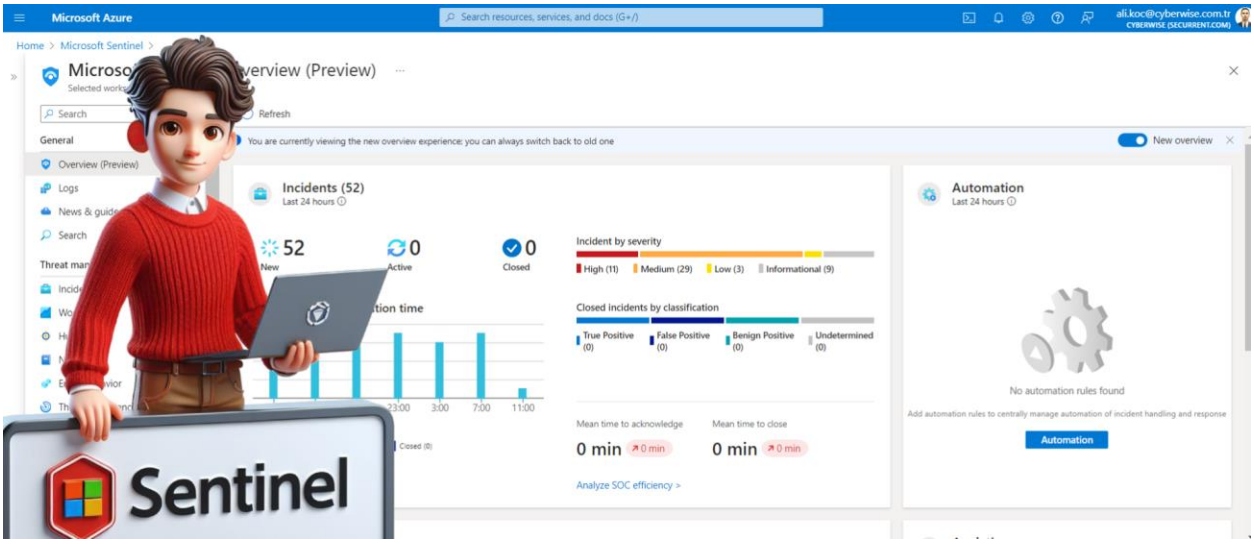
Microsoft Sentinel – The Ultimate Blog Series Part 1



