LetsDefend Çalışma Notları:

SOC TEMELLERİ: **-Ahmet Arif Arslan-**

SOC nedir?

Güvenlik Operasyon Merkezi (SOC), bilgi güvenliği ekibinin bir kuruluşun güvenliğini sürekli olarak izlediği ve analiz ettiği tesistir. SOC ekibinin temel amacı, teknolojiyi, insanları ve süreçleri kullanarak siber güvenlik olaylarını tespit etmek, analiz etmek ve müdahale etmektir.

SOC Modellerinin Türleri

Güvenlik gereksinimlerine ve bütçeye bağlı olarak, çeşitli SOC türleri vardır:

Şirket içi SOC

İşletme kendi siber güvenlik ekibini kurar. Dahili bir SOC kurmayı düşünen firmalar, sürekliliği desteklemek için bir bütçeye sahip olmalıdır.

sanal SOC

Güvenlik ekibinin kendi tesisi yoktur ve genellikle farklı konumlarda uzaktan çalışır.

Ortak Yönetilen SOC

Ortak Yönetilen SOC, harici bir Yönetilen Güvenlik Hizmet Sağlayıcısı (MSSP) ile çalışan dahili SOC personelinden oluşur. Bu tür bir model için koordinasyon gerçekten önemlidir.

Komut SOC

Büyük bir bölgedeki daha küçük SOC'leri denetleyen kıdemli bir grup. Bu modeli kullanan kuruluşlar arasında büyük telekom sağlayıcıları ve savunma ajansları bulunur.

SOC Analisti ve Sorumlulukları

Bu bölümde bir SOC analistinin ne olduğunu, SOC içindeki yerini ve genel anlamda işle ilgili ne tür sorumlulukları olduğunu tartışacağız. İşin teknik yönünü öğrenmeden önce bu bölümleri dikkatlice okumak önemlidir, bu şekilde SOC analisti olmak isteyen adaylar gelecekteki kariyerlerinin nasıl olacağını hayal edebilirler.

Bir SOC analisti, bir sisteme yönelik herhangi bir tehdidi analiz eden ilk kişidir. Durum gerektirdiğinde, olayları üstlerine iletir ve böylece tehditleri yakalamayı mümkün kılar. SOC'de önemli bir rol oynuyor çünkü araştıran ilk kişi o.

Genel Rutin

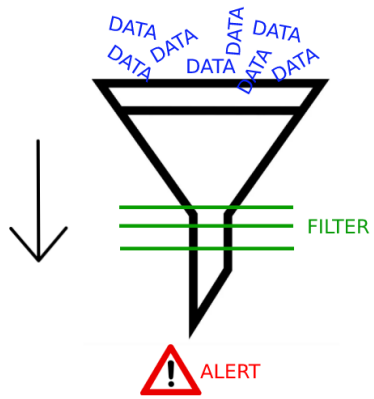
Gün boyunca bir SOC analisti genellikle SIEM'deki uyarıları inceler ve hangilerinin gerçek tehditler olduğunu belirler. Bir sonuca varmak için EDR, Log Management ve SOAR gibi çeşitli güvenlik ürünlerini kullanacaktır.

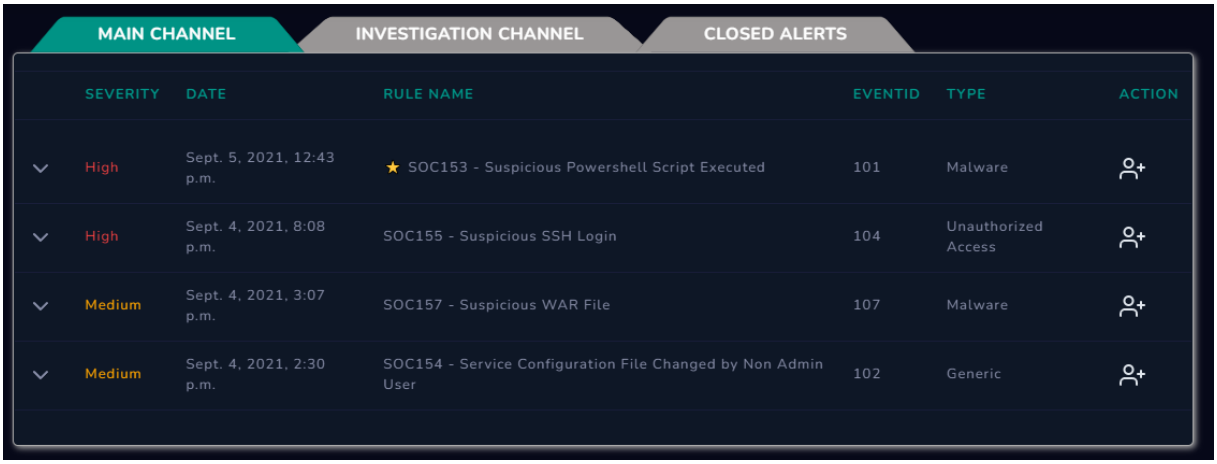
SİEM nedir?

Güvenlik bilgileri ve olay yönetimi (SIEM), bir ortamdaki olayların gerçek zamanlı olarak günlüğe kaydedilmesini sağlayan bir güvenlik çözümüdür. Olay günlüğünün asıl amacı, güvenlik tehditlerini tespit etmektir.

Genel olarak SIEM ürünleri bir takım özelliklere sahiptir. SOC analistleri olarak bizi en çok ilgilendirenler, topladıkları verileri filtreler ve herhangi bir şüpheli olay için uyarı oluştururlar.

