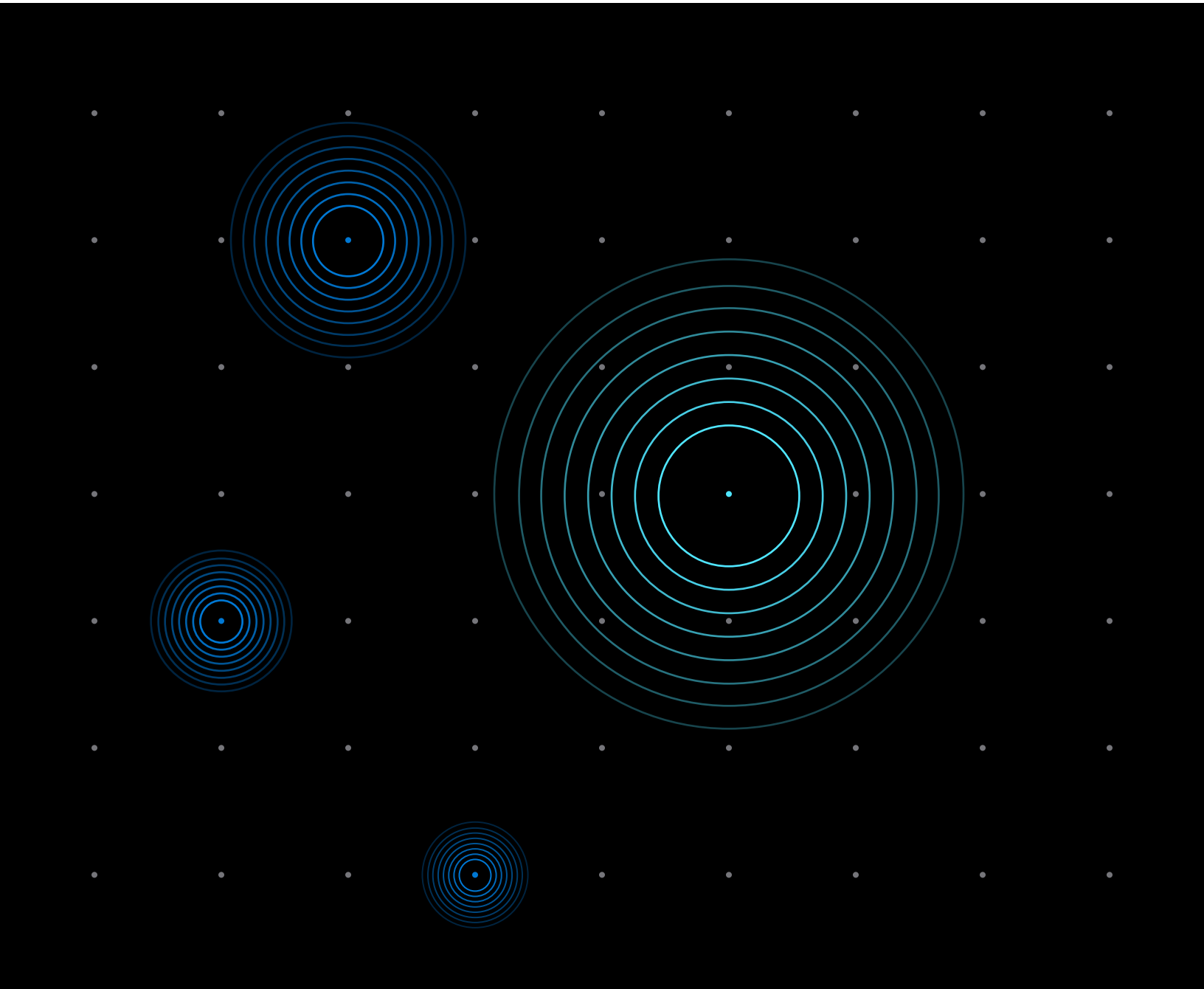
E-bokserie

Microsoft Azure

Azure Sentinel:
Tre användningsfall för hotidentifiering och undersökning



Azure Sentinel använder maskininlärning för att profilera användare, enheter och miljö, och upptäcka angrepp som inte kan fångas upp med hjälp av fördefinierade metoder. Det innebär att Tier 1-analytiker kan ägna mindre tid åt att gå igenom berg av data och mer tid åt att lyfta fram relevanta incidenter.

Ditt företag står inför en växande armé av alltmer sofistikerade säkerhetshot.

För att kunna upptäcka och försvara sig mot dem krävs intelligent analys, effektivt lagarbete och avancerade verktyg. Microsoft Azure Sentinel uppfyller de här behoven med en skalbar och molnbaserad SIEM-lösning som också gör det enklare att samordna och automatisera hanteringen av hot.

