PROBLEM:
THREAT OVERLOAD

70% OF ORGANIZATIONS SWAMPED BY CYBERTHREAT DATA

78%
of security practitioners identify threat intelligence as a critical part of achieving a strong security posture

ONLY **27%**
of security practitioners believe their organizations are very effective in utilizing threat data to pinpoint cyberthreats

ONLY **31%** of board and C-level stakeholders receive threat information that can be used to inform them about critical security issues their organizations are facing

WHY COMPANIES STRUGGLE

THE TOP REASONS FOR THREAT RESPONSE INEFFECTIVENESS:

Lack of staff expertise	Lack of ownership	Lack of suitable technologies
69%	58%	52%

THE INADEQUACY OF ORGANIZATIONS' PROCESSES AND REPORTING TECHNIQUES CREATES ADDITIONAL CHALLENGES FOR PRIORITIZING THREAT DATA

70%	52%	43%	49%
say it's difficult to prioritize malicious activity data without a threat intelligence platform	believe their companies need a qualified threat analyst to maximize the value of threat intelligence	say the data isn't used to drive decision making within their organization's security operations center	say their IT security team doesn't receive or read threat intelligence reports

THE SOLUTION

79%

BELIEVE A THREAT INTELLIGENCE PLATFORM IS NECESSARY TO MAXIMIZE THE VALUE OF THREAT DATA

70%	59%	51%
say threat intelligence platforms pinpoint and prioritize indicators of compromise (IOCs)	say threat intelligence platforms integrate threat data with other enabling security solutions (such as SIEM)	say threat intelligence platforms improve the threat analytics process

2/3 of organizations either have or are planning to deploy a threat intelligence platform

* The report, "The Value of Threat Intelligence: A Study of North American and United Kingdom Companies," was based on a survey of 1,072 IT or IT Security Practitioners.

Get the full report: anomali.com/ponemon

Ponemon INSTITUTE

ANOMALI