Microsoft Defender Hotinformation | Microsoft Security

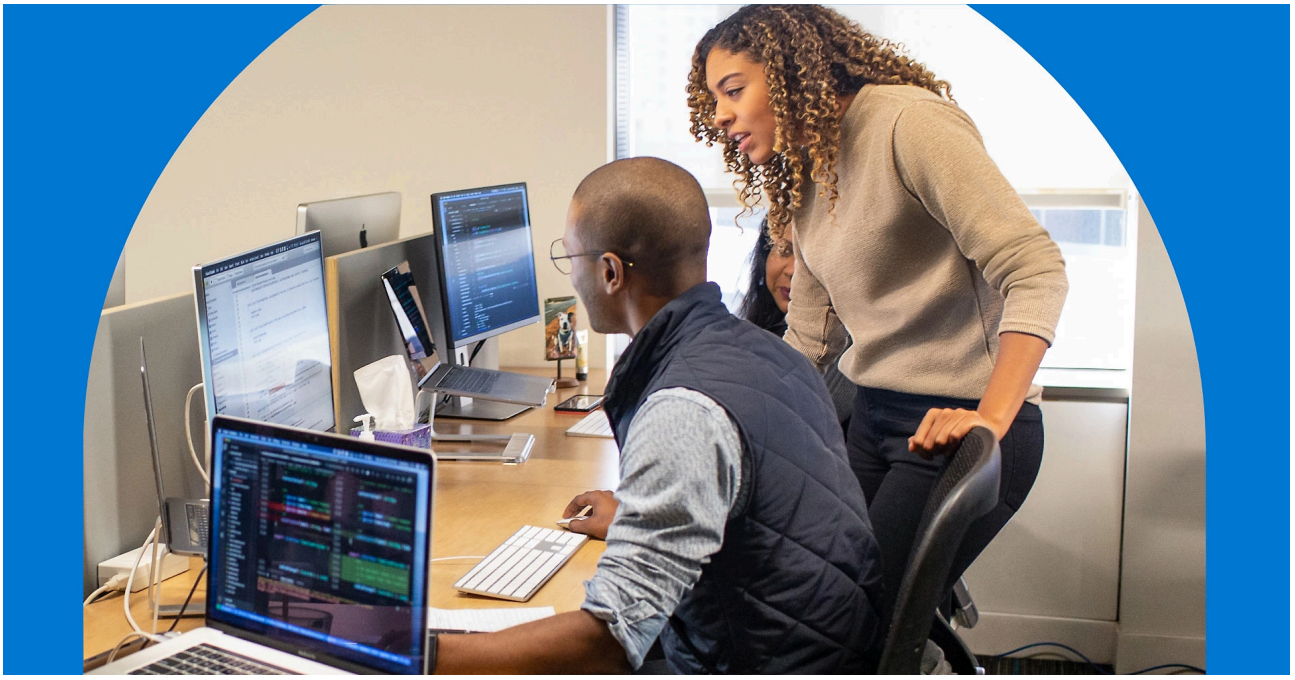
Archived: 2026-04-05 12:48:41 UTC

Stärk din nolltillit-status– ett nytt enhetligt förhållningssätt till säkerhet är här

Läs bloggen

Avslöja och neutralisera moderna angripare och cyberhot som utpressningstrojaner.

Kontakta Sales om du vill starta en kostnadsfri utvärderingsversion eller utforska licensalternativ.



Microsoft Defender Hotinformation

Avslöja dina angripare

Hjälp till att exponera och eliminera moderna cyberhot och deras infrastruktur med hjälp av dynamisk hotinformation.

Identifiera angripare och deras verktyg

Förstå dina angripare och deras onlineinfrastrukturer så att du kan identifiera dina potentiella cyberhotexponeringar med hjälp av en fullständig karta över internet.

Påskynda identifiering och åtgärd av cyberhot

Upptäck hela omfattningen av en cyberattack. Förstå en onlineangripares alla verktyg, förhindra åtkomst för alla deras datorer och kända enheter och blockera kontinuerligt IP-adresser eller domäner.

