EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

ANOMALI

# Cyber Threat Intelligence – Transforming Data Into Relevant Intelligence

**April 2023 EMA Research Report**

**Christopher M. Steffen, CISSP, CISA**, Managing Research Director and **Ken Buckler, CASP**, Research Analyst
*Information Security, Risk and Compliance Management*

Table of Contents

# Introduction

Many organizations have leveraged cyber threat intelligence (CTI), a powerful tool, for over two decades. Until recent years, threat intelligence was extremely expensive and only the largest organizations with budgets that allowed for such investment adopted it. However, in recent years, CTI has become much more affordable and accessible, with tools dedicated to processing and distributing CTI. Combined with CTI sharing partnerships and information sharing and analysis centers (ISACs), CTI is now more accessible than ever, even for small businesses that were previously financially restricted from accessing this important cybersecurity tool.

However, this sharing and accessibility present new challenges that result in increased CTI data, which must be analyzed for relevance and processed within the organization. It also presents challenges of integrating CTI data with cybersecurity tools, such as SIEM, XDR, or network and endpoint protection. What was once a rare occurrence with signatures that users could input to these tools manually now requires constant data streams that automatically update tools with the latest threat indicators.

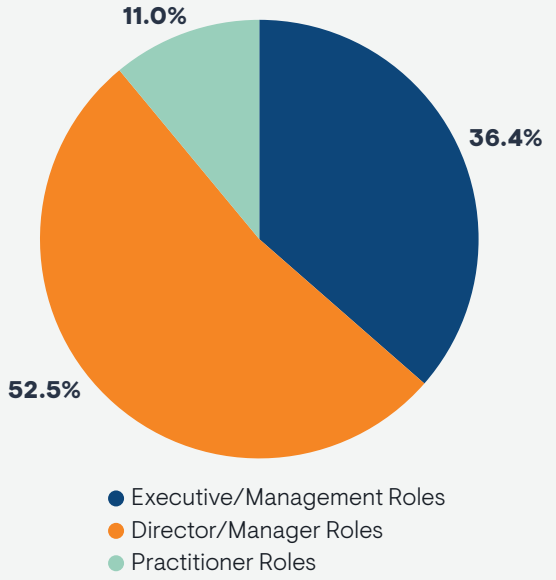
In this research, Enterprise Management Associates set out to discover which CTI sources, methods, and integrations are currently working in the industry and where there is room for improvement. What we found was that many organizations are struggling with CTI, especially when it comes to data quality. The research provides key insights on the CTI sources organizations are having the most success with and how organizations can better leverage CTI in their everyday operations and technology integrations. Most importantly, the research highlights how organizations' CTI data filtering attempts are counterproductive and how to better leverage CTI.

# Research Methodologies

EMA surveyed 125 professionals across more than 20 different industry verticals from organizations with 500 or more employees. We analyzed the results by filtering and cross-slicing the data to determine which CTI strategies are working best and which provide opportunity for improvement.

Respondents covered a broad number of industries, from computer/technical services to retail services, manufacturing, and even government and defense. Through analyzing these responses, we found that the successes and challenges remain mostly the same regardless of industry.

At the end of this report, you will find an overview of the organization sizes and verticals, as well as the job titles and overall functional duties of the respondents.



# Key Findings

## CTI Methods and Tools

- **94%** of organizations have a dedicated CTI team
- **75%** of organizations without a dedicated CTI team spend up to 25% of their time processing and responding to CTI
- **58%** of organizations utilize threat bulletins and reports as the most common CTI source
- **51%** of organizations utilize CTI sharing partnerships, which seems to be the more preferred method of CTI sharing over the 18% of organizations that utilize ISACs or other threat-sharing organizations

## Leveraging Threat Intelligence

- **61%** of organizations provide CTI to their security operations team as their primary CTI consumer
- **84%** of organizations focus on proactively providing CTI to the rest of their organization
- **34%** of organizations state that proactive defense of their network using CTI is the most important aspect of CTI, and another 23% state that data relevance is the most important aspect
- **30%** of organizations state that their primary challenge with CTI is useless “noise”

## Impact and Results

- **72%** of organizations believe more CTI sharing is needed through mutual partnerships
- **12%** of organizations do not have sufficient staff to analyze and respond to CTI
- **82%** of organizations have seen a decrease in successful attacks since implementing their current CTI program
- **46%** of organizations consider the quality of data of their CTI platform the most important feature

# Voices of the Survey – Respondent Quotes and Feedback

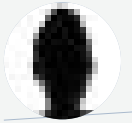
# Select Open-Ended Responses

## Describe how your organization leverages threat intelligence in your daily operations. What is one feature or capability your threat intelligence platform does not have, but you wish it had?

**Threat information is used to facilitate security decisions for fortifying the organization against bad actors** [including] educating users, implementing new policies, and incorporating software/hardware infrastructure.

*IT Architect, Oil/Gas/Chemicals Industry*

We utilize [our solution] to analyze system and related network logs. **From that real-time scanning, we generate alerts and auto-block malicious activity before it can infect the network.**



*C-Level Executive, Retail/Wholesale/Distribution Industry*

Our CTI platforms lack flexibility to integrate into different systems or platforms seamlessly without compromising quality, agility, and quantity. **We need enhanced protocols to optimize such data transitions.**

*CIO/CTO/VP Information Technology, Computer/ Technology Services Industry*

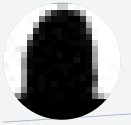
We use traditional intelligence to monitor network traffic and incident reports to form our strategy in terms of what to focus on to lessen incidents. **We have deep web searches to focus our automated response and have live personnel at times with separate plans of response for particular instances.**

*Information Security Director, Education Industry*

**We get our most valuable information from trusted industry partners.** If there were a way to better share CTI information in real time in a very secure digital venue, this would be very valuable.

*Information Security Director, Finance/Financial Services/ Banking/Crypto Industry*

Currently, our platform is somewhat lacking in integrating with other key security tools, such as SIEM, our firewall, and EDR. **Integration will be our main focus moving forward.** Improved integration will be critical to supporting our company as it grows.



