

+134:23:454:12

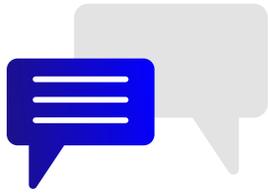
WHITE PAPER

Business Strategy  
Marketing  
Product  
Network  
Sales  
Process  
Management

# Building a Threat Intelligence Program

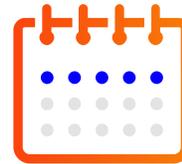
Research findings on best practices and impact

# Methodology



# 351

total responses  
from cybersecurity  
decision makers in  
the United States



## FIELD DATES:

March 30th -  
April 4th 2018

APPROXIMATELY



# 15 MINUTE ONLINE SURVEY

instrument (53 total questions)

Survey respondents  
were provided by  
Branded Research.  
Branded has a global  
reach of over  
**3 BILLION  
RESPONDENTS.**



## Overall margin of error

# +/- 5 POINTS

at a **95%** confidence  
interval



# Major Themes



Those who describe their threat intelligence program as more mature than their competitors' are often utilizing threat intelligence platforms to aggregate and monitor data in one place.



Organizations with threat intelligence programs in place indicate sharing of information is key.



Healthy organizations have threat intelligence infrastructure in place.



The majority of decision makers say their organizations plan to invest more in threat intel programs in the coming year.

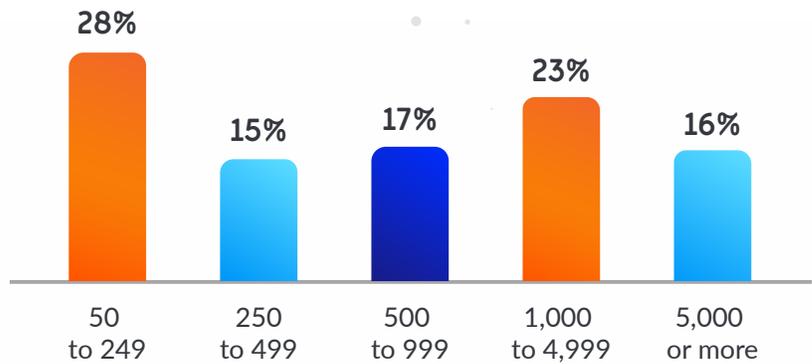
# Demographics

**100%**  
of respondents...

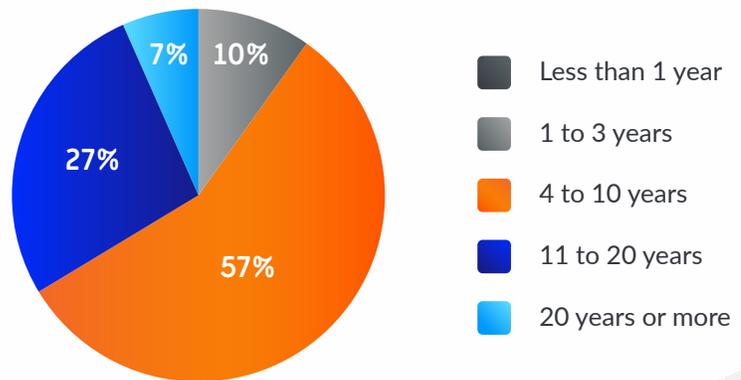
Work **full-time** in IT departments; and are **decision makers** for **cybersecurity** services, technologies, or solution purchases within their organizations



