SOC'UN GELECEĞİ:
YAPAY ZEKA DESTEKLİ

Modern Güvenlik Operasyonlarında Öncü Rol!

Orta Doğu'daki birçok kuruluş, kritik güvenlik operasyon merkezlerini (SOC'ler) yönetme ve yürütme biçimlerini yeniden gözden geçiriyor. Bölge, jeopolitik önemi, zengin doğal kaynakları ve dijital teknolojilere hızlı adaptasyonu nedeniyle siber saldırıların odak noktası haline geldikçe, güçlü siber güvenlik önlemlerine duyulan ihtiyaç hiç olmadığı kadar kritik hale gelmiştir. Raporlar, Orta Doğulu şirketlerin %55'inin önümüzdeki yıl dijital ve teknoloji kaynaklı riskleri azaltmayı önceliklendirdiğini göstermektedir ki bu oran, %53 olan küresel ortalamanın üzerindedir.[1]

Bölgedeki dijital dönüşüm, ekonomiyi çeşitlendirme ve ham madde bağımlılığını azaltmaya yönelik stratejik bir araç olarak devam etmektedir. Siber güvenliğin güçlendirilmesi ve kritik altyapının korunması, resmi dijital girişimlerin dayanıklılığını sağlamak açısından kilit öneme sahiptir.

Buna ek olarak, cihaz sayısındaki artış ve giderek daha da dağıtık hale gelen BT ortamı, saldırı yüzeyini genişletmekte ve kurumları siber tehditlere karşı daha savunmasız hale getirmektedir. Küresel siber güvenlik iş gücü açığı 2023 yılında 4 milyon kişiye ulaşmıştır ve Orta Doğu'da nitelikli güvenlik uzmanı eksikliği bu sorunu daha da derinleştirmektedir.[2] Bu eksiklik, işletmeleri giderek daha karmaşık hale gelen siber tehditlere karşı savunmasız bırakmaktadır.

SOC'lerin daha çevik, uyarlanabilir ve yapay zeka destekli yetkinliklerle donatılmış hale getirilmesi, bu evrilen tehditlere karşı proaktif bir şekilde pozisyon almak için hayati önem taşımaktadır.

BARİKAT ve Palo Alto Networks ile Modern SOC Deneyimine Evrilin!

BARİKAT ve Palo Alto Networks'ün birleşen uzmanlığıyla SOC yapınızı yeniden tasarlayın. Bu iş birliği, Palo Alto Networks'ün Cortex® otonom SecOps platformuna dayalı danışmanlık, teknik ve yönetilen hizmetler sunar. Birlikte, kuruluşunuzun gelişen siber tehditlerin önünde kalabilmesi için ihtiyaç duyduğu yol haritasını, uzmanlığı ve yapay zeka destekli SOC çözümlerini sağlıyoruz.

Siber güvenlik alanında lider konumda olan BARİKAT, Türkiye'de ve uluslararası düzeyde güçlü bir varlığa sahiptir. Dünya genelinde 600'ün üzerinde kurumsal müşteriye hizmet veren ve 40'tan fazla üreticiyle iş ortaklığı bulunan BARİKAT, derin teknik uzmanlığı ve sürekli gelişime olan bağlılığıyla siber güvenlikte mükemmelliği temsil eder.

BARİKAT'ı farklılaştıran en önemli unsur, Palo Alto Networks'ün ileri teknolojilerini kendi geliştirdiği çözümlerle entegre edebilme yeteneğidir. Bu sayede kesintisiz ve son derece etkili bir SOC deneyimi sunar. Müşteriler, özel ihtiyaçlarına göre uyarlanmış çözümler talep etmektedir. Yüzlerce başarılı uygulama deneyimiyle BARİKAT, güvenlik operasyonlarının en yüksek verimlilik ve etkinlikle optimize edilmesini sağlayacak derin tecrübeye sahiptir.

BARİKAT mühendislik ekipleri, Palo Alto Networks'ün Cortex ürün ailesinde çeşitli sertifikasyonlara sahiptir. BARİKAT Ar-Ge birimi tarafından geliştirilen platform, Palo Alto Networks çözümleriyle entegre çalışmakta ve buna ek olarak varlık izleme, SLA yönetimi ve saldırı yüzeyi takibi gibi yetenekler de sunmaktadır.