Bir uyarı örneği: Windows işletim sistemindeki bir kişi 10 saniye içinde 20 yanlış parola girmeye çalışırsa, bu şüpheli bir etkinliktir, parolasını unutan birinin parolasını bu kadar çok kez yeniden girmeye çalışması olası değildir. kısa bir dönem. Bu nedenle eşik değerlerini aşan bu tür aktiviteleri belirlemek için bir SIEM kuralı/filtresi oluşturuyoruz. Bu SIEM kuralı gereği böyle bir durum oluştuğunda uyarı oluşturulacaktır.



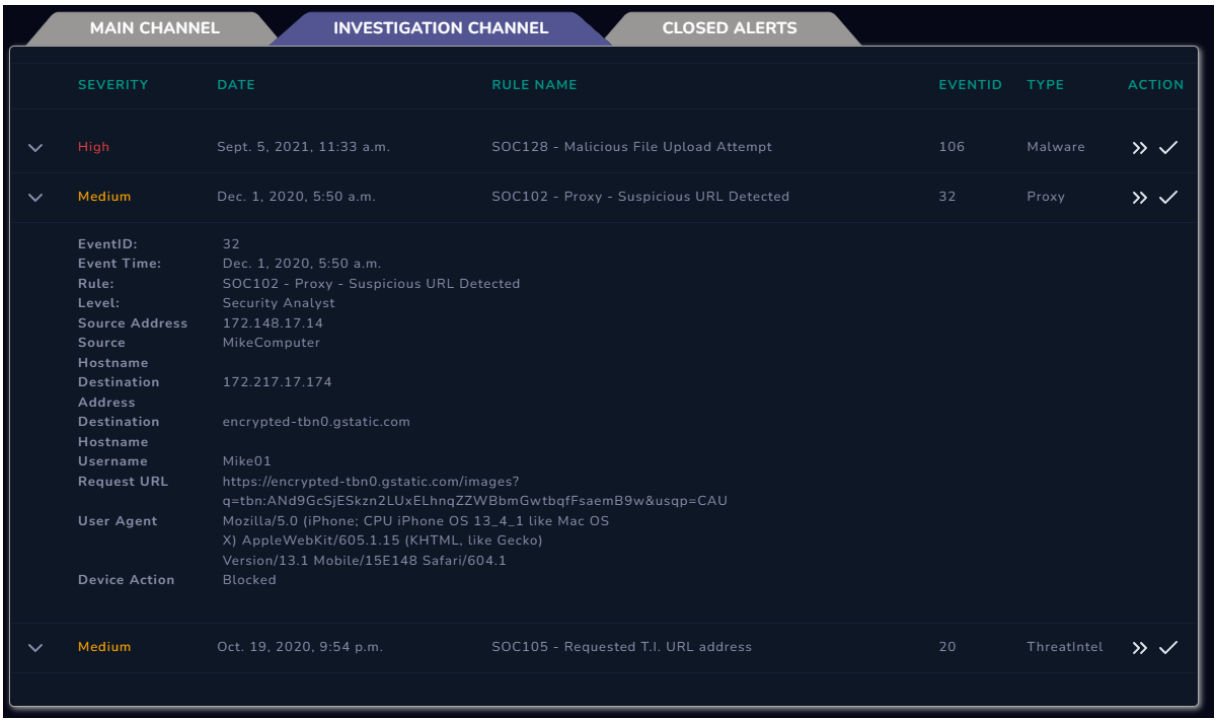


SOC Analisti ve SIEM Arasındaki İlişki

SIEM çözümlerinin birçok özelliği olmasına rağmen, SOC analistleri olarak genellikle sadece uyarıları takip ediyoruz. Konfigürasyonlar ve kural korelasyonları geliştiren başka gruplar/kişiler de vardır.

Yukarıda bahsettiğimiz gibi, uyarılar filtrelerden geçirilen veriler tarafından oluşturulur. Uyarılar öncelikle bir SOC analisti tarafından analiz edilir. Güvenlik operasyonları merkezindeki bir SOC analistinin görevi tam olarak burada başlar. Temel olarak, oluşturulan bu uyarının gerçek bir tehdit mi yoksa yanlış bir alarm mı olduğuna karar vermelidir.

Bir SOC analisti olarak diğer SOC ürünleri (EDR, Log Management, Threat Intelligence Feed vb.) yardımıyla bu uyarılarla ilgili detayları analiz etmeli ve son olarak bunların gerçek tehdit olup olmadığını belirlemeliyiz.



Yeni oluşturulan uyarıları “Ana Kanal”(“Main Channel”) da görebiliriz, bu kanalı paylaşılan bir kanal gibi düşünebiliriz. Takım arkadaşlarınız bu simülasyonda görülemez, ancak gerçek bir çalışma durumunda takım arkadaşlarınız bu paneli görebileceklerdir. Üzerinde çalışmak istediğiniz uyarıyı seçtikten sonra “İşlem”(“Action”) isimli alanda bulunan “Sahiplik Al”(Take

Ownership) butonuna tıklayarak uyarıyı sahiplenip "İnceleme Kanalı"na(Investigation Channel) yönlendiriniz. Bu şekilde takım arkadaşlarınız aktif olarak hangi uyarı üzerinde çalıştığınızı görebilirler. Aynı zamanda, bu, diğer uyarıları seçebilmeleri için halihazırda hangi uyarı üzerinde çalıştığınızı görmelerine yardımcı olacaktır. Bu şekilde ekibiniz tüm uyarıları hızla inceleyebilir.