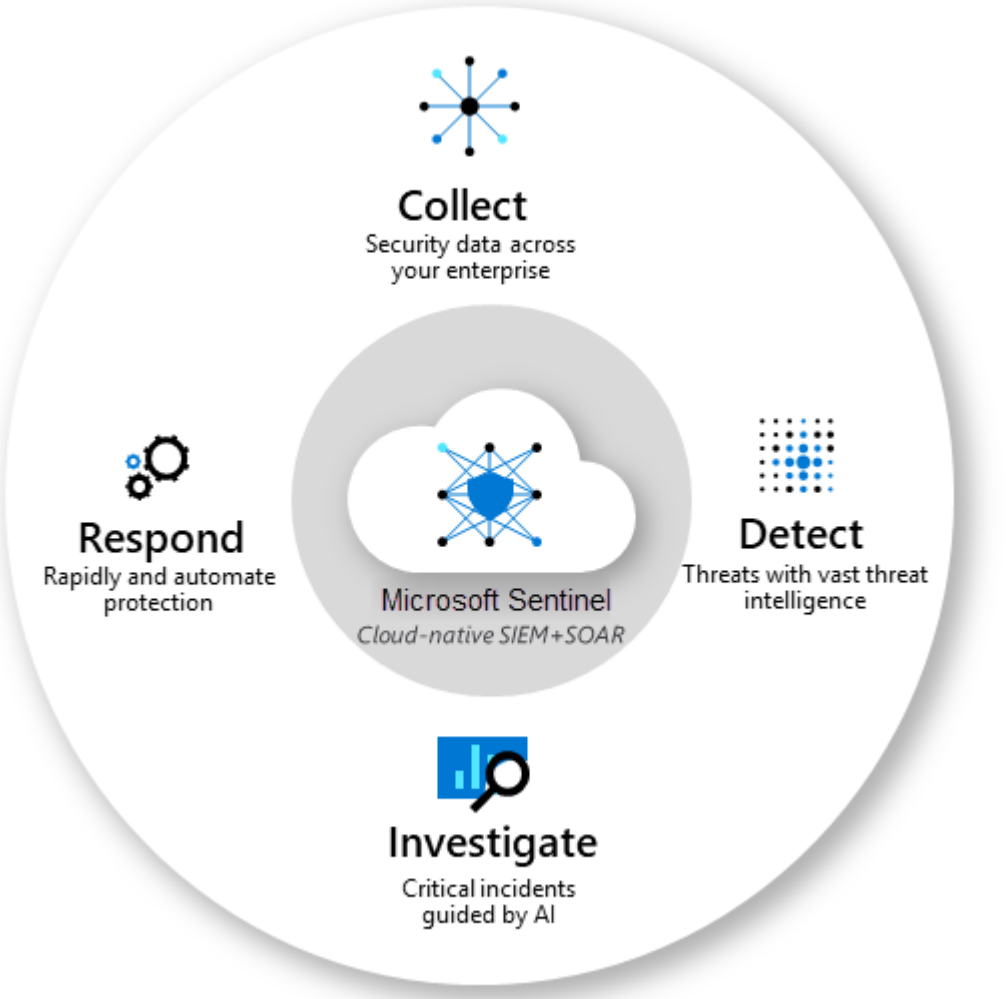
Sentinel, Microsoft' un bulut tabanlı yeni nesil SIEM / SOAR ürünüdür. Microsoft Sentinel, kurum genelinde Intellegent Security analytics ve threat intelligence ile saldırı algılama, tehdit görünürlüğü, proaktif avlanma ve threat response elde etmekle beraber, Azure Sentinel bir SIEM ürününden fazlasıdır. Kurumsal seviyede gerek yerleşik gerekse bulut tabanlı alt yapınızın "intelligent security analytics" olarak isimlendirilen akıllık güvenlik analizi yapan bir üründür. Tüm kurumunuzdaki loglarının tamamının alındığı incelendiği değerlendirildiği bir ortam olarak nitelendirebiliriz.

Microsoft Sentinel, giderek karmaşıklaşan saldırıların, artan uyarı hacimlerinin ve uzun çözüm sürelerinin stresini hafifletmekle beraber kurum genelinde tüm yapıyı kuş bakışı görmenize olanak tanımaktadır.

Microsoft Sentinel, Log Analytics ve Logic Apps gibi kanıtlanmış Azure hizmetlerini yerel olarak içerir. Microsoft Sentinel, araştırmanızı ve algılamanızı yapay zeka ile zenginleştirir. Microsoft'un tehdit zekası akışını sağlar ve kendi tehdit zekanızı getirmenize olanak tanımaktadır.

Bulut temelli olduğu için veri toplama işi son derece kolaydır. Özellikle Microsoft'un kendi sistemleri baz alındığında Office 365 gibi bir alt yapıyı aktif olarak kullanıyorsanız kolay bir şekilde Office 365 aktivitelerini ve olaylarını Sentinel ile toplayabilirsiniz. Bununla birlikte globalde yer alan bir çok firmayı doğrudan entegrasyon ile bağlayabilir ve logları toplayabilirsiniz. F5, Fortinet, Symantec, Check Point ve bir çok vendor'ı bunlara örnek kabul edebilirsiniz.

Microsoft Sentinel çalışma yapısını incelerken 4 ana başlıktan bahsedebiliriz.