*CISO/CSO/VP Information Security, Computer/ Technology Software Industry*

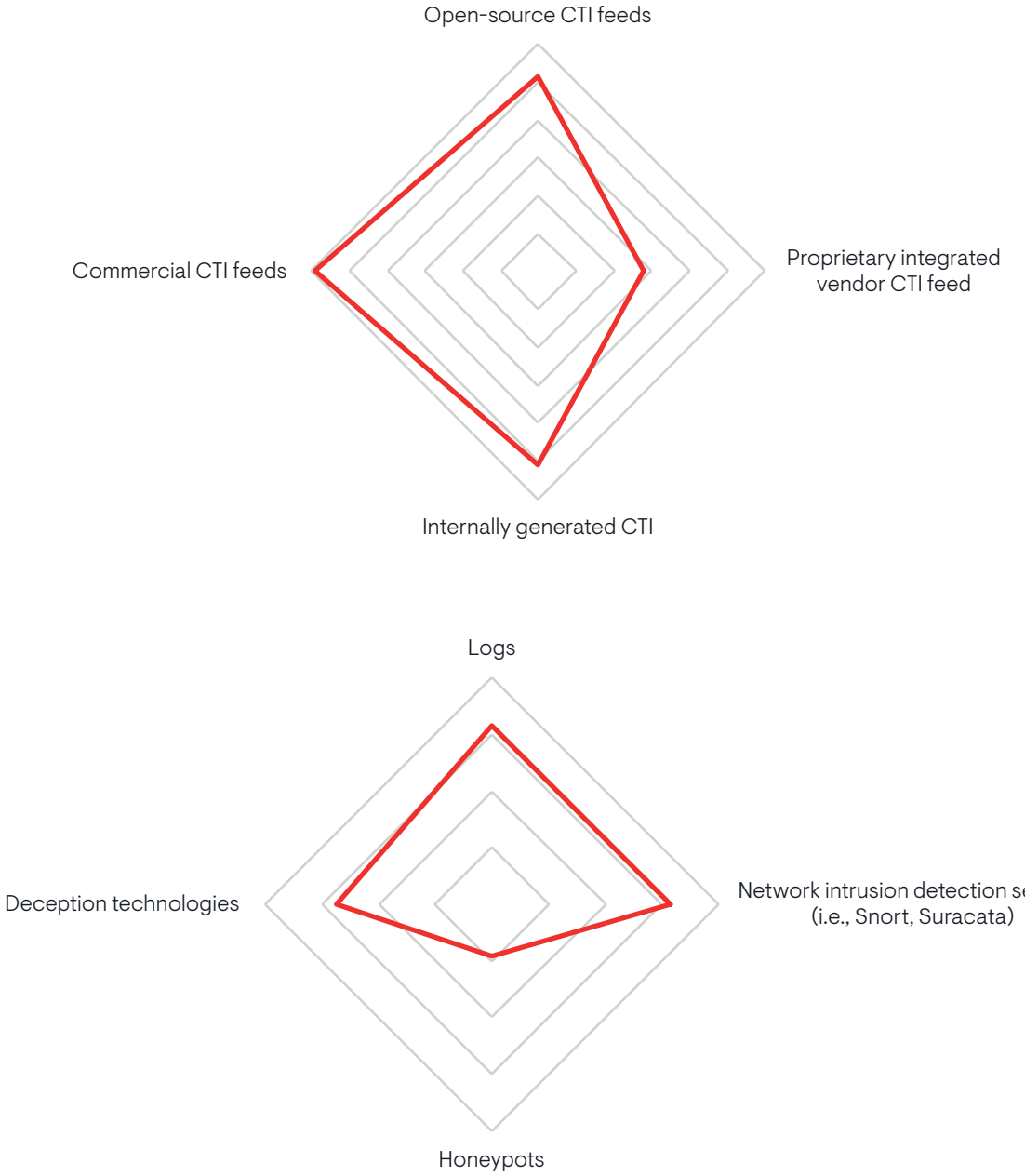
# CTI Methods and Tools

# CTI Sources – Structured Data

Analyzing preferred CTI data sources, we broke them into three categories – structed data sources, unstructured data sources, and data sharing.

Commercial CTI feeds were the most preferred data source when it comes to structured data, with a tie for second place between open source and internally generated CTI. It's clear that organizations prefer curated, filtered data and shy away from proprietary feeds.

Internal CTI sources seem to be evenly split between network intrusion sensors and log analysis, with deception the third most popular response. Despite the availability of commercial and open source honeypots, few organizations leverage them.



# CTI Sources – Unstructured Data

When it comes to unstructured data, organizations seem to prefer cybersecurity focused websites and threat bulletins from non-government entities over government bulletins and reports.

Non-government threat bulletins and cybersecurity websites may be preferred over government sources due to the timeliness of the data. After all, the government typically has a longer approval process to share threat intel, while commercial and nonprofit entities likely have more flexibility.

Social media, which can be powerful at delivering threat indicators to a broad audience quickly, was the least preferred method for CTI sources, most likely due to the reliability and trustworthiness of the data source.

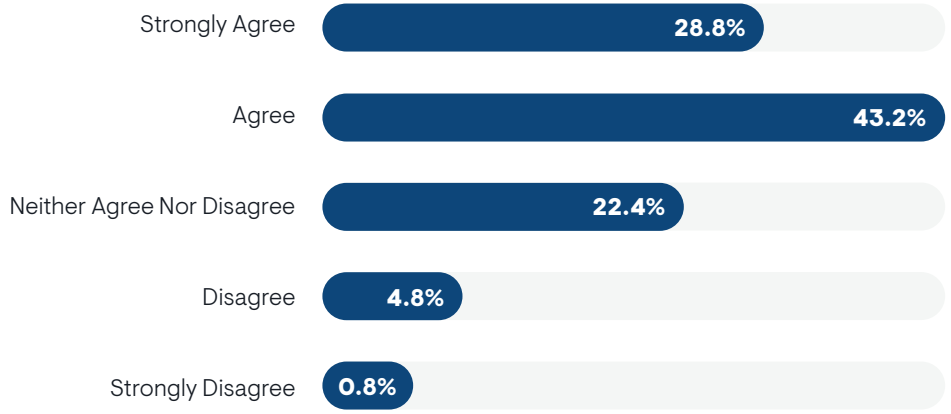
# CTI Sources - Data Sharing

Organizations clearly understand the importance of mutual CTI data sharing. However, organizations seem to prefer CTI sharing partnerships directly with other organizations instead of ISACs, which are more community-focused.

Very surprising is the low adoption of ISACs, which are typically devoted to providing industry-relevant threat data. Only 18% of organizations utilize ISACs, and ISACs were the least used CTI source.

This desire to directly share with other organizations could open the door for improvement of CTI platforms, allowing direct data sharing with other organizations. This, of course, would require a standardized format for CTI data so the date could be leveraged across different vendors.

OUR ORGANIZATION NEEDS TO PARTICIPATE IN MORE MUTUAL CTI DATA-SHARING PARTNERSHIPS

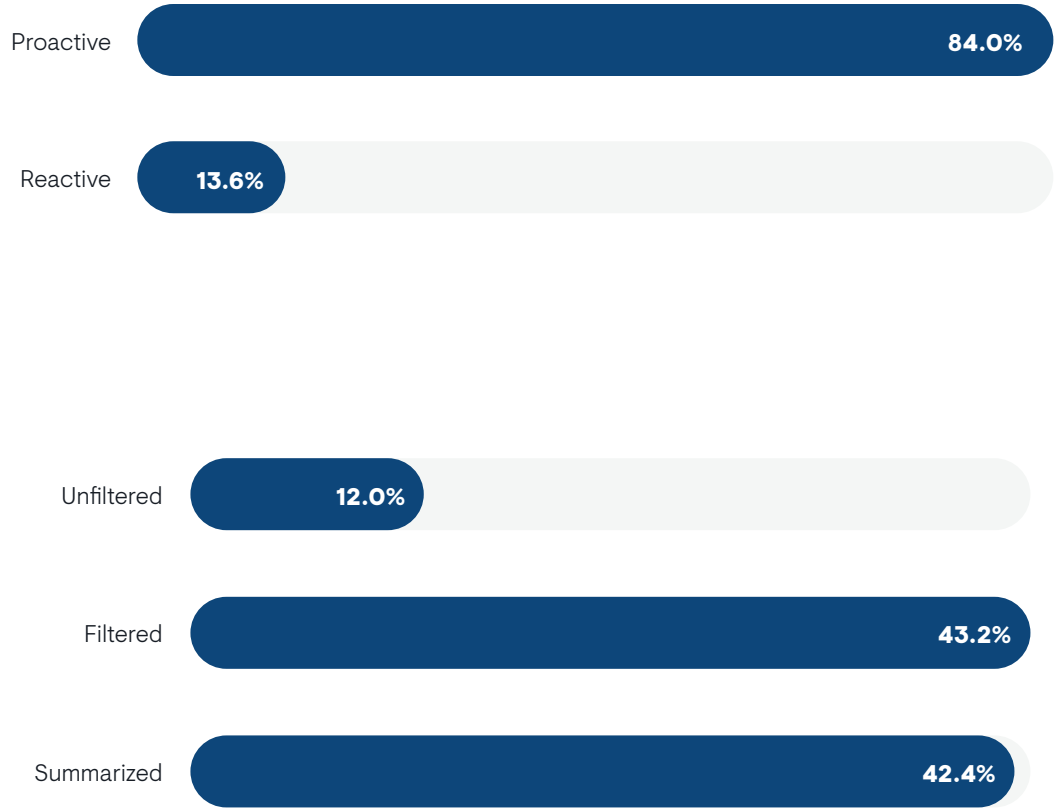



# Leveraging Threat Intelligence

# CTI Data Primary Usage and Filtering

When it comes to usage of CTI data and filtering, most organizations utilize CTI in a proactive manner, trying to prevent threats instead of simply trying to detect them after an incident. The high adoption rate of focusing on proactive CTI usage instead of just incident response is encouraging and shows that organizations are adopting a more proactive stance for cybersecurity operations.