I Azure Sentinel samlas funktioner för problemdetektering, hotöverblick, proaktiv detektering och incidenthantering för hela företaget, så att du kan

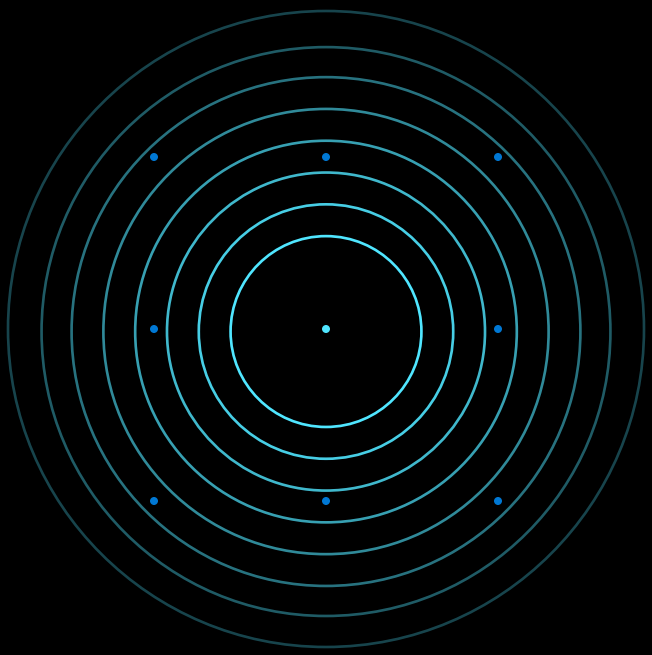
- **samla in data i molnskala** – för alla användare, enheter, appar och infrastrukturer, både lokalt och i flera molnmiljöer
- **identifiera tidigare upptäckta hot** och minimera felaktigt positiva identifieringar med hjälp av analys och oöverträffad hotinformation från Microsoft
- **undersöka hot med artificiell intelligent,** leta efter misstänkta aktiviteter i stor skala och dra nytta av flera års arbete med cybersäkerhet hos Microsoft
- **reagera snabbt på incidenter** med inbyggd samordning och automatisering av vanliga uppgifter.

I den här e-boken tar vi en närmare titt på tre vanliga scenarier för att ge säkerhetsanalytiker möjlighet att upptäcka och utreda hot. Vi går igenom en rad grundläggande funktioner, från avvikelsedetektering till automatisk aviseringsprioritering och utredning av hot.

Användningsfallen förutsätter att du redan har anslutit datakällorna till Azure Sentinel. Mer information om grundläggande installation och datainmatning finns i Snabbstartsguiden till Azure Sentinel.

01 /

Användningsfall nr 1: Avvikelsedetektering

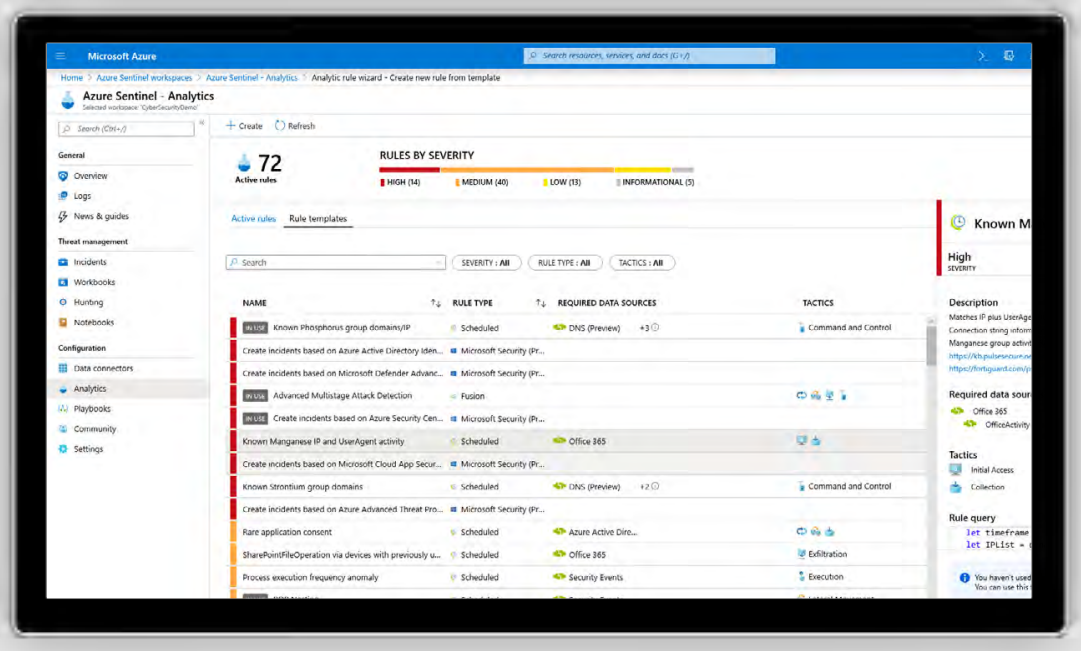


Azure Sentinel använder maskininlärning för att profilera användare, enheter och miljö, och upptäcka angrepp som inte kan fångas upp med hjälp av fördefinierade metoder.

Traditionella säkerhetsprogram använder fördefinierade regler för att upptäcka hot. Även om detta kan vara en effektiv metod när den tillämpas på kända hot, är det inte lika effektivt när nya typer av risker uppstår. Azure Sentinel använder maskininlärning för att profilera användare, enheter och miljö, och upptäcka angrepp som inte kan fångas upp med hjälp av fördefinierade metoder. Det innebär att Tier 1-analytiker kan ägna mindre tid åt att gå igenom berg av data och mer tid åt att lyfta fram relevanta incidenter.

Enkelt uttryckt tillhandahåller Azure Sentinel inbyggda och användningsklara mallar. Mallarna har utformats av Microsofts säkerhetsexperter och analytiker utifrån kända hot, vanliga angreppsvektorer och välkända mönster för misstänkta aktiviteter. Tack vare mallarna kan du använda avancerad analys utan att behöva skapa egna maskininlärningsmodeller eller vara datavetare.

Om du aktiverar mallarna varnas du automatiskt om avvikelser som kan tyda på ett angrepp. Du kan också anpassa dem för att söka efter eller filtrera olika typer av aktiviteter som är specifika för ditt företag.