Türkiye Cumhuriyeti Millî Savunma Bakanlığı ve NATO tarafından akredite edilen BARİKAT, güçlü güvenlik çözümleri sunar. BARİKAT Akademi, analistlerin ve müşteri ekiplerinin becerilerini güncel tutmak amacıyla sürekli eğitim programları, atölye çalışmaları ve sertifikasyonlar sunarak önemli bir rol oynar. Bu benzersiz yaklaşım, Palo Alto Networks'ün ileri teknolojilerini ve BARİKAT'ın kendi geliştirdiği çözümleri bir araya getirerek müşterilerimiz için kesintisiz ve son derece etkili bir SOC deneyimi yaratır.

1. "Rising Threat Of Cyber Attacks In The Middle East," *a&s Middle East, January 20, 2025.*
2. "ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap ," *ISC2, November 3, 2023.*
3. "Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities ," *World Economic Forum, January 13, 2025.*

Gelişen Tehditlerin Bir Adım Önünde Olun:
Kurumunuza Özel SOC Stratejisiyle

Yapay zekâ teknolojisi geliştikçe hem siber güvenlik savunmalarını güçlendirmek hem de daha sofistike siber saldırılar oluşturmak için kullanılmakta ve bu durum tehdit ortamını giderek daha karmaşık hâle getirmektedir. Bu nedenle, işletmenin özgün ihtiyaçlarına özel olarak uyarlanmış net ve etkili bir güvenlik stratejisine sahip olmak hayati öneme sahiptir.

BARİKAT, ekip çalışmasının önemini vurgular ve her müşterinin ihtiyaçlarını ve karşılaştığı zorlukları çözüm sürecine entegre eder. Bu süreç; detaylı değerlendirmeleri, özel olarak hazırlanmış önerileri, uygulamayı ve müşterilerin güvenlik hedeflerine ulaşmasını sağlamak için sürekli desteği içerir. BARİKAT, Palo Alto Networks'ün ileri düzey güvenlik teknolojilerini kullanır ve bunları kendi geliştirdiği yazılımlarla tamamlayarak kurumların belirli sorun noktalarına doğrudan çözüm üretir.

> Gelişen teknolojilerin sağladığı benzeri görülmemiş düzeydeki karmaşıklık, kötü niyetli aktörlerin dolandırıcılık ve sosyal mühendislik saldırıları düzenleme, dezenformasyon üretme ve fidye yazılımları yürütme yeteneklerini daha önce hiç görülmemiş bir hızda, kapsamda ve ölçekte artırmaktadır. Kurumların neredeyse %47'si, Yapay Zekâ 4.0 (GenAI) tarafından desteklenen düşmanca gelişmeleri birincil endişe kaynağı olarak göstermektedir.[3]
>
> – Dünya Ekonomik Forumu 2025

Her iş birliği, müşterinin mevcut güvenlik duruşunun risk bazlı bir değerlendirmesiyle başlar. Bu değerlendirmede BARİKAT'ın kendi metodolojilerinin yanı sıra ISO/IEC 27001 ve NIST gibi uluslararası kabul görmüş standartlar da kullanılır. Ardından, Palo Alto Networks Cortex çözümlerini tespit, orkestrasyon ve müdahale süreçlerine entegre eden çok aşamalı bir yol haritası oluşturulur.Stratejik plan ve uygulama takvimi üzerinde mutabık kalındıktan sonra BARİKAT, birlikte geliştirilen yol haritasındaki öncelikler doğrultusunda harekete geçer ve özel olarak uyarlanmış SOC dönüşüm çözümünü uygular. Palo Alto Networks Cortex platformu ile BARİKAT'ın kişiselleştirilmiş yönetilen hizmetlerinin birleşimi sayesinde, tehdit tespitinde artış, daha hızlı yanıt süreleri ve karmaşık ortamlarda daha fazla görünürlük sağlanır.

BARİKAT'ın Ar-Ge birimi tarafından geliştirilen platform; varlık izleme, SLA takibi ve proaktif saldırı yüzeyi yönetimi gibi yetenekleri entegre ederek kurumların riski azaltmalarına, mevzuatlara uyum sağlamalarına ve gelişen tehditlerin önünde kalmalarına yardımcı olur. BARİKAT'ın yapay zekâ destekli SOC çözümünde Cortex platformunun yanı sıra dış saldırı yüzeyi yönetimi (EASM), operasyonel teknoloji (OT) sensörleri ve özel API'ler kesintisiz şekilde entegre edilir. Ortaya çıkan ortak çözüm, her kuruluşun kendine özgü ihtiyaçlarına göre özelleştirilmiş eksiksiz ve akıllı bir güvenlik yaklaşımı sunar.