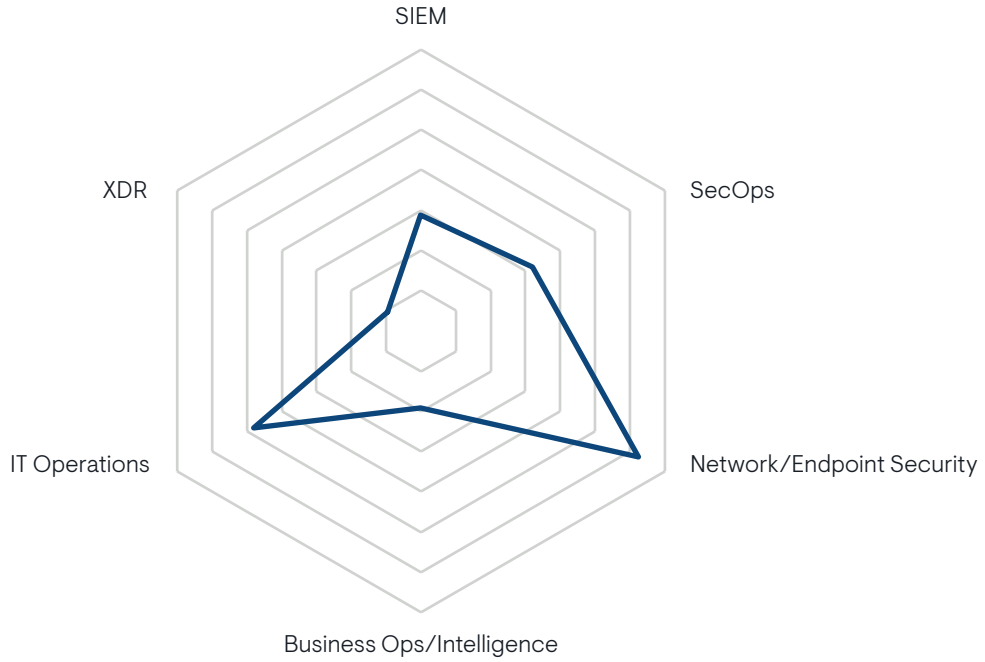
Organizations seem to prefer filtered or summarized CTI data over unfiltered, with only 12% of organizations using raw, unfiltered data. The usage of filtered or summarized data seems to be almost evenly split, with only slightly more organizations focusing on filtered data.



# CTI Integration Priorities

Integration with network and endpoint security solutions is the highest priority for most organizations when it comes to threat intelligence, with IT operations a close second. This is not surprising, since CTI has always been traditionally leveraged at a network level to monitor for known malicious domains, IP addresses, or files.

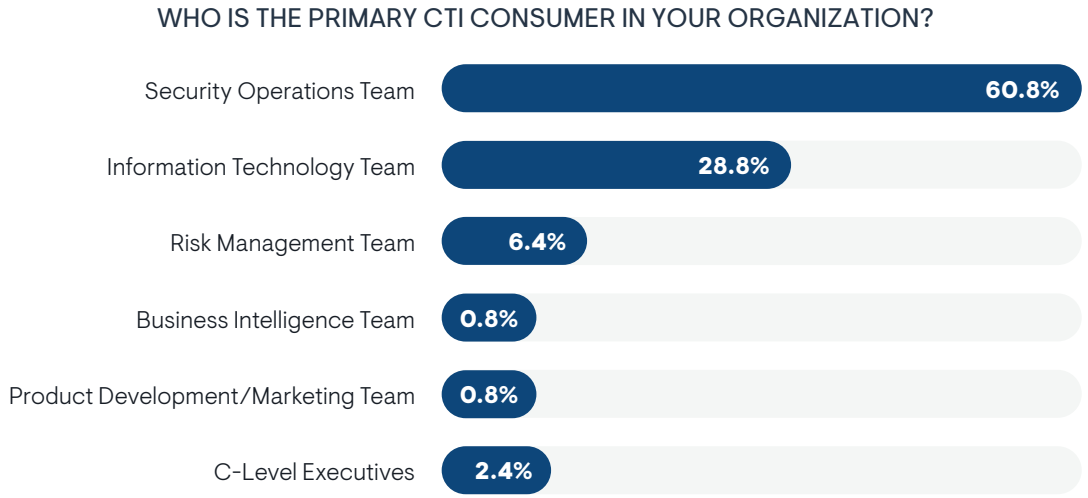
While business operations/intelligence and XDR can provide valuable insights regarding CTI indicators and trends, they were the lowest priority for integration of CTI. These underutilized priorities present hidden opportunities to enhance CTI usage, especially for organizations that have already invested in XDR or business intelligence tools.

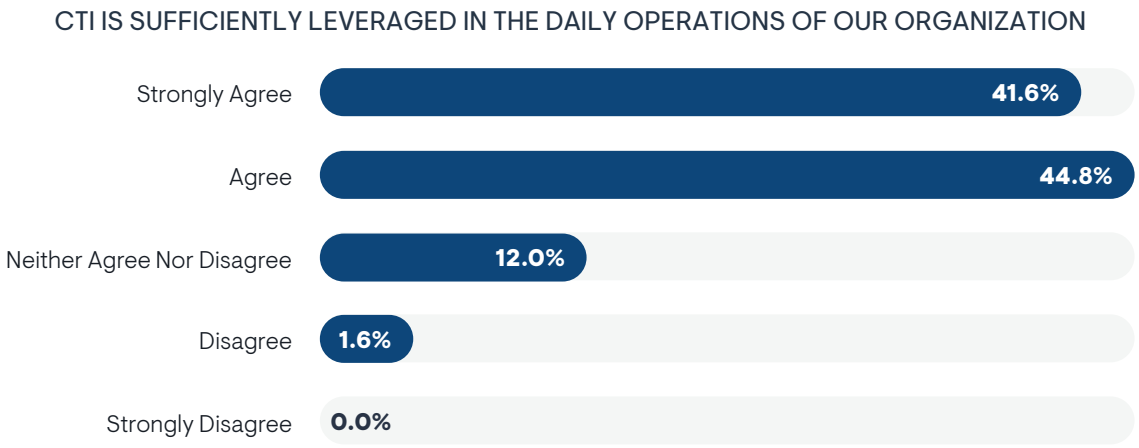


# Consumers of CTI and Leveraging in Daily Operations

Not surprisingly, the security operations team is the primary CTI consumer, with the information technology team the next highest priority and risk management a distant third place. It is interesting that the primary consumer for CTI in 2.4% of organizations is C-Level executives. While it's important to keep executives in the loop regarding current threats, executives typically have little ability to directly utilize the tools CTI will be integrated with to protect the enterprise.

Most organizations agree that CTI is sufficiently leveraged in the daily operations of their organizations, with 86.4% agreeing or strongly agreeing. Only 1.6% of organizations do not believe CTI is sufficiently leveraged in their daily operations.