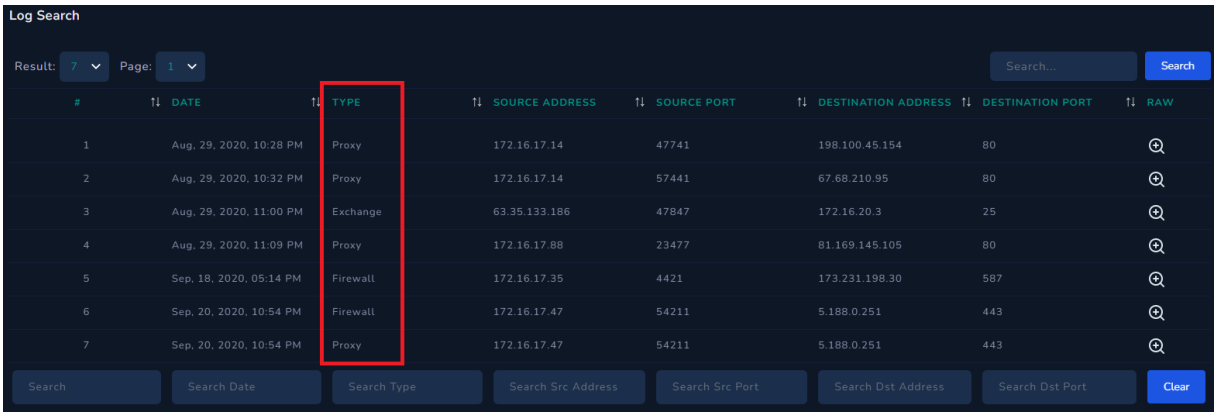
Uyarıya tıkladığınızda ilgili detayları görebilirsiniz. Bu şekilde araştırma için gerekli bilgileri (hostname, IP adresi, dosya hash bilgisi vb.) toplayabilirsiniz.

Günlük Yönetimi Nedir?

Adından da anlaşılacağı gibi bir log yönetimi çözümüdür. Kısacası bir ortamdaki tüm loglara (web logları, işletim sistemi logları, FW, PRoxy, EDR vb.) erişim sağlar ve bu logların tek noktadan yönetilmesine imkan verir. Böylece kullanılabilirliği artırır ve zamandan tasarruf sağlar.

Günlüklere bir noktadan erişemezsek, aynı sorgunun (örneğin,letsdefend.io'daki tüm kullanıcıları belirlemek istiyorum) çeşitli cihazlara gönderilmesi gerekir. Bu, hata payımızı ve harcamamız gereken süreyi artıracaktır.

LetsDefend'de "Log Management" sayfasına gittiğinizde Proxy, Exchange, Firewall gibi çeşitli log kaynaklarının "Type" olarak listelendiğini göreceksiniz. Bu, tüm bu log kaynaklarının tek bir yerde toplandığı ve Proxy, FW vb. kaynaklardan gelen log çıktılarını tek bir sorgu ile görebileceğimiz anlamına gelir.



Kullanım amacı

SOC Analistleri olarak genellikle belirli bir adresle iletişim olup olmadığını kontrol etmek ve bu iletişimin detaylarını görmek için “Log Yönetimi” kullanıyoruz. Diyelim ki bir kötü amaçlı yazılımla karşılaştınız ve onu çalıştırdıktan sonra “letsdefend.io” adresiyle iletişim kurduğunu ve ondan komutları çalıştırdığını tespit ettiniz. Bu durumda komuta kontrol merkezi “letsdefend.io”dur, komuta kontrol merkezi ile iletişim kurmaya çalışan herhangi bir cihaz olup olmadığını görmek için şirketinizin Günlük Yönetiminde “letsdefend.io” araması yapabilirsiniz.

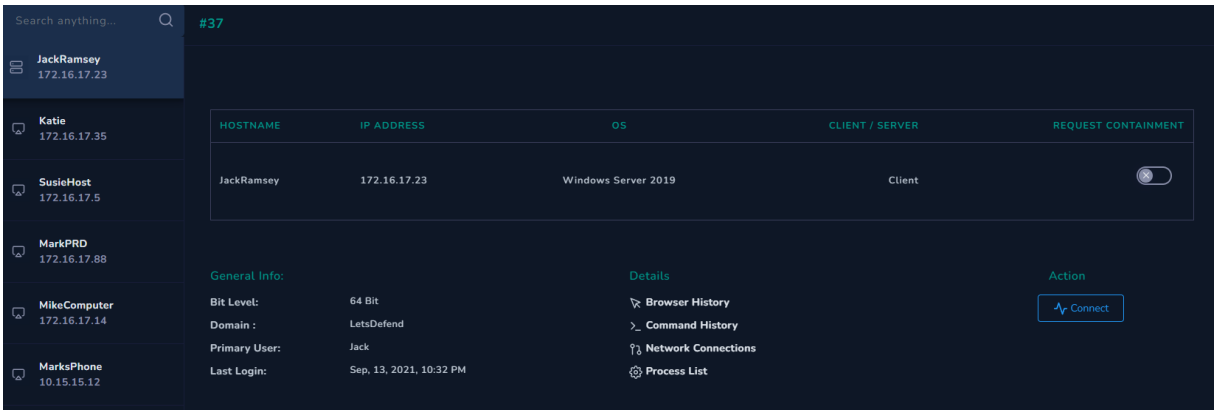
Bu çözüm bize ikinci bir durum sağlar: Ağınızdaki LetsDefendHost cihazının 122.194.229.59 IP adresine veri sızdırdığını belirten bir SIEM uyarısı görüyorsunuz. İnceleme yaptınız, cihazı ağdan ayırdınız, gerekli işlemleri yaptınız ve artık kontrol sizde. Ancak hala ele almadığımız bir şey var, şüpheli IP adresine (122.194.229.59) veri gönderen başka cihazlar var mı? Uyarı sadece LetsDefendHost'u içeriyor olabilir, ancak yine de sistemin algılamamış olabileceği bir şey olup olmadığını görmek için şüpheli adresi Günlük Yönetiminde aramalı ve herhangi bir bağlantı bulmaya çalışmalıyız.

