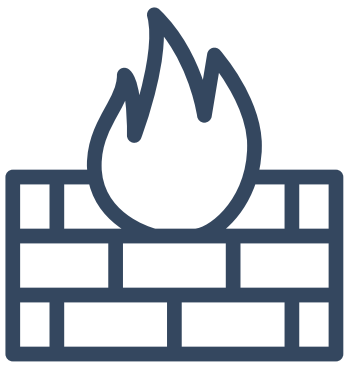
THREAT BLOCKR®

4 SECURITY TOOLS' CYBER INTELLIGENCE LIMITATIONS

(And how to solve for them!)

1 | FIREWALL



- Limited in how much **external threat intelligence** it can ingest
- **Bogged down** by decrypting traffic and performing deep packet inspections
- Difficult to configure and maintain **outbound traffic** monitoring and enforcement

THREAT BLOCKR®

2

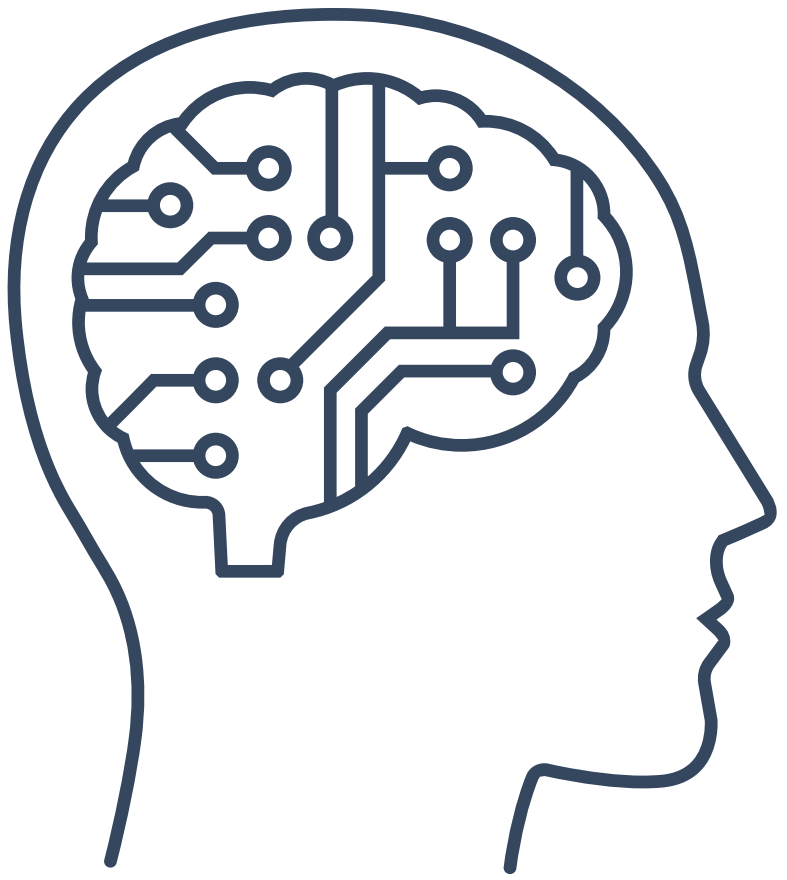
SIEM

Utilizes **massive amounts of bandwidth** to run and produce alerts

Requires specialized employees to manage/triage tons of alerts

Reactive in nature and **focused on threats instead of threat actors**

THREAT BLOCKR®



3

TIP

(THREAT INTELLIGENCE PLATFORM)

- Still reliant on one **vendor's curated view** of the threat landscape
- Can be utilized by other tools and technologies but **cannot enforce** on its own

THREAT BLOCKR®

4

EDR/MDR/XDR

- Produce large amounts of **redundant alerts** for staff to sort through
- **Uses massive amounts of bandwidth** to secure endpoints
- Effectiveness **dependent security staff** and talent to manage and maintain

THREAT BLOCKR®

SO...HOW DOES THREATBLOCKR FILL THESE CYBER INTELLIGENCE GAPS?

THREAT BLOCKR®

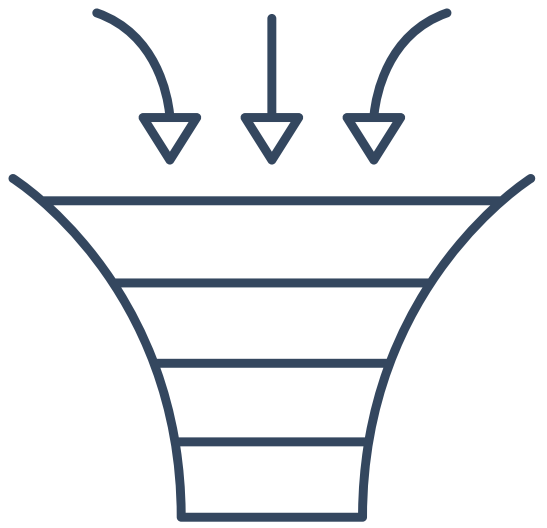
1 FOCUS ON THREAT ACTOR

(INSTEAD OF JUST THE THREATS)

- Utilize the cyber intelligence community to focus on **where threat actors are** (IP addresses)
- **Block the traffic** going to and from known threat actors
- Threats change all the time, but threat actor cyber intelligence is **much more stable**

THREAT BLOCKR®

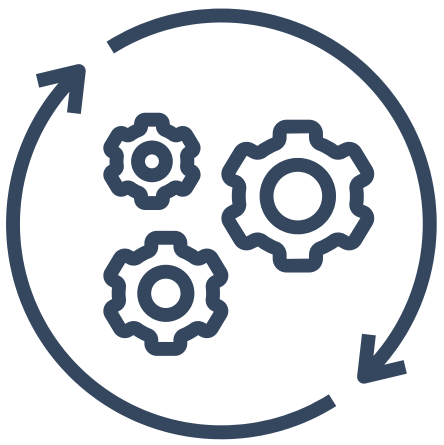
2



LEVERAGE AS MUCH CYBER INTELLIGENCE AS POSSIBLE

- Source from **public, private, and open source** feeds and lists
- Enforce on all traffic – **both inbound and outbound** – based on full intelligence community
- Utilize the cyber intelligence community's **full view of the threat landscape**

THREAT BLOCKR®



3

ENFORCE AUTONOMOUSLY AT LINE SPEED

- Remove traffic going to and from known threat actors **at the network level**
- Patented use of a Bloom filter allows for enforcement **without impacting network performance**
- **Run and update automatically**, freeing up staff to focus on unknown threats

THREAT BLOCKR®

MORAL OF THE STORY? WHEN IT COMES TO CYBER INTELLIGENCE... MORE IS MORE.

THREAT BLOCKR®