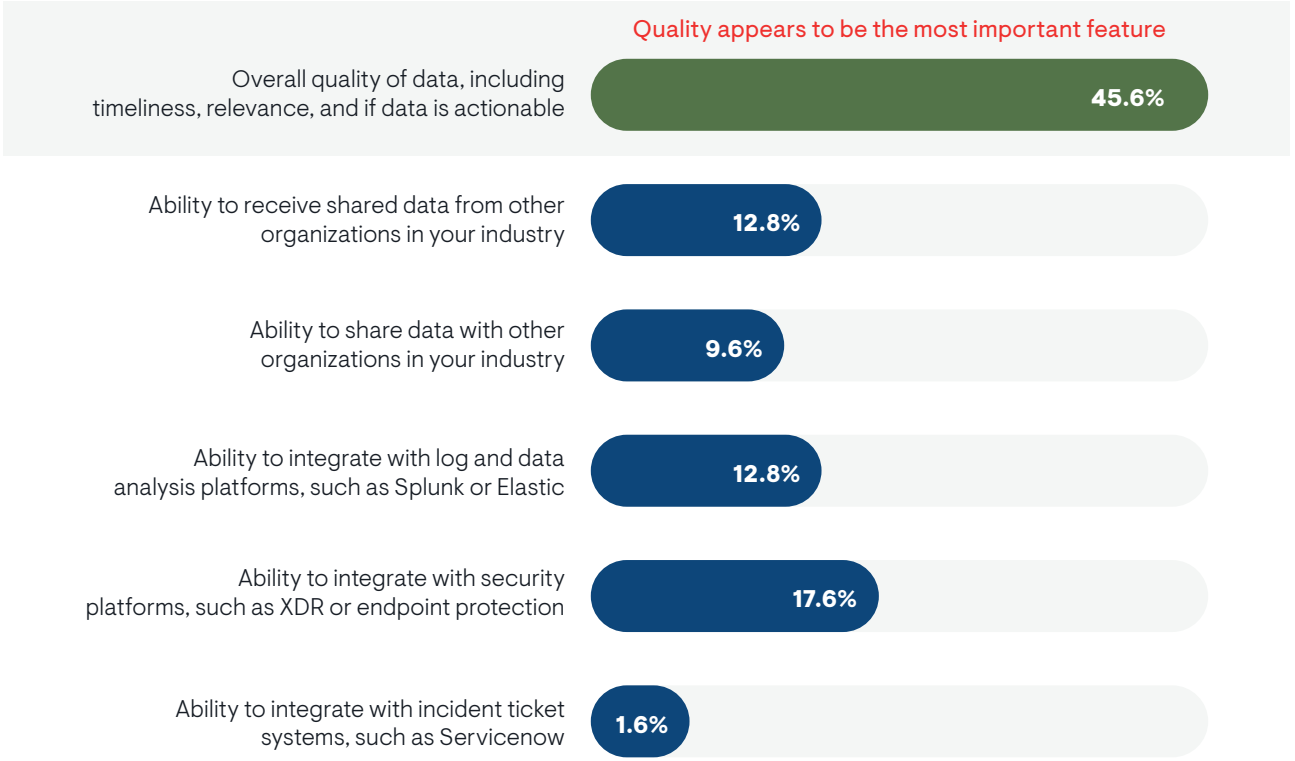



# What do you consider the most important feature of your CTI platform?

Data quality is the most important feature of CTI platforms according to almost half of all organizations. The next most important feature is the ability to integrate with other platforms, such as XDR or endpoint protection.

Without quality data, CTI will struggle to provide a return on investment. Organizations recognize that while integrations are important, the most important feature of CTI is the quality of the data itself.

While useful for optimizing operations, integration with incident ticket systems, such as ServiceNow, is the lowest priority when it comes to CTI platform features.

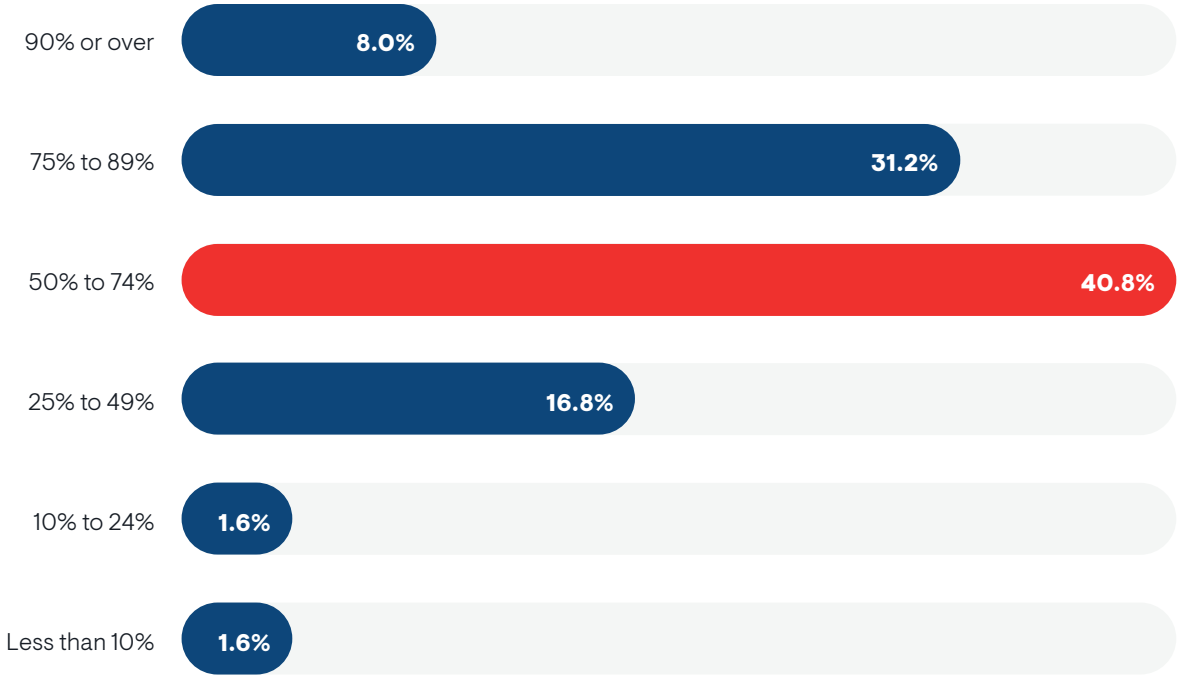


# What percentage of CTI provided by the CTI team do you believe is useful to your organization and not "noise?"

While data quality is the most important feature of CTI for most organizations, data quality is clearly a severe issue. With 40% of organizations reporting that between 25% and 50% of the CTI data they receive is "noise" and not useful, organizations are clearly struggling to spend considerable time on filtering out data that does not apply to their organization.

Only 8% of organizations believe that 90% or more of their CTI data is useful. Even worse, 20% of organizations believe that 50% or more of their CTI data is useless noise.

Clearly, CTI data quality is a problem the cybersecurity industry still struggles with.

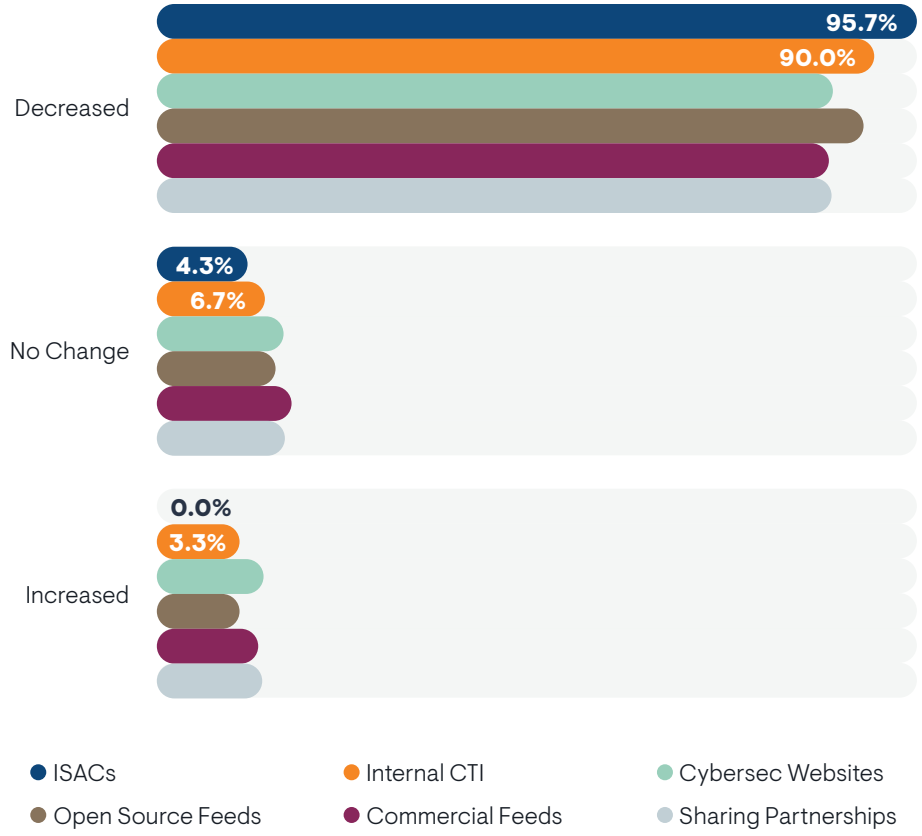


# Impact and Results

# How do CTI sources affect successful cyber attacks?

Overall, most CTI sources see decreased successful attacks, but ISACs appear to be the most important source, presenting an underutilized resource. These threat-sharing organizations are typically focused on specific industries, and in the case of this research, were part of the most successful strategies in decreasing successful cyber attacks. Unfortunately, with only 18% of organizations utilizing ISACs, this means most are missing out on the most impactful CTI resource available.

Internal threat intelligence came in at a close second for performance, meaning that if organizations aren't already processing their internal data for CTI indicators, they probably should start doing so.