- **Collect** : Hem on-premises hem de multi cloud tüm kullanıcılar, cihazlar, uygulamalar ve altyapı genelinde bulut ölçeğinde veri toplamaktadır. Microsoft ürünleri desteği, common event format ve syslog gibi log formatlarının desteklemesi sayesinde tüm kullanıcı, aygıt ve alt yapınızdan bilgileri kolay bir şekilde toplayabilirsiniz.
- **Detect** : Microsoft'un analizlerini ve benzersiz threat intelligent özelliklerini kullanarak daha önce tespit edilmemiş tehditleri tespit etmenize ve false pozitif çıktıları en aza indirmenizi sağlar. Microsoft Sentinel ise milyonlarca düşük veya yüksek seviye güvenlik olaylarını makine öğrenmesi kullanarak gerektiğinde çok hızlı karar verebilmeniz için ihtiyacı olan kaynağı alıp ve sonucu ürettikten sonra bir daha birdaha ihtiyaç haline kadar tekrar düşük kaynak kullanımına devam etmektedir. Bu cevap süresinde herhangi bir farklılığa sebebiyet vermemektedir.
- **Investigate** :Yapay zeka ile tehditleri araştırır ve Microsoft'un yıllara dayanan siber güvenlik çalışmalarından yararlanarak şüpheli etkinlikleri geniş ölçekte avlamanızı sağlar.

- **Respond** :Yerleşik düzenleme ve ortak görevlerin farklı otomasyonlar sayesinde olaylara hızla yanıt vermektedir. Ayrıca gerçekleşebilen entegrasyonlar sayesinde koşulsuz ve üretken bir yapı oluşmaktadır.

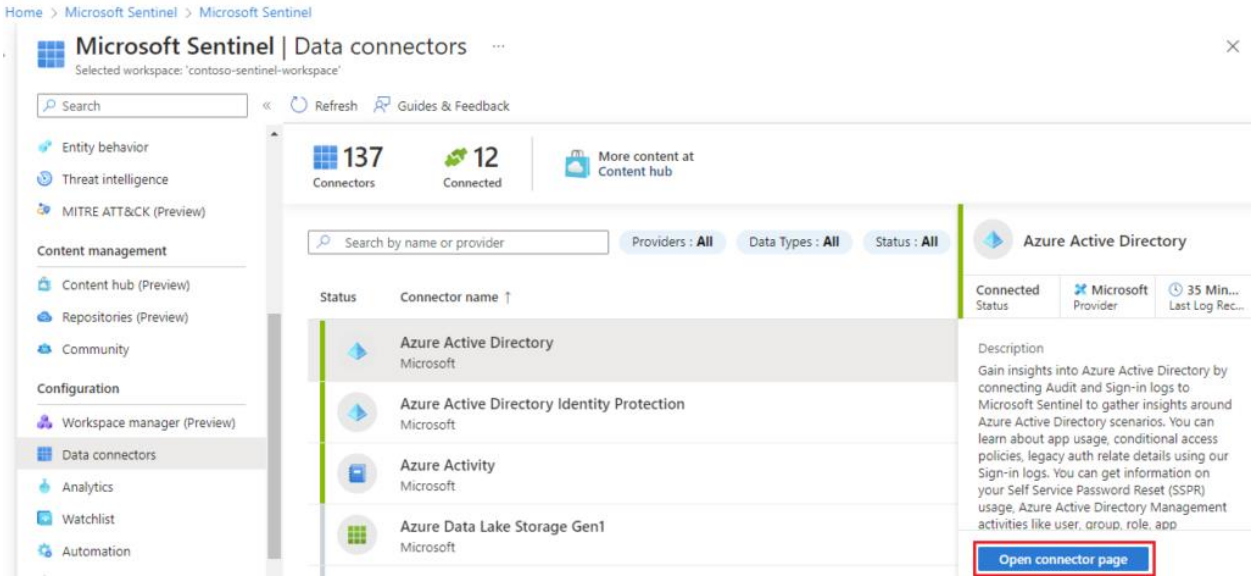
Data Connector'ler ile Veri Toplama

Microsoft Sentinel'e bağlanmak için öncelikle veri kaynaklarının bağlanması gerekmektedir.