Förbättra dina säkerhetsverktyg och arbetsflöden

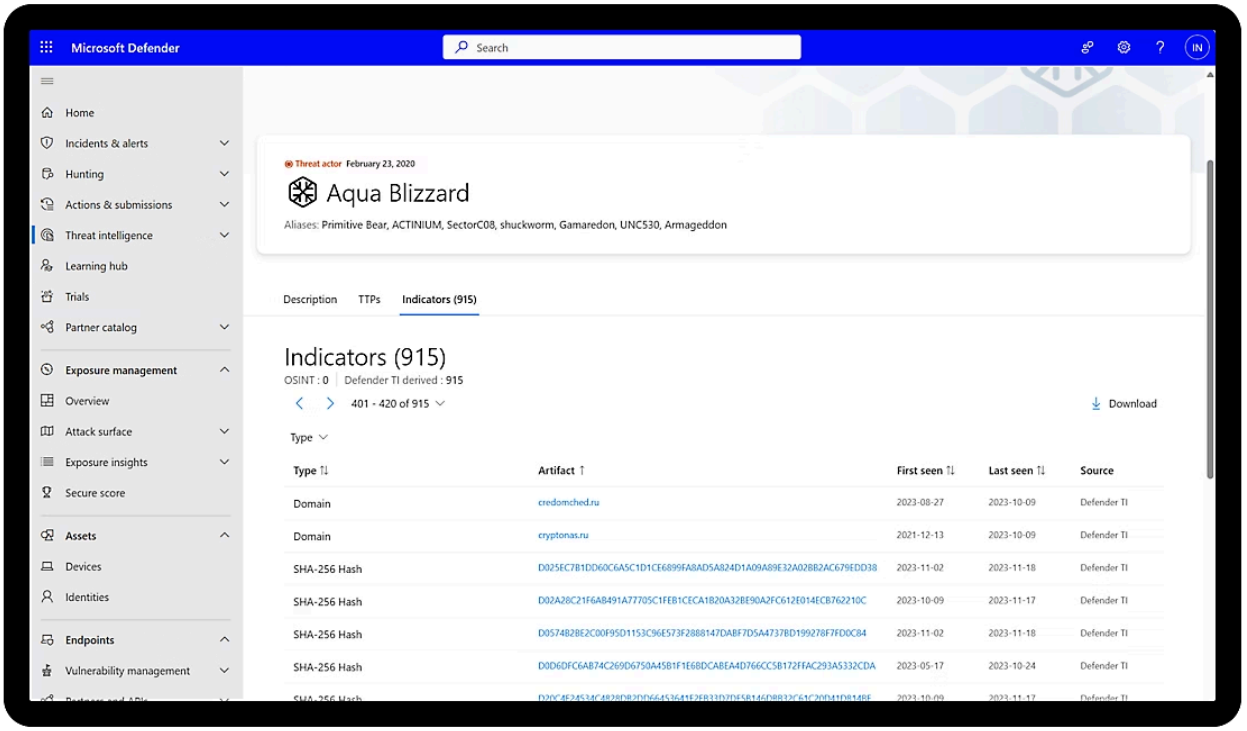
Utöka räckvidd och synlighet för dina befintliga säkerhetsinvesteringar. Få större sammanhang och förståelse för cyberhot med Microsoft Defender XDR, Microsoft Sentinel och Microsoft Security Copilot.

Microsoft Defender Hotinformation

Lär om hur Defender Hotinformation gör det möjligt för säkerhetsexperter att få direkt tillgång till och agera på vår kraftfulla databas med hotinformation som bygger på 78 biljoner signaler och mer än 10 000 multidisciplinära experter över hela världen.

