ALTAY TAKIMI

SOC FUNDAMENTALS RAPORU

Hazırlayan : Efe Körün

Tarih : 07.02.2025

İÇİNDEKİLER

1.GİRİŞ

Bu rapor, Güvenlik Operasyonları Merkezi (SOC) ile ilgili organizasyonel yapı, ekiplerin görevleri, olay yönetim süreçleri ve kullanılan güvenlik araçlarını kapsamlı bir şekilde incelemektedir. Siber güvenliğin giderek daha kritik hale gelmesiyle birlikte, SOC yapılanmalarının önemi artmış ve bu alandaki teknolojiler hızla gelişmiştir.

Rapor, SOC'un işleyişini anlamak ve etkili bir güvenlik operasyonu yönetimi sağlamak isteyenler için rehber niteliğinde hazırlanmıştır. Siber güvenlik alanında çalışan profesyoneller ve konuya ilgi duyanlar için önemli bilgiler içeren bu çalışma, kuruluşların tehditlere karşı daha güçlü bir savunma mekanizması oluşturmasına katkıda bulunmayı amaçlamaktadır.

2. SOC Nedir?

Güvenlik Operasyonları Merkezi (SOC), bir kuruluşun siber güvenliğini sürekli olarak izleyen, güvenlik olaylarını analiz eden ve tehditlere karşı aksiyon alan bir birimdir. SOC, güvenlik analistleri, mühendisler ve yöneticilerden oluşan profesyonel bir ekip ile teknolojik çözümleri kullanarak tehditleri tespit eder, analiz eder ve yanıt verir.

3. SOC'un Amacı ve Önemi

3.1 SOC'un Amacı

SOC'un amacı, siber tehditleri en hızlı şekilde tespit edip ortadan kaldırarak şirketlerin güvenliğini sağlamaktır. 7/24 izleme yaparak güvenlik açıklarını bulur, tehditleri analiz eder ve olası saldırılara karşı önlem alır. Bu sayede hem veri kayıplarının hem de maddi ve itibari zararların önüne geçilir.

3.2 SOC'un Önemi

SOC'un önemi ise bir şirketin saldırıları fark etme ve bunlara tepki verme hızını artırmasında yatmaktadır. Uzman ekipler ve ileri teknolojiler sayesinde altyapıdaki tehditler anında tespit edilerek müdahale edilir. Eğer SOC olmazsa, şirketler saldırıları geç fark edebilir ve bu da büyük kayıplara yol açabilir. Kısacası, SOC bir şirketin siber savunma kalkanıdır ve iş sürekliliğini korumada büyük rol oynar.

Şekil 1 SOC Genellemeleri

4. SOC'un Temel Yapı Taşları Ve Süreçleri

4.1 SOC'un Temel Yapı Taşları:

İnsan Kaynağı:

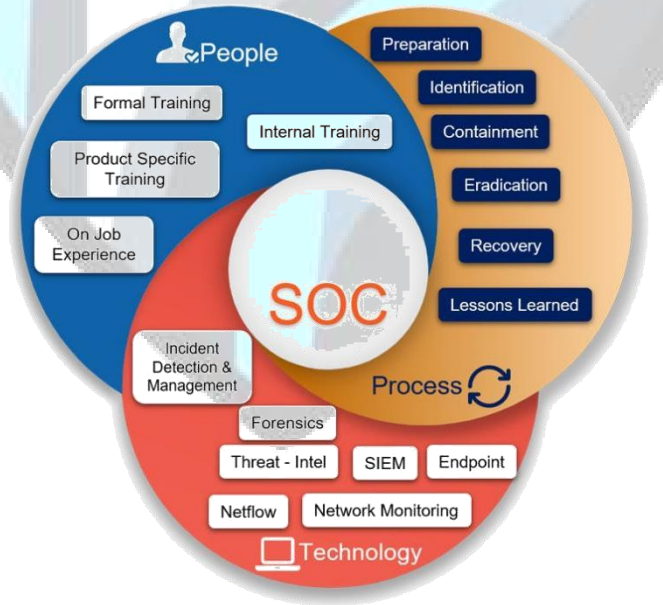
SOC'un en kritik unsurlarından biri nitelikli insan kaynağıdır. Siber güvenlik uzmanları, analistler ve mühendisler; tehditleri tespit etme, analiz etme ve müdahale süreçlerinde kilit rol oynar. Bu profesyonellerin geniş bir teknik bilgiye sahip olmalarının yanı sıra problem çözme becerileri gelişmiş olmalıdır. Ayrıca, siber tehditlerin dinamik doğası gereği sürekli kendilerini güncel tutmaları büyük önem taşır.

