threater

Seeing the Big Picture:

How Threater Harnesses Cyber Intelligence

What is the cyber intelligence community?

The “cyber intelligence community” refers to the network of government agencies, open source organizations, and private companies dedicated to gathering, analyzing, and disseminating information about cyber threats, vulnerabilities, and activities.

What kind of information can we learn?

Cyber intelligence can generally be split into two categories: the **“what”** of the attacks themselves and the data of **“who”** is deploying them.

Cyber Intelligence Data Type 1: The “What”

This intelligence refers to the actual applications and attacks threat actors deploy.

WHAT IT TELLS US

- Information about the applications and resources threat actors are using to enter and compromise networks
- What the malicious code does once it’s deployed
- How the code can hide itself from current detection systems

LIMITATIONS

Threat actors can adapt and change these attacks almost instantaneously once discovered, bypassing detections and staying one step ahead.

Cyber Intelligence Data Type 2: The "Who"

This intelligence refers to the people behind the attacks—**the threat actors themselves.** These are often large cybercriminal conglomerates conducting mass attacks that can cause millions of dollars of damage to organizations.

WHAT IT TELLS US

- Where these attacks are coming from and where exfiltrated data is sent
- IP addresses of known threat actors

HOW IT'S USED

This data can be leveraged "left of boom" to filter out known threat actors but most technologies cannot process enough cyber intelligence from the community as a whole to effectively enforce against known threat actors.

Threater harnesses this intelligence with proprietary filtering algorithms to enforce and eliminate communication to and from known threat actors.

Technology	Cyber Intelligence Limitation	Threater's Solution
Firewall	Relies mostly on proprietary view of threat landscape and is vastly limited in the amount of external threat intelligence it can enforce on	Can source and enforce on near-unlimited cyber intelligence data by focusing on the threat actor/IP address through a patented Bloom Filter
EDR/MDR/XDR	Can only enforce once the threat/threat actor is in the network and is reactionary by design	Sits "left of boom" as a foundational layer of proactive enforcement on network traffic
SIEM	Reactive in nature, requires vast resources to manage and maintain because it is evaluating traffic from known threat actors, and can't enforce	Runs and updates autonomously in real time in a proactive position in the security stack, eliminating traffic to and from known threat actors
TIP	Sources vast amounts of cyber intelligence but cannot enforce on its own	Can both source *and* enforce upon large amounts of cyber intelligence data