İşletmeye Sağladığı Faydalar:

- **Güvenlik Duruşunu Güçlendirir:** Siber tehdit riskini azaltarak güvenlik seviyenizi artırır.

- **Operasyonel Verimliliği Artırır:** Siber güvenlik ihtiyaçlarınızın karşılandığını bilerek esas iş faaliyetlerinize güvenle odaklanmanızı sağlar.

- **Tehdit Tespiti ve Müdahaleyi Geliştirir:** Gerçek yaşamdan alınan tehdit simülasyonlarıyla daha erken ve daha doğru tespit ve müdahale imkânı sunar.

- **Sürdürülebilir Güvenlik Dönüşümü Sağlar:** Kuruma özel yol haritası ile sürekli iyileşme ve gelişen tehditlere uyum sağlama imkânı sunar; uzun vadeli faydalar ve siber tehditlere karşı dayanıklılık kazandırır.

3. " Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities ", World Economic Forum, January 13, 2025.

İleri Düzey SOC Yönetimi İçin
Üst Düzey Uzmanlığa Erişim!

Günümüzün siber güvenlik ekiplerinin, SOC'larını etkin bir şekilde yönetmek ve geliştirmek için gerekli uzmanlıkla donatılmış olmaları gerekmektedir. Siber güvenlik alanındaki hızlı gelişmeler, sürekli beceri gelişimini zorunlu kılar. BARİKAT, Palo Alto Networks ile olan iş birliği sayesinde hem analiz ekiplerine hem de müşteri ekiplerine sürekli eğitim sağlamada kilit rol oynamaktadır.

BARİKAT Akademi aracılığıyla sunulan çeşitli eğitim programları, atölye çalışmaları ve sertifikasyonlar; analistlerin en güncel siber güvenlik gelişmeleriyle uyumlu beceriler edinmesini sağlar. Bu eğitimler, gerçek dünyadaki tehdit senaryolarına odaklanır ve analistlerin her kuruma özel ihtiyaçlara yönelik kanıtlanmış uygulamaları ve kullanım senaryolarını benimsemelerine yardımcı olacak pratik deneyimler sunar.

> 2024'ten bu yana siber güvenlik alanındaki yetkinlik açığı %8 oranında artmıştır. Her üç kuruluştan ikisi, güvenlik gereksinimlerini karşılamak için gerekli yetenek ve becerilerden yoksundur. Kuruluşların yalnızca %14'ü, günümüzde ihtiyaç duydukları insan kaynağına ve yetkinliklere sahip olduklarından emin olduğunu belirtmektedir.[4]
>
> 2025 Dünya Ekonomik Forumu'na göre:

BARİKAT ayrıca seviye bir ve seviye iki analistlerle geçici iş gücü desteği de sağlar; böylece güvenlik duruşunda herhangi bir boşluk oluşmaz. BARİKAT'ın iştiraklerinden biri olan Çatı (shared services birimi), sürekli eğitim ve sertifikasyon olanakları sunar (örneğin: Palo Alto Networks Certified Network Security Engineer [PCNSE]). Bu kapsamlı yaklaşım, kurumların en güncel siber güvenlik teknolojileri ve uygulamaları konusunda uzman, yüksek nitelikli profesyonellere erişimini güvence altına alır.

BARİKAT, OT güvenliği, bulut güvenliği ve ileri düzey tehdit avcılığı alanlarında uzmanlaşmış birçok analistiyle yüksek personel bağlılığı sağlamaktadır. Bu da kurumun SOC uzmanlığını daha da güçlendirmektedir.

BARİKAT'ın Hollanda'ya yapacağı yakın vadeli genişleme yatırımı, küresel yetenek eksikliklerini telafi etmeye yardımcı olmak için "follow-the-sun" (günün 24 saati kesintisiz hizmet) modeline geçişte önemli bir adımdır. Bu model sayesinde farklı bölgelerde bilgi birikimi paylaşımı ve 7/24 kesintisiz hizmet sağlanabilecektir.