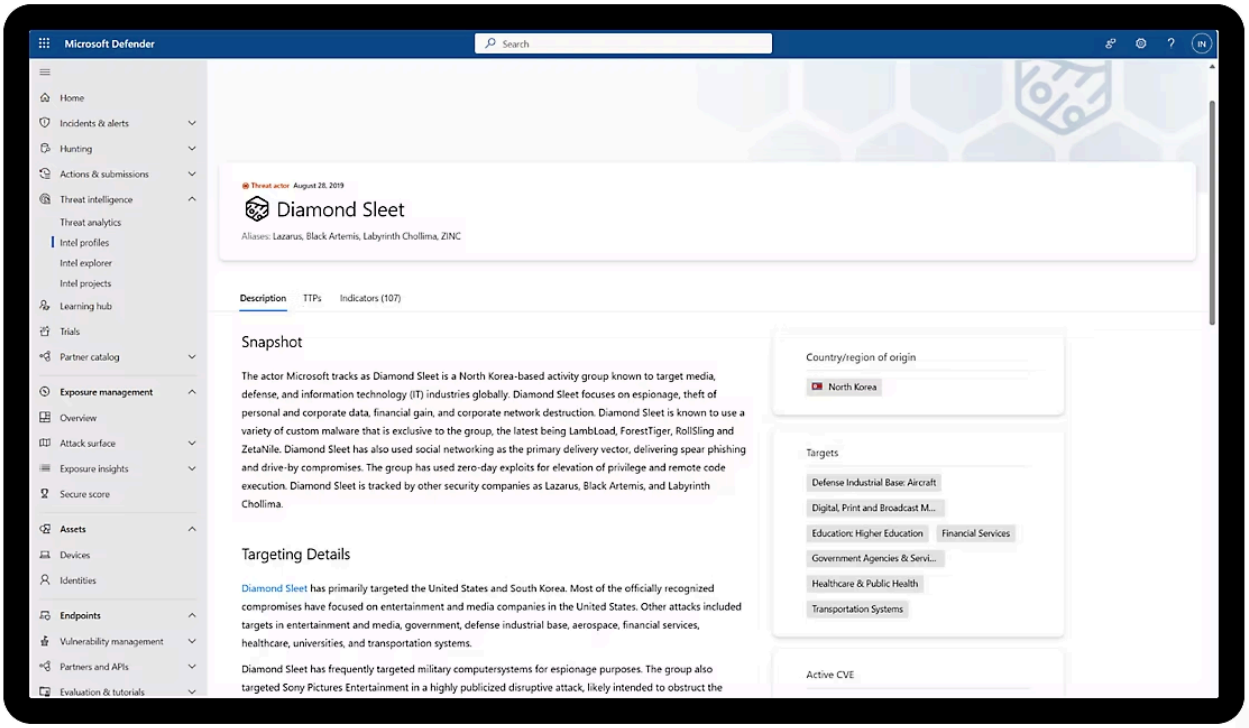
Funktioner

Upptäck och eliminera cyberhot med Defender Hotinformation.



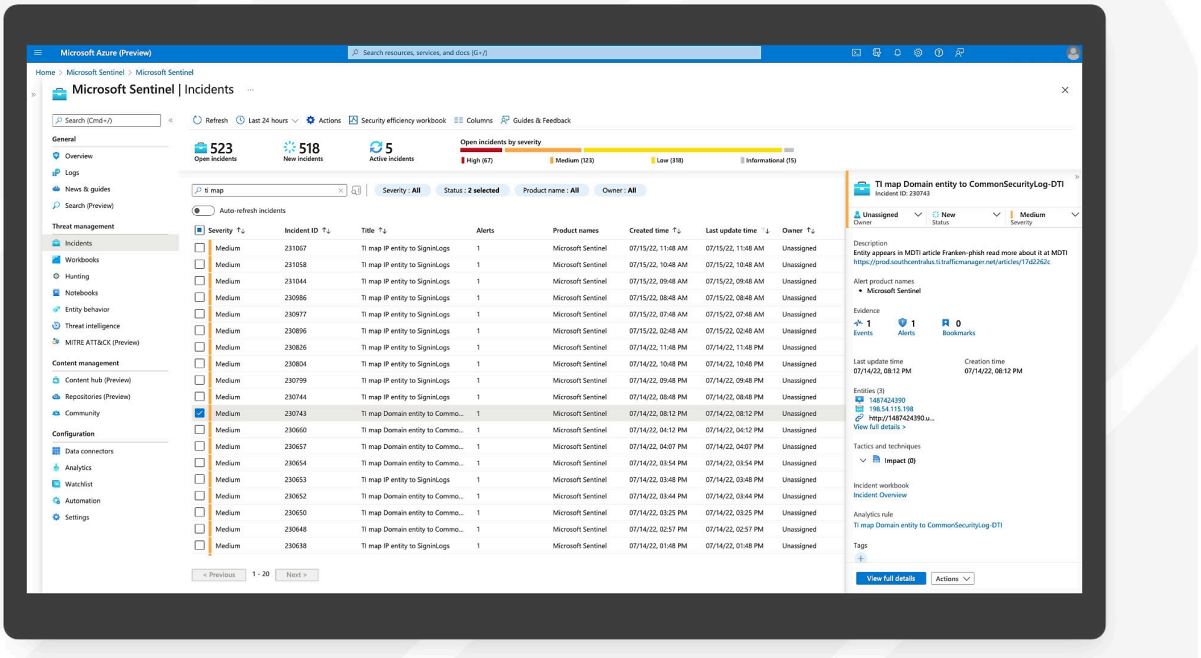
Få kontinuerlig hotinformation

Få en fullständig visning av internet och spåra dagliga förändringar. Skapa hotinformation för ditt eget företag för att förstå och minska exponeringen.



