FORRESTER®

The Private Sector Needs A Holistic View Of The Threat Landscape

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY IBM | JUNE 2019

Private Sector Firms Struggle To Build A Holistic View Of The Threat Landscape

Today's cyberthreat landscape is more complex and challenging than ever before. The private sector is struggling with an overwhelming amount of data and data sources that need to connect to create actionable insights. Private sector companies need a data-agnostic system that connects internal, external, and open source data sources to perform threat investigations efficiently. Firms today must often connect four or more data sources to get a useful view of the current and developing threats. While some firms are using more advanced tools to investigate threats, many still rely on manual search-and-find techniques or spreadsheets, leaving their business and customers vulnerable to attack.

In March 2019, IBM commissioned Forrester Consulting to conduct a study about threat investigation strategies and technology.

Key Findings

Fifty-two percent of firms use four or more data sources — and 37% of firms use five or more — to perform an investigation.

It takes three or more days on average for 35% of firms to investigate a threat.

Almost a third of firms still rely on spreadsheets; 30% rely on manual searches to connect data sources and understand the threat landscape.

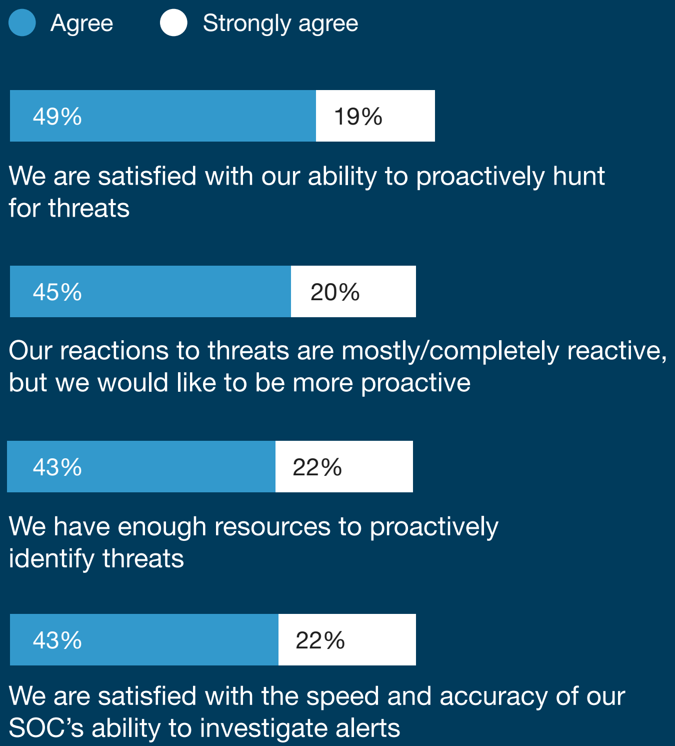
Overview
Situation
Challenges
Opportunity
Conclusion

Few Firms Are Satisfied With Their Ability To Be Proactive

It is critical to have both the skills and resources to proactively hunt for threats. Businesses need both people and technology that can proactively investigate threats that dwell in networks or that evade rules-based systems. Ideally, they should find threats prior to a cyberattack. However, 65% of firms agree that their responses to threats are mostly reactionary, but they would like to be able to be more proactive.

Only 27% of firms completely agree they have the right resources to proactively identify threats.

"Please select your level of agreement for each of the following statements about your company's security strategy."



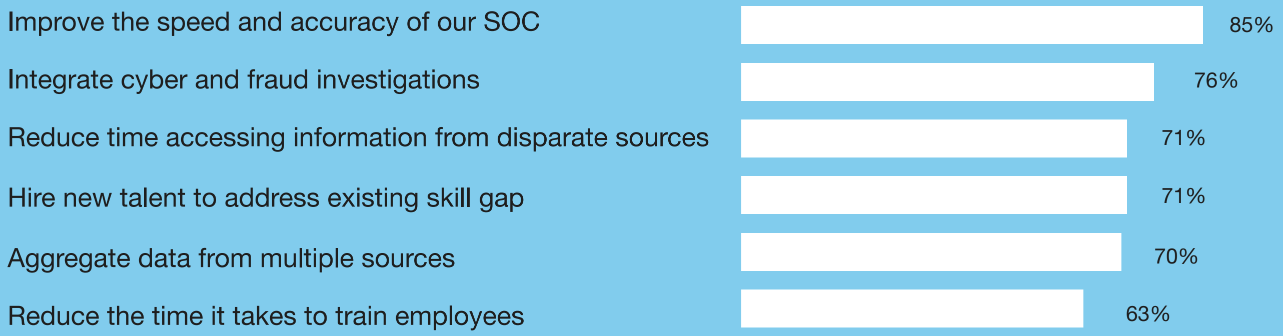
Base: 108 US SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, May 2019

