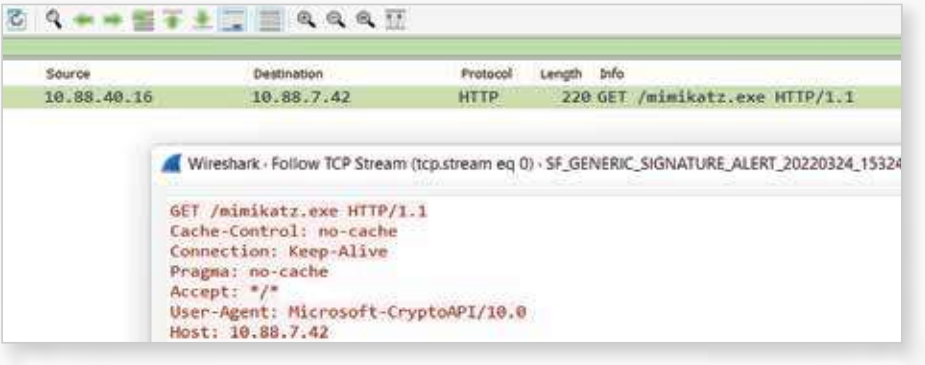
Gerçek Dünya Etkisi:

Mimikatz ile çıkarılan verileri ağın daha derinlerine inmek ve ek cihazları tehlikeye atmak için tehdit aktörleri kullanır.

Mimikatz aracını indirme girişimini algılama



Saldırganın yolunu domain denetleyicisine eşleme



Mimikatz yürütülebilir dosyasının http indirmesini gösteren ekli Pcap

TIA Portalına Bağlanma

Bir endüstriyel limanın (veya herhangi bir bilgisayar kontrollü üretim veya üretim ortamının) işleyişini kontrol eden en önemli cihazlar arasında HMI'lar ve operatör/mühendislik istasyonları bulunmaktadır.
Bunlara ve onları kontrol eden PLC'lere erişim sağlamak, bir tehdit aktörü için en büyük ödüller arasındadır.
Hack the Port olayı sırasında, SCADAfence Platformu, 8888 numaralı bağlantı noktasına harici bir bağlantı tespit etti. Bağlantı noktası 8888, Siemens TIA Yöneticisinin (TIA Portalı) entegre yapılandırma web uygulaması için kullanılır.

Bu, tehdit aktörlerinin PLC'ye erişmeye çalıştıklarını gösterdi. Yine Platform tarafından algılanan iki yönlü iletişim, bu bağlantıyı başarıyla kurduklarını ve PLC'nin tehlikeye girdiğini gösterdi.

Siemens tarafından yerel kullanıcı erişimi için kısıtlanması önerilen TIA Portal portlarından biri olan 8888 numaralı TCP portuna bağlantı kuruldu.