Microsoft Sentinel, Microsoft çözümleri için kullanıma hazır olan ve gerçek zamanlı bağlantı sağlayan birçok bağlayıcıyla birlikte gelir. Bu bağlayıcılara örnek vermek gerekirse;

- Microsoft Defender XDR, Microsoft Defender Cloud, Office 365, Microsoft Defender for IoT ve daha fazlası gibi Microsoft tüm kaynakları.
- Microsoft Entra Id, Azure Activity, Azure Storage, Azure Key Vault, Azure Kubernetes hizmeti ve daha fazlası olan tüm Azure hizmet kaynakları.

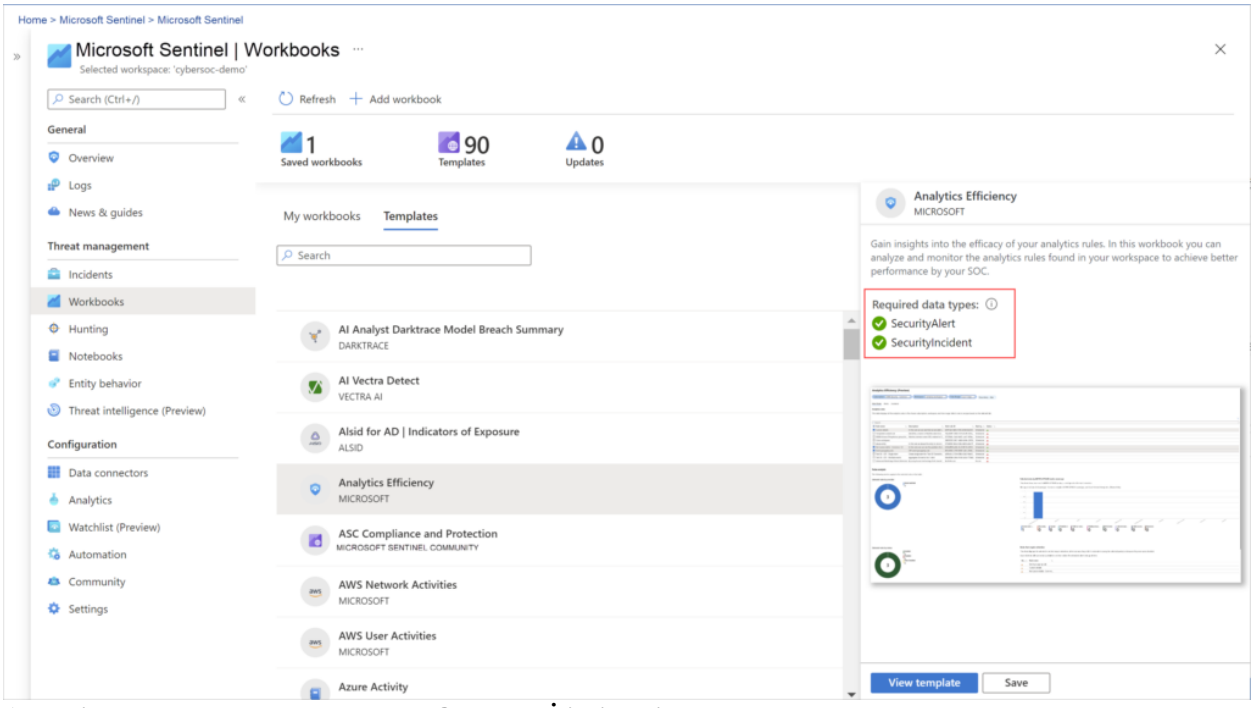
Microsoft Sentinel, Microsoft dışı çözümler için daha geniş güvenlik ve uygulama ekosistemlerine yönelik yerleşik bağlayıcılara sahiptir. Veri kaynaklarınızı Microsoft Sentinel'e bağlamak için ortak olay biçimi, Syslog veya REST-API de kullanabilirsiniz.