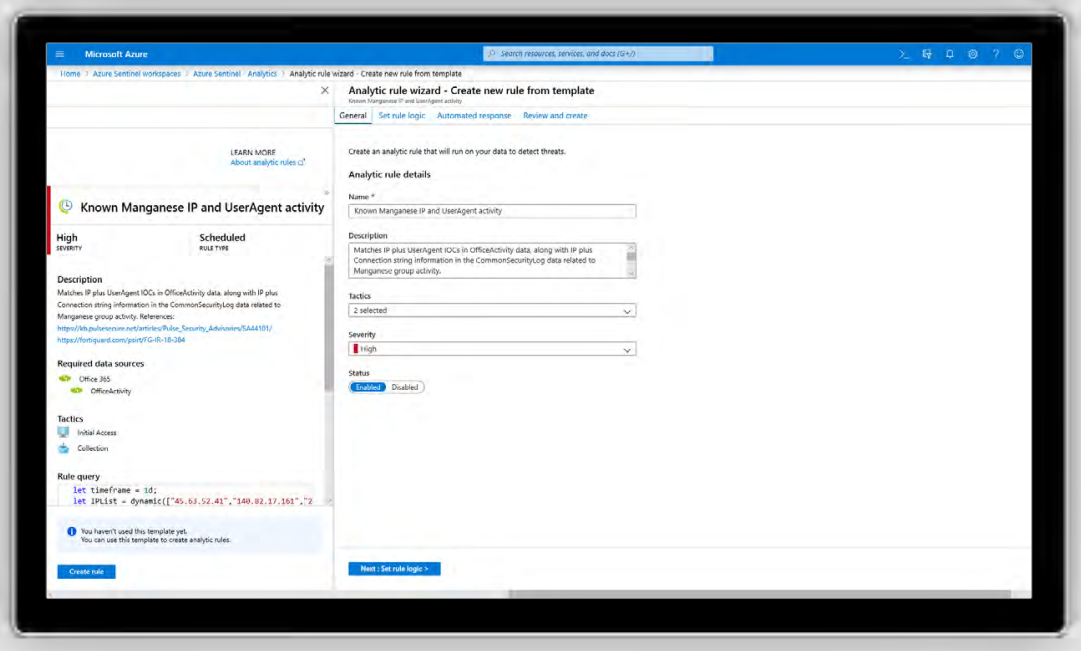


Analysalternativ i Azure Sentinel.

Visa alla användningsklara detekteringsmallar som är tillgängliga i Azure Sentinel genom att välja **Analytics** och sedan **Rule templates**. Den här fliken innehåller alla inbyggda regler i Azure Sentinel.

I Azure Sentinel ingår fyra typer av regler.

- **Microsoft-säkerhet:** Skapa automatiskt Azure Sentinel-incidenter av varningar som genereras i andra säkerhetslösningar från Microsoft i realtid.
- **Fusion:** Samordna många osäkra varningar och händelser från olika produkter till tillförlitliga och användbara incidenter. Vi ska diskutera Fusion närmare i nästa avsnitt.
- **Beteendeanalys med maskininlärning:** Upptäck hot baserat på avvikelser i användarbeteende.
- **Schemalagda:** Distribuera schemalagda frågor skrivna av Microsofts säkerhetsexperter.

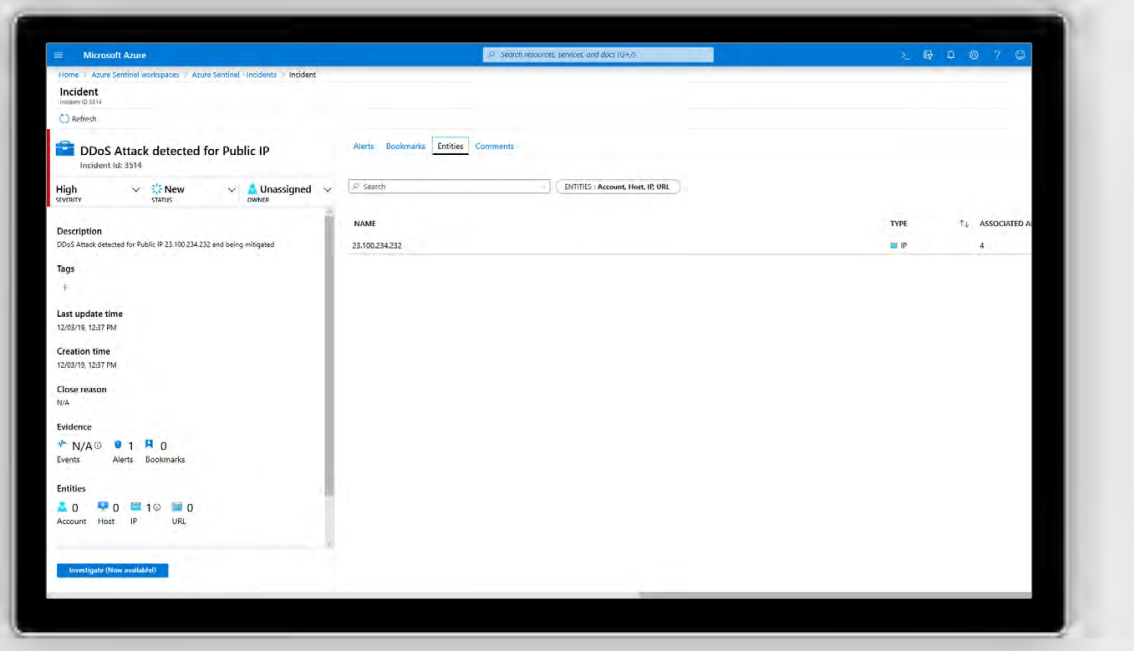


Regelguiden.