İşletmeye Sağladığı Faydalar:

- **Siber güvenlik operasyonlarını etkin şekilde yönetin:** Güvenlik operasyonlarının sorunsuz ve etkili şekilde yürütülmesini sağlamak için yetkinlik açıklarını giderin.
- **Sürekli öğrenme ve gelişime odaklanın:** Süregelen eğitim girişimleriyle siber güvenlikteki en son gelişmelerden faydalanın.
- **Analistlerin iş yükünü azaltın:** Cortex XSOAR® playbook'ları ve otomatik yanıtlarla, küçük ekiplerinizin daha büyük ortamları etkin şekilde yönetmesini sağlayın.
- **Nitelikli profesyonel havuzu oluşturun:** Palo Alto Networks ve yerel üniversitelerle iş birliği içinde yürütülecek ortak eğitim programları ve stajlarla yetkin insan kaynağı geliştirin.

4. " Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities "

Güçlü SOC Güvenliği İçin
Yapay Zekâ Destekli Tehdit Tespiti

Yapay zekâ destekli güvenlik operasyonları, gelişmiş tehdit tespiti, yanıt ve yönetim yetenekleri sağladığı için kritik öneme sahiptir. Bu sayede kurumlar en güncel siber tehditlere karşı korunur. Yapay zekâ odaklı güvenlik operasyonlarının entegrasyonu, verimliliği ve etkinliği artırır.

BARİKAT, Palo Alto Networks'ün Cortex platformunu kullanarak yenilikçi çözümlerle modern bir SOC deneyimi sunar. Bu entegrasyon sayesinde gerçek zamanlı tehdit analizi, otomatik yanıtlar ve sürekli izleme mümkün hale gelir. Yazılım modülleri, playbook'ların ve korelasyon senaryolarının etkinliğini doğrulayarak performansın en üst düzeye çıkmasını sağlar.

Bu iş birliğinin değeri, Palo Alto Networks ürün portföyü ile BARİKAT SOC'un birleşiminden doğar. Bu sayede tek bir yapay zekâ destekli platformda uçtan uca güvenlik sağlanır.

> Yapay zekâ destekli siber güvenlik risklerinin fark edilmesiyle, bu teknolojilerin gerekli güvenlik önlemleri olmadan hızla hayata geçirilmesi arasında bir paradoks bulunuyor. Kurumların %66'sı, yapay zekânın 2025 yılında siber güvenlik üzerinde büyük bir etki yaratmasını beklerken; yalnızca %37'si, bu araçların devreye alınmadan önce güvenlik değerlendirmesini yapan süreçlere sahip olduklarını bildiriyor.[5]
>
> 2025 Dünya Ekonomik Forumu'na göre:

Platform, gelişmiş orkestrasyon ve otomasyon (Cortex XSOAR), genişletilmiş tespit ve yanıt (Cortex XDR®), proaktif saldırı yüzeyi yönetimi (Cortex Xpanse®) ve yapay zekâ destekli SOC (Cortex XSIAM®) özelliklerini benzersiz şekilde bir arada sunar.Buna ek olarak, BARİKAT'ın kendi geliştirdiği özel yazılım çözümleri, Palo Alto Networks ürün portföyünü tamamlayarak saldırı yüzeyi izleme ve varlık yönetimi gibi ek kabiliyetler sağlar. Tehdit istihbaratının alınması, korelasyonu ve olayların yükseltilmesi süreçlerinin tümü, yapay zekâ destekli tek bir platformda standartlaştırılmış olarak sunulur. Bu sayede müşteri ortamlarında tutarlı ve hızlı tespit sağlanır.

BARİKAT'ın yapay zekâ destekli güvenlik araçları, her kurumun SOC verimliliğini ve etkinliğini artırır. Ortaklaşa sunulan bu çözümler, tehditleri geleneksel yöntemlere kıyasla daha hızlı tanımlayıp bertaraf edebilir, böylece proaktif güvenlik önlemleri sağlanır. Palo Alto Networks'ün yeni nesil SOC analitiğinden yararlanan BARİKAT, gelişmiş tehdit aktörlerinin kullandığı gizli kalıpları, taktikleri, teknikleri ve prosedürleri (TTP'ler) tespit ederek önleyici savunma kabiliyetlerini güçlendirir.

İşletmeye Sağladığı Faydalar:

- **Yanıt Sürelerini Azaltın:** Potansiyel tehditlere karşı daha hızlı aksiyon alarak daha kısa müdahale süreleri elde edin. Kurumlar, BARİKAT'ın yapay zekâ destekli çözümlerini kullandıktan sonra ortalama tespit süresi (MTTD) metriklerinde iyileşme bildirmektedir.