EDR nedir?

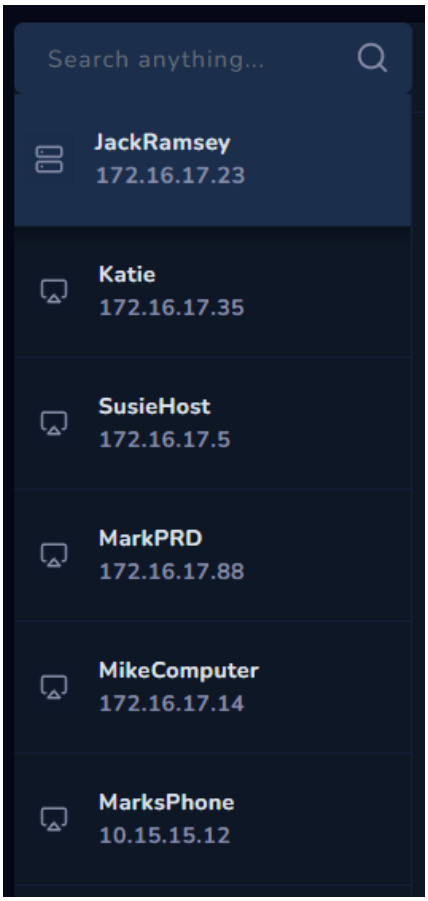
Uç nokta tehdit algılama ve yanıt (ETDR) olarak da bilinen uç nokta algılama ve yanıt (EDR), gerçek zamanlı sürekli izleme ve uç nokta verilerinin toplanmasını kurallara dayalı otomatik yanıt ve analiz yetenekleriyle birleştiren entegre bir uç nokta güvenlik çözümüdür. (Tanım kaynağı: mcafee.com)

EDR ile Analiz

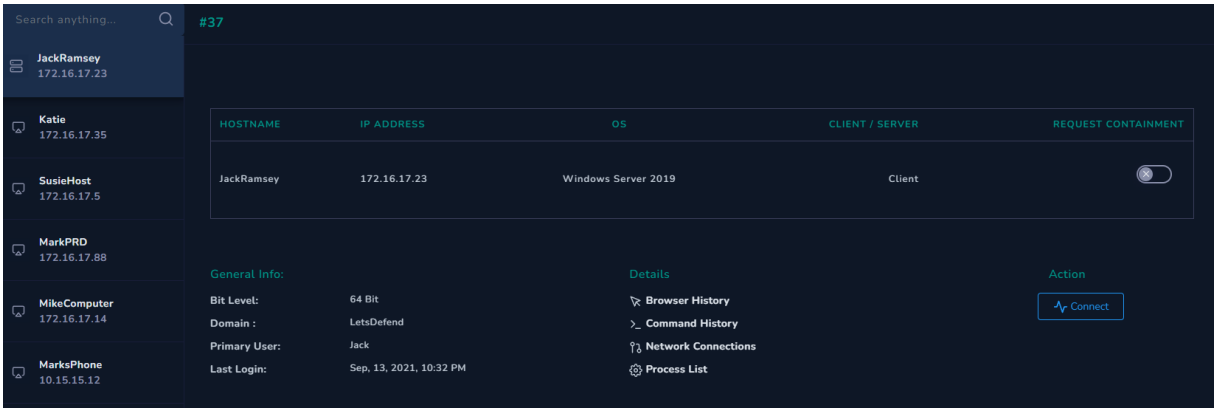
Bir analist olarak EDR ile neler yapabileceğimizi anlamak için LetsDefend'deki “Endpoint Security”ye bir göz atalım.