Overview
Situation
Challenges
Opportunity
Conclusion

Firms Prioritize Improving SOC To Proactively Hunt Threats

Improving the speed and accuracy of their security operations centers (SOCs) is a priority for 85% of firms. Only 22% of firms are completely satisfied with the speed and accuracy of their SOCs when investigating threats. Improvement requires aligning disparate data sources, implementing multiple tools, and hiring/training staff members. After speed and accuracy, firms prioritize accessing information from disparate sources and integrating cyber and fraud investigations.

“What is the priority at your organization to improve your SOC’s ability to triage alerts?”



Base: 108 US SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, May 2019

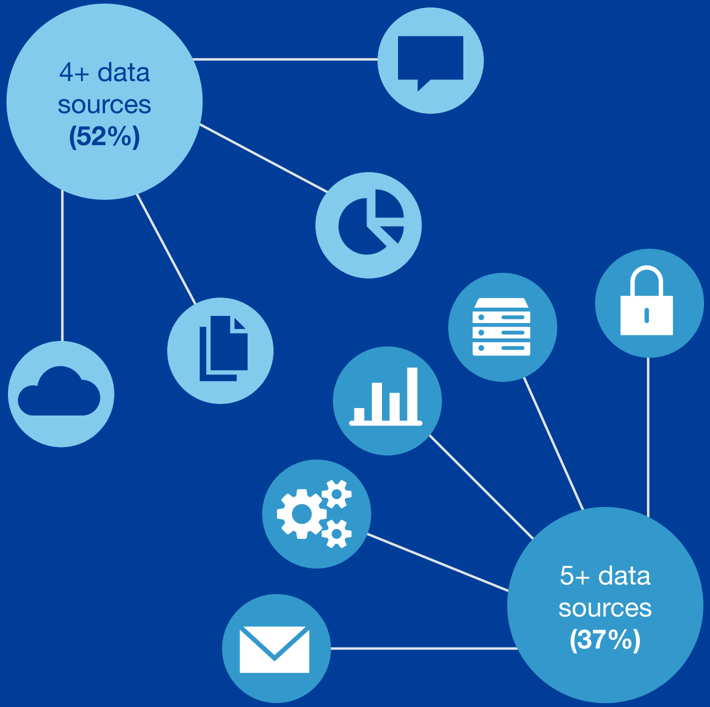
A Fractured View Of The Threat Landscape

Our study shows that over half of firms (52%) are relying on four or more data sources (internal, external, and open source) to perform investigations, and 37% are relying on five or more data sources. Organizations need systems that connect data sources, creating a holistic view of data to properly identify and prevent potentially devastating attacks.

A chief security architect for a US-based internet firm confirmed, "One of our biggest challenges is connecting all our tools and getting them to work together."

Our study found that only 44% of firms can connect all their data sources when conducting investigations, leaving the majority of firms with an incomplete view of their data.

"Which of the following data sources do your investigators rely on to perform an investigation/threat hunt?"



Base: 108 US SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, May 2019

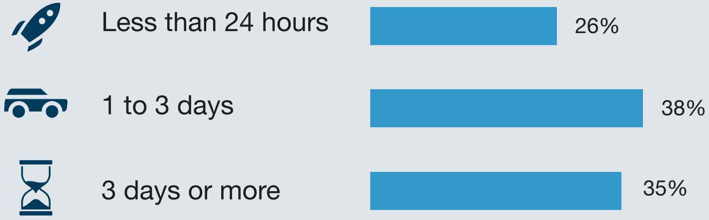
Timing Is Critical In Threat Investigations

On average, it takes 35% of firms three or more days to investigate a threat. For 38% of firms, it takes between one and three days. Firms estimate that their SOC staff spends roughly 38% of their week performing proactive threat investigations.

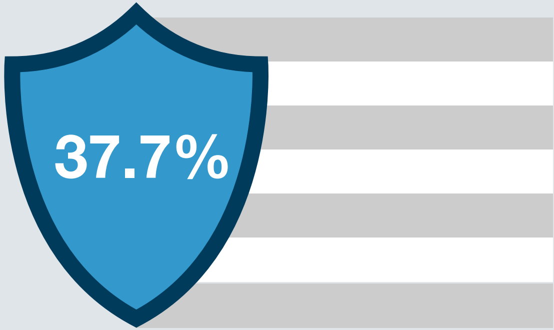
A security consultant in telecommunications explained: “We try to investigate threats within an hour of an alert, often with a simple challenge email. Others require more sophisticated investigations. A tool that links your data together is critical for fast triage.”