Workbook Kullanarak Interaktif Raporlar Oluşturma

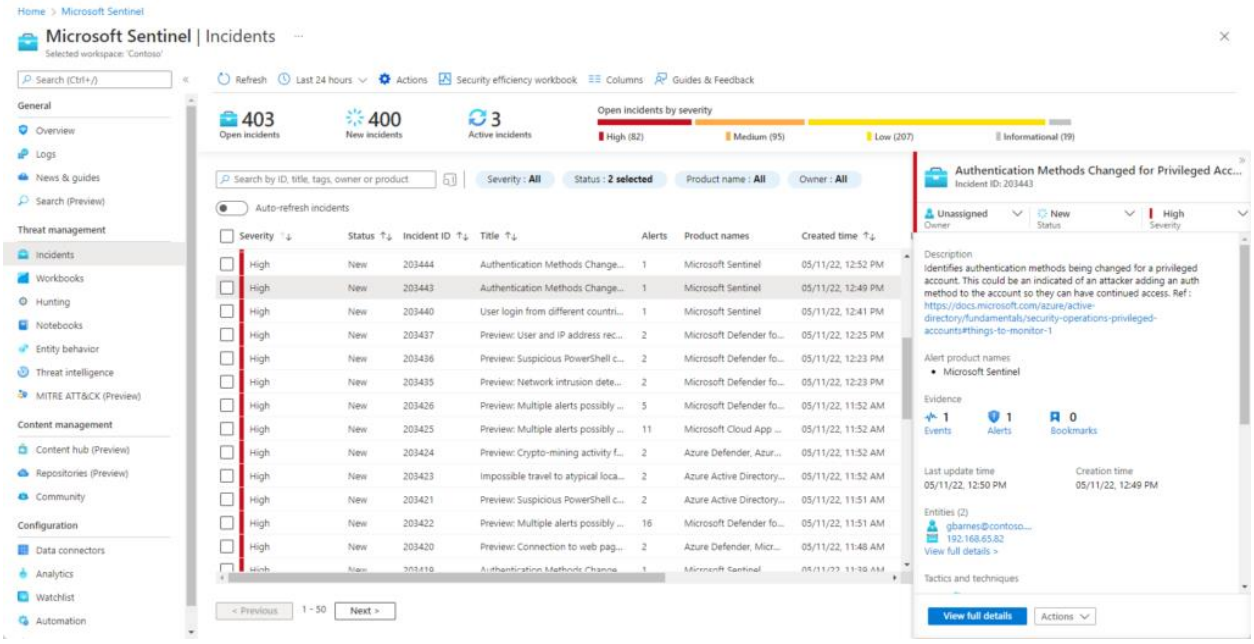
Microsoft Sentinel'e ekleme yaptıldıktan sonra, Azure Monitor çalışma kitaplarıyla tüm verilerinizi izleyebilirsiniz.

Workbooklar Microsoft Sentinel'de Azure Monitor'den farklı şekilde görüntülenir. Ancak Azure Monitör'de Workbook oluşturmayı görmeniz yararlı olabilir. Microsoft Sentinel, verileriniz arasında özel Workbook oluşturmanıza olanak tanımaktadır. Microsoft Sentinel ayrıca, bir veri kaynağına bağlanır bağlanmaz verilerinizle hızlı bir şekilde data elde etmenize olanak sağlayan yerleşik workbook şablonlarıyla birlikte gelir.



Analytic Rulles Kullanarak Uyarıları Olaylarla İlişkilendirme

Microsoft Sentinel, olası toplanacak olan gerekli gereksiz loglardan oluşan gürültüyü azaltmanıza ve gözden geçirip araştırmanız gereken uyarı sayısını en aza indirmenize yardımcı olmak için uyarıları olaylarla ilişkilendirmek için analiz kullanır. Olaylar, birlikte araştırabileceğiniz ve çözebileceğiniz eyleme dönüştürülebilir olası bir tehdidi gösteren ilgili uyarı gruplarıdır. Yerleşik bağıntı kurallarını olduğu gibi kullanın veya kendi kurallarınızı oluşturmak için başlangıç noktası olarak kullanabilirsiniz. Microsoft Sentinel ayrıca ağ davranışınızı anlamak ve ardından kaynaklarınızdaki anomalileri aramak için makine öğrenmesi kuralları sağlamaktadır. Bu analizler, farklı varlıklarla ilgili düşük uygunluk uyarılarını olası yüksek uygunluk güvenlik olaylarına birleştirerek noktaları birbirine bağlar.