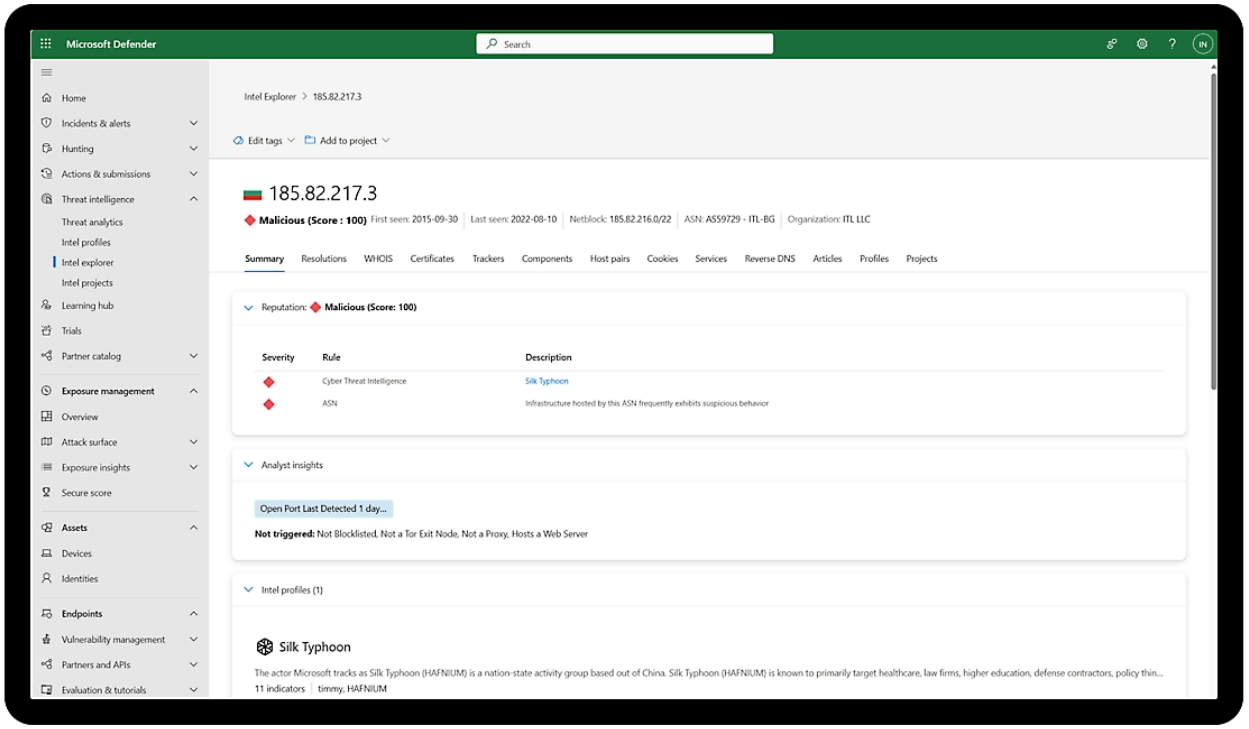
Exponera angripare och deras metoder

Förstå gruppen bakom en onlineattack, deras metoder och hur de vanligen arbetar.