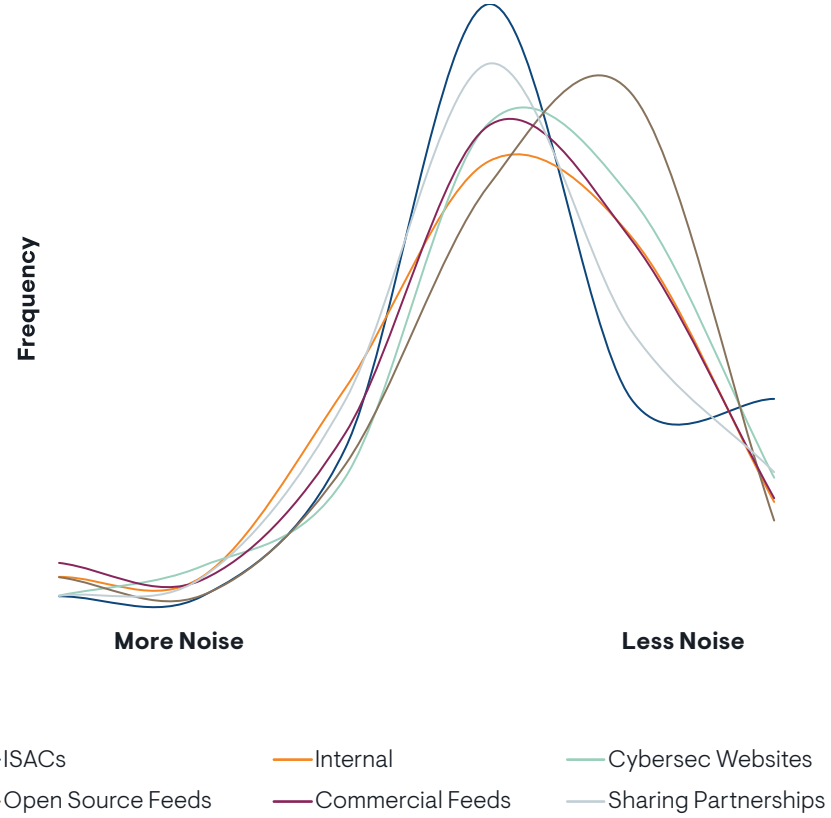


# How do CTI sources affect noise?

On average, ISACs, cybersecurity websites, and open source feeds appear to contain less noise than commercial feeds and internal sources, with ISACs providing the best data quality more often than other sources. Open source data feeds also presented a strong signal-to-noise ratio for most organizations, but came in last place for the highest data quality tier of less than 10% noise.

When looking at sources with less than 10% noise, ISACs outperformed all other sources and open source feeds outperformed all other sources at the 11% to 25% noise percentage tier.

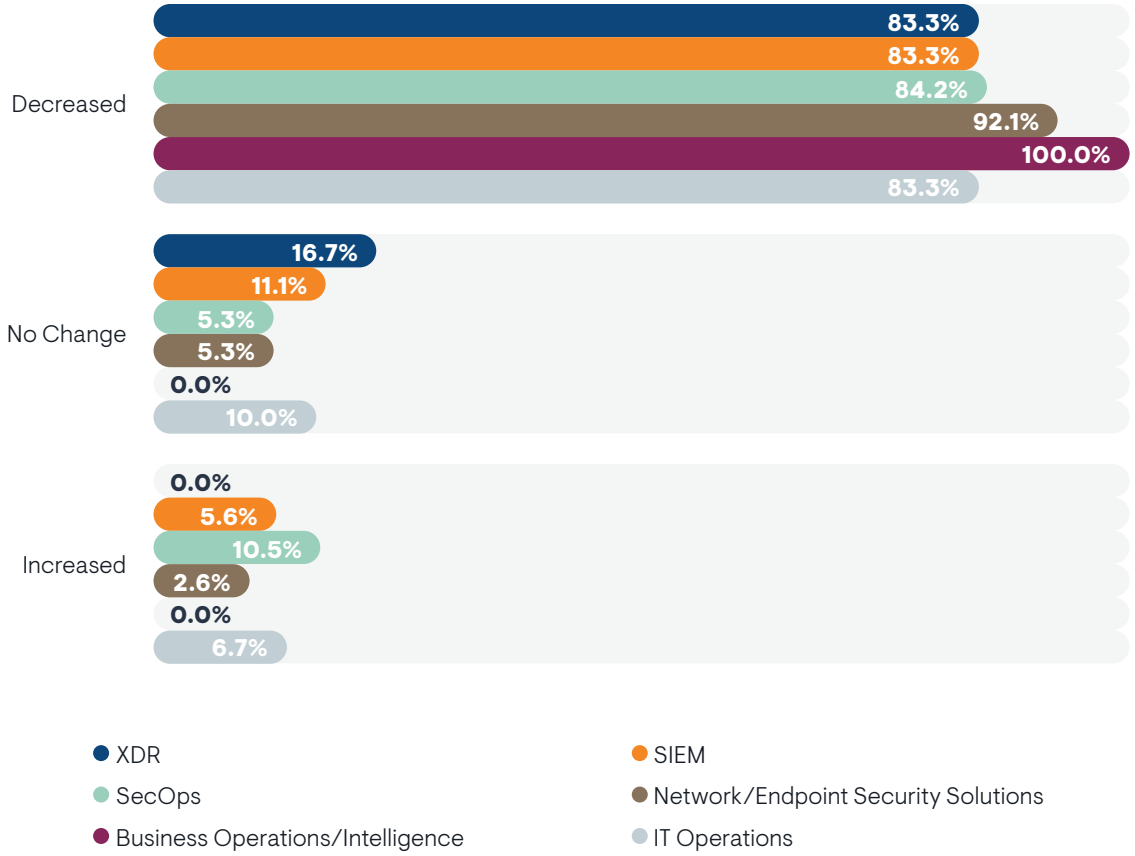
With only 18% of organizations utilizing ISACs, it's clear that this untapped resource could greatly help organizations with their CTI challenges.



# How do CTI integration priorities affect successful cyber attacks?

Integration of CTI with business operations/intelligence and network/endpoint solutions seems to be the most effective priority for reducing successful cyber attacks, with a slight advantage over other methods.

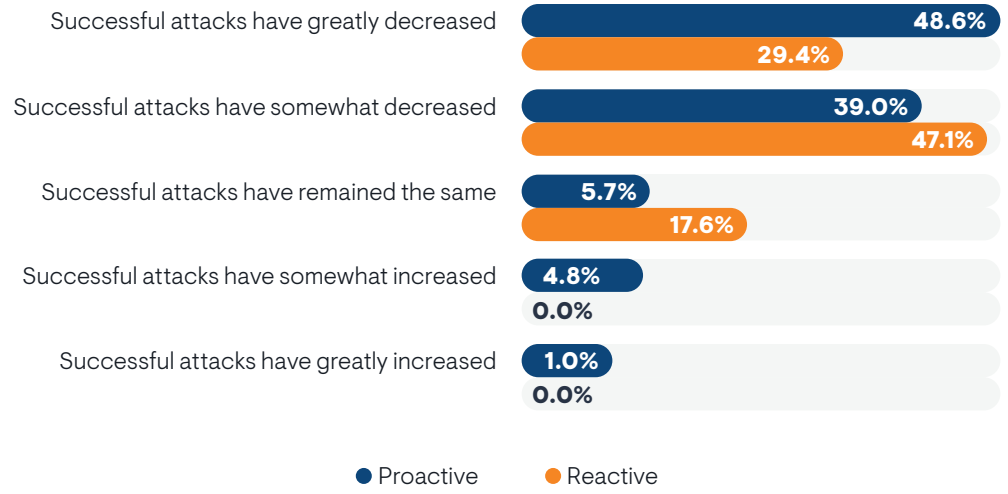
However, it should be noted that the performance of all priorities listed here should be considered acceptable, and extra consideration should be given to priorities that did not result in an increase of successful cyber attacks – namely, XDR and business operations/intelligence. Even more impressive, business intelligence integrations saw a decrease in successful cyber attacks for all organizations leveraging them.