Playbook'ları Kullanarak Ortak Görevleri Otomatikleştirme ve Düzenleme

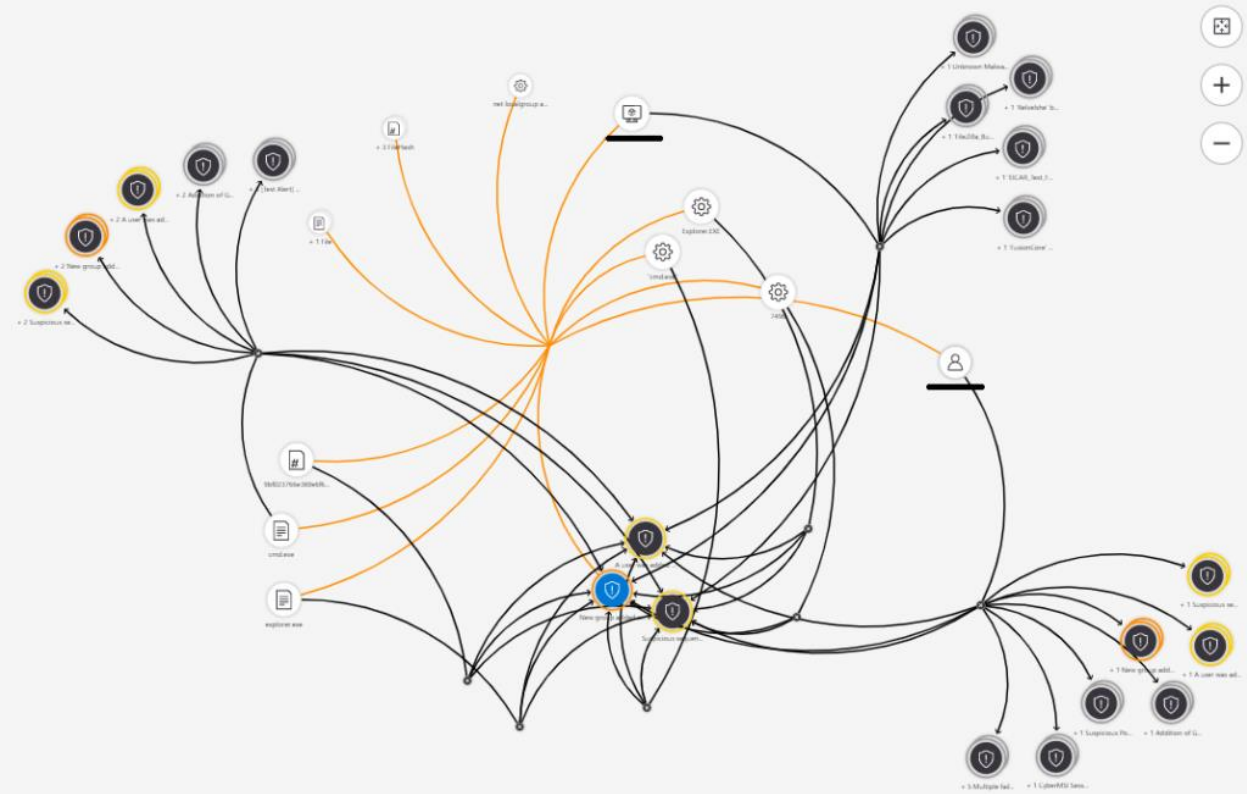
Microsoft Sentinel'in otomasyon ve düzenleme çözümü, yeni teknolojiler ve tehditler ortaya çıktıkça ölçeklenebilir otomasyon sağlayan yüksek oranda genişletilebilir bir mimari sağlamaktadır. Azure Logic Apps ile playbook'lar oluşturmak için, çeşitli hizmetler ve sistemler için birçok bağlayıcı içeren sürekli genişleyen bir yapıya sahipsiniz. Bazı bağlayıcı örneklerini ele alırsak;

- Uç nokta için Microsoft Defender
- Microsoft Defender for Cloud Apps
- ServiceNow
- HTTP istekleri
- Microsoft Teams
- Slack
- Microsoft Entra Kimliği
- Jira
- Zendesk

Örneğin, Jira proje yönetim sistemini kullanıyorsanız iş akışlarınızı otomatikleştirmek için Azure Logic Apps'i kullanarak ve belirli bir uyarı veya olay her oluşturulduğunda Jira'da bir ticket açacak yapıyı entegre edebilirsiniz.