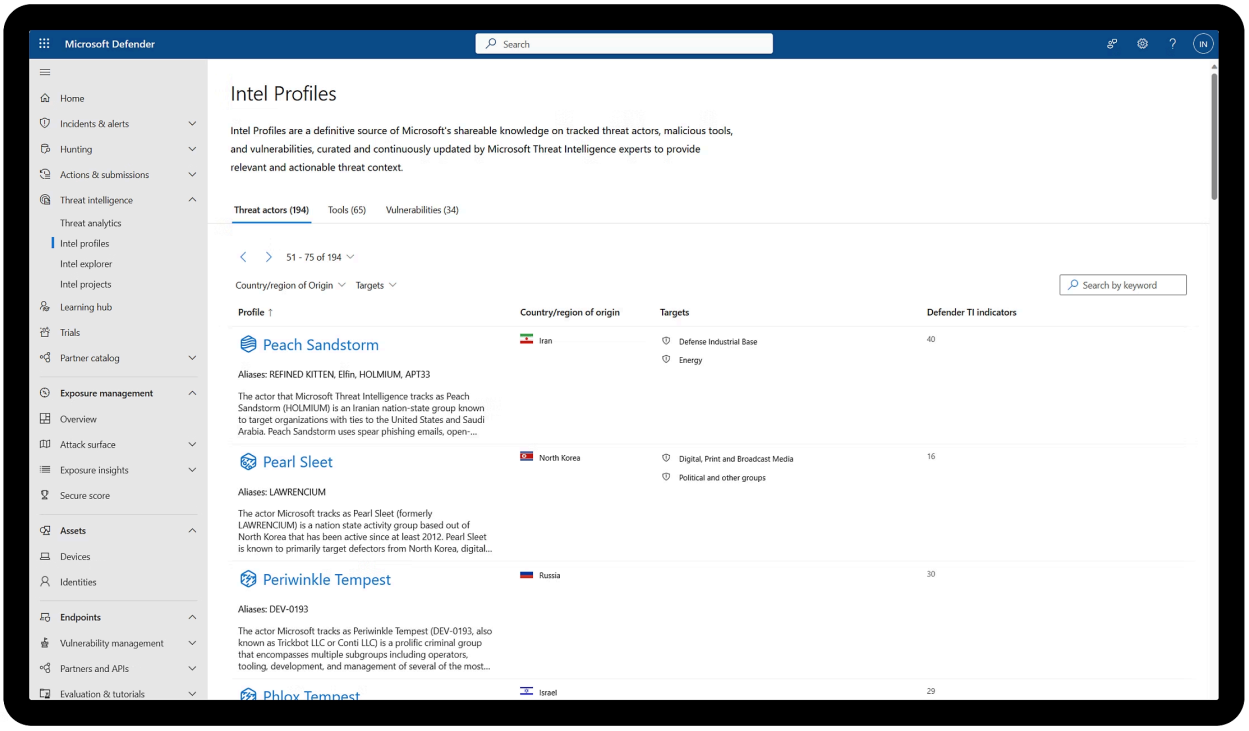
Förbättra varningsundersökningar

Få ännu bättre incidentdata i Microsoft Sentinel och Defender XDR med färdig och obearbetad hotinformation för att förstå och avslöja den fulla omfattningen av ett cyberhot eller en cyberattack.



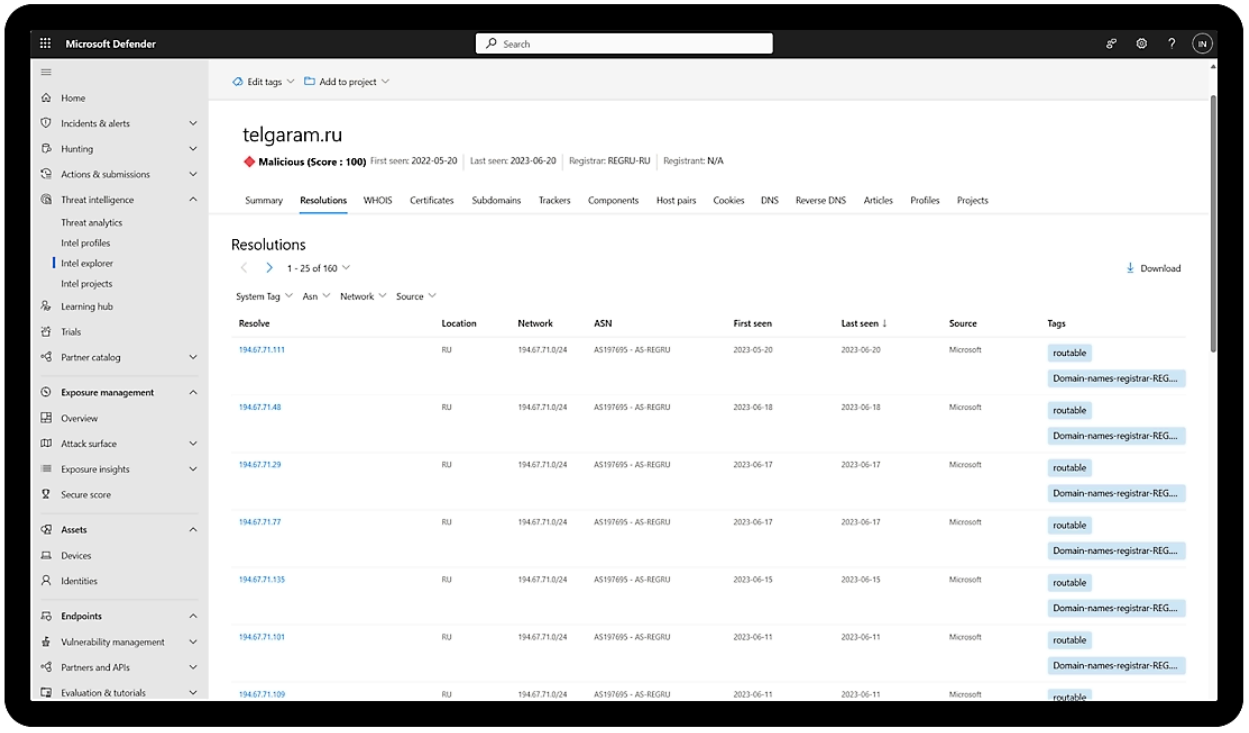
Påskynda incidentsvar

Undersök och ta bort skadlig infrastruktur, till exempel domäner och IP-adresser, och alla kända verktyg och resurser som hanteras av en cyberangripare eller cyberhotfamilj.



