Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH INSIGHTS REPORT

The XDR Payoff: Better Security Posture

Organizations that aggregate, correlate, and analyze signals across multiple security controls experience fewer successful attacks, have a better overall security posture, and live with less daily stress on their teams.

By Dave Gruber, Senior Analyst
Adam DeMattia, Director of Research

September 2020

This ESG Research Insights Report was commissioned by Trend Micro and is distributed under license from ESG.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Executive Summary

The advent of cross-controls detection and response (known as XDR) creates a new opportunity for security teams to gain leverage. Building on the learnings from endpoint detection and response (EDR), XDR analyzes security telemetry across endpoint, network, email, and cloud security controls to provide broader visibility in modern, complex attacks. XDR further promises efficiency gains, helping more junior security analysts address a larger percentage of attacks without escalation to limited, senior security resources.

As the XDR movement gains momentum, organizations are hungry to understand and quantify how and why XDR can make a difference to rationalize investments. To answer this question, Trend Micro and ESG recently completed a research study to identify organizations utilizing techniques similar to those that XDR solutions bring to the table. These techniques include automating the aggregation, correlation, and analysis of security data across multiple security controls to detect and respond to modern threats. The research identifies specific positive business outcomes achieved by these organizations and explores related outcomes for organizations that are not following these practices.

Going into the research, we hypothesized that organizations that had invested in XDR-like automation techniques would see improved outcomes, including faster identification of complex attacks, improved response times, more efficient use of security personnel, and an overall improvement in security posture. All of our hypothesis proved to be true. Security organizations that have already invested in operationalizing the aggregation, correlation, and analysis of signals across multiple security controls generally believe that they experience fewer successful attacks, have a better overall security posture, and live with less daily stress on their teams. These same organizations say that they are able to investigate and respond to threats faster, and ignore significantly fewer alerts.

Security organizations that have already invested in aggregation, correlation, and analysis of signals across multiple security controls experience fewer successful attacks, have a better overall security posture, and live with less daily stress on their teams.

Siloed data is the norm for most organizations, with 41% reporting highly or mostly fragmented data and 61% reporting manual approaches to integrating and aggregating data from various security controls. While many organizations are attempting to combat these silos by implementing a SIEM, more than half say they are frustrated with the level of complexity, redundancy, and expert resources required to operate their SIEM.

When we asked those who have invested most significantly in automating aggregation, correlation, and analytics *how many full-time equivalent (FTE) people it would take to replace their automated systems*, organizations reported an average of 8 FTEs, which, for most, translates into an untenable additional investment. When we looked at organizations that have not yet invested in automated aggregation, correlation, and analytics, we found that those organizations ignored nearly twice the number of alerts as those who have invested, effectively creating a blind spot and ongoing unknown/unaddressed risk.

Full-time equivalent people needed to replace XDR.
8
FTEs

XDR promises a new approach to automating the ongoing aggregation, correlation, and analysis of security data, delivering increased fidelity and efficiency for security teams that are struggling to keep up with the rapidly expanding and complex threat landscape. With no end in sight for the skills

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

shortage and accelerating timelines for digital transformation initiatives, security teams need a force multiplier now more than ever.

The remainder of this paper outlines the specific research data and associated conclusions. As XDR solutions become more widely adopted, specific metrics and outcomes will become available to further validate our findings.

Current Situation

Security teams are facing unprecedented change. Five key macro-trends are influencing this change:

- The threat landscape continues to become more sophisticated as adversaries work to evade security controls.
- The attack surface in most organizations is rapidly expanding, with more diversity in device types than ever before.
- While defense-in-depth approaches have proven to provide robust security, the proliferation of individual security controls is producing massive amounts of alerts, telemetry, and noise, making it challenging for security teams to triage and prioritize where to focus.
- A worldwide skills shortage of experienced, knowledgeable security analysts continues to leave many organizations absent of the people and skills needed to keep up.
- The recent global COVID-19 coronavirus pandemic has accelerated digital transformation initiatives, requiring further unplanned investments in additional security controls.

These five macro-trends have pushed security teams to a near breaking point. Modern security teams need to gain leverage to keep up. XDR creates a new opportunity to acquire this leverage.

Introducing XDR

XDR is the next step in the evolution of detection and response automation. It builds on the proven concepts that come from endpoint detection and response (EDR) solutions, enabling security analysts to detect and respond to threats that make it past traditional security controls. Different from EDR offerings, XDR solutions come preassembled to ingest security telemetry from multiple security controls, correlating and analyzing signals to identify and isolate threats. XDR removes much of the “heavy lifting” that was required to assemble this data in SIEMs and data lakes, allowing security teams to focus on detection and investigation instead of building and managing custom aggregation and analysis tools.