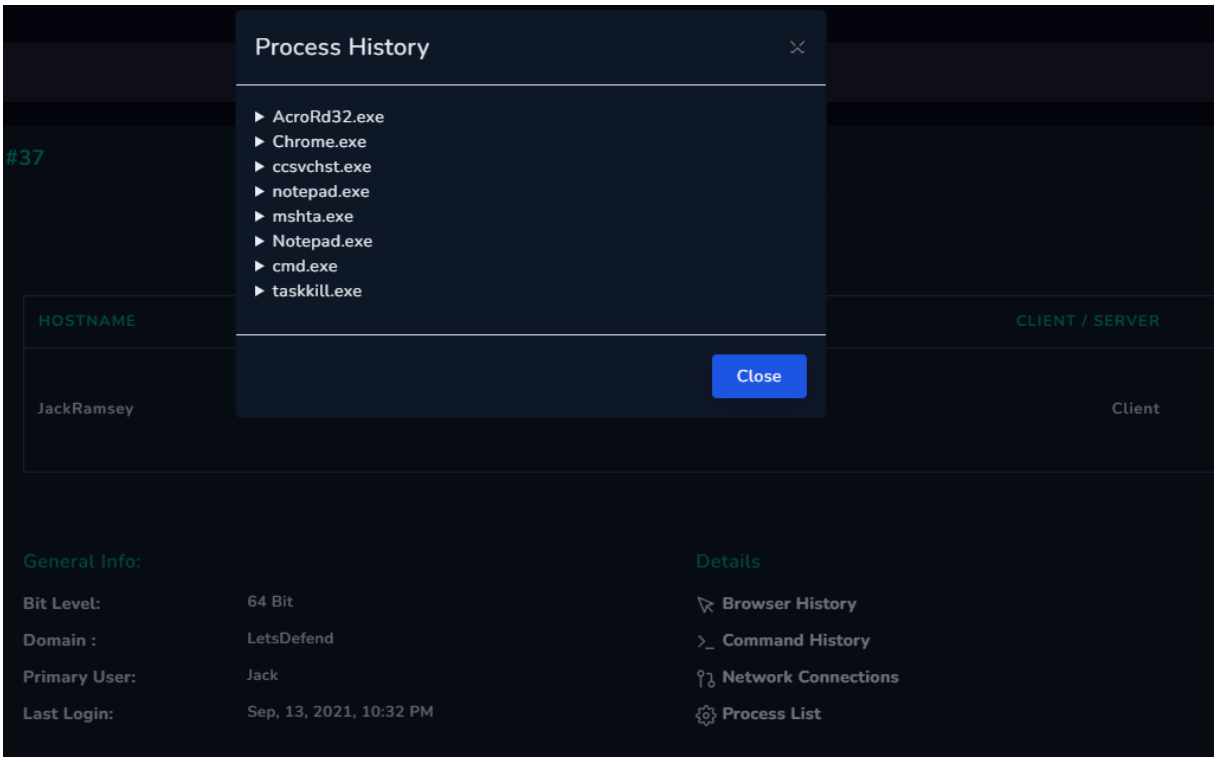


Görselde görüldüğü gibi, erişilebilir uç nokta cihazları solda listelenmiştir. Arama çubuğunda uç noktaları arayabiliriz veya bir IOC'miz varsa (IP adresi, dosya karması, işlem adı vb.) tüm ana bilgisayarlar arasında arama yapabiliriz.



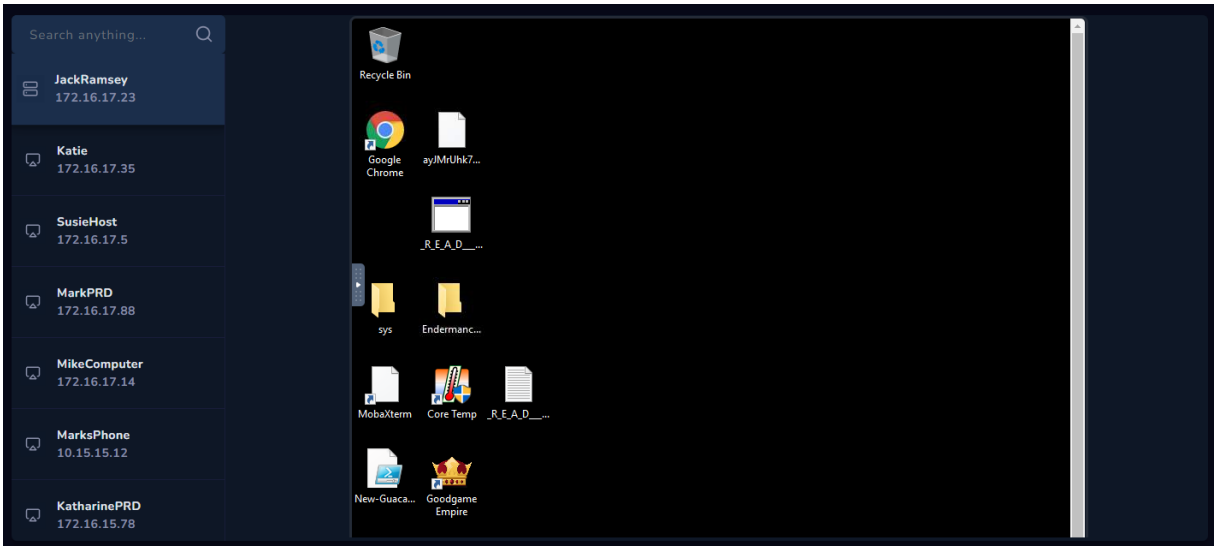
Sağ tarafta cihaz hakkında genel bilgiler ve “Tarayıcı Geçmişi”, “Ağ Bağlantıları” ve “İşlem Listesi” gibi görüntülenebilen bölümler bulunur.





Canlı Soruşturma

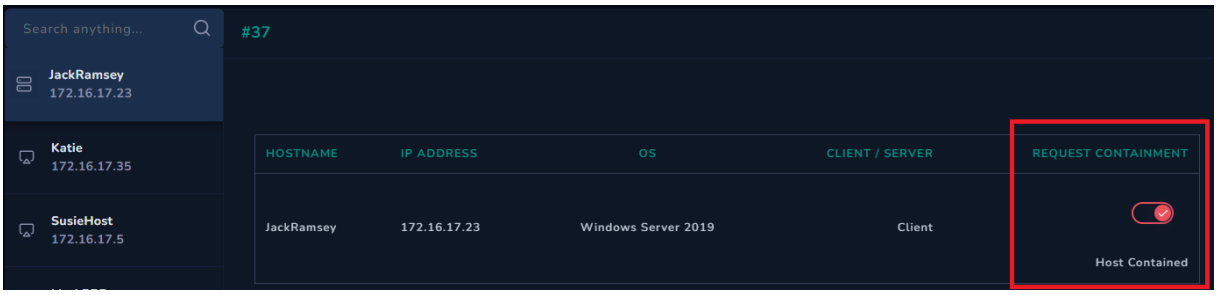
Ayrıca “Bağlan” butonuna tıklayıp analizimize orada devam etmek için makinenin kendisine erişebiliriz.