Just over a quarter (26%) of firms can investigate a threat in less than 24 hours.

“On average, how long does it take your investigators to investigate a threat?”*



“On average, what percentage of a normal week is your SOC staff performing proactive hunting?”



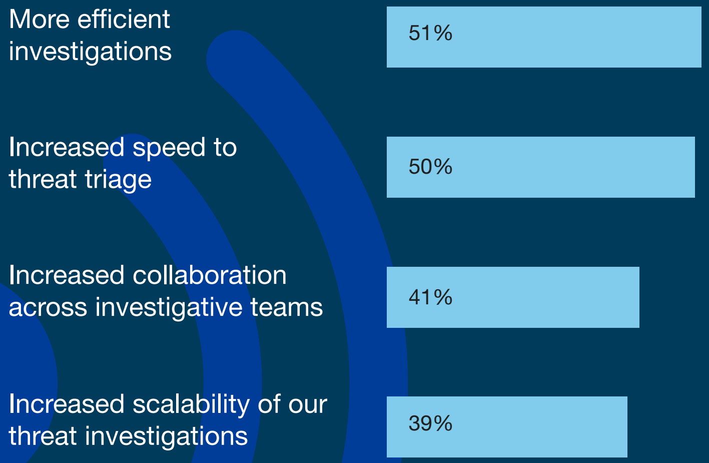
Base: 108 US SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy
*Note: Percentages do not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, May 2019

Firms Seek Short-Term Benefits First

When asked about a system that would process data to provide the needed context to identify threats, firms focused on short-term benefits. They want to increase the efficiency of their investigations, speed up the triage of threats, and make threat investigations more scalable.

Firms are less focused on longer-term efficiencies, such as visual analysis tools that can create a visual output of the threat and drive better communication of cyberincidents to leadership and law enforcement.

“What are/would you expect the most important benefits to be of a data-agnostic system that processes data in near real time to provide the needed context about specific threats identifiers?”



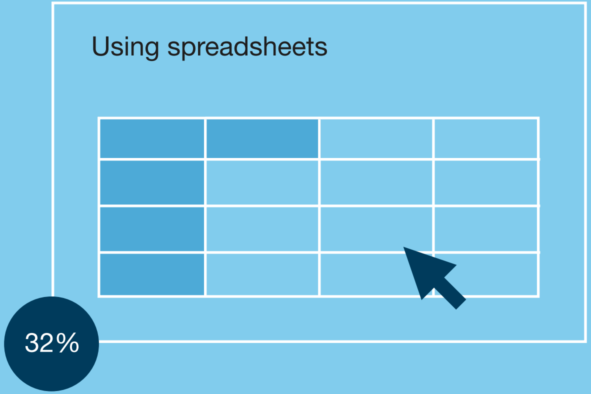
Base: 108 US SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, May 2019

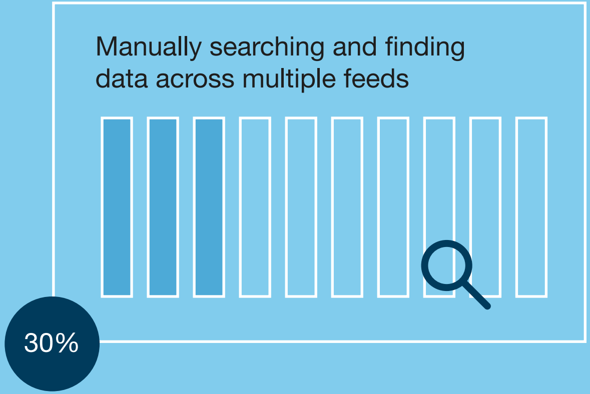
Time To Move Away From Manual Processes

Investigators need access to all available data sources to complete and resolve investigations thoroughly. Speed and accuracy are critical, so firms need big data analysis tools and linking analytics tools to efficiently connect data sources and build a holistic view of the threat landscape. Firms must weigh the cost of faster, more accurate systems against the cost of high-risk threats to decide how far they will go in threat analytics.

The security consultant in telecommunications explained: "A data-agnostic tool allows us to pinpoint weak spots in our network. It has also allowed us to proactively detect and triage threats faster."

