ARTEX ve Otonom Saldırı Araçlarına Karşı Savunma Rehberi

Saldırılar makine hızında. Savunmanız da öyle olmalı.

Bu rehber kimler için? Kurumunu ARTEX ve benzeri otonom saldırı araçlarına karşı hazırlamak isteyen CISO'lar, SOC yöneticileri ve güvenlik mimarları için. Rehber, Cloud Security Alliance'ın (CSA) eylem planını özetliyor ve her adımın Netzilo ile nasıl hayata geçirilebileceğini gösteriyor.

Ne değişti?

ARTEX, açık kaynak kodlu olarak yayımlanmış otonom bir sızma testi aracı. İçindeki yapay zekâ ajanları, bir kurumun internete açık sistemlerini bağımsız biçimde keşfediyor, tespit ettikleri açıkları deniyor ve içeri girmeyi başarana kadar girişimlerini sürdürüyor. Araç kısa sürede tehdit gruplarının eline geçti ve finans, kamu, teknoloji, savunma ve sağlık sektörlerindeki kurumlara yönelik saldırılarda kullanıldığı bildirildi.

Cloud Security Alliance (CSA), 800'ü aşkın CISO'nun katıldığı acil durum toplantısının ardından 25 Kasım 2026'da bir eylem planı yayımladı. CSA, bu yeni araç sınıfını **Agentic Offensive Framework (AOF)** olarak adlandırıyor. Vardığı sonuç net: Saldırılar makine hızında ilerlerken her müdahale için onay beklemek artık bir seçenek değil.

RAKAMLARLA YENİ DÖNEM

3 saatten kısa
Bazı saldırılarda ayrıcalıklı erişime ulaşmak için gereken süre

Birkaç saat
Eksik bırakılan temizliğin ardından saldırganın geri dönmesi için geçen süre

800+
CSA'nın acil durum toplantısına katılan CISO sayısı

Sahadan çıkan ders: Ajanları saldırının her aşamasında kullanan ekipler, saldırganlarla aynı hızda hareket edebildi. Tuzaklar saldırganları yavaşlattı, hatta durdurdu. Yarım bırakılan temizlik ise saatler içinde yeni bir sızmayla sonuçlandı.

1 SALDIRI NASIL İLERLİYOR, NETZILO NEREDE DURDURUYOR?

AŞAMA	SALDIRGAN	NETZILO
1 **Keşif**	İnternete açık tüm varlıkları tarar: iş ortağı portalları, eski uygulamalar, MCP sunucuları ve yapay zekâ ağ geçitleri. Bulduğu her şeye inanır.	**Keşif, saldırgan için bir tuzağa dönüşür.** Yayımladığınız her uygulamanın, MCP sunucusunun ve AI ağ geçidinin yanında, kendi yapılandırmasından üretilmiş ve sahte anahtarlar taşıyan inandırıcı kopyalar durur. Saldırgan bunlardan birine dokunduğu anda tüm sistemlerinizden engellenir. Gerçek uygulamalar ise sıfır güven erişimiyle görünmez kalır.
2 **Anahtar avı**	Unutulmuş anahtarların peşine düşer; ilk hedefi yapay zekâ servis anahtarlarıdır.	Yapay zekâ sağlayıcı anahtarları AI Ağ Geçidi'nden hiç çıkmaz. Kullanıcılar ve ajanlar kendi kimlikleriyle bağlanır; harcama ve token limitleriyle sınırlandırılır.
3 **Ajanları ele geçirme**	Araç açıklamalarına ve yanıtlarına gizlediği talimatlarla kurumunuzun kendi ajanlarını yönlendirir.	Her istem, araç çağrısı ve MCP yanıtı anlık olarak denetlenir. Çok adımlı saldırı zincirleri tamamlanmadan durdurulur.
4 **Yanal hareket**	İlk erişim noktasından ayrıcalıklı erişime ilerler; çoğu zaman tedarikçi ve CI bağlantılarından yararlanır.	Erişim, alt ağ ve port düzeyine kadar daraltılır; her bağlantıda cihaz güvenliği denetlenir. Bir tedarikçinin erişimi, bağlı olduğu grubun kaldırılmasıyla kesilir.
5 **Geri dönüş**	Temizlik yarım kaldıysa birkaç saat içinde yeniden içeri girer.	Yanıt Eylemleri; bir oturumu, ajanı, kullanıcıyı veya hesabı bir saniyeden kısa sürede izole eder. Tuzaklar temizlikten sonra da yerinde kalır ve geri dönen saldırganı yakalar.

