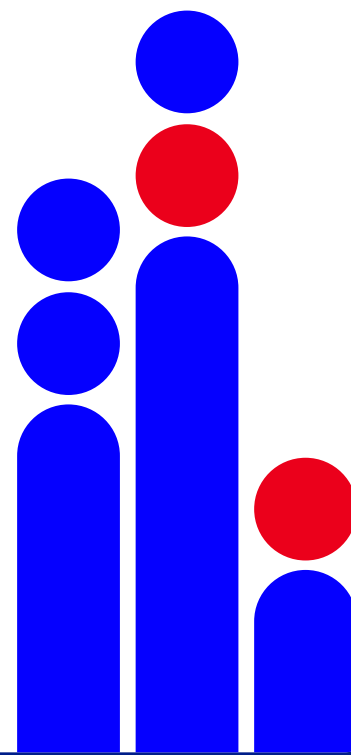


Key Findings

The 2025 State of Threat Intelligence

In 2025 businesses faced nonstop disruption from cybercrime, state-sponsored threats, and geopolitical concerns. Executives agree that now more than ever, threat intelligence is an essential component of enterprise data security.



Usage & Adoption

Executives have become reliant on threat intelligence for maintaining enterprise cybersecurity in 2025. Across the board, threat intelligence is being taken more seriously as risks grow.

83%

of enterprises have a full-time threat intelligence team

76%

say threat intelligence influences decisions at least weekly; 32% say daily

Threat intelligence isn't just for the SOC. Other active consumers include:

IT ops	73%
Incident response	48%
Risk management	47%



Evolving Market Needs

Top pain points for organizations evaluating threat intelligence vendors:

01.	Credibility	50%
02.	Ineffective integrations	48%
03.	Information overload	46%

Top success metrics for threat intelligence programs:

01.	Faster detection/response	54%
02.	Improved team efficiency	50%
03.	Fewer incidents	40%

Despite enterprise desires for more robust threat intelligence, vendors aren't always up to par. Choosing a customized solution for your organization's needs is essential to a successful cybersecurity stack.



Future Outlook for 2026

Looking ahead, executives anticipate a higher need for threat intelligence and are seeking out seamless integration with their security tools and workflows. As attackers mature, so must enterprises.

81%

plan to consolidate threat intelligence vendors in the next two years



91%

expect to increase threat intelligence spending in 2026



87%

anticipate significant maturity growth in the next two years



Top initiatives for future threat intelligence development:

36%

combining threat intelligence with internal data

25%

integrating into new workflows

18%

enhancing risk analysis

Read More About CISOs' Approach to Threat Intelligence

Get the Report