Teknolojiler:

SOC yapısının temelini, gelişmiş güvenlik yazılımları ve donanımları oluşturur. Kullanılan başlıca teknolojiler arasında SIEM (Security Information and Event Management), IDS/IPS sistemleri (Saldırı Tespit ve Önleme Sistemleri), güvenlik duvarları, VPN cihazları ve tehdit istihbarat platformları yer alır. Bu araçlar, güvenlik tehditlerinin hızlı bir şekilde tespit edilmesi ve etkin müdahaleyi mümkün kılar.

Süreçler:

SOC operasyonlarının başarısı, sistematik ve iyi tasarlanmış süreçlere bağlıdır. Bu süreçler, tehditlerin izlenmesi, tespit edilmesi ve yanıtlanması aşamalarını kapsamaktadır. Güvenlik olaylarının yönetiminde kullanılan yöntemler ve metodolojiler, etkin ve proaktif bir savunma mekanizması oluşturulmasına katkı sağlar.



Şekil 2 SOC Temel Yapı Taşları

4.2 SOC’un Olay yönetimi süreçleri ve Görevleri

SOC'un işleyişi, tehditleri gerçek zamanlı olarak izleme, değerlendirme ve uygun yanıtları oluşturma süreçlerini kapsar. Bu olay yönetimi süreçleri;Önleme (Prevention) Monitor (İzleme), Tespit (Detection), Analiz (Analysis) ve Müdahale (Response) olmak üzere beş temel aşamada incelenir.

4.2.1 Önleme (Prevention) Süreci

➔Sistem ve ağ altyapılarında güvenlik önlemleri iyileştirilir.

➔Yama yönetimi sürekli takip edilerek güncel güvenlik açıkları giderilir.

➔Kullanıcılara güvenlik bilinci kazandırmak için eğitimler verilir.

➔Sürekli tehdit avcılığı (threat hunting) faaliyetleri yapılarak proaktif yaklaşımlar benimsenir.

Amacı: Potansiyel tehditleri ortadan kaldırarak sistemlerin daha güvenli hale getirilmesini sağlamaktır.

4.2.2 Monitor (İzleme) Süreci

➔Ağ ve sistem aktiviteleri sürekli takip edilir.

➔Log verileri analiz edilerek olağan dışı hareketler tespit edilmeye çalışılır.

➔Güvenlik araçlarından gelen alarmlar değerlendirilir.

➔Anormal olaylar için otomatik uyarı mekanizmaları oluşturulur.

Amacı: Olası tehditleri erken tespit ederek saldırıları engellemektir.

4.2.3 Tespit (Detection) Süreci

➔Şüpheli trafik, kötü amaçlı yazılım ve yetkisiz erişim gibi tehditler belirlenir.

➔Güvenlik açıklarını kullanan saldırı girişimleri incelenir.

➔Anormal kullanıcı davranışları tespit edilerek olası ihlaller belirlenir.

➔Kritik sistemlerde olağandışı değişiklikler gözlemlenir.

Amacı: Potansiyel güvenlik olaylarını hızlıca tespit etmek ve analiz sürecine yönlendirmektir.

4.2.4 Analiz (Analysis) Süreci

➔Gelen uyarılar incelenerek yanlış alarmlar elenir.

➔Saldırının kaynağı, yöntemi ve hedefi detaylı olarak analiz edilir.

➔Tehditin yayılma potansiyeli ve sistem üzerindeki etkileri değerlendirilir.

➔Önceki tehditlerle karşılaştırma yapılarak benzer olaylarla ilişkisi belirlenir.

Amacı: Gerçek tehditleri belirleyerek etkili bir müdahale planı oluşturmaktır.

4.2.5 Müdahale (Response) Süreci

➔Tespit edilen saldırılar için anında aksiyon alınır.

➔Zararlı etkinliklerin durdurulması için sistemler izole edilir.

➔Güvenlik açıkları kapatılarak sistem güçlendirme çalışmaları yapılır.

➔Gelecekte benzer saldırıları önlemek için politika ve güvenlik önlemleri güncellenir.