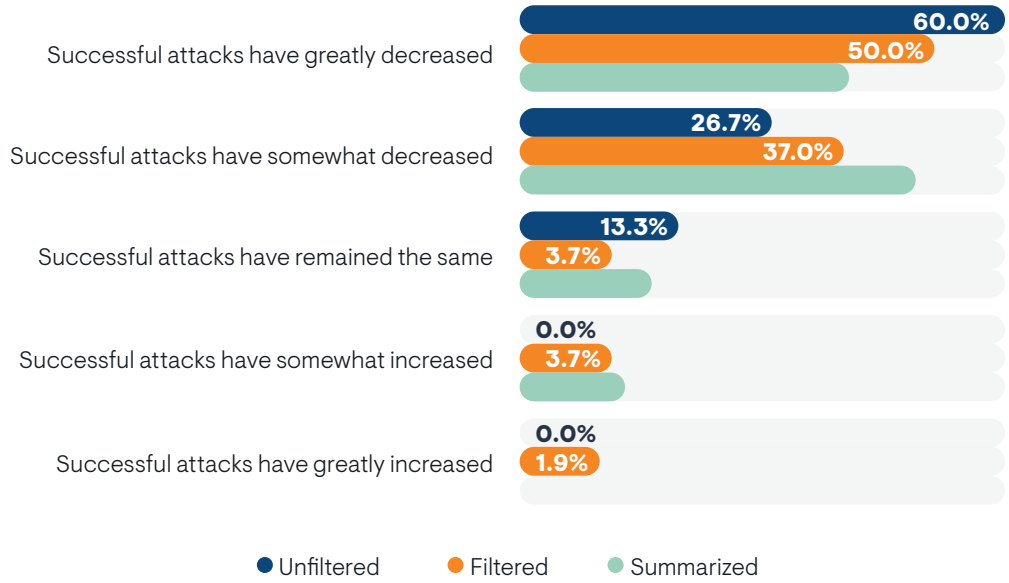


# How do CTI strategies affect successful cyber attacks?

From proactive vs. reactive usage of CTI data, proactive usage is a much more effective strategy than reactive usage. This is not surprising and falls in line with industry usage trends.

However, what is surprising is that the least-used data format, unfiltered data, provides the most effective protection against cyber attacks. This is concerning because only 12% of the industry uses unfiltered data as part of their CTI activities. The most likely explanation for this is that instead of trusting the data they receive, organizations over-filter data for relevance, resulting in sensors missing critical threat indicators.



# Enhancing CTI Platforms

Threats, data, integration, and time were the most common themes when examining user responses for how to better improve today's CTI platforms.

Many of these responses focused on quality of data, as well as the ability to integrate the data with existing tools in the environment, such as SIEM or XDR.

An interesting trend in the data is that a significant number of respondents want to see artificial intelligence become more common in threat intelligent platforms, helping process CTI more efficiently and effectively.

Overall, many respondents were very happy with their current CTI platforms and focused more on issues with the data being processed by those platforms.

# EMA Perspective

Cyber threat intelligence has been around for a long time in the industry, and it's very surprising that after several decades, organizations still struggle with effectively leveraging this critical cybersecurity tool.

After reviewing the data, EMA believes that a significant shift in industry practices concerning CTI is needed. While it is good that CTI data is used to proactively block threat indicators, such as file hashes, IP addresses, or malicious emails and domains, data sources and integration priorities must shift.

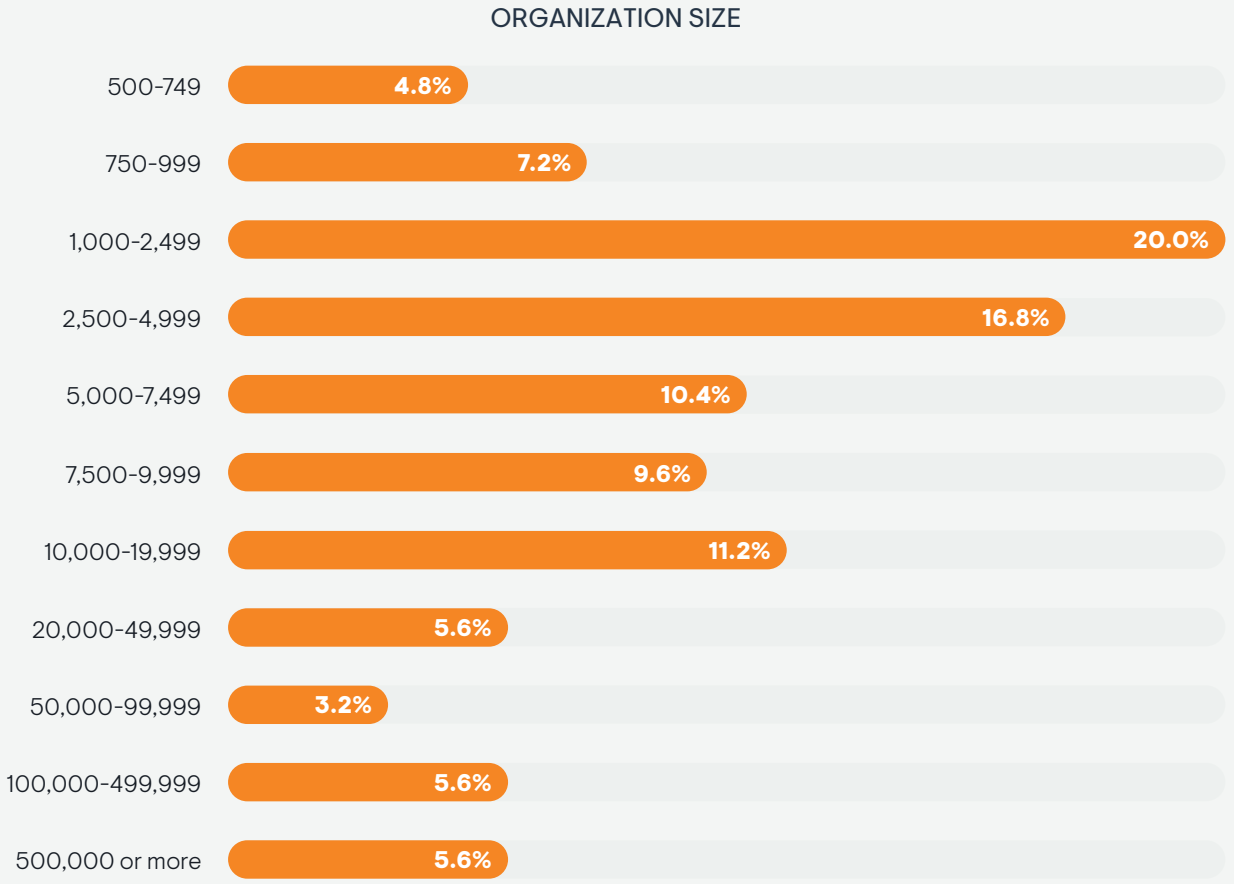
With usage by only 18% of the industry but a decrease of successful cyber attacks in 96% of those that utilize it, ISAC adoption should be increased across the board. Ideally, CTI platforms should have the ability to connect to and automatically share or consume CTI data within the ISAC.

Maintaining integration with network and endpoint solutions should remain a high priority for organizations due to its effectiveness, but integration with XDR and business intelligence tools should also be a higher priority than what is currently established due to the clear return on investment in utilizing these tools. XDR and business intelligence can provide additional insights regarding CTI that other tools might not.