Om du vill använda en inbyggd mall klickar du på **Create rule**. (Observera att regelalternativen som visas beror på datakällorna.)

Då öppnas en regelguide baserat på den valda mallen. Alla uppgifter fylls i automatiskt. För **Scheduled rules** eller **Microsofts säkerhetsregler** kan du anpassa logiken så att den passar din organisation bättre, eller lägga till fler regler baserade på den inbyggda mallen. Den nya regeln visas på fliken **Active rules**.

I följande exempel visas ett mönster för avvikande inloggningsaktivitet. Azure Sentinel har tillämpat beteendeanalys baserat på maskininlärning för att identifiera avvikelsen.

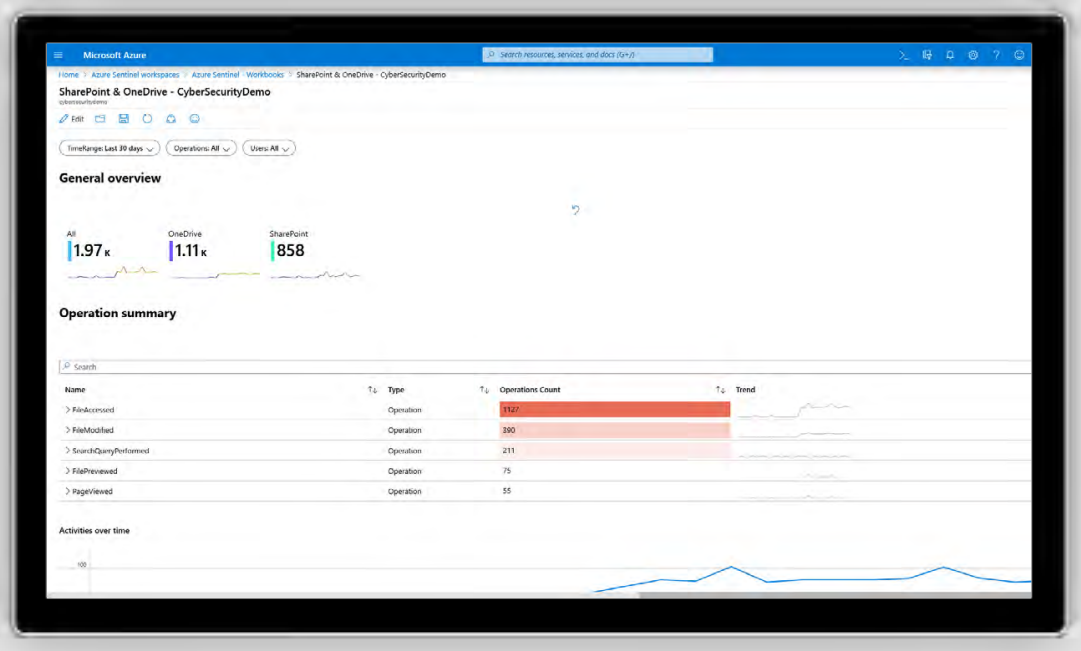


En incident i Azure Sentinel.

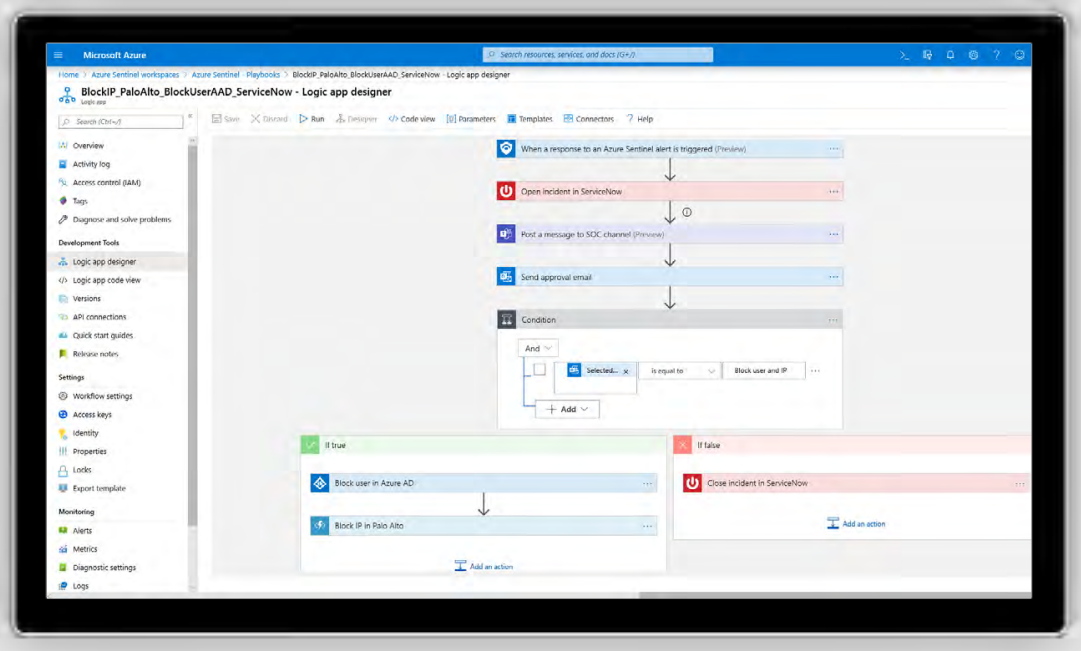
Du kan använda Azure Sentinel på flera sätt för att undersöka och reagera. Du kan till exempel utforska säkerhetsdata och upptäckta problem med hjälp av inbyggda arbetsböcker. De är samlingar av visualiseringar som hjälper dig att få ett fågelperspektiv över företagets säkerhetsläge.