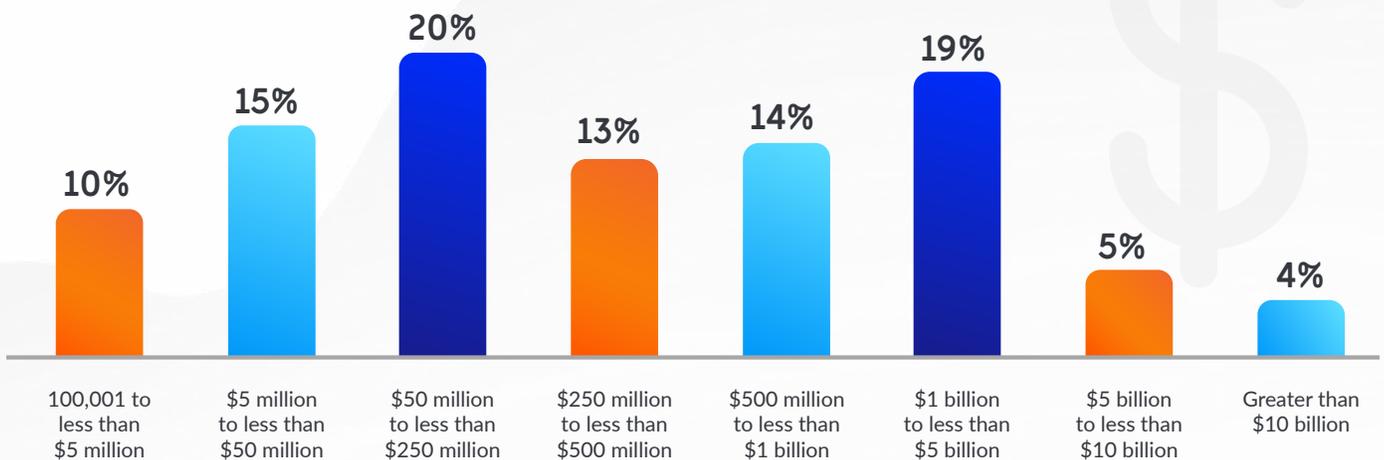
Approximately how many employees are in your company at all locations worldwide?



How long have you been employed in your current role?



In your best estimate, what was your organization's total revenue for last year?



# Current Trends

**In organizations that have fully-mature threat intelligence programs, nearly half (46%) experienced significant revenue growth within the last year.**



Those who describe their threat intelligence program to be **more mature (69%)** than competitors' are often **utilizing threat intelligence platforms to aggregate and monitor data** in one place...

And, there is little disagreement on the most effective infrastructure for threat intelligence programs among cybersecurity decision makers. Those who describe their threat intelligence program to be more mature (69%) than competitors' are often utilizing threat intelligence platforms to aggregate and monitor data in one place, compared to those who describe their threat intelligence program to be on-par (35%) with industry competitors.

Organizations that are experiencing significant or strong growth have threat intelligence infrastructure in place. Organizations with fully-mature threat intelligence programs are more likely to experience significant or strong revenue growth (94%) than those organizations that don't have fully-mature threat intelligence programs in place (88%)

Those with fully-mature threat intelligence programs in place are reaping the rewards. Cybersecurity decision makers surveyed in this group say that their organizations' threat intelligence programs prevented phishing attacks (72%), ransomware attacks (65%) and business email compromise (67%).

Furthermore, threat intelligence programs have proven a necessity for organizations both large and small. More than half of all organizations with threat intelligence programs say their organizations' programs have prevented phishing attacks (67%), ransomware attacks (58%), breach of customer data (60%), insider threats (57%), business email compromise (55%), and supply chain attacks (49%).

More than half of all organizations with threat intelligence programs say their organizations' programs have prevented:

**67%**  
Phishing Attacks



**58%**  
Ransomware Attacks



**60%**  
Breach of Customer Data



**57%**  
Insider Threats



**55%**  
Business Email Compromise



**49%**  
Supply Chain Attacks



**More than 70% of all respondents agree at some level that they do not have the staff or resources to monitor all cybersecurity threats.**

Even of those with fully-mature threat intelligence programs, still 29% of cybersecurity decision makers said they don't have the staff or resources to monitor all cybersecurity threats that face the business.

Efforts to attribute such threats remain a challenge for all cybersecurity decision makers – 53% agree they are rarely ever able to use breach data to identify where a cybersecurity threat is from.

Most cybersecurity decision makers within organizations with threat intelligence programs in place, say they are able to obtain information pertaining to the location the cyber attack originated from (74%) and the types of cyber weapons used (67%) during or after an attack.