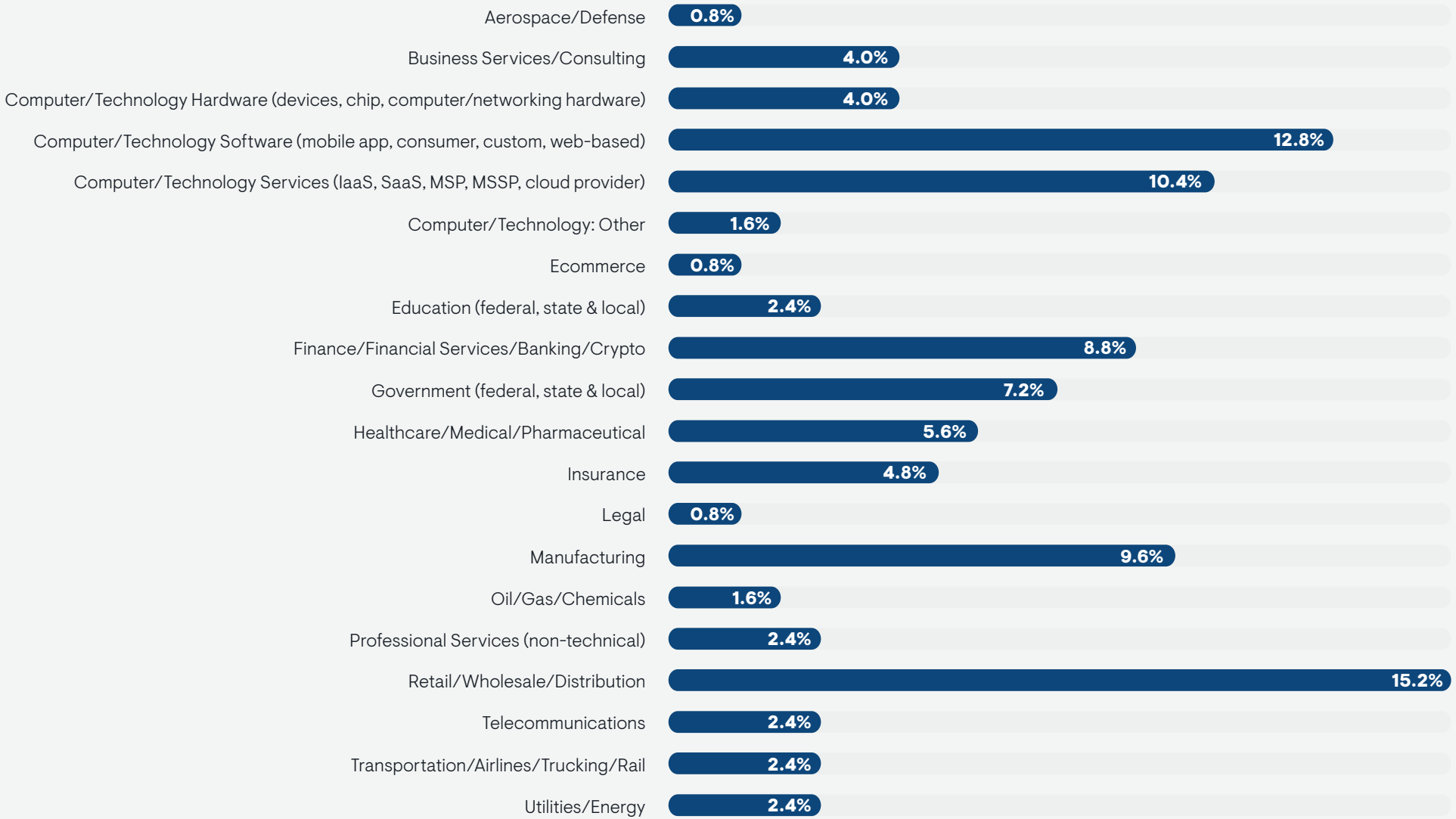
Finally, the most important takeaway from this research is that organizations need to stop filtering their CTI data and trust the data to be relevant to their organization. The problem with filtering data is that it assumes your organization knows everything in their environment. The harsh reality is that shadow IT is still a problem, even in 2023, and attackers aren't going to ignore vulnerable assets simply because they're not on your asset list.

CTI can be a powerful tool when properly leveraged and integrated with organizations' environments. By adjusting how they utilize CTI, organizations can realize a better return on investment in these tools.

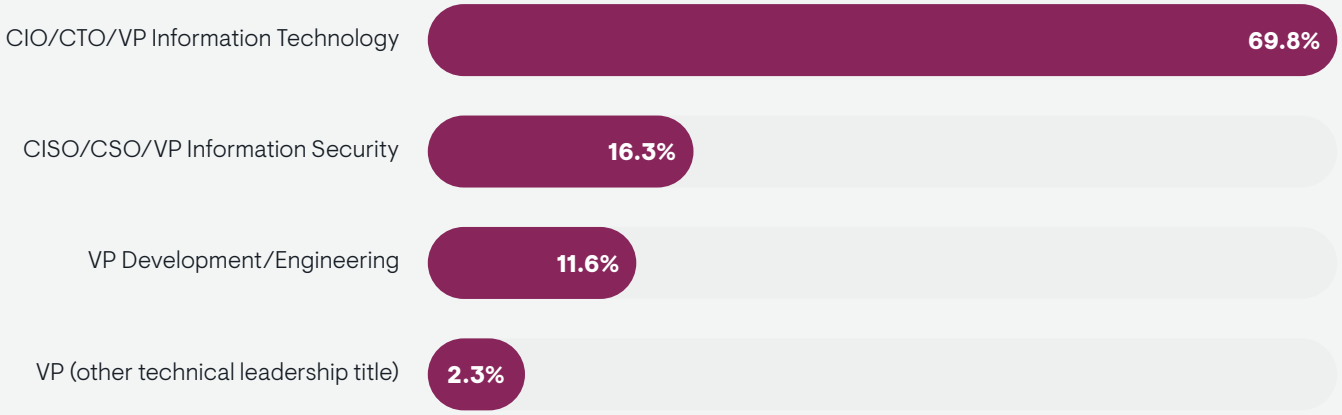
# Demographics


ORGANIZATION SIZE
500-749
4.8%
750-999
7.2%
1,000-2,499
20.0%
2,500-4,999
16.8%
5,000-7,499
10.4%
7,500-9,999
9.6%
10,000-19,999
11.2%
20,000-49,999
5.6%
50,000-99,999
3.2%
100,000-499,999
5.6%
500,000 or more
5.6%