"Which of the following describes how your organization is connecting internal, external, and open source data sets to create a holistic view of the threat landscape?"





Base: 87 US SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, May 2019

Overview
Situation
Challenges
Opportunity
Conclusion

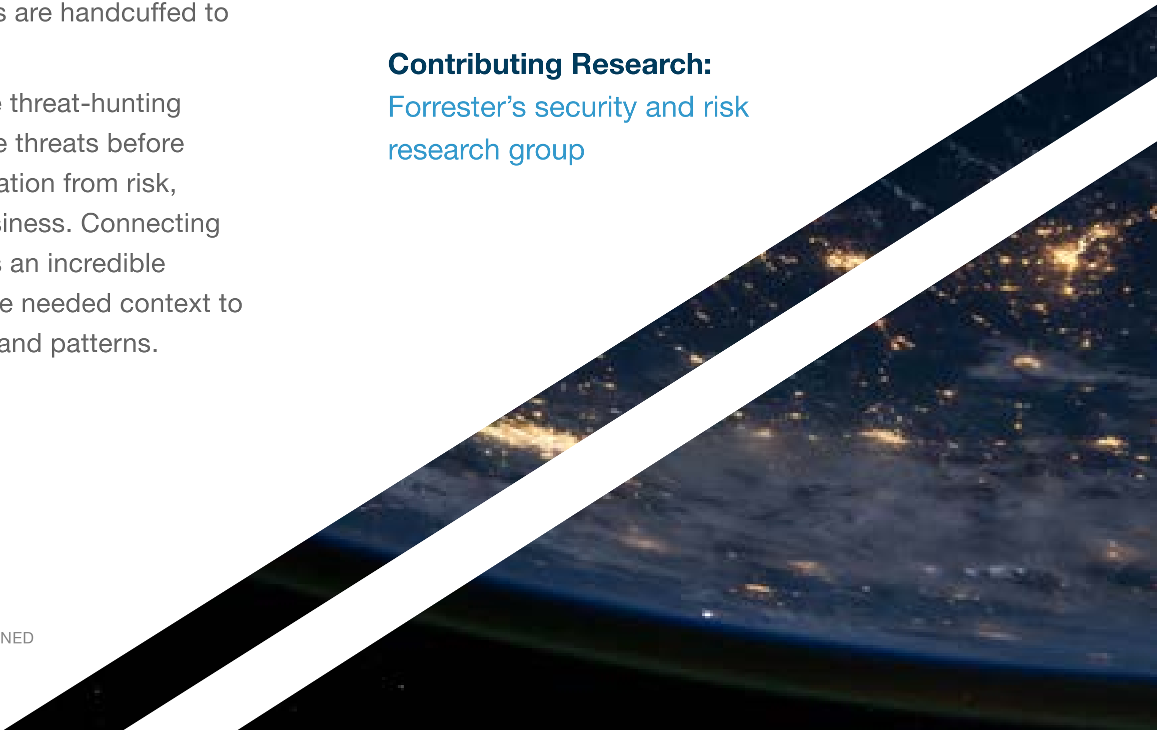
Conclusion

Efficient and swift cyberthreat investigations are critical for businesses to keep proprietary and customer information safe. This requires a holistic view of all data from internal, external, and open source data sources. Without this, investigators are handcuffed to manual processes and spreadsheets.

Private businesses must implement a proactive threat-hunting strategy to create actionable insights and triage threats before serious damage is done. This requires collaboration from risk, compliance, and security teams across the business. Connecting data sources will allow investigators to process an incredible amount of data in near real time and provide the needed context to efficiently and accurately identify threat trends and patterns.

Project Director:
Sarah Brinks,
Market Impact Consultant

Contributing Research:
Forrester's security and risk research group



Methodology

This Opportunity Snapshot was commissioned by IBM. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of SOC management, technologist, and operation managers involved in threat detection and security and risk assessment strategy and two phone interviews with threat detection decision makers. The custom survey began and was completed in May 2019.

Demographics

GEOGRAPHY

US 100%

NUMBER OF EMPLOYEES

49% 1,000 to 4,999

30% 5,000 to 19,999

21% 20,000 or more

DEPARTMENT

80% IT/technology

10% IT/cybersecurity

6% Risk and compliance

4% Operations

POSITION

32% Director

31% Manager

19% C-level

17% Vice president

Note: Percentages may not total 100 because of rounding.

ABOUT FORRESTER CONSULTING
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®