Even though a compelling 82% of cybersecurity decision makers from organizations with a threat intelligence program in place agreed their programs are sophisticated enough to handle any cybersecurity threat, more than four-in-five (84%) said that their organization should be investing more in its threat intelligence program.



**Most cybersecurity decision makers within organizations with threat intelligence programs in place, say they are able to obtain information pertaining to the**

**location the cyber attack originated from (74%) and the types of**

**cyber weapons used (67%)**

**during or after an attack.**

# Impact on Business

**Organizations that have threat intelligence programs have saved an average of 8.8 million dollars in the last twelve months.**

Nearly four-in-five (78%) cybersecurity decision makers with threat intelligence programs said that their organizations have successfully used those programs in the last year to block threats that otherwise would have cost the business a significant sum of money.

Cybersecurity professionals that felt they had leading threat intelligence programs (84%) compared to their competitors' reported that they had blocked threats to the business within the last twelve months that would have cost the business a significant sum of money, compared to 70% from organizations who say that their threat intelligence programs are on-par with industry competitors.

Surprisingly, only about one-in-ten (12%) organizational leaders considered the ability to avoid embarrassing, public disclosures of information to be a top-three factor when evaluating the success of a threat intelligence program. When asked about the most important factors for evaluating the success of threat intelligence programs, the majority of cybersecurity decision makers cite protecting personal client information (67%), removing risks faced from cyber-crime activities (59%), and protecting monetary assets of the organization (53%) as primary considerations.



Surprisingly, only about **one-in-ten (12%)** organizational leaders considered the ability to avoid embarrassing, public disclosures of information to be a **top-three factor** when evaluating the success of a threat intelligence program.



Organizations that have threat intelligence programs have saved an average of **8.8 million dollars** in the last twelve months.



When it comes to preventing threats, not all industries are having similar success. In companies that have threat intelligence programs, cybersecurity decision makers in telecom and communications

(90%), retail and consumer product goods (86%), hi-tech (79%), and banking and finance (71%) said that their organizations' threat intelligence programs blocked threats within the last year that otherwise would have cost a significant sum of money. Compared to only 63% in utilities and 58% in manufacturing that say the same.

When it comes to future threats, nearly three-in-five (57%) cybersecurity decision makers surveyed say their organizations are more susceptible to cybersecurity threats in 2018 than they were in 2017.

When it comes to future threats,

**nearly three-in-five**

**(57%)**

cybersecurity decision makers surveyed say their organizations are more susceptible to cybersecurity threats in 2018 than they were in 2017.

# Growing the Program

**Cybersecurity decision makers overwhelmingly agree that their organizations should be investing more in their threat intelligence programs.**

More than half (52%) of the cybersecurity decision makers surveyed agree that their organizations do not have the staff or resources necessary to monitor all cybersecurity threats that their organizations face. 83% indicated that their organizations should be investing more in their threat intelligence programs.

Over the next twelve months, the majority (61%) of cybersecurity decision makers surveyed say their organizations plan to invest more into threat intelligence programs. Fewer than two-in-five (37%) say their organizations plan to invest about the same as last year in their threat intelligence programs.

Companies that are experiencing the most success financially are also investing heavily in their threat intelligence programs. More than three-quarters of companies experiencing significant revenue growth plan to invest more in their threat intelligence programs over the next twelve months (78%).



**More than three-quarters (78%)** of companies experiencing significant revenue growth **plan to invest more in their threat intelligence programs** over the next twelve months.

While organizational leaders say they are committed to expanding the capabilities of their programs, their teams do not feel that message. More than three-in-five (70%) C-Suite leaders in organizations surveyed said they plan to invest more in their organizations' threat intelligence programs in the next twelve months while fewer Director and VP level employees (57%) say the same.



**83%**

indicated that their organizations should be investing more in their threat intelligence programs.



# Managing the Program

**Organizations with threat intelligence programs in place are constantly digesting data – more than two-in-five (41%) cybersecurity decision makers say their organization monitors or interacts with threat intelligence data 24 hours a day.**

The majority of cybersecurity decision makers from organizations with threat intelligence programs in place, report they have implemented tools such as a: firewall (76%), threat intelligence platform (67%), log management (63%), intrusion prevention/protection (60%), end-point detection and response (59%), and indicator feed/blocklists (54%).