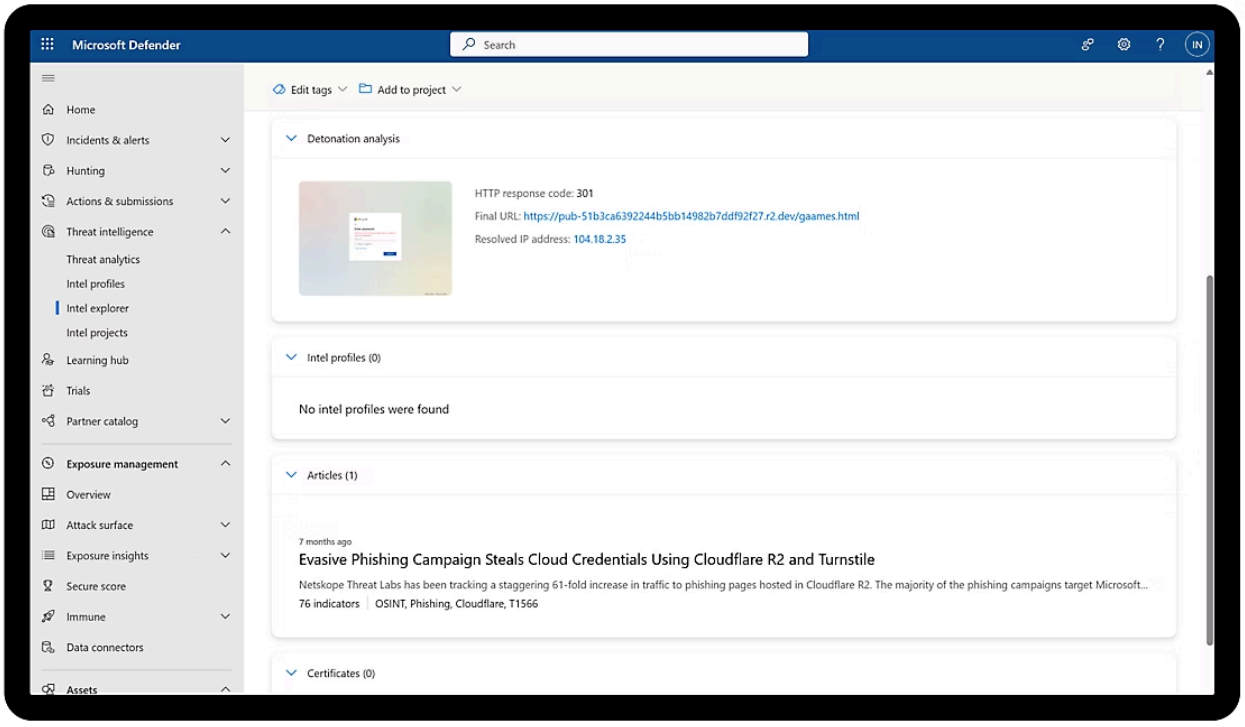
Jaga cyberhot som ett team

Samarbeta enkelt med undersökningar över team med arbetsytan i Defender Hotinformation och dela kunskap om cyberhotaktörer, verktyg och infrastruktur med projekt och intelligensprofiler.



Expandera skydd och förbättra säkerhetsstatusen

Upptäck automatiskt skadliga enheter och stoppa cyberhot utifrån genom att blockera interna resurser från att få åtkomst till farliga internetresurser.



Fil och URL-intelligens (detonation)

Skicka in en fil eller URL för att omedelbart få reda på dess rykte. Utöka säkerhetsincidenter med kontextbaserad hotad intelligens.