SCADAfence GLOBAL VAD

OTD BILIŞIM

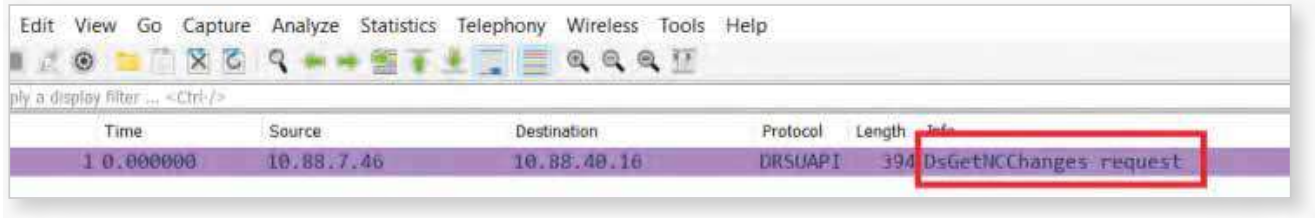
DCSync Saldırısı

Hack the Port, dikkate değer güvenlik açıklarına sahip bir dizi Raspberry PI cihazını içeriyordu. Çoğu kırmızı ekip, Raspberry PI ağında bir yer edinmeyi başardı ve bir veya daha fazla aracı cihaz kullanarak ağa daha derin erişim sağlamak için bunu bir atlama noktası olarak kullandılar.
Bu durumda, bir domain denetleyicisine karşı bir DCSync saldırısı başlatmak için Raspberry PI ağının güvenliği ihlal edildi.
Saldırgan önce Raspberry PI'yi ele geçirdi ve domain denetleyicisine saldırmadan önce bunu SSH aracılığıyla bir HMI'ya erişmek için bir atlama noktası olarak kullandı. Saldırganlar, SMB protokolünü kullanarak domain denetleyicisinden bilgi elde etmek için kendi denetimlerini kullandılar.

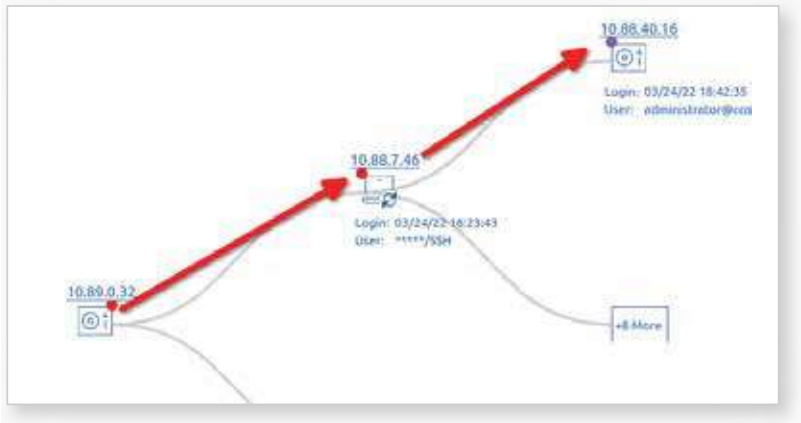
Gerçek Dünya Etkisi:

DCSync saldırısı, halihazırda bir ağa sızmış olan tehdit aktörleri tarafından gerçekleştirilen geç aşamadaki bir saldırıdır. Active Directory'nin yönetici kontrolünü elde etmek için kullanılır. Bir kez sahip olduklarında, her domain denetleyicisine zarar veren değişiklikleri çoğaltabilirler.

DCSync saldırısını gösteren bir uyarı



Saldırganın domain denetleyicisine giden yolu



Saldırganın domain denetleyicisine giden yolu

Log4J Karşı Saldırı Yapıyor

Açık kaynaklı günlük kitaplığı Apache Log4J'de 2021'in sonunda büyük bir güvenlik açığı tespit edildi. SCADAfence, saldırı keşfedildikten hemen sonra Log4J güvenlik açığı için destek ekledi. Hack The Port'ta kırmızı ekip, keşfedilmemesini umarak bu bilinen güvenlik açığını bir saldırı düzenlemek için kullandı. Bu saldırının hedefi, bir IO-link ENIP adaptörü olan AL1970 idi. SCADAfence Platformu, cihazda uzaktan kod yürütmek için Log4J güvenlik açığını kullanma girişimini hemen tespit etti.

Gerçek Dünya Etkisi:

Log4J güvenlik açığı, tehdit aktörlerinin bir cihazın tam kontrolünü ele geçirmesine ve kötü amaçlı kod çalıştırmasına, kötü amaçlı yazılım saldırıları başlatmasına ve ağa tamamen sızmasına olanak tanır.