Du kan också skapa spelböcker för att automatiskt reagera på hot.

Slutligen kan du använda utredningsverktyg för att utforska incidenter och lära dig vilken respons som är mest effektiv. Vi ska titta närmare på några av de här verktygen i avsnitt tre av guiden.



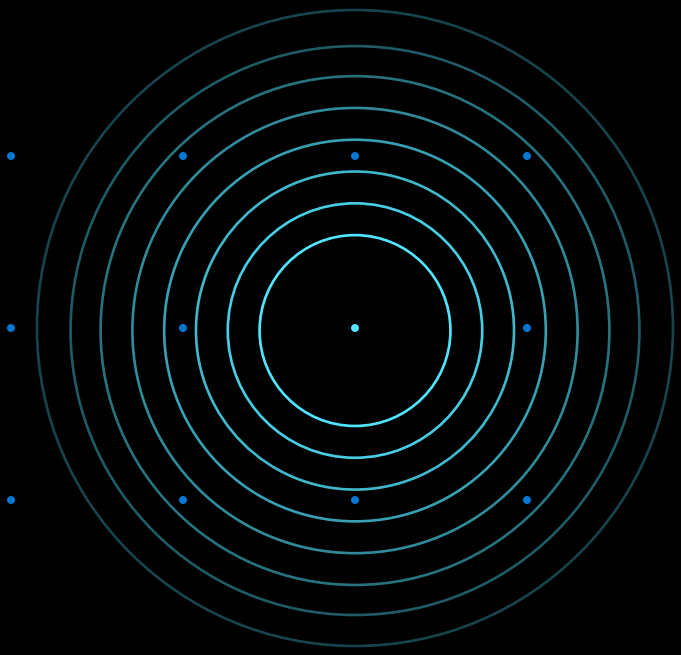
En Azure Sentinel-arbetsbok.



Spelbokslogik som används för att automatisera hanteringen av hot.

02 /

Användningsfall nr 2: Eskalera varningar till incidenter



Du kan använda varningar för att identifiera allvarliga problem som kräver intelligent samordning – en funktion som är inbyggd i Azure Sentinel.

När mängden data som flödar in och ut ur företaget växer och IT-systemen blir allt mer komplexa och sammanvävda kan det bli svårt för säkerhetsteamet att hantera alla varningar. Tyvärr har en betydande del av alla varningar som genereras i säkerhetslösningar inte särskilt stort värde var för sig. Du kan använda dem för att identifiera allvarliga problem som kräver intelligent samordning – en funktion som är inbyggd i Azure Sentinel.

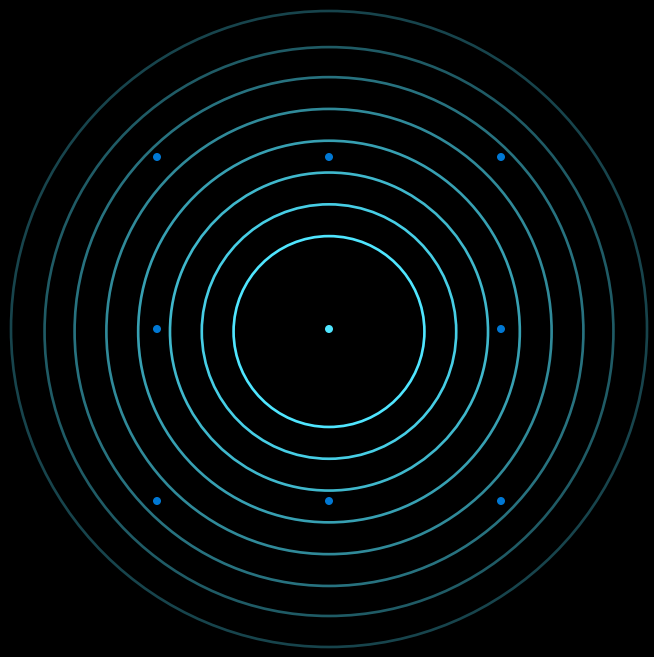
Den här funktionen kallas avancerad detektering av angrepp i flera steg och ställer minimala krav på kompetens för att sortera varningar. Avancerad maskininlärning används för att korrekt identifiera verkliga hot och minimerar antalet felaktigt positiva identifieringar med upp till 90 procent. Varje incident tilldelas en viss prioritet, så att säkerhetsteamet kan fokusera på den mest relevanta informationen.

Beroende på vilka datakällor du har anslutit kan du identifiera en mängd olika avvikelsescenarier. Till exempel om du använder Azure Active Directory Identity Protection och Microsoft Cloud App Security kan Azure Sentinel detektera att en användare försökt logga in från en plats som är omöjlig att hinna nå sedan den senaste inloggningen. Det går också att identifiera att platsen inte är typisk för användaren. Därefter samordnas informationen med avvikande Office 365-aktivitet, till exempel att användaren hämtar en stor mängd information från kontot.