For some, threat intelligence programs are specifically tailored to information obtained in previous, well-known cyberattacks. At least one-in-three cybersecurity decision makers surveyed said that the following threats prompted their organizations to change their threat intelligence programs: CryptoLocker (44%), Cloudbleed (37%), WannaCry (33%), and TeslaCrypt (33%).

The largest enterprise firms surveyed indicate programmatic changes due to well-known threats more-so than smaller organizations, including the cyber-threats known as: Cloudbleed (46% vs. 37%), TeslaCrypt (40% vs. 31%), WannaCry (40% vs. 31%), Heartbleed (37% vs. 27%), and Stuxnet (35% vs. 20%).

Sharing threat intelligence is a concern for many. More than four-in-five (81%) cybersecurity decision makers agree that, given all of the additional cyber threats that surface each day, coordinating data sharing with governments is one of the priorities for their threat intelligence programs. Organizational leaders (87%) strongly echo this sentiment.



The largest enterprise firms surveyed indicate programmatic changes due to well-known threats more-so than smaller organizations, including the cyber-threats known as:

**Cloudbleed**  
46% vs. 37%

**TeslaCrypt**  
40% vs. 31%

**WannaCry**  
40% vs. 31%

**Heartbleed**  
37% vs. 27%

**Stuxnet**  
35% vs. 20%



# Threat Intel Sharing

**Two-in-three (66%) cybersecurity decision makers in organizations with threat intelligence programs said their business looks to the government for information or data on cyber threats.**

Cybersecurity decision makers with threat intelligence platforms are significantly less likely (66%) than competitors with no threat intelligence programs (80%) to look to the government for information or data on cyber threats.



**Cybersecurity decision makers** with threat intelligence platforms are significantly less likely (66%) than **competitors with no threat intelligence programs** (80%) to look to the government for information or data on cyber threats.

More than two-in-three (68%) cybersecurity decision makers indicate that the government has programs designed to assist companies combating cybersecurity threats. More than one-in-three (36%) cybersecurity decision makers surveyed say that their organizations currently shares threat intelligence data with a government group.

Roughly two-in-five (41%) cybersecurity decision makers from organizations with threat intelligence programs in place, report that sharing information with governments and other NGO groups is integral to their threat intelligence program development. Only 15% of cybersecurity decision makers from organizations with threat intelligence programs saw no benefit in sharing information with government or NGO groups.

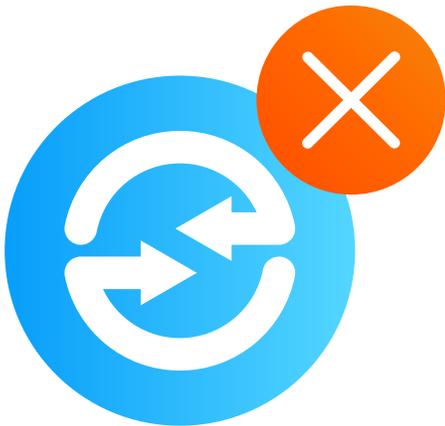


Roughly two-in-five

**(41%)**

cybersecurity decision makers with threat intelligence programs in place, report that sharing information with governments and other NGO groups is integral to their program development.





Additionally, 40% of cybersecurity decision makers in organizations with threat intelligence programs said that their organizations do not share threat intelligence data with any external group.

Cybersecurity decision makers from organizations with fully-mature threat intelligence programs (55%) find sharing information with governments or NGO groups an integral component to their threat intel programs. This is even more than the previously mentioned 41% of all cybersecurity decision makers with threat intel programs who say the same.

55%

Cybersecurity decision makers from organizations with fully-mature threat intelligence programs find sharing information with governments or NGO groups an integral component to their threat intel programs.