Log4J saldırısını gösteren bir uyarı

Ekli PCAP IP 192.168.0.32, Log4j / Log4Shell güvenlik açığını kullanarak 10.88.5.24'e saldırdığını gösteriyor

SCADAfence GLOBAL VAD

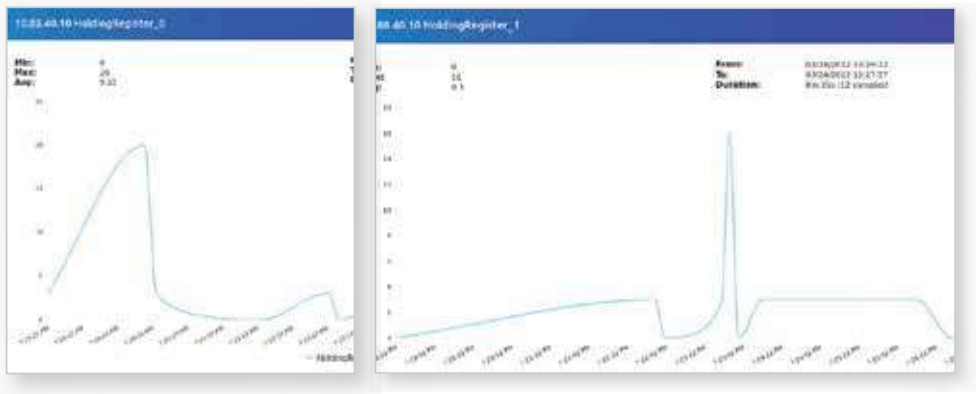
OTD BILIŞIM

Ele Geçirilmiş Bir Domain Denetleyicisinden Değer Analizi Değişiklikleri

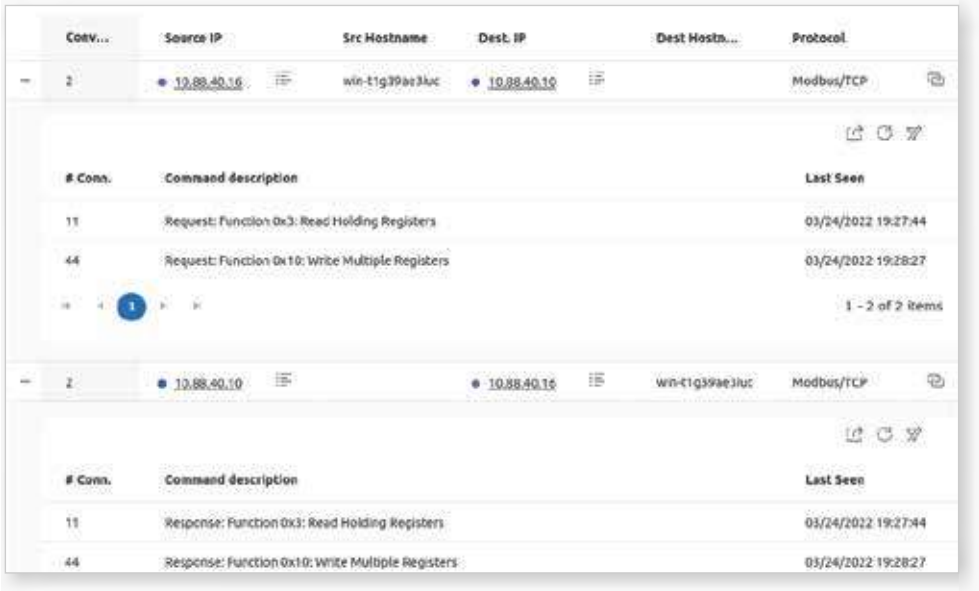
SCADAfence Platformunun en hayati özelliklerinden biri olan Değer Seviyesi özelliği, temel OT komut seviyesi algılamasının ötesine geçerek PLC'ye gönderilen gerçek OT değişken değerlerini alır.
Hack the Port olayı sırasında, SCADAfence Platformu, güvenliği ihlal edilmiş bir domain denetleyicisinden kaynaklanan değer düzeyi değişiklikleri algıladı. Değerlerdeki beklenmeyen değişiklikler bir ihlali gösterir ve gerçek dünya senaryosunda büyük bir saldırıyı gösterebilir. Bu durumda saldırgan, hem PLC'yi hem de bağlı makine/sensörleri kesintiye uğratmak için Modbus protokolü aracılığıyla PLC'deki değerleri önemli ölçüde daha yüksek bir değere değiştirmiştir. Saldırganın amacı, su kaynağına zararlı katkı maddeleri dökerek zarar vermekti.