Sınırlama

Saldırıya uğramış bir makineyi ağdan izole etmeliyiz. Bunun arkasında önemli nedenler vardır: Saldırganın iç ağ ile bağlantısını kesebilmek ve iç ağ boyunca hareketini engellemek.

Bu nedenle güvenlik açıkları giderilip tekrar kullanılabilir hale gelene kadar cihazın iç ve dış ağlardan bağlantısı kesilmelidir. EDR çözümlerinin “Containment” özelliğini kullanarak izolasyonun gerçekleşmesini sağlayabiliriz. Bu özellik, seçilen cihazın yalnızca EDR merkezi ile iletişim kurmasını sağlar. Bu, cihaz ağdan izole edilmiş olsa bile analizimize devam edebileceğimiz anlamına gelir.



Hızlı ipucu

Dosya karması, dosya adı vb. gibi herhangi bir IOC'niz varsa, tüm ana bilgisayarlar arasında EDR'de bir arama yapabilir ve bir eşleşme olup olmadığını görebilirsiniz. Örneğin, diyelim ki bir cihazın saldırıya uğradığından eminsiniz ve MD5 karması “ac596d282e2f9b1501d66fce5a451f00” olan bir dosya aldınız. Bu hash değerini EDR'de arayabilir ve bu dosyanın başka cihazlarda var mı yoksa yürütülmüş mü olduğunu belirleyebilirsiniz. Böylece bu saldırıdan kimlerin etkilendiğini anlayabilirsiniz

SOAR (Güvenlik Düzenleme Otomasyonu ve Yanıtı)

SOAR, Güvenlik Düzenleme Otomasyonu ve Yanıtı anlamına gelir. Bir ortamdaki güvenlik ürünleri ve araçlarının birlikte çalışmasını sağlar ve bu nedenle SOC ekip üyelerinin işlerini kolaylaştırır. Örneğin, Virustotal'da bir SIEM uyarısının kaynak IP'sini otomatik olarak arar ve böylece SOC analistinin yükünü hafifletir.

Zaman Kazandırır

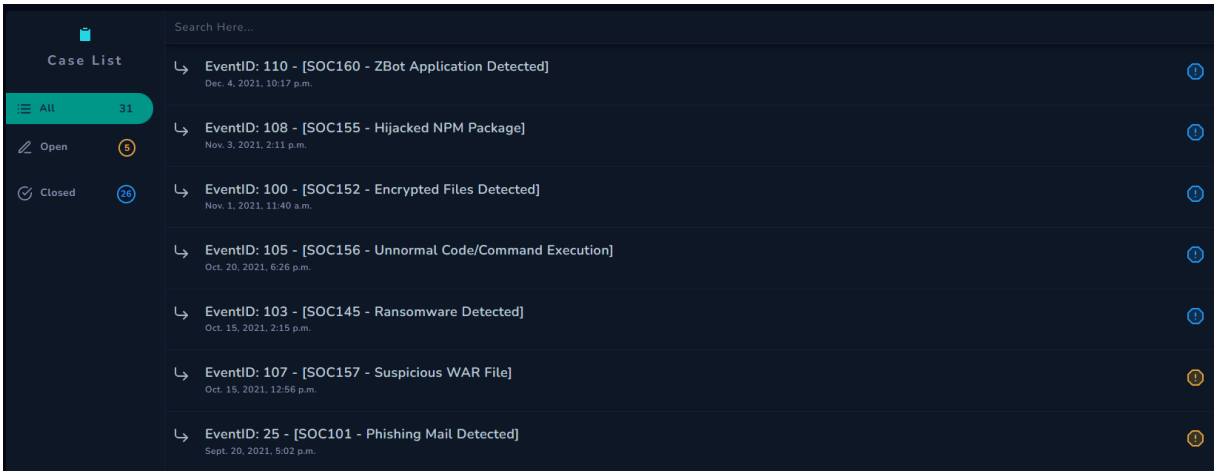
SOAR, süreçleri otomatikleştiren iş akışları aracılığıyla zaman kazandırır. Sık kullanılan bazı iş akışları şunlardır:

IP adresi tekrarlama kontrolü

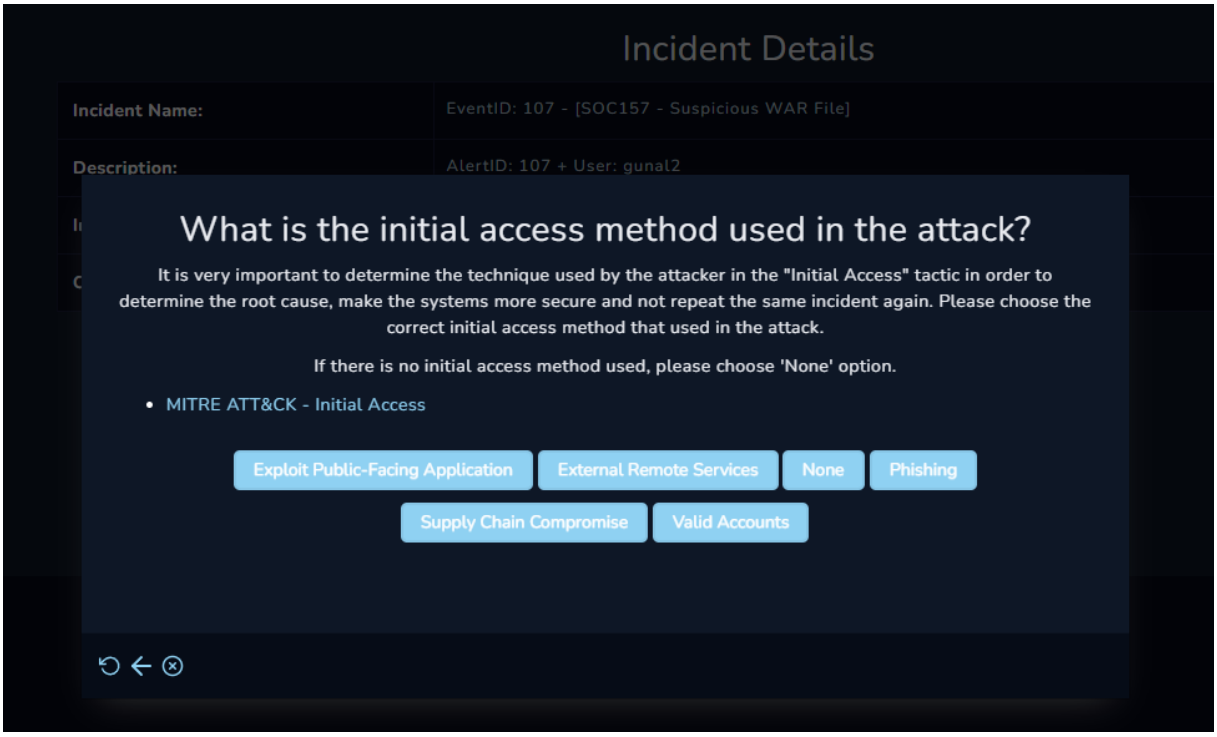
karma sorgu

Bir korumalı alan ortamında edinilen bir dosyayı tarama

“Vaka Yönetimi”ni SOAR ile aynı şey olarak düşünebiliriz. SIEM (İzleme) sayfasında oluşturduğunuz vakalar için buradan ticket açabilirsiniz. Sayfaya baktığımızda ilk gördüğümüz şey açık ve kapalı davaların bir listesi.



Herhangi bir açık vakaya tıkladığımızda otomatik olarak atanan bir başucu kitabı görüyoruz. Bu playbook'u takip ederek ilgili SIEM (İzleme) uyarısını inceleyebiliriz.

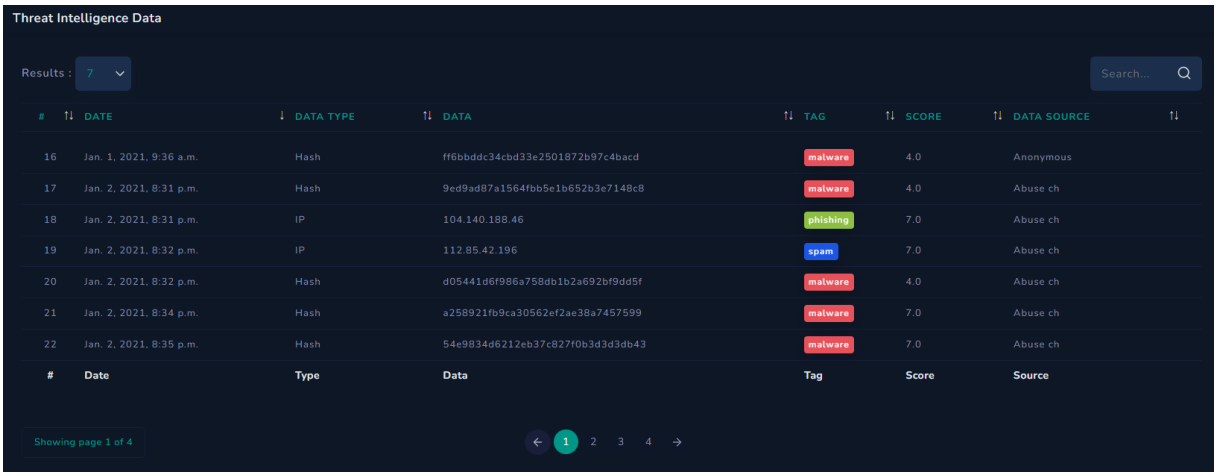


Tehdit İstihbaratı Akışı

Bir SOC ekibi en son tehditleri hemen bilmeli ve uygun önlemleri almalıdır. Tehdit İstihbarat Akışları bu ihtiyacı karşılamak için oluşturulur. Bir araştırma yaparken bu kaynakları SOC analistleri olarak kullanabiliriz.

Tehdit İstihbarat Akışı, üçüncü taraf bir şirket tarafından sağlanan verilerdir (kötü amaçlı yazılım karmaları, C2 etki alanı/IP adresleri vb.).

LetsDefend'in “Tehdit Intel” sayfasına bakarsak, çok sayıda veri (hash, IP vb.)



Buradaki veriler, önceki kötü niyetli faaliyetlerden elde edilen eserlerden oluşur. Kötü amaçlı yazılımın karması veya bir komuta ve kontrol merkezinin IP adresi olabilir. Bir SOC analisti olarak, elimizdeki bir hash dosyasının geçmişte kötü niyetli bir senaryoda kullanılıp kullanılmadığını belirlemek için tehdit istihbaratı beslemelerini araştırabiliriz.

İşte kullanabileceğiniz bazı ücretsiz ve popüler kaynaklar:

https://www.virustotal.com/

https://talosintelligence.com/

Dikkat Etmemiz Gereken Noktalar:

Görünmeyen yayınlar aracılığıyla çalıştırdığımız veriler

Diyelim ki VirusTotal'da bir .exe'ye ait bir hash çalıştırdık ve geçmişte bununla ilgili şüpheli bir şey bulamadık. Dosyanın temiz olduğunu düşünmemeliyiz, bu bir hata olur. Yine de gerekli dosya analizlerini (statik/dinamik) yapmak konusunda titiz davranmalıyız.