Detta kan tyda på obehörig inloggningsaktivitet med hjälp av stulna autentiseringsuppgifter, följt av datastöld. Var för sig kan varningar som genereras av sådana aktiviteter försvinna bland stora mängder triviala varningar. Med Azure Sentinel samordnas de till en incident med stor inverkan som kan generera en automatisk respons och utlösa en utredning. Bäst av allt är att avancerad detektering av angrepp i flera steg som standard är aktiverad i Azure Sentinel. Du behöver inte göra något särskilt för att dra nytta av den här funktionen.

03 /

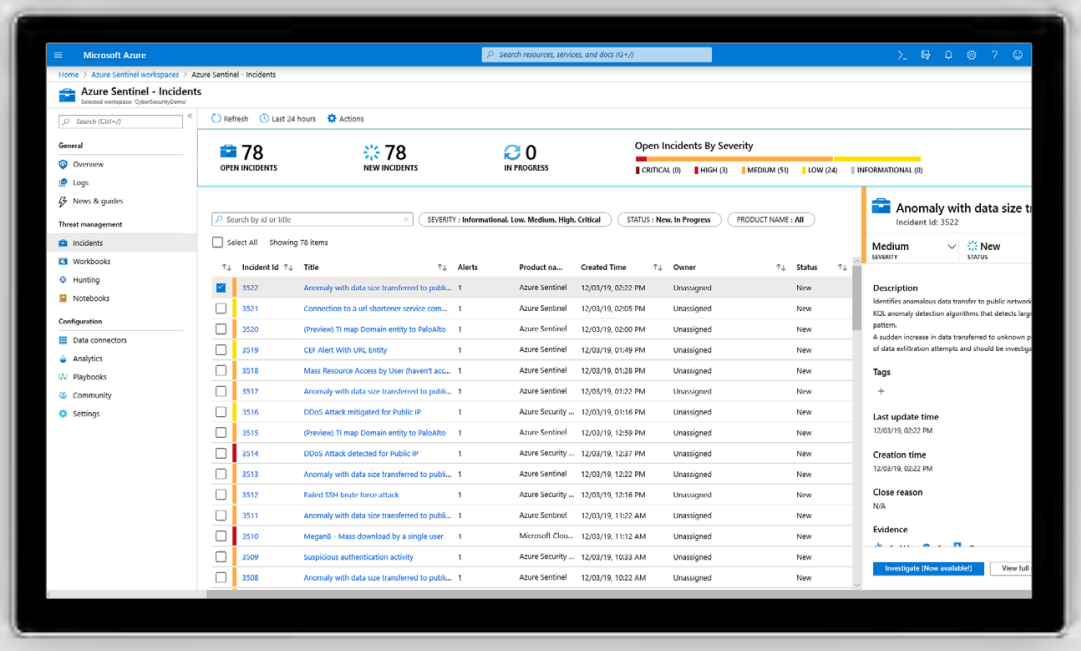
Användningsfall nr 3: Undersöka hot



Azure Sentinel förser säkerhetsteam med kraftfulla och intuitiva verktyg för att utreda hot snabbt och korrekt välja det mest effektiva svaret.

Genom att sätta dig in i grundorsaken till komplexa hot kan du vidta åtgärder för att minimera framtida risker.

De här verktygen är väldigt intuitiva och enkla att använda, vilket innebär att du kan låta fler i teamet hjälpa till med analyser, en uppgift som tidigare bara kunde utföras av specialutbildade experter. Verktygen är visuella och grafbaserade och ger användare möjlighet att utreda utan att behöva skriva komplexa frågor (även om en rik, frågebaserad sökning också är tillgänglig för faktiska Tier 3-analytiker). För det andra ger de en guidad upplevelse som gör det enklare att snabbt ringa in de viktigaste aspekterna av ett hot. Utredningsverktygen i Azure Sentinel har tagits fram av Microsofts forskare och bygger på metodtips från analytiker. De kan även användas för att söka efter oupptäckta hot.



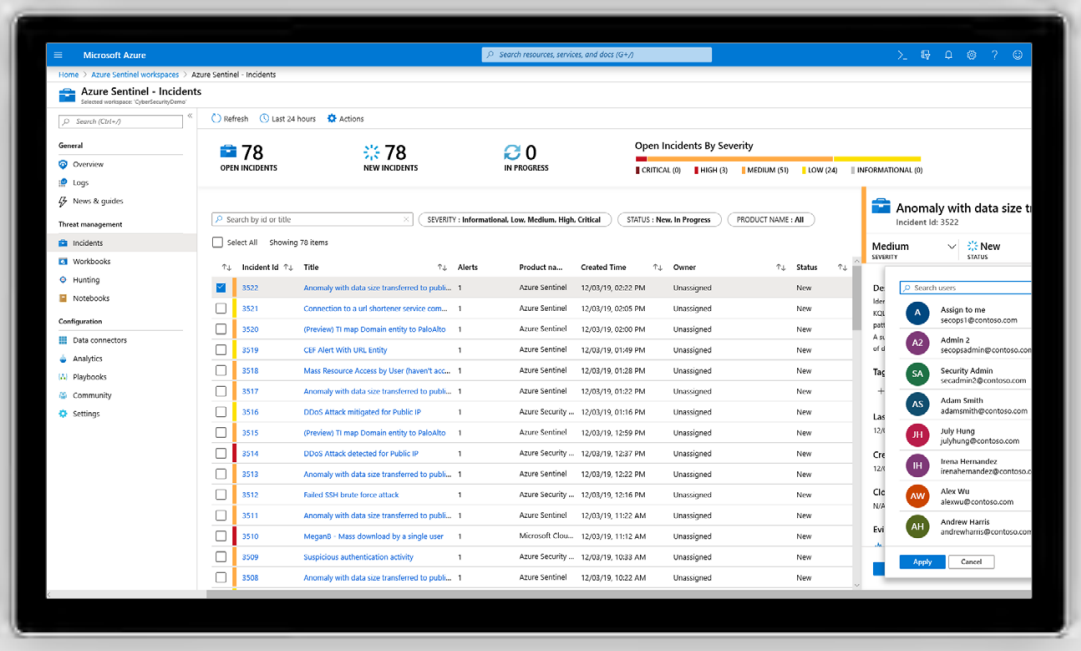
Sidan Incidents i Azure Sentinel.

