Microsoft Security

Microsoft Defender Threat Intelligence

Unmask your adversaries, their infrastructure, and their tooling

Digital transformation has enabled incredible efficiencies, but it has also led to a dramatic increase in hidden security risks—like ransomware—that are more difficult to detect than ever before, causing costly breaches, business disruption, and loss of critical data.

Pinpointing these threats requires you to know how they operate—in other words, you need threat intelligence.

Breaches have increased more this year **than in the past five years combined**.

What is threat intelligence?

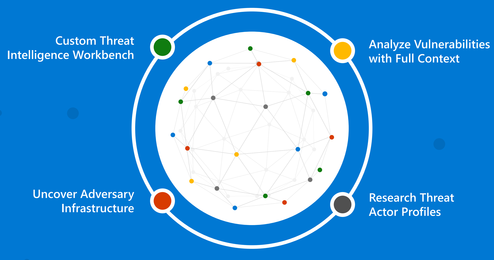
Threat intelligence is the contextual knowledge about threat actors and their motivations, capabilities, techniques, and infrastructure—and it's key to detecting and addressing threats with minimal false positives.

Microsoft derives leading threat intelligence from more than 24 trillion signals collected daily paired with the expertise of leading security experts, and this threat intelligence paired with AI is core to the detections built into Microsoft's SIEM and XDR products, including Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud.

But threat actors are constantly evolving, largely thanks to the internet. If you have an online presence, you are connected to every other entity, including adversaries. In a landscape that changes this fast, access to raw threat intelligence enables you to dive even deeper, uncovering the full extent of a threat actor's infrastructure.

Microsoft Defender Threat Intelligence

Protect your organization from modern adversaries with a 360-degree view of your threat exposure.



Microsoft Defender Threat Intelligence maps how the internet changes day by day to give you a constantly-up-to-date view of everything your organization has interacted with.

For example, let's say a single IP address is flagged by Microsoft Sentinel. You block that IP address.

But one IP address is just one small part of a threat actor's infrastructure. What other IP addresses is that bad actor associated with?

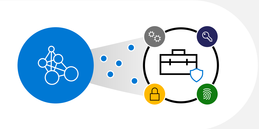
With Microsoft Defender Threat Intelligence, you can identify the bad actor associated with this IP and the rest of their infrastructure, allowing you to preemptively mitigate potential attacks by blocking all of their tools and methods.

Accelerate investigation and remediation with deeper context.

Take your investigations deeper and ensure that you're addressing the full extent of a threat. Microsoft Defender Threat Intelligence offers visibility into the changing threat landscape, so you can see and mitigate everywhere your organization has touched adversary infrastructure—even infrastructure yet to be captured in public TI.

Unlock visibility into your adversaries and their infrastructure.

Threats are evolving every single day, and so is their infrastructure. Microsoft Defender Threat Intelligence uses direct observations and dynamic threat intelligence to unmask threat actors and their tools—allowing you to track how adversaries evolve.



Enhance your security stack with custom-built threat intelligence.

Microsoft Defender Threat Intelligence's analyst workbench is simple and makes it easy for analysts to leverage and customize real world threat intelligence for investigations, mitigation, and more. Use this threat intelligence with your security stack to enhance detections, assist in investigation, and accelerate time to resolution.

Ready to learn more?

Get more information about how you can get started with Microsoft Defender Threat Intelligence at aka.ms/mdti.

Learn more