- **Tehdit Tespitinde Doğruluğu Artırın:** Daha etkili güvenlik önlemleri elde edin.

- **Tespit ve Önceliklendirmede Öngörülebilirliği Artırın:** Otomasyon sayesinde tutarlı ve güvenilir tespit ve önceliklendirme süreçleri sağlayın.

- **Siber Olayların Etkisini En Aza İndirin:** İş sürekliliğini koruyarak kesinti ve operasyonel aksaklıkları azaltın.

- **Sürekli İyileşmeyi Teşvik Edin:** Gelişen tehditlere karşı uyum sağlayarak dirençli ve sürdürülebilir çözümler geliştirin.

5. " Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities "

BARİKAT Hakkında

Bölgesel bir siber güvenlik lideri olan BARİKAT, dijital geleceği güvence altına alma misyonuyla uzmanlaşmış bilgi birikimi ve inovasyonla hareket etmektedir. Yüzlerce kuruluşun güvendiği BARİKAT, yönetilen güvenlik hizmetlerinden tehdit tespiti ve danışmanlığa kadar uçtan uca güvenlik hizmetleri sunar. Sadece siber güvenliğe odaklanmamız, işletmelere dayanıklı dijital altyapılar kurma gücü verir.

Daha fazla bilgi için: **www.barikat.com.tr**

Palo Alto Networks Hakkında

Küresel siber güvenlik lideri olan Palo Alto Networks (NASDAQ: PANW), sürekli inovasyon aracılığıyla dijital yaşam tarzımızı korumaya kendini adamıştır. Dünya genelinde 70.000'den fazla kuruluş tarafından güvenilen şirket, ağ, bulut, güvenlik operasyonları ve yapay zekâ alanlarında kapsamlı ve yapay zekâ destekli güvenlik çözümleri sunar. Unit 42® uzmanlığı ve tehdit istihbaratıyla desteklenen bu çözümler, platformlaştırma odağı sayesinde kurumların güvenlik süreçlerini ölçeklenebilir şekilde sadeleştirmesine olanak tanır ve inovasyonu destekleyen güvenlik sağlar

Daha fazla bilgi için: **: www.paloaltonetworks.com**

BARİKAT ve Palo Alto Networks Ortaklığının Değeri

• **İnovasyon Odaklı Ortaklık:** Palo Alto Networks ile süregelen iş birliği, siber güvenlik çözümlerini geliştirmeye yönelik ortak inovasyona dayanmaktadır.

• **Kanıtlanmış Uzmanlık:** BARİKAT'ın mühendislik ekibi, Palo Alto Networks'ün Cortex ürün ailesi üzerinde uygulamalı deneyime ve PCNSE sertifikası dahil olmak üzere birçok teknik sertifikaya sahiptir.

• **Tanınmış Mükemmeliyet**: BARİKAT, sektörde birçok ödül ve takdir kazanmıştır. Bunlar arasında yönetilen güvenlik hizmetleri sağlayıcılığı (MSSP) ve OT güvenlik hizmetlerinde yerel düzeyde liderlik yer almaktadır. Öne çıkan bazı yetkinlikler:

- Türkiye Cumhuriyeti Millî Savunma Bakanlığı ve NATO tarafından akredite edilmiştir.
- T.C. Sanayi ve Teknoloji Bakanlığı tarafından Ar-Ge merkezi olarak yetkilendirilmiştir.
- E-Turquality logosu sahibidir.

• **Kapsamlı Güvenlik Çözümleri:**

- Türkiye ve Körfez İşbirliği Konseyi (GCC) ülkelerinde SOC (Güvenlik Operasyon Merkezi) işletmekte olup, Avrupa'da (Hollanda) genişleme planları mevcuttur.

- Kritik altyapıları korumak amacıyla hem BT (IT) hem de endüstriyel (OT) ortamları destekleyen OT odaklı güvenlik alanında kanıtlanmış deneyime sahiptir.

- SOC ekipleri, gerçek tehdit simülasyonlarıyla desteklenen yoğun ve sürekli eğitimlerden geçmekte, böylece derin uygulamalı uzmanlık kazanmaktadır.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_wp-the-future-of-soc_061125