Amacı: Tehditleri en aza indirerek sistemin güvenliğini ve sürekliliğini sağlamaktır.

Şekil 3 SOC Analisti temel görevleri

5. SOC Ekip Hiyerarşisi

5.1 L1 Güvenlik Analisti

Seviye 1 SOC Analistleri SOC ekibinin ilk savunma hattını temsil eder. Sistem yöneticisi yetkinliklerine, programlama becerilerine ve temel siber güvenlik yeteneklerine sahiptirler.

➤Alarmların doğruluğunu kontrol eder ve olayların öncelik sırasını belirler.

➤Saldırı sinyali veren alarmlar için "ticket" oluşturarak seviye 2 SOC Analistlerine haber verir.

➤Zafiyet taramaları yapar ve tarama raporlarını değerlendirir.

➤Güvenlik izleme araçlarının yönetimi ve yapılandırılmasından sorumludur.

➤Log verilerini analiz ederek potansiyel tehditleri belirler.

5.2 L2 Güvenlik Analisti

Seviye 2 SOC Analistleri, Seviye 1 SOC Analistlerinin görevlerini desteklemekle birlikte daha derinlemesine analiz yaparlar.

➤Problemin kaynağına inebilme yeteneğine ve baskı altında krizi yönetebilme becerisine sahiptirler.

➤Seviye 1 SOC Analistlerinin oluşturduğu ticket'ları detaylı olarak inceler.

➤Tehdit istihbaratlarını değerlendirerek etkilenen sistemleri ve saldırının kapsamını belirler.

➤Saldırıya maruz kalan sistemler üzerindeki bilgileri analiz eder ve ilerideki muhtemel tehditlere karşı hazırlıklar yapar.

➤Kurtarma ve iyileştirme planlarını belirleyip uygular.

5.3 L3 Uzman Güvenlik Analisti

Seviye 3 SOC Analistleri SOC ekibinin en teknik uzmanlarından biridir ve ileri seviye analiz ile tehdit avcılığı yaparlar.

➤Seviye 1 ve 2 SOC Analistlerinin yetkinliklerine ek olarak veri görselleştirme araçlarına hakimdirler.

➤Tanımlanan zafiyetleri ve varlık envanteri verilerini detaylı olarak gözden geçirirler.

➤Tehdit istihbaratlarını temel alarak ağ içerisinde yerleşmiş gizli tehditleri ve bu tehditlerin tespit yöntemlerini belirlerler.

➤Sistemlere sızma testleri yaparak dayanıklılıklarını ve düzeltilmesi gereken açıkları tespit ederler.

➤Tehdit avcılığı yöntemlerini kullanarak güvenlik izleme araçlarını optimize ederler.

5.4 SOC Manager

SOC yöneticisi, ekibin operasyonlarını ve stratejisini yöneten en üst düzey pozisyondur.

➤Seviye 1, 2 ve 3 SOC Analistlerinin yetkinliklerine ek olarak güçlü liderlik ve iletişim yeteneklerine sahip olmalıdır.

➤Ekibin ruhunu diri tutarak etkin bir iş birliği ortamı yaratır.

➤SOC operasyonlarının sorunsuz ilerlemesini sağlar ve ekibin faaliyetlerini denetler.

➤SOC ekibi için eğitim programları geliştirir ve işe alım süreçlerini yönetir.

➤Saldırı ve olay yönetimi süreçlerini planlayarak olay raporlarını gözden geçirir.

➤Uyumluluk raporları yayınlar ve denetleme süreçlerini destekler.

SOC'un önemini üst yönetim düzeyine aktararak iş stratejilerine entegrasyonunu sağlar.

5.5 Siber Tehdit Istibarat Ekibi

Siber tehdit istihbarat ekibi, kurumun maruz kalabileceği mevcut ve potansiyel tehditler hakkında bilgi toplamak, analiz etmek ve bu bilgileri operasyonel karar alımında kullanmakla sorumludur.

➤Tehdit aktörlerinin amaçlarını ve metotlarını belirlemek için kapsamlı analizler yapar.

➤Kurum güvenliğine zarar verebilecek tehditler hakkında bilgi toplar, zenginleştirir ve ilgili birimlere sunar.

➤Tehdit avcılığı (threat hunting) faaliyetlerini destekleyerek saldırı öncesinde proaktif adımlar atılmasını sağlar.