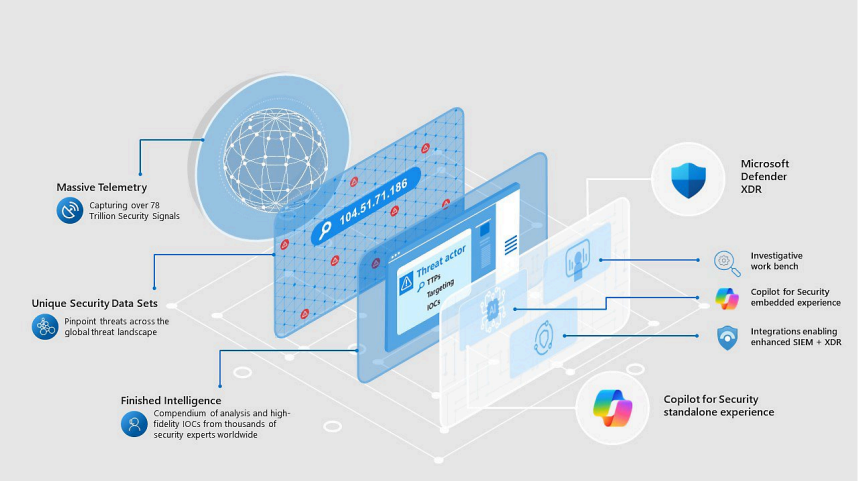
Tillbaka till flikar

Microsoft Security Copilot är nu allmänt tillgängligt

Använd frågor formulerade med naturligt språk när du ska undersöka incidenter med Copilot – nu integrerat i hela Microsoft Security-produktsviten.

Så här använder du Microsoft Defender Hotinformation

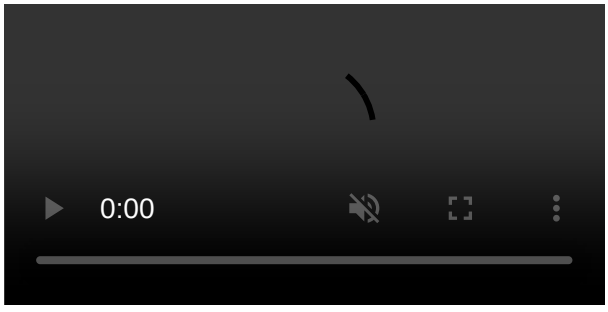
Microsoft spårar fler än 78 biljoner signaler dagligen. Det hjälper säkerhetsteam att identifiera sårbarheter med större effektivitet och att ligga steget före dagens cyberhot.



Enhetlig plattform för säkerhetsåtgärder

Försvara din digitala egendom med den enda säkerhetsplattformen(SecOps) som erbjuder fullständiga funktioner för utökad identifiering och åtgärder (XDR) och säkerhetsinformation och händelsehantering (SIEM).

Animering av startsidan för Microsoft Defender-instrumentpanelen



Enhetlig portal

Upptäck och avbryt cyberhot i nära realtid och effektivisera undersökning och åtgärder.

Tillbaka till flikar

Utforska Defender Hotinformation-licenser

Standardversionen av Defender Hotinformation

Använd den kostnadsfria versionen av Defender Hotinformation för att hantera globala cyberhot.

Den kostnadsfria versionen innehåller:

- Offentliga indikatorer för kompromisser (IOCs)
- Intelligens med öppen källkod (OSINT)
- Databas för standardiserade namn på sårbarheter och exponeringar (CVE)
- Artiklar och analyser från Microsoft Threat Intelligence (*begränsad*[1])
- Defender Hotinformation-datamängder (*begränsad*[2])
- Informationsprofiler (*begränsad*[3])

Premium -version av Defender Threat Intelligence

Få fullständig åtkomst till den operativa, strategiska och taktiska intelligensen i Defender Threat Intelligence-innehållsbiblioteket och undersökande workbench.

Premium-versionen innehåller:

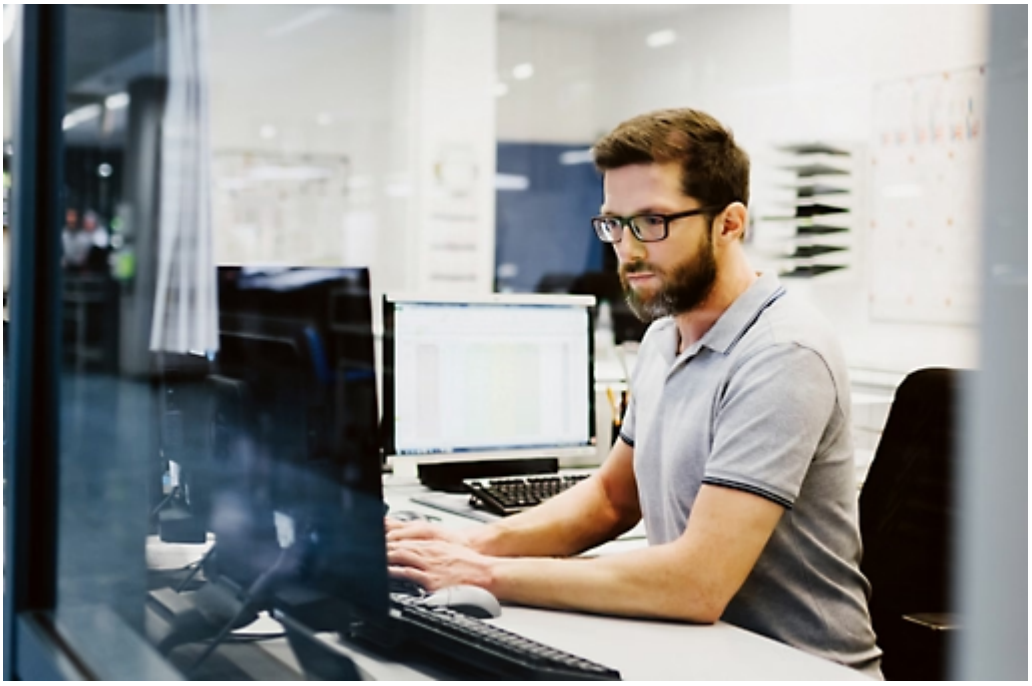
- Offentliga indikatorer för kompromisser (IOCs)
- Intelligens med öppen källkod (OSINT)
- Databas för vanliga säkerhetsrisker och exponeringar (CVE)
- Artiklar och analyser från Microsoft Threat Intelligence
- Defender Threat Intelligence-datamängder
-
-
-
- Webbadress och filinformation