2 CSA'NIN EYLEM PLANI VE NETZILO'NUN KARŞILIĞI

Netzilo, CSA'nın 20 önerisinden 10'unu doğrudan karşılıyor.

CSA ÖNERİSİ	NETZILO İLE
BU HAFTA	
Saldırganın arayacağı noktalara tuzak kurun.	Yayındaki her uygulama, MCP sunucusu ve AI ağ geçidi için sahte anahtarlar taşıyan tuzak kopyalar oluşturulur. Tek bir temas, ilgili adresin tüm sistemlerde engellenmesi için yeterlidir.
En kritik uygulamaların giriş noktalarını kapatın.	Uygulamalar sıfır güven erişimiyle internetten gizlenir veya kimlik doğrulama, grup yetkileri ve cihaz denetiminin arkasında yayımlanır.
Kendi ajanlarınızı güvenceye alın.	Cihaz, SDK, tarayıcı ve AI Ağ Geçidi katmanlarında aynı denetim uygulanır: model ve araç izinleri, koruma kuralları ve davranış grafiği.
BU AY	
Yapay zekâ harcamalarını ve token kullanımını izleyin.	Kullanıcı, ajan ve model bazında raporlama yapılır. Saatlikten yıllığa kadar farklı dönemler için harcama, token ve istek limitleri belirlenir.
Müdahale yetkisini önceden verin.	Yanıt Eylemleri ile oturum, ajan, kullanıcı, grup, cihaz veya hesap düzeyinde izolasyon sağlanır. İzolasyon cihazlarda bir saniyeden kısa, ağ geçitlerinde ise yaklaşık iki saniye içinde gerçekleştirilir.
Tedarikçi ve üçüncü taraf erişimini sınırlayın.	Tedarikçi, MSP ve CI erişimleri gruplara bağlanır. İlgili grubun kaldırılması erişimi anında keser.
Uç noktalardaki açıkları kapatın.	EDR'nin göremediği ajan etkinlikleri görünür hâle gelir: istemler, araç çağrıları, başlatılan süreçler, dosyalar ve bağlantılar. EDR'si çalışmayan cihazların erişimi engellenir.
BU ÇEYREK	
Güvenlik gereksinimlerine uygun modellere ve yedek modellere erişim sağlayın.	Önde gelen sağlayıcıların modelleri ile kurum içinde çalışan açık modeller (Ollama, vLLM, SGLang) tek bir ağ geçidinde sunulur. Hata veya zaman aşımı durumunda otomatik olarak yedek modele geçilir.
Dışa giden trafiği varsayılan olarak kapatın.	Kritik uygulamaların çevresinde alt ağ ve port düzeyinde en az yetki politikaları ile mikro segmentasyon uygulanır.
Saldırıları çalışma anında yakalayın.	Ajanların araç çağrıları, süreçleri, dosya erişimleri ve bağlantıları üzerinde anlık koruma kuralları uygulanır; saldırı zincirleri tespit edilir.

Kalan 10 öneride de (yapay zekâ destekli alarm triyajı ve eksiksiz iyileştirme gibi) Netzilo; kayıt, erişim iptali ve ajan denetimiyle katkı sağlar.

3 İLK HAFTA İÇİN KONTROL LİSTESİ

- ☐ **Pazartesi:** En kritik üç uygulamanızı Netzilo üzerinden yayımlayın ve tuzakları etkinleştirin.
- ☐ **Çarşamba:** Kodlama, masaüstü ve kurum içi ajanlarınızı Netzilo'ya bağlayın; koruma kurallarını etkinleştirin.
- ☐ **Cuma:** Her tedarikçi, MSP ve CI süreci için ayrı bir grup ve en az yetki politikası tanımlayın.
- ☐ **Salı:** Yapay zekâ sağlayıcı anahtarlarını AI Ağ Geçidi'ne taşıyın ve limitleri belirleyin.
- ☐ **Perşembe:** Ekibinizin onay beklemeden uygulayabileceği Yanıt Eylemlerini yazılı hâle getirin.

ARTEX'e karşı ne kadar hazırsınız?

Kurumunuzun mevcut durumunu birlikte değerlendirelim ve ilk hafta için uygulanabilir bir yol haritası oluşturalım.

Görüşme planlayın → www.netzilo.com.tr

Kaynak: Cloud Security Alliance, The Third Wave: ARTEX and Agentic Offensive Frameworks, 25 Kasım 2026.