

SentinelOne Singularity XDR

Siber güvenlik risk ortamı hızla geliyor ve değişiyor. Saldırı vektörleri, uç noktalardan ağlara, oradan da buluta doğru arttıkça, birçok işletme güvenlik açıklarını korumak için her vektörü sınıfının en iyisi bir çözümle ele alıyor. Ancak bu spesifik koruma araçları, tüm teknoloji yığınındaki noktaları güvence altına alamaz. Sonuç olarak, güvenlik verileri herhangi bir bağlam veya korelasyon olmaksızın ayrı ayrı toplanıp analiz edilir, bu da güvenlik ekiplerinin tespit ve müdahale sürecinde boşluklara yol açar. Ayrıca, manuel soruşturma süreci genellikle yavaş ve zahmetli olabilir; bu da güvenlik ekiplerinin tehditleri kontrol altına almasında, gecikmelere neden olur.

Singularity XDR

SentinelOne Singularity XDR, güvenlik ekiplerine merkezi, uçtan uca kurumsal görünürlük, güçlü analitik, otomatik yanıt vs. gibi olanaklar sağlayarak, tespit ve müdahale yeteneğini birden çok güvenlik katmanında birleştirir ve etki alanını genişletir. Singularity XDR ile müşteriler, tüm teknoloji yığının savunmak için birleşik ve proaktif güvenlik önlemleri alabilirler; bu da devam eden saldırıların işi etkilemeden önce güvenlik analistleri tarafından tanımlanmasını ve durdurulmasını kolaylaştırır.

Temel Özellikler

01 | Cross-stack görünürlüğü ile kör noktaları ortadan kaldırın

Singularity XDR, kuruluşların her türlü teknoloji ürünü veya platformundan gerçek zamanlı olarak yapılandırılmış, yapılandırılmamış ve yarı yapılandırılmış verileri sorunsuz bir şekilde almasını sağlayarak veri silolarını ve kritik kör noktaları ortadan kaldırır. Çözüm, güvenlik ekiplerinin uç noktalar, bulut iş yükleri, IoT cihazları, ağlar ve daha fazlası dahil olmak üzere tüm platformlardan farklı güvenlik çözümleriyle toplanan verileri tek bir panoda görmesini sağlar. Singularity XDR, analistlerin çok sayıda farklı çözümden gelen olay bilgilerini tek bir bağlamsal "olay" halinde bir araya getirerek elde edilen iç görülerden yararlanmalarını sağlar. Ayrıca, müşterilere tam kurumsal görünürlük ve otonom önleme, tespit ve müdahale için merkezi bir yaptırım ve analitik katman nokta merkezi sağlayarak, kuruluşların siber güvenlik zorluklarını birleşik bir bakış açısıyla ele almalarına yardımcı olur.

02 | Cross-stack korelasyonu gizli saldırıları ortaya çıkarın

SentinelOne patentli Storyline™ teknolojisi, bir döngüdeki tüm olayları ve etkinlikleri otomatik olarak benzersiz bir tanımlayıcıyla birbirine bağlar.

ÇÖZÜMÜN AVANTAJLARI



Artan SOC Verimliliği ve Üretkenliği

İşletim sisteminin bir programda olması veya bir gösterge panelinin olması gecikmeleri en aza indirir. Bir platform ve bir iş akışı, uyarıların sayısını azaltır, kör noktaları ve veri boşluklarını ortadan kaldırır ve bir yanıt sırasında güvenliğin erişmesi gereken ara yüzlerin sayısını azaltır.



Hızlı Değer Alma Süresi

Birden çok farklı üründe kullanıma hazır entegrasyonlar, mevcut siber güvenlik yatırımınızın değerini hızla en üst düzeye çıkarmanızı sağlar.



Basitleştirilmiş Operasyonlar ve İş Akışları

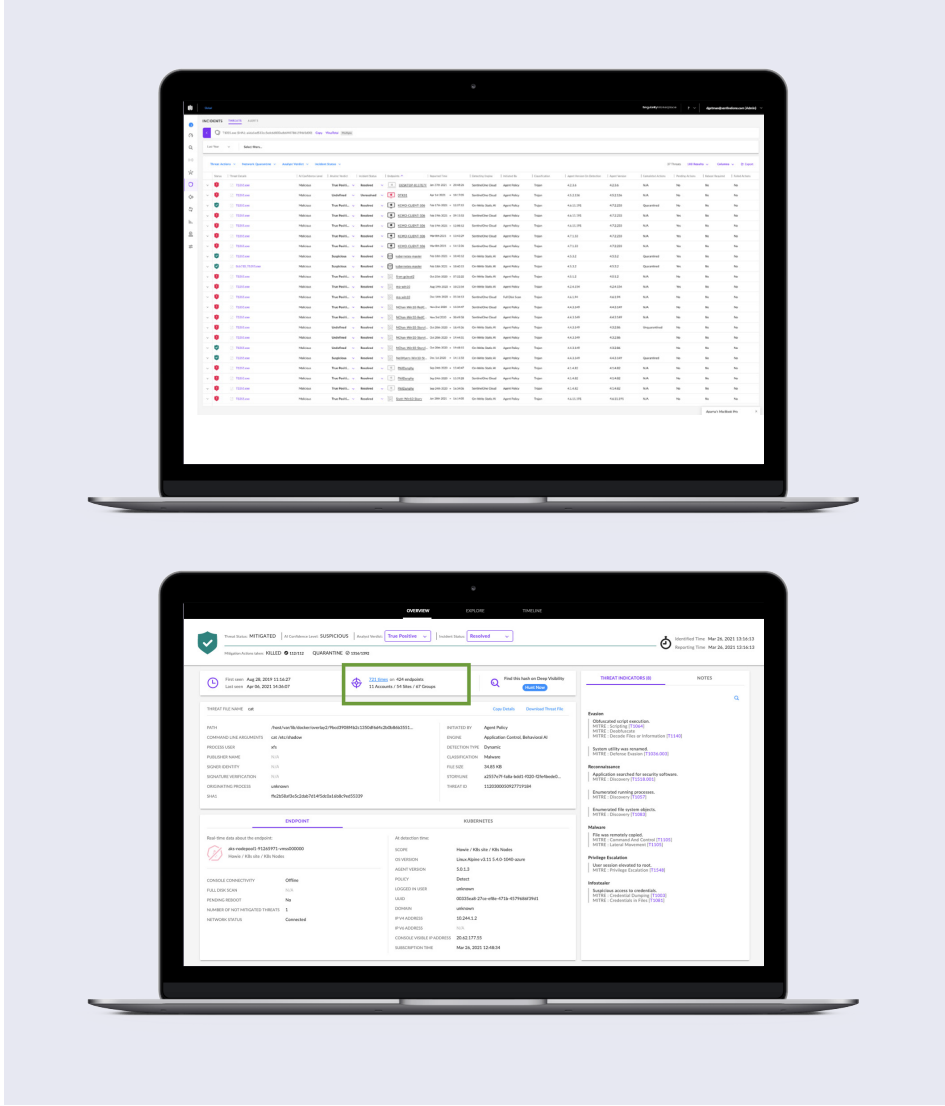
Silolar halinde veri akışları için tek bölme görünürlük ve analiz elde edin.



Azaltılmış Toplam Mülkiyet Maliyeti (TCO)

Tam entegre bir siber güvenlik platformuyla birbirinden farklı çözümlerin kurulum ve entegre edilme maliyetlerini azaltın.

Bu, güvenlik ekiplerinin manuel olarak olayları birbirine bağlamak için saatler, günler veya haftalar harcamak yerine saniyeler içinde, olup biteni tam olarak görmesine olanak tanır. SentinelOne'ın davranış motoru, dosya/kayıt değişiklikleri, hizmet başlatma/durdurma, süreçler arası iletişim ve ağ etkinliği dahil olmak üzere ortamınızdaki tüm sistem etkinliklerini izler. Gizli davranışları izlemek, dosyasız saldırıları, yanal hareketleri ve aktif olarak çalıştırılan rootkitleri etkili bir şekilde tanımlamak için kötü niyetli davranışlara işaret eden teknikleri ve taktikleri tespit eder. Singularity XDR, ilgili etkinliği otomatik olarak girişim düzeyinde iç görü sağlayan birleşik uyarılarla ilişkilendirir ve kuruluşların, uyarıların tek bir olay olarak sınıflandırılmasını kolaylaştırmak için farklı vektörler arasındaki olayları ilişkilendirmesine olanak tanır.



TEMELENTTEGRASYONLAR



ENDPOINT



IOT



CLOUD



THREAT INTEL



IDENTITY



EMAIL



NETWORK

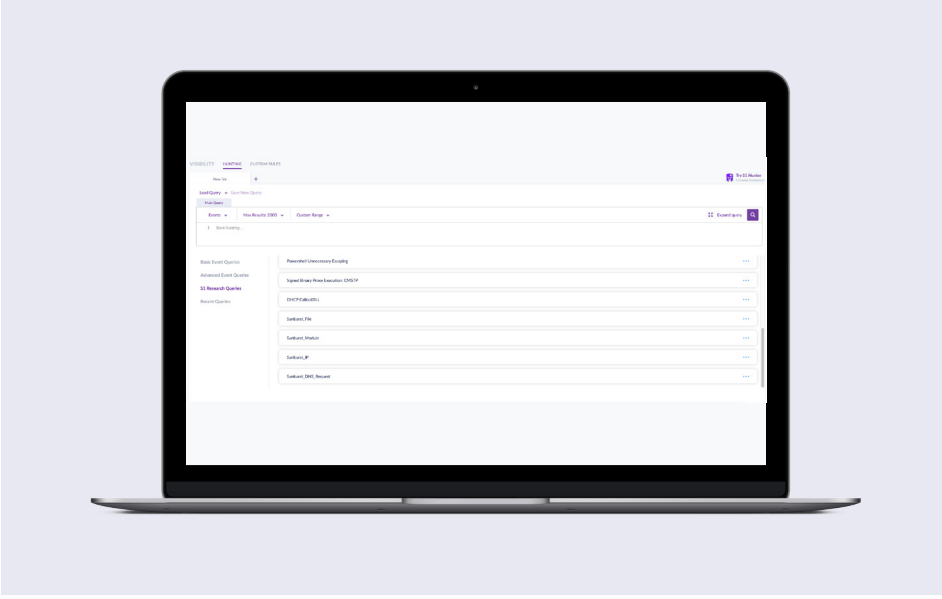


SASE

03 | Entegre tehdit istihbaratıyla tehditleri otomatik olarak zenginleştirin

Singularity XDR, önde gelen 3. taraf yayınlarından ve uç nokta olaylarını gerçek zamanlı tehdit istihbaratıyla otomatik olarak zenginleştiren tescilli kaynaklarımızdan algılama ve zenginleştirme için tehdit istihbaratını toplar. Güvenlik ekiplerine IP'ler, güvenlik açıkları ve etki alanları gibi güvenlik ihlali Göstergeleri (IoC'ler) için, ek bağlamsal risk puanları alma yetkisi verir. Örneğin, Recorded Future entegrasyonumuz ile tehditler, 800.000'den fazla kaynaktan otomatik olarak zenginleştirilerek, müşterilerin tehdit araştırması ve

önceliklendirme kabiliyetlerini hızlandırmalarına olanak tanır. Müşteriler ayrıca, yeni loC'leri ve Taktikleri, Teknikleri ve Prosedürleri (TTP'ler) ortaya çıkarmak için sürekli olarak yeni metodolojileri değerlendiren SentinelOne araştırması tarafından oluşturulan bir arama sorgu kitaplığından da yararlanabilirler.



04 | Farklı etki alanlarında yanıtı otomatikleştirin

Singularity XDR, analistlerin tehditleri tek tıkla, komut dosyası yazmadan, bir ya da birkaç cihazda ya da tüm cihazlarda otomatik olarak çözmek için gerekli tüm eylemleri gerçekleştirmelerini sağlar. Analistler, tek tıklamayla ağ karantinası gibi iyileştirme eylemlerini yürütebilir, hileli bir iş istasyonundaki ajanı otomatik olarak dağıtabilir veya bulut ortamlarında politika uygulamasını otomatikleştirebilirler. Singularity XDR, müşterilerin Storyline Active-Response (STAR) ile ortamlarına özel, otomatikleştirilmiş algılama kuralları oluşturmak için sunduğu iç görülerden yararlanmalarına da olanak tanır. STAR, işletmelerin iş bağlamlarını birleştirmelerine ve EDR çözümünü ihtiyaçlarına göre özelleştirmelerine olanak tanır. Storyline Active-Response (STAR) özel algılama kurallarıyla, sorguları, kurallar eşleşmeler algıladığında uyarıları ve yanıtları tetikleyen otomatik arama kurallarına dönüştürebilirsiniz. STAR, ortamınıza özgü özel uyarılar ve yanıtlar oluşturma esnekliği sağlar; örneğin, ortamınızdaki tehditleri otomatik ve hızlı bir şekilde tespit etmek ve kontrol altına almak için bir işlemi otomatik olarak sonlandırma gibi.

05 | Önde gelen SOAR araçlarıyla sorunsuz entegrasyon

SOC ekibinizin kullandığı başka güvenlik araçları ve teknolojileri olabileceği için, SentinelOne, Singularity Marketplace aracılığıyla SIEM ve SOAR gibi üçüncü taraf sistemlere entegrasyon sağlayan geniş bir ürün portföyü sunar. Singularity Uygulamaları; ölçeklenebilir, sunucusuz, "Hizmet Olarak İşlev" bulut platformumuzda barındırılır ve API özellikli BT ve Güvenlik kontrolleriyle birkaç tıklamayla birleştirilir. Singularity Marketplace, platformumuzun bir parçasıdır. Bu nedenle entegrasyon sağlandıktan sonra, etki, ürün içinde anında görünür hale gelir; karmaşık kod yazma engellerini ortadan kaldırır ve otomasyonu satıcılar arasında basit ve ölçeklenebilir hale getirir. Güvenlik ekipleri, farklı etki alanlarındaki güvenlik araçları arasında birleşik ve planlanmış bir yanıt oluşturarak, yüksek hızlı tehditleri düzeltmek ve ortadan kaldırmak için en iyi eylem planını kolayca uygulayabilir.

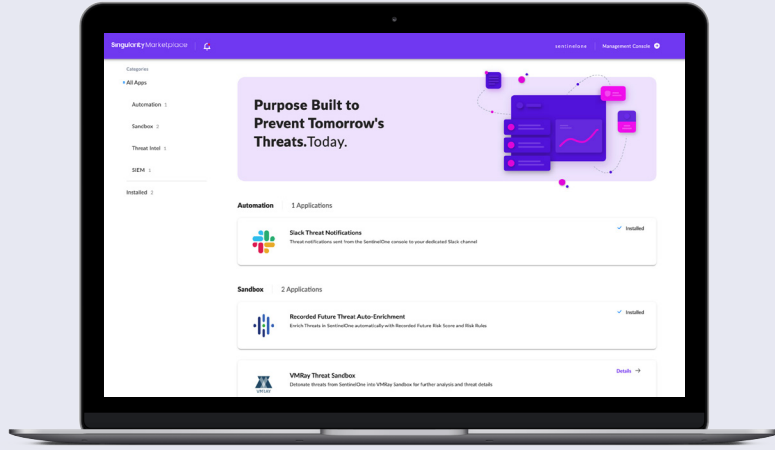
“

Veri toplamak, çoğu üretici için büyük bir zorluktur. Güvenlik verilerinin hacmi, hızı ve çeşitliliğini barındırmak için, XDR teknolojilerinin, hibrit BT genelinde ölçekli olarak güvenlik verilerini toplayabilen ve işleyebilen modern bir veri hattıyla sabitlenmesi gerekir.

XDR teknolojileri, güvenlik ekibine kurumsal güvenlik yığını genelinde otomatikleştirilmiş iç görüler sağlamak için, otomatikleştirilmiş makine yapımı veri ve ilişki sağlayabilmelidir.

Dave Gruber

KIDEMLİ ANALİST, KURUMSAL STRATEJİ GRUBU



06 | Güvenlik ekibinizi ölçeklendirin ve SOC verimliliğini artırın

Singularity XDR, aşağıdaki özelliklerle, genişletilmiş tehdit algılaması, araştırması, müdahalesi ve avı için tek ve birleşik bir platform sağlar.

- Verileri birden çok kaynak genelinde alan ve standartlaştıran tek öncelikli uyarı kaynağı.
- Saldırıların güvenlik katmanları genelinde ilerleyişini hızlı bir şekilde anlamak için tek bir birleştirilmiş görünüm.
- Tehditlere hızla yanıt vermek ve tehditlerin proaktif olarak izini sürmek için tek platform.



ÇÖZÜMÜN ÖNEMLİ NOKTALARI



Birçok Kaynaktan Sorunsuz Bir Şekilde Veri Alın

Her türlü teknoloji ürünü veya platformundan gerçek zamanlı olarak yapılandırılmış, yapılandırılmamış ve yarı yapılandırılmış verileri alma.



Kurumsal Yığınınız Genelinde Saldırı Girişimlerini Ortaya Çıkarın

Farklı verileri zengin hikayelere dönüştürmek için kurumsal güvenlik yığını genelinde gerçek zamanlı, otomatikleştirilmiş makine yapımı bağlam ve korelasyon elde edin.



Eyleme Geçirilebilir, Otomatik Yanıtlarla Saldırıları Hızla Kontrol Altına Alın

Tehditleri, kuruluş genelindeki bir ya da birkaç cihazda ya da tüm cihazlarda komut dosyası oluşturmadan tek tıklamayla otomatik olarak çözün.



Soruşturmayı ve Tehdit Avcılığını Hızlandırın

Gelişmiş düşmanları proaktif olarak ortaya çıkarmak için merkezi bir veri havuzunda ortak bir sorgu yeteneği sağlayın.

SentinelOne, Müşteriye Öncelik Veren bir Şirkettir

Sürekli ölçüm ve iyileştirme, müşteri beklentilerini aşmamızı sağlar.

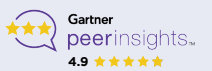


97 %

Of Gartner Peer Insights™ "Voice of the Customer" Reviewers recommend SentinelOne

97 %

Customer Satisfaction (CSAT)



About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

© SentinelOne 2021

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

S1-BRIEF_SING_XDR-04082021