Relaterade produkter

Använd förstklassiga säkerhetsprodukter från Microsoft för att förhindra och upptäcka cyberattacker på din organisation.

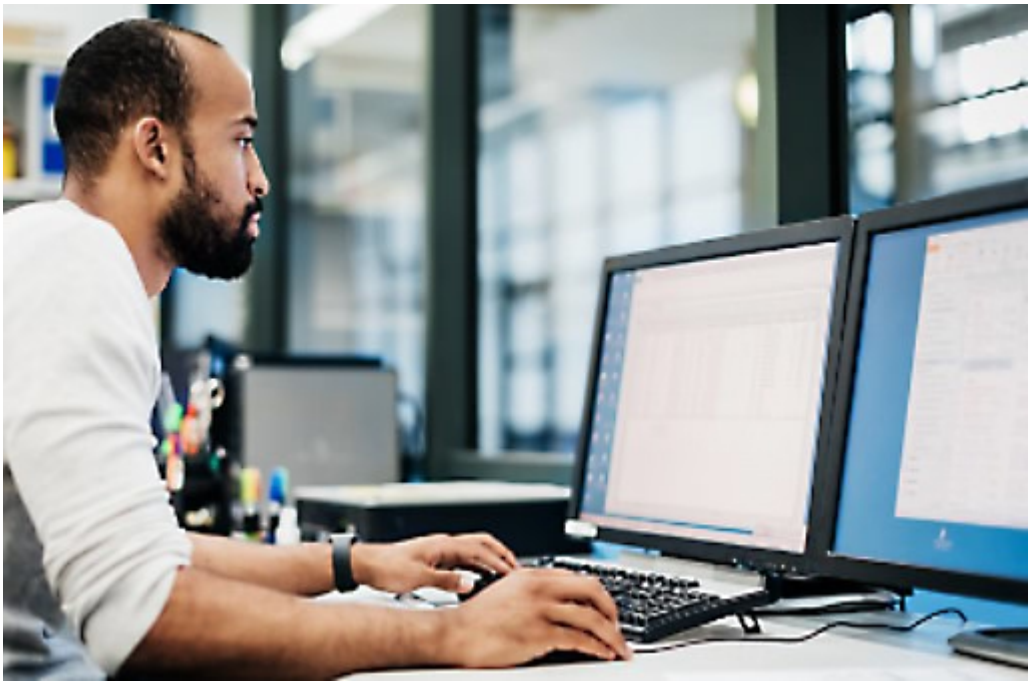
Microsoft Sentinel

Se och stoppa cyberhot i hela företaget med intelligent säkerhetsanalys.



Microsoft Defender för molnet

Öka skyddet i din miljö med flera moln och hybridmoln.



Microsoft Defender – hantering av extern attackyta

Förstå din säkerhetsposition bortom brandväggen.

Fler resurser

Läs hotinformationsbloggen

Läs mer om nya erbjudanden för hotinformation från Microsoft.

Skydda ditt företag med hotinformation

Lär dig hur du använder hotinformation på Internet för att skydda din organisation mot cyberattacker.

Regelverk och implementering

Kom igång med hotinformationslösningar för din organisation idag.

Besök Microsoft Defender Hotinformation-bloggen

Lär dig av Defender Hotinformation-experter, se vad som är nytt och låt oss höra från dig.

Skydda allt

Gör din framtid säkrare. Utforska dina säkerhetsalternativ i dag.

Source: https://www.riskiq.com/blog/external-threat-management/sysrv-hello-cryptojacking-botnet/