MAXIMIZE YOUR INTELLIGENCE DATA

The Value of Using Diverse Threat Feeds

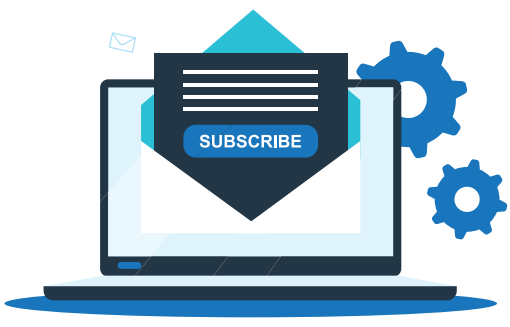
287
days

It takes an average of 287 days to identify and contain a data breach.[1]

Security teams can utilize threat intelligence to accelerate their detection process to find and contain a breach faster.

Organizations that are more successful in containing cyber attacks are 58% more likely to subscribe to threat intelligence feeds than their less successful peers.[2]

58%
more likely
to subscribe



Threat intelligence comes through feeds that provide various levels of information regarding adversaries and their capabilities and infrastructure.

What Are They?

Commercial Feeds

Commercial feeds are information aggregated by vendors from professional research and customer telemetry information.

Advantages	Disadvantages
• Enables triage • Expands threat visibility	• Uneven coverage • Difficult to measure

OSINT Feeds

Open Source Intelligence (OSINT) feeds are made up of threat data collected and shared among cybersecurity professionals that anyone can access for free.

Advantages	Disadvantages
• Cost savings • Great breadth	• Blindspots • Lacking context

Threat Intelligence Feeds

ISAC Feeds

Information Sharing and Analysis Center (ISAC) feeds are curated by industry-specific organizations. These organizations share information on cyber threats and facilitate data sharing between the public and private sectors.

Advantages	Disadvantages
• High ROI • Relevant coverage	• Many dependencies • Possibly vendor-specific

Download our eBook:
Using Diverse Threat Intel Feeds to Maximize Your Intelligence Data
to learn more and choose what's right for you.

Download the eBook

Sources:
1. 2021 Cost of a Data Breach report from Ponemon
2. Nemertes 2019-2020 Cloud and Cybersecurity Research Study

ANOMALI