While formal XDR offerings are relatively new to the market, the concepts that they are built upon are proven and have been in practice for many years, utilized by some of the most mature, effective security teams. XDR creates an opportunity to deliver a new level of automation and fidelity to security teams that are struggling to keep up with the rapidly expanding threat landscape.

The Road to XDR: Why EDR Has Become a Mainstay for Most Security Teams

Security architects work tirelessly to assemble and maintain a collection of security controls aimed to protect data, applications, and infrastructure. Defense-in-depth strategies have become commonplace for many organizations, depending on “best-of-breed,” standalone security controls for each element of the infrastructure. While this approach has proven sound for many, it creates additional challenges for other organizations, including silos of uncorrelated security data and an overwhelming amount of security alerts that require triage and investigation.

While early detection efforts primarily leveraged network telemetry to monitor for anomalous behaviors, forensic teams still needed to access endpoint data to understand the impact and methods of attacks. This realization precipitated the invention of endpoint detection and response (EDR) tools that could gather historical endpoint telemetry, allowing investigators to recreate or “roll back the tape” to see and investigate prior attacks. Endpoint detection and response offered a new level of visibility previously unavailable through traditional network analysis techniques.

While EDR tools were initially used for forensics analysis, security teams realized that primary security controls such as antivirus, firewalls, email security, and others have logical limits to their abilities to prevent attacks, resulting in the success of tiny portions of attacks to compromise infrastructure. This realization led security teams to adopt a “prevent what you can and detect and respond to what you cannot” approach, catapulting EDR into a mainstream component for the modern SOC.

As attacks have become more sophisticated, even EDR solutions lack sufficient context into ATPs and other stealthy attacks. Mature, well-funded security teams have overcome this challenge by aggregating and correlating security telemetry from multiple security controls, combined with advanced analytics, to provide rapid, high-fidelity visibility into modern attacks. Our research demonstrates that those organizations that have employed this approach experience fewer successful attacks, respond to threats faster, and ignore fewer alerts. While this approach has shown superior results, these practices often involved significant time, money, and specialized talent to aggregate, integrate, and analyze signals from across the many security controls employed to protect data, applications, and infrastructure. For these reasons, only elite security teams have been able to implement this approach successfully.

But Isn’t That What a SIEM Is All About?

For the past five years, organizations have attempted to utilize their SIEM to perform a similar function. The idea has been to ingest logs and as much security telemetry into the SIEM as possible, and then to layer on rules to uncover, investigate, and respond to threats. Yet, all too often, SIEMs struggle to effectively correlate events, leaving this process to the security analysts as they piece together attack signals.

While SIEMs are widely adopted, ESG research shows that few organizations feel that their SIEM has delivered on this promise, and most feel that too many expert resources are required to both implement and utilize a SIEM effectively for day-to-day security operations. That said, most believe that the SIEM has improved their organization’s ability to investigate threats. Those organizations that have invested heavily in building custom rules, customizing data ingest, and adding analytics report the most significant advances in their security posture. However, those same organizations also report that specially trained experts are required to achieve these results.

Understanding the Value of XDR

Because XDR is a relatively new solution category, ESG’s research team utilized a technology alignment approach to identify and quantify how and where XDR brings value. The specific objective of the research was to identify organizations that are already utilizing technology automation that closely aligns with XDR, in an effort to assess specific benefits, in contrast to organizations that do not.

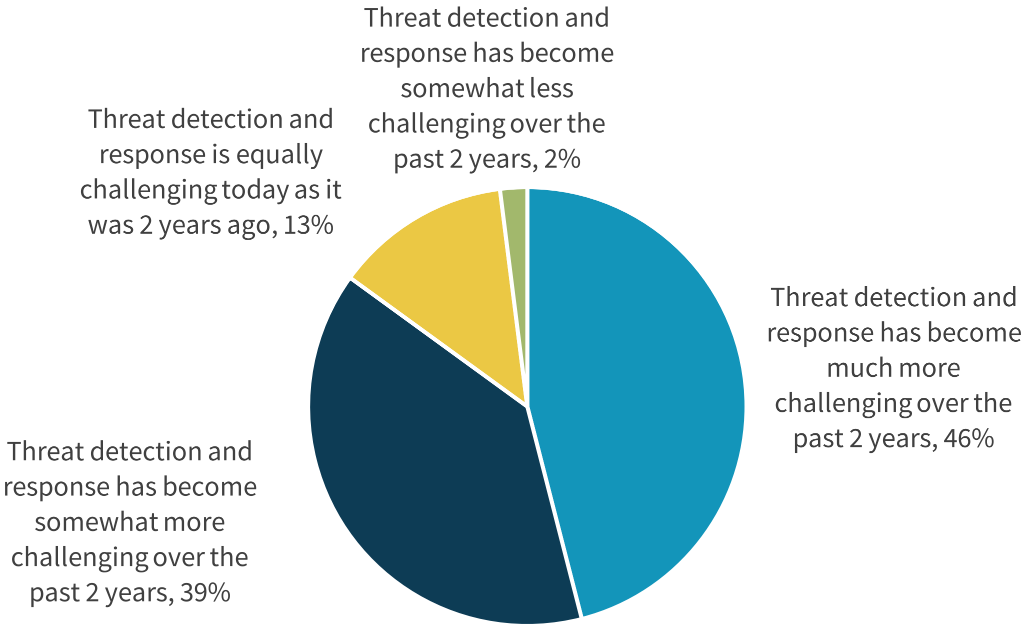
500 respondents were surveyed across multiple industries in North America during the summer of 2020 to understand current approaches to detection and response, including investment in various types of automation.