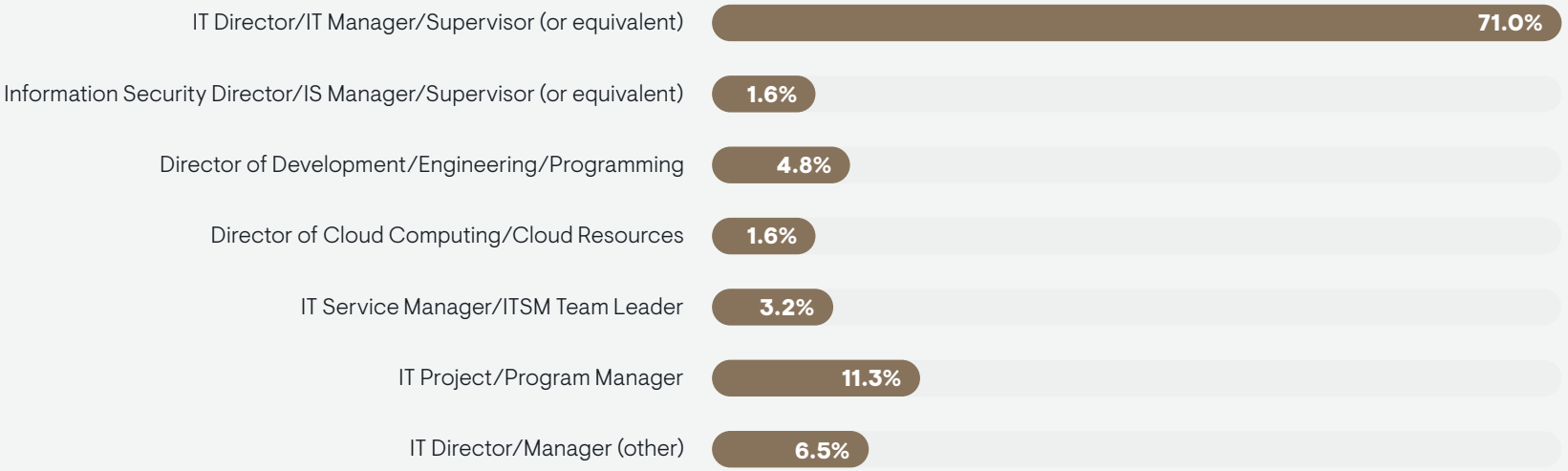
## PRIMARY INDUSTRY



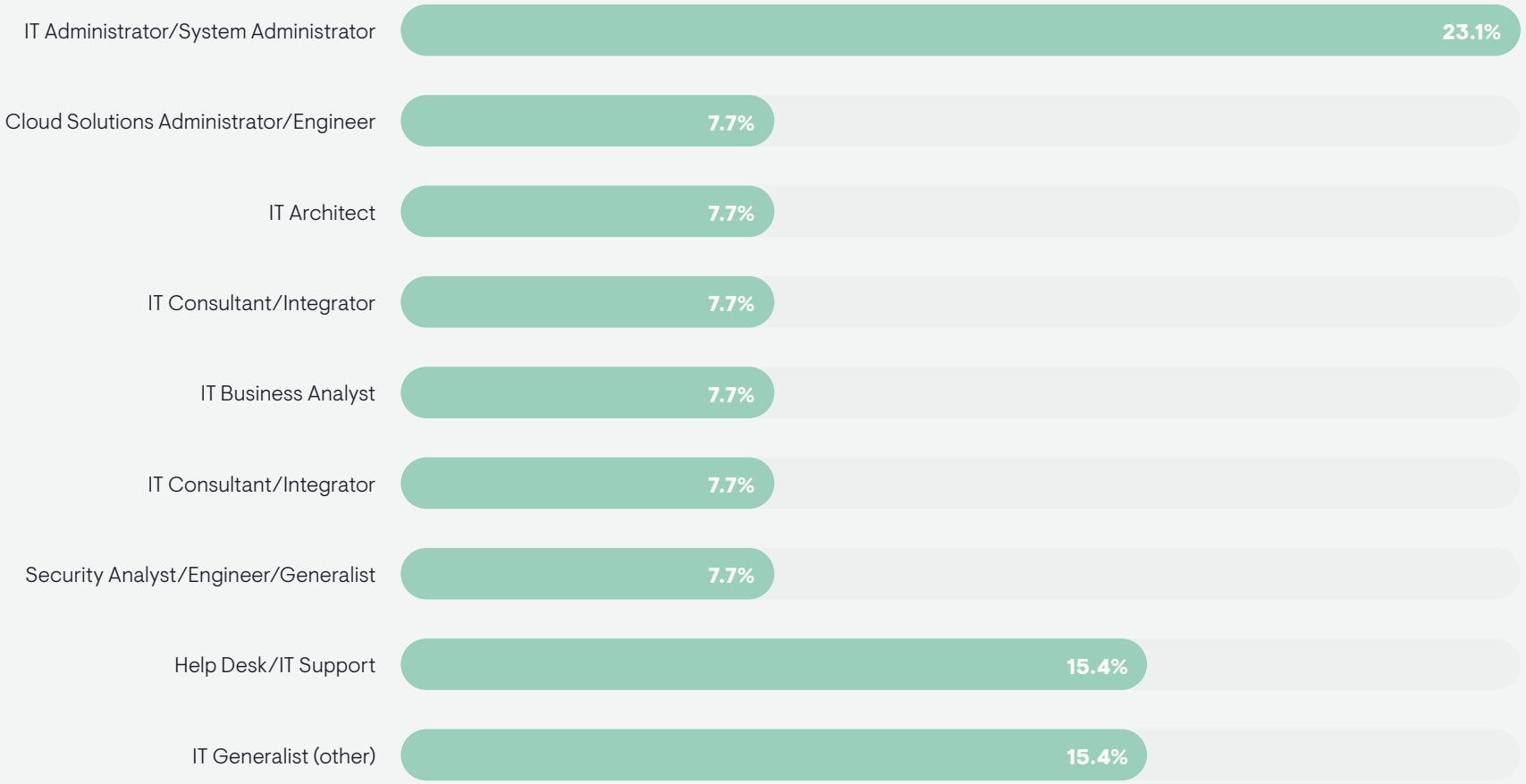
## EXECUTIVE ROLES




## DIRECTOR/MANAGER ROLES

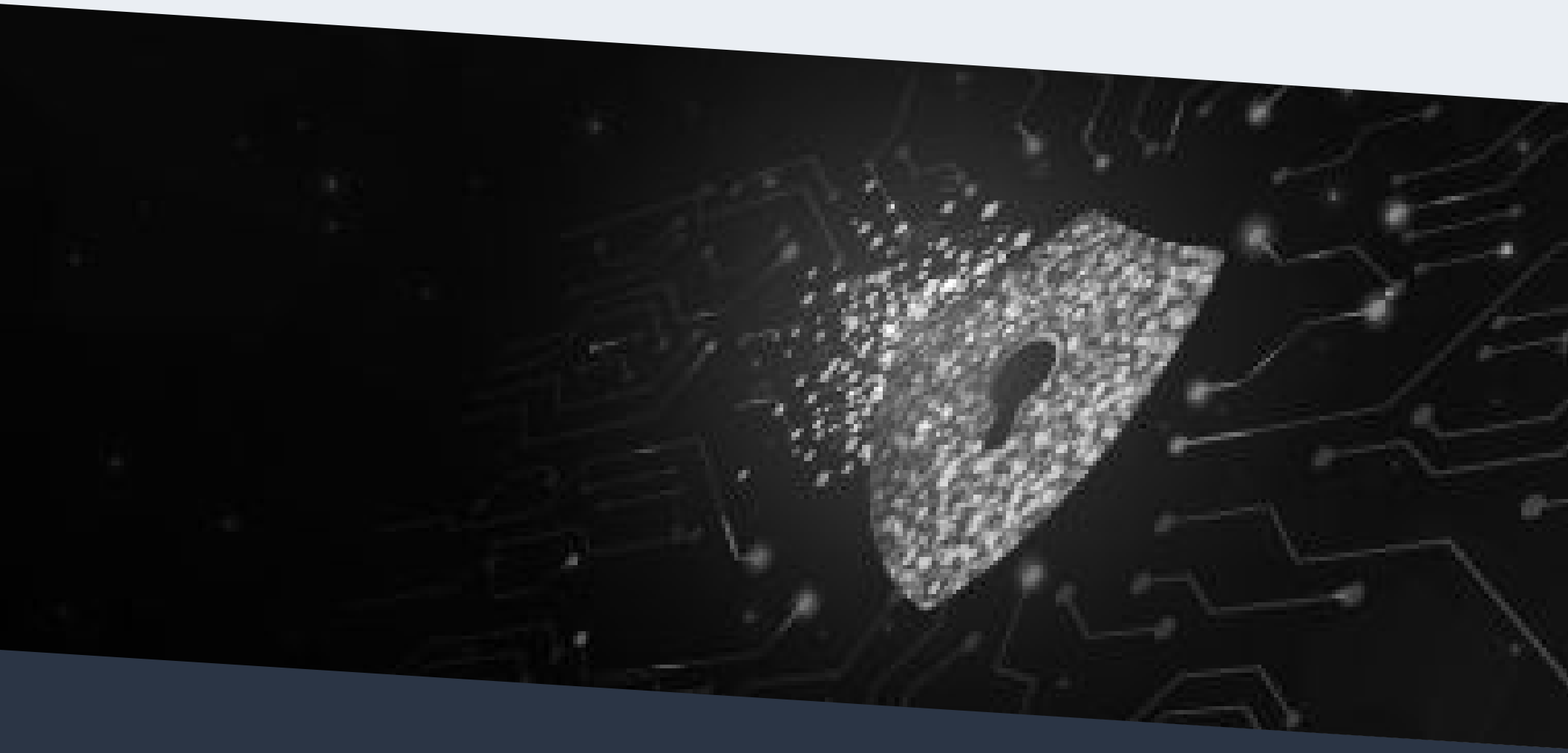


## PRACTITIONER ROLES




## Anomali

Anomali is the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. Anchored by big data management and refined by artificial intelligence, the Anomali XDR platform delivers proprietary capabilities that correlate the largest repository of global intelligence with telemetry from customer-deployed security solutions, empowering security operations teams to detect threats with precision, optimize response, achieve resiliency, and stop attackers and breaches. Our SaaS-based solutions easily integrate into existing security tech stacks through native cloud, multi-cloud, on-premises, and hybrid deployments. Founded in 2013, Anomali serves public and private sector organizations, ISACs, MSSPs, and Global 1000 customers around the world in every major industry. Leading venture firms including General Catalyst, Google Ventures, and IVP back Anomali. Learn more at **https://www.anomali.com/**.



## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com. You can also follow EMA on Twitter or LinkedIn.



2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com

4264.040623