Du utgår från sidan **Incidents**. Här ser du grundläggande information om varje incident, inklusive hur allvarlig den är, för att kunna bestämma vad som ska utredas först.

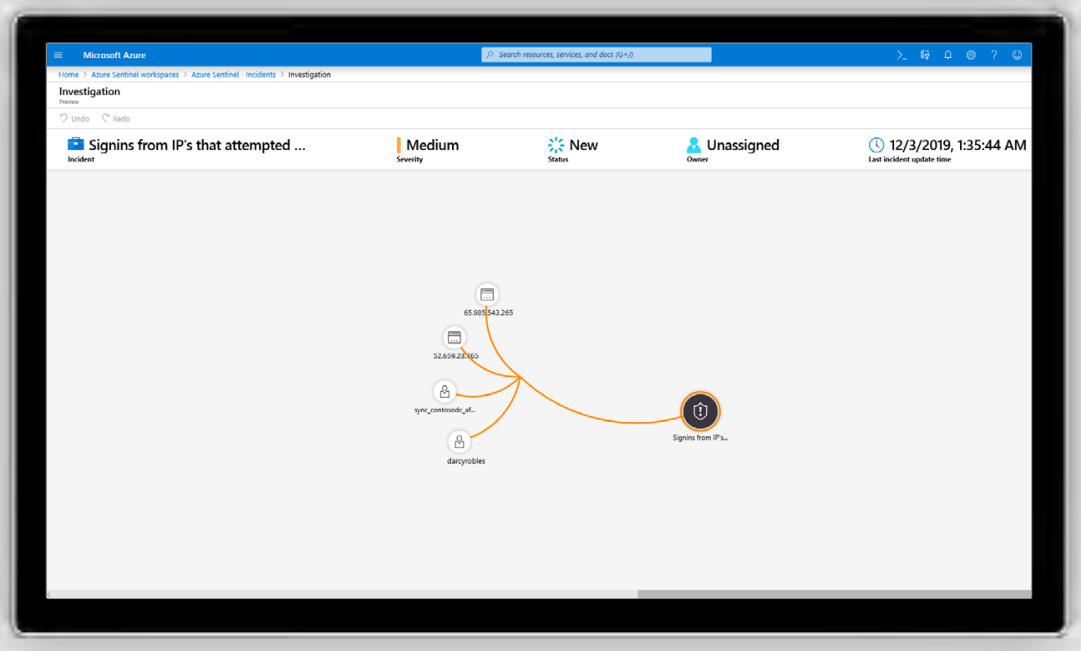
Välj bara en incident för att påbörja en utredning. Du kan visa mer information, de varningar som har genererats och sedan öka detaljnivån till underliggande händelser. Du kan också tilldela incidenter till en viss användare och lägga till kommentarer när utredningen fortskrider.

Om du vill fördjupa dig i en incident kan du använda utredningsgrafen för att

- **enkelt se samband mellan olika datakällor** med hjälp av en visuell graf som genereras automatiskt av rådata
- **utöka utredningens omfattning** med inbyggda undersökningsfrågor för att få grepp om intrångets omfattning
- **använda fördefinierade undersökningsalternativ** för att se till att du ställer rätt frågor inför ett hot.



Tilldela en incident i Azure Sentinel.