Gerçek Dünya Etkisi:

Bu gerçek bir olay olsaydı, bu uyarı, tehdit aktörlerinin güvenlik kontrollerini ihlal etmeyi başardığını ve büyük aksamalara neden olduğunu gösterirdi. SCADAfence Platformunun Değer Düzeyi değişiklik uyarıları, HMI kamufle etmek için tehlikeye atılmış olsa bile, hasarın yapıldığını kanıtlar.



SCADAfence Platform Value, Modbus protokolü aracılığıyla güvenliği ihlal edilmiş bir etki alanı denetleyicisinden yapılan bir PLC üzerindeki değişiklikleri algılar.



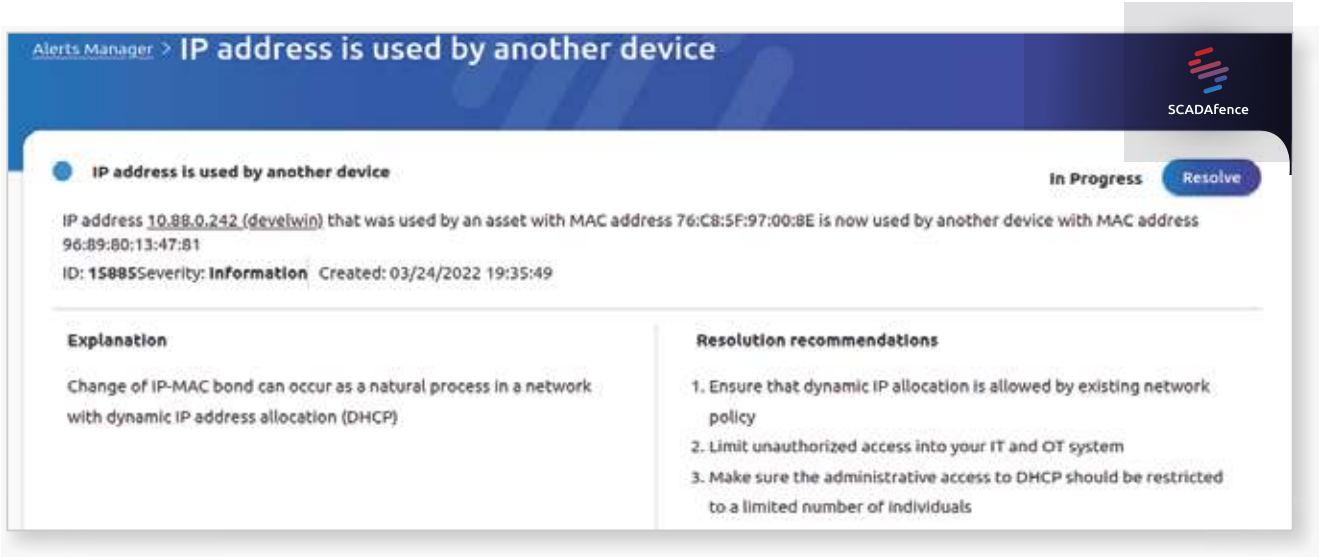
PLC'deki değer seviyesi değişikliklerini gösteren bir uyarı

SCADAfence GLOBAL VAD

OTD BILIŞIM

Tüm Yeni Kırmızı Takım Senaryolarını Tespit Etme

Kırmızı ekiplerden biri saldırı senaryosu üzerinde çalışmayı tamamlarken, bir başka kırmızı ekip sırayla görev aldı. SCADAfence Platformu, ağa eklenen yeni IP adresleri nedeniyle değişikliği tespit edebildi. Aynı IP adresinin yeni bir cihaz tarafından kullanılması, potansiyel olarak IP'yi kullanan bir cihazın sahneyi terk ettiğini ve yeni bir cihazın girdiğini, aynı IP'yi aldığını ve dolayısıyla ilgili bir olayı tetiklediğini gösterdi.