IP adreslerinin el değiştirebileceğini unutmamalıyız.

Örneğin bir saldırganın AWS üzerinden bir sunucu oluşturduğunu ve onu komuta ve kontrol merkezi olarak kullandığını varsayalım. Daha sonra çeşitli tehdit istihbarat beslemeleri bu IP adresini kötü amaçlı bir adres olarak listelerine kaydetti.

2 ay geçtikten sonra saldırgan sunucuyu kapattı ve bir başkası kişisel blogunu bu sunucuya taşıdı. Bu, blogu ziyaret eden kişilerin kötü niyetli içeriğe maruz kaldığı anlamına gelmez. Bu IP adresinin geçmişte kötü niyetli amaçlarla kullanılmış olması, kötü niyetli içerik barındırdığı anlamına gelmez.

SOC Analistleri için Yaygın Hatalar

Herhangi bir kişi gibi, SOC analistleri de hata yapar. Bu bölümde SOC analistleri tarafından sıklıkla yapılan hatalardan bahsedeceğiz ve bu hataları kendimiz yapmaktan nasıl kaçınabileceğimizi tartışacağız.

VirusTotal Sonuçlarına Aşırı Bağlı

Sandbox'ta Kötü Amaçlı Yazılımların Hızlı Analizi

Yetersiz Günlük Analizi

Virüs Toplam Tarihlerine Bakmak

VirusTotal Sonuçlarına Aşırı Bağlı

Bazen bir dosyanın URL'sini analiz ettikten ve adresin zararsız olduğunu gördükten sonra VirusTotal'ın yeşil ekranında görüntülenen sonuca güvenebiliriz. Ancak VT tarafından algılanamayan bir AV Bypass tekniği kullanılarak geliştirilmiş yeni bir kötü amaçlı yazılım

var. Bu nedenle VirusTotal'ı destekleyici bir araç olarak kabul etmeli ve analizlerimizi bunu göz önünde bulundurarak yapmalıyız.

Daha fazla okumak için konuyla ilgili ayrıntılı bir blog yazısı: https://medium.com/maverislabs/virustotal-is-not-an-incident-responder-80a6bb687eb9

Sandbox'ta Kötü Amaçlı Yazılımların Hızlı Analizi

Korumalı alan ortamında 3 ila 4 dakikalık bir analiz her zaman doğru sonuçlar vermeyebilir. İşte nedenler:

Bir korumalı alan ortamını algılayan ve kendini etkinleştirmeyen kötü amaçlı yazılım İşlemden 10-15 dakika sonrasına kadar etkinleştirilmeyen kötü amaçlı yazılım

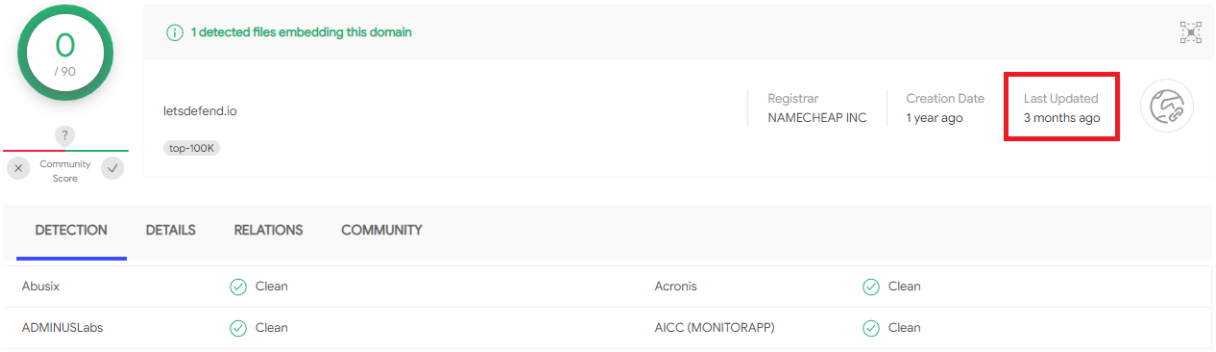
Bu nedenle analiz süresi mümkün olduğunca uzun tutulmalı ve mümkünse gerçek bir ortamda gerçekleştirilmelidir.

Yetersiz Günlük Analizi

Zaman zaman log analizlerinin doğru yapılmadığını görüyoruz. Örneğin, bir kötü amaçlı yazılım parçasının “LetsDefend” ana bilgisayar adına sahip bir cihaz tespit ettiğini ve bu kötü amaçlı yazılımın gizlice “letsdefend.io” adresine veri gönderdiğini varsayalım. Bir SOC analisti olarak, bu adrese başka bir cihazın bağlanmaya çalışıp çalışmadığını belirlemek için “Log Management” çözümlerini kullanmalıyız.

Virüs Toplam Tarihlerine Bakmak

VirusTotal'da yaptığınız arama daha önce sorgulandıysa önbellekten bir sonuç görüntülenecektir. Örneğin: VirusTotal üzerinde “letsdefend.io” adresini arattık ve sonuç aşağıda.



Saldırgan olsaydım, VirusTotal'da temiz bir URL adresi arayabilir ve ardından içeriği kötü amaçlı içerikle değiştirebilirdim. Bu yüzden sadece arama önbelleğine bakmamalıyız, yeni bir arama başlatmalıyız.