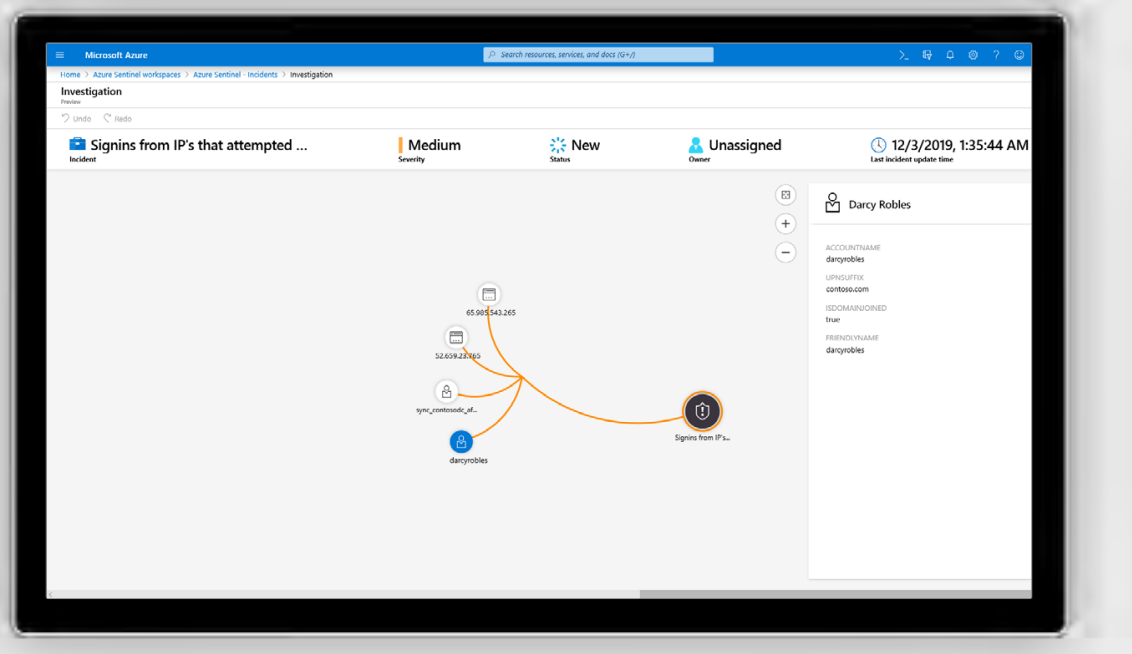


Utredningsgrafen i Azure Sentinel.

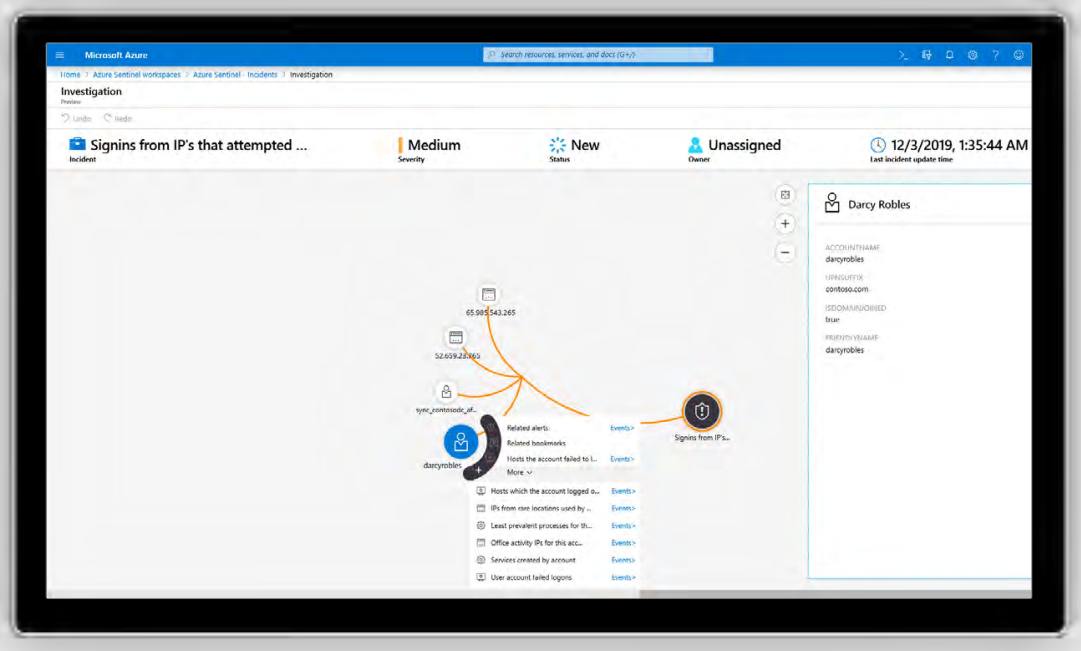
Om du vill använda utredningsgrafen väljer du en incident och trycker sedan på **Investigate**. Då öppnas utredningsgrafen.

Välj en entitet för att öppna fönstret **Entities**, där du kan granska information om entiteten.

Hovra över varje entitet för att visa en lista med **utredningsfrågor** formulerade av våra säkerhetsexperter för att fördjupa utredningen.



Utforska en entitet från fönstret Entities.



Föreslagna undersökningsfrågor.

Du kan också visa relaterade varningar, detaljstudera associerade händelser och frågor och utforska en tidslinje med händelser. Alla funktioner är enkla att använda genom att peka och klicka, men ger ändå kraftfulla insikter om vilken typ av hot du står inför. När en utredning är klar kan du snabbt reagera på hot med hjälp av spelböcker.

En säkerhetsspelbok är en samling procedurer som kan köras från Azure Sentinel som svar på en varning. Den hjälper till att automatisera och samordna din respons och kan köras manuellt eller ställas in för att köras automatiskt när vissa varningar utlöses. Läs mer om spelböcker.

De här verktygen är väldigt intuitiva och enkla att använda, vilket innebär att du kan låta fler i teamet hjälpa till med analyser, en uppgift som tidigare bara kunde utföras av specialutbildade experter. Verktygen är visuella och grafbaserade och ger användare möjlighet att utreda utan att skriva komplexa frågor.

Prova Azure Sentinel i dag.

Exemplen visar hur Azure Sentinel kombinerar möjligheten att automatiskt upptäcka relevant information med kraftfulla verktyg för att förstå, utreda och reagera på potentiella hot. Tillsammans hjälper funktionerna ditt team att fokusera på det väsentliga och använda sin kompetens där den behövs mest.

Azure Sentinel erbjuder även andra avancerade funktioner som vi inte tar upp i den här introduktionen. Forskare kan använda ett robust frågespråk för att utföra avancerad hotdetektering och spårning. Du kan skapa sofistikerade spelböcker för att automatisera hanteringen av komplexa hot baserat på resultat som genereras av Azure Sentinel. Du kan även samordna säkerhetsanalyser från alla källor i hela företaget. Ta reda på hur enkelt det är att komma igång.

Prata med en Azure-specialist om Azure Sentinel nu