IP/MAC korelasyonu ile senaryo değişiklikleri tespit edildi

SCADAfence GLOBAL VAD

OTD BİLİŞİM

Liman Güvenliğini Korumanın Yaşamsal Önemi

- Her yıl dünya çapında sevk edilen çok miktarda maddi mal şaşırtıcıdır. Tahminler, okyanus veya deniz sınırındaki her büyük ülkedeki deniz limanlarına 100.000 gemiyle okyanus yoluyla 815,6 milyon 20 fitlik nakliye konteynırının seyahat ettiği yönündedir.
- Denizcilik sistemlerine yönelik siber saldırılar son üç yılda %900 arttı.
- Başarılı bir saldırının maliyeti de artıyor. Sigortacı Lloyd's of London, Asya limanlarına yönelik tam ölçekli bir siber saldırının tek başına 110 milyar dolara mal olabileceğini ve her sanayileşmiş ülke üzerinde büyük dalgalanma etkileri olabileceğini tahmin ediyor.
- Bu limanları işleten makinelerin siber bütünlüğünü sağlamak için kaya gibi sağlam bir OT siber güvenlik sisteminin önemi göz ardı edilemez. Hack-The-Port alıştırması, en son teknolojinin bile, nasıl yapılacağını bilenler tarafından istismar edilebilecek güvenlik açıklarına sahip olduğunu gösterdi.

thal edilen mallar, konteyner gemileri, su filtreleme sistemi ve en önemlisi liman çalışanlarının fiziksel güvenliği, uygun erişim sağlandığında zarar verebilecek tehdit aktörlerine karşı savunmasızdır. Bu nedenle, tümü, OT ağının herhangi bir yerindeki yetkisiz veya şüpheli etkinlikleri gerçek zamanlı olarak algılayabilen ve uyarabilen bir OT savunma sistemine ihtiyaç duyar.

SCADAfence GLOBAL VAD

OTD BİLİŞİM

Sonuç: SCADAfence Platformu Üstünlüğünü Kanıtlıyor

SCADAfence Platformu, kurgusal limana karşı en geniş çeşitlilikte kırmızı ekip saldırı girişimini tespit etmeyi başardı. SCADAfence Platformu, çok sayıda dikkat dağıtıcı yanlış pozitif olmayanları ayırarak güvenilmeyen x.509 sertifikalarından ve DCSync saldırılarından yetkisiz PLC başlatma/durdurma komutlarına ve diğerlerine kadar ağlarındaki ihlaller için uyarılar oluşturdu.

> SCADAfence mavi ekibi, en az yanlış alarm ile tüm mavi ekip kanalı içinde en kapsamlı raporlama bilgilerini sağladı.

Anlatıcı 29/03/2022
Her şeyden önce, lütfen tüm ekibinizin, tüm BLUE ekip kanalı için en kapsamlı raporlama ayrıntılarını sağladığınızı bilmesini sağlayın.

SCADAfence ekibi, Hack The Port etkinlik organizatörleri tarafından tebrik edilir.

SCADAfence Platformunun gerçek dünya senaryolarında siber güvenlik ihlallerini tespit etme ve doğru alarmlar üretme yeteneği, bugün dünyadaki birçok endüstriyel limanda olduğu gibi bu limanı da büyük güvenlik olayları yaşamaktan koruyacaktır.

Bu vaka çalışması bunu göstermek için mükemmel bir örnektir.

SCADAfence GLOBAL VAD

OTD BİLİŞİM