➤Büyük SOC ekipleri tehdit istihbaratı konusunda özel ekiplere sahip olabilirken, daha küçük ekipler genellikle dışarıdan tehdit istihbaratı hizmeti alabilir.

➤Toplanan bilgiler siber savunma stratejilerinin güncellenmesine yardımcı olur.

SOC ekibinin bu yapısı, kurumların tehditlere karşı daha dayanıklı ve etkin bir savunma mekanizması oluşturmasını sağlar.

Şekil 4 SOC Analisti Hiyerarşisi

6. SOC Çalışma Modelleri

6.1 Internal Managed SOC

Bu modelde, şirket kendi güvenlik operasyonlarını tamamen kendi iç ekibiyle yönetir. Kendi personelinizle, kendi tesisinizde güvenliği sağlamak, daha fazla kontrol ve özelleştirme imkanı sunar, ancak maliyetli olabilir.

6.2 Distributed SOC / Co-Managed SOC

Dağıtılmış SOC, bir yandan şirket içindeki güvenlik ekibiyle çalışırken, diğer yandan dışarıdan bir güvenlik sağlayıcıdan destek alır. Bu, işlerin bir kısmının dışarıya verilmesiyle kaynakların verimli kullanılması anlamına gelir. Yani, hem iç hem dış kaynaklarla bir takım çalışması yapılır.

6.3 Yönetilen SOC (Managed SOC)

Yönetilen SOC, güvenliği tamamen dışarıya devretmek isteyen şirketler için uygundur. Bir güvenlik hizmet sağlayıcısı (MSSP), tüm güvenlik işlemlerini yönetir. Bu sayede şirketler, güvenlik konusundaki iş yükünü azaltıp uzmanlardan yardım alabilir.

6.4 Komanda SOC (Command SOC)

Komanda SOC, güvenlik operasyonlarında doğrudan yer almaz, ancak diğer SOC'lere ve kurumlara önemli istihbarat sağlar. Yani, operasyonel değil, daha çok stratejik bir role sahiptir ve tehditlere karşı bilgi verir.

6.5 Fusion Center

Füzyon merkezleri, farklı departmanlarla işbirliği yaparak güvenlik stratejilerini belirler. Burada, güvenlik operasyonları sadece bir bölüm değil, şirketin genel stratejisini oluşturan bir yapı olarak çalışır. Daha gelişmiş bir SOC türüdür ve çok yönlüdür.

6.6 Multi-functional SOC (SOC / NOC)

Bu modelde, SOC ve ağ operasyon merkezi (NOC) görevleri birleştirilir. Yani, hem güvenlik hem de ağ yönetimi birlikte yürütülür. Küçük şirketler için verimli ve maliyet dostu bir çözüm olabilir.

6.7 Sanal SOC (Virtual SOC)

Sanal SOC, fiziksel bir tesise ihtiyaç duymaz ve genellikle uzaktan çalışanlar veya dış bir sağlayıcı tarafından yönetilir. Güvenlik hizmetlerini esnek bir şekilde sunar, ancak kurum içi personel bulunmaz.

6.8 SOCaaS (SOC as a Service)

SOCaaS, bulut tabanlı bir çözüm sunar ve güvenlik hizmetlerini dışarıdan almanızı sağlar. Abonelik bazlı bir hizmet modelidir, böylece ihtiyacınız olduğunda tam ya da kısmi güvenlik hizmetlerini kolayca alabilirsiniz.

Şekil 5 SOC Çalışma Modelleri

7. SOC Tarafından Kullanılan Araçlar

7.1 IDS (Intrusion Detection System - Saldırı Tespit Sistemi)

IDS, ağ trafiğini ve sistem etkinliklerini izleyerek zararlı hareketleri tespit eden bir güvenlik aracıdır. IDS sistemleri, siber tehditleri algılayarak SOC ekibine uyarılar gönderir. İki temel türü bulunmaktadır:

Ağ Tabanlı IDS (NIDS): Ağ trafiğini analiz ederek anormallikleri tespit eder.

Ana Bilgisayar Tabanlı IDS (HIDS): Belirli bir cihaz veya sistem üzerinde çalışan işlemleri ve dosya değişikliklerini izler.

7.2 IPS (Intrusion Prevention System - Saldırı Önleme Sistemi)

IPS, IDS'nin bir adım ötesine geçerek, tespit edilen zararlı hareketleri otomatik olarak engelleyen bir sistemdir. IPS sistemleri genellikle güvenlik duvarlarıyla entegre çalışır ve şu şekilde sınıflandırılır:

Ağ Tabanlı IPS (NIPS): Ağ üzerindeki trafiği analiz ederek tehditleri engeller.