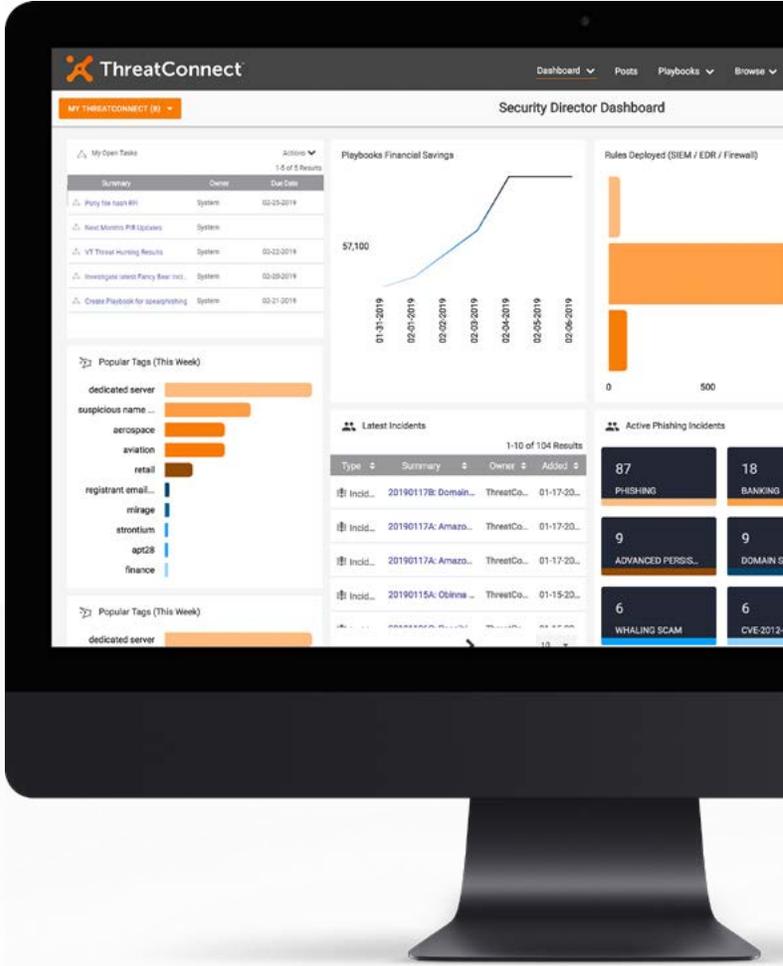
### Building a Threat Intelligence Program

More than two-in-five cybersecurity decision makers within organizations with a threat intelligence program, report sharing malware data (55%), general threat data (49%), ransomware data (42%), and specific threat attribution (44%) data with governments and NGO groups. Slightly fewer indicated they share real-time threat data (41%), after-the-fact incident data (40%), attribution data (40%), or APT data (35%).

More than four-in-five (84%) cybersecurity decision makers surveyed agree that a better relationship with government groups would foster a better environment for exchanging threat intelligence data. Nine-in-ten (90%) organizational leaders agree that a better relationship with government groups would foster a better environment for exchanging threat intelligence data.

Governments and NGO groups prove to be a vital and desired component of many threat intelligence programs. Nearly three-in-four (72%) cybersecurity decision makers surveyed agree that governments do an excellent job of providing real-time threat data to help their organizations when a threat is occurring.

Yet, there are still ways in which governments and NGO's could make sharing threat intelligence a more valuable endeavor to private enterprise. When it comes to specific changes, nearly one-in-two cybersecurity decision makers said that governments could help by creating and distributing defensive tools and techniques to help combat known cyber-attacks (48%), creating industry groups that are tasked with working on cybersecurity threats specific to their industry (48%), and by providing regular briefings for cybersecurity employees about the most recent trends in cyber-attacks (48%).



Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit [www.ThreatConnect.com](http://www.ThreatConnect.com).

[ThreatConnect.com](http://ThreatConnect.com)

3865 Wilson Blvd., Suite 550  
Arlington, VA 22203

[sales@threatconnect.com](mailto:sales@threatconnect.com)

1.800.965.2708