From our research, we learned that 85% of organizations say that threat detection and response (TDR) is getting harder (see Figure 1). Additionally, 81% say that improving TDR is a high priority toward which they have allocated funding in 2020.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 1. TDR Has Become More Challenging

Which of the following statements best characterizes your opinion about threat detection and response? (Percent of respondents, N=500)



Source: Enterprise Strategy Group

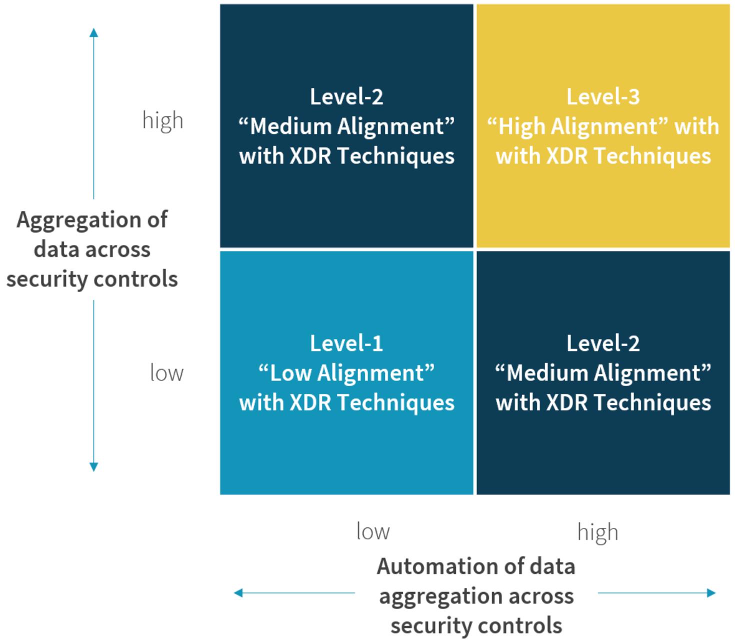
Fifty-seven percent of respondents say that one of the primary challenges that they are facing is that the threat landscape is getting exponentially more sophisticated, while 41% believe that the complexity of their overall security stack is overwhelming. Finding enough skilled resources further continues to plague 39% of organizations.

Organizations Aligning with XDR Approaches Report Better Overall Security Posture

ESG research began by creating a model to assess the value that organizations realize when implementing similar approaches to XDR. The goal was to establish three cohorts that would represent levels of alignment, with level-3 representing those companies that were most aligned with XDR techniques. As we see from the model in Figure 2, our assessment was based on two dimensions: first, the level of aggregation and correlation across multiple security controls; and second, the level of automation that has been applied to this process.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 2. ESG's XDR Value Assessment Model


high
Aggregation of data across security controls
low
Level-2 "Medium Alignment" with XDR Techniques
Level-3 "High Alignment" with with XDR Techniques
Level-1 "Low Alignment" with XDR Techniques
Level-2 "Medium Alignment" with XDR Techniques
low
high
Automation of data aggregation across security controls

Respondents were placed into one of three stages of alignment, based on their responses to 2 questions, the inputs:

1. How would you describe the information/data in your organization's various security, threat detection, and response controls?

   Siloed ← → Single source of truth

2. How would you describe the process of integrating and aggregating data from your organization's various security, threat detection, and response controls?

   Manual ← → Automated

ESG employed this characteristic-based system as a proxy for XDR.

Source: Enterprise Strategy Group

As demonstrated in Figure 3, our highest level of XDR alignment was seen in 21% of organizations, which are already aggregating, correlating, and analyzing data from across security controls in a highly automated way.