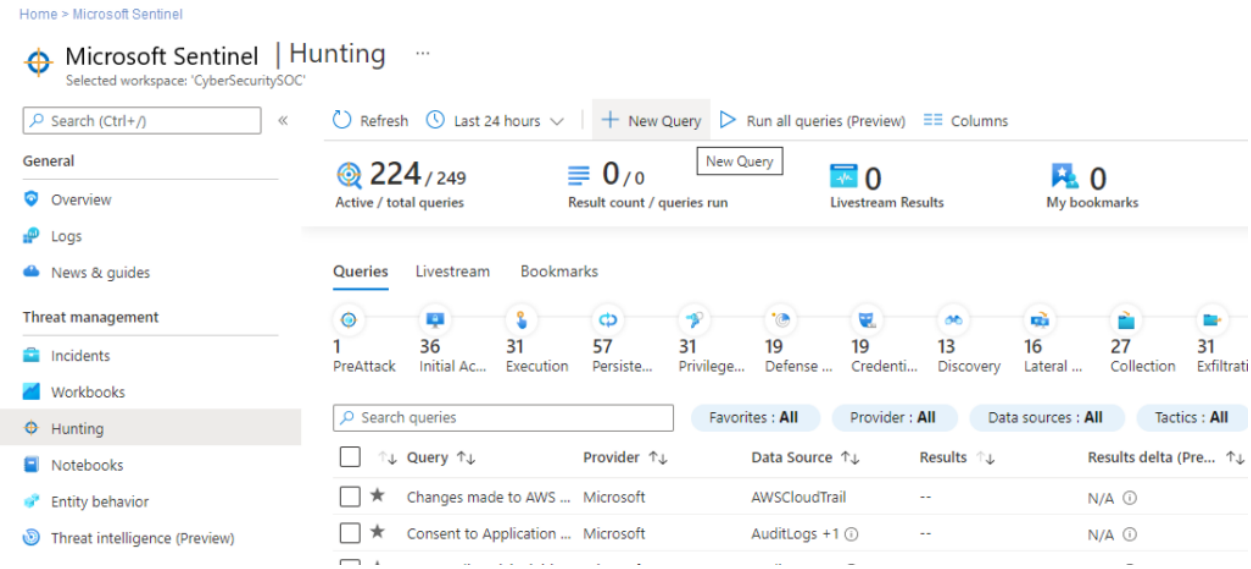
Güvenlik Tehditlerinin Kapsamını ve Kök Nedenini Araştırma

Microsoft Sentinel derin araştırma araçları, kapsamı anlamanıza ve olası bir güvenlik tehdidinin detay nedenini bulmanıza yardımcı olur. Belirli bir varlıkla ilgili ilginç sorular sormak için etkileşimli grafikte bir varlık seçebilir ve tehdidin kök nedenini bulmak için bu varlığın ve bağlantılarının detayına gidebilirsiniz.



Threat Hunting Çalışmaları

Microsoft Sentinel'in , bir uyarı tetiklenmeden önce kuruluşunuzun veri kaynaklarında güvenlik tehditlerini proaktif olarak avlamanızı sağlayan MITRE çerçevesini temel alan güçlü tehdit avcılığı arama ve sorgulama araçlarını kullanabilirsiniz. Threta Hunting sorgunuzu temel alan Custom Detection Rule'lar oluşturabilirsiniz. Ardından bu içgörüleri güvenlik olayı yanıtlayanlarınıza uyarı olarak ortaya çıkacaktır.



Part 2 'de Sentinel'in devreye alınma süreci ve Data Connectorlerin oluşturulma süreçlerini işleyeceğiz.