Ana Bilgisayar Tabanlı IPS (HIPS): Bireysel cihazlara yönelik tehditleri tespit edip önler.

7.3 SIEM (Security Information and Event Management - Güvenlik Bilgi ve Olay Yönetimi)

SIEM sistemleri, farklı kaynaklardan gelen log verilerini toplayarak analiz eder, anlamlandırır ve olası güvenlik tehditlerini belirleyerek SOC ekibine bildirir. SIEM, olaylara ilişkin detaylı raporlar sunarak siber tehditlerin daha hızlı çözülmesine yardımcı olur. Temel özellikleri şunlardır:

Merkezi Log Yönetimi: Farklı sistemlerden gelen günlük kayıtlarını bir araya getirir.

Gerçek Zamanlı İzleme ve Uyarılar: Anlık tehdit tespiti yaparak hızlı aksiyon alınmasını sağlar.

7.4 SOAR (Security Orchestration, Automation, and Response - Güvenlik Düzenleme, Otomasyon ve Yanıtlama)

SOAR, SOC ekibinin tehditleri algılamasını ve bunlara yanıt vermesini otomatikleştiren bir sistemdir. SIEM ile entegre çalışarak tehditlerin analiz edilmesini sağlar ve otomatik yanıt mekanizmaları geliştirir. Başlıca avantajları şunlardır:

Olay Yönetimi: Farklı kaynaklardan gelen tehdit verilerini toplar ve sınıflandırır.

Otomatik Yanıt Mekanizmaları: Belirlenen olaylara karşı otomatik müdahale sunar.

Tehdit İstihbaratı Entegrasyonu: Küresel tehdit verileriyle eşleştirme yaparak analizleri güçlendirir.

7.5 DLP (Data Loss Prevention - Veri Kaybı Önleme)

DLP, hassas verilerin yetkisiz erişim veya sızıntıya karşı korunmasını sağlayan bir güvenlik aracıdır. Şirketlerin gizli bilgilerini koruyarak, veri ihlallerini önlemeye yönelik politikalar uygular. DLP sistemleri şunları içerebilir:

Ağ Tabanlı DLP: Şirket içindeki veri trafiğini denetler ve hassas bilgilerin dışarı çıkmasını önler.

Son Kullanıcı DLP: Çalışanların bilgisayarlarındaki veri hareketlerini izleyerek veri sızıntısını engeller.

7.6 NGFW (Next Generation Firewall - Yeni Nesil Güvenlik Duvarı)

NGFW (Next Generation Firewall - Yeni Nesil Güvenlik Duvarı): Yeni nesil güvenlik duvarları, geleneksel güvenlik duvarlarının sunduğu temel koruma önlemlerinin ötesine geçerek daha gelişmiş güvenlik özellikleri sunar. NGFW, ağ trafiğini daha ayrıntılı analiz eder ve tehditleri daha etkin bir şekilde engeller.

Derin Paket İncelemesi (DPI): Trafikteki verileri analiz ederek kötü amaçlı içerikleri tespit eder.

Entegre IPS/IDS: Saldırı tespit ve önleme mekanizmalarını içerir.

SSL/TLS Şifre Çözme: Şifreli trafiği analiz ederek güvenlik açıklarını tespit eder.

Bulut ve Tehdit İstihbaratı Entegrasyonu: Güncel tehdit verileriyle sürekli olarak kendini günceller.

7.7 UTM (Unified Threat Management - Birleşik Tehdit Yönetimi)

UTM, firewall, IDS/IPS, antivirüs, VPN ve web filtreleme gibi birden fazla güvenlik fonksiyonunu tek bir platformda sunan güvenlik cihazlarıdır. Temel avantajları şunlardır:

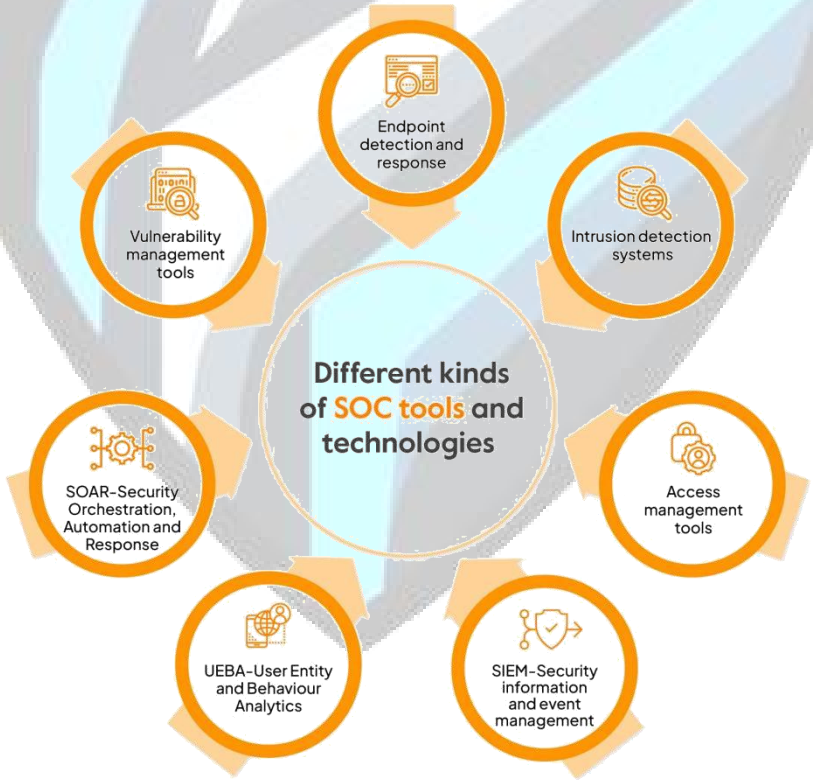
Merkezi Yönetim: Tüm güvenlik politikalarının tek bir platformdan yönetilmesini sağlar.

Gelişmiş İçerik Filtreleme: Zararlı içeriklerin sisteme girişini engeller.

Antivirüs ve Antispam: Kötü amaçlı yazılımlara ve istenmeyen e-postalara karşı koruma sunar.

7.8 GRC Sistemleri (Governance, Risk, and Compliance - Yönetim, isk ve Uyumluluk)

GRC sistemleri, kurumsal risklerin etkili bir şekilde yönetilmesini ve uyumluluk süreçlerinin optimize edilmesini sağlayan bir yapı sunar. Erken uyarı sistemleri sayesinde SOC ekibinin tehditlere hızlı müdahale etmesine yardımcı olur, Olası güvenlik tehditlerini önceden analiz eder ayrıca Mevzuat ve standartlara uyumu sağlayıp şirket güvenlik politikalarını düzenler ve denetler.



Şekil 6 SOC Araç Türleri

8. SONUÇ

Sonuç olarak SOC, modern kuruluşlar için siber tehditlere karşı en güçlü savunma hatlarından biri haline gelmiştir. Etkin bir SOC yapılanması, tehditleri hızla tespit edip müdahale ederek güvenlik açıklarını en aza indirir. Bu sayede veri kayıpları, finansal zararlar ve itibar kaybı gibi riskler önlenebilir.

Rapor kapsamında ele alınan SOC bileşenleri, ekip yapıları, olay yönetim süreçleri ve kullanılan teknolojiler, kuruluşların siber güvenlik stratejilerini oluştururken göz önünde bulundurması gereken temel unsurları içermektedir. Siber tehditlerin artmaya devam ettiği günümüzde, güçlü bir SOC yapısına sahip olmak, kurumsal güvenliği sağlamak için kritik bir faktördür.

Şirketlerin ve kamu kurumlarının SOC yatırımlarını artırarak güvenlik operasyonlarını daha verimli hale getirmesi kaçınılmaz bir gereklilik haline gelmiştir. Etkili bir SOC yönetimi, yalnızca mevcut tehditlere karşı koruma sağlamakla kalmaz, aynı zamanda gelecekteki siber saldırılara karşı da proaktif bir savunma mekanizması sunarak kuruluşların güvenliğini güçlendirir.

KAYNAKÇA

https://bulutistan.com/blog/soc/

https://elfanet.com.tr/tr/main/article/soc-nedir/31

https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir

https://www.bgasecurity.com/2018/11/soc-nedir-calisma-yapisi-ve-faydalari/

https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir/

https://uzmanposta.com/blog/soc/

https://www.ihsteknoloji.com/blog/guvenlik-operasyon-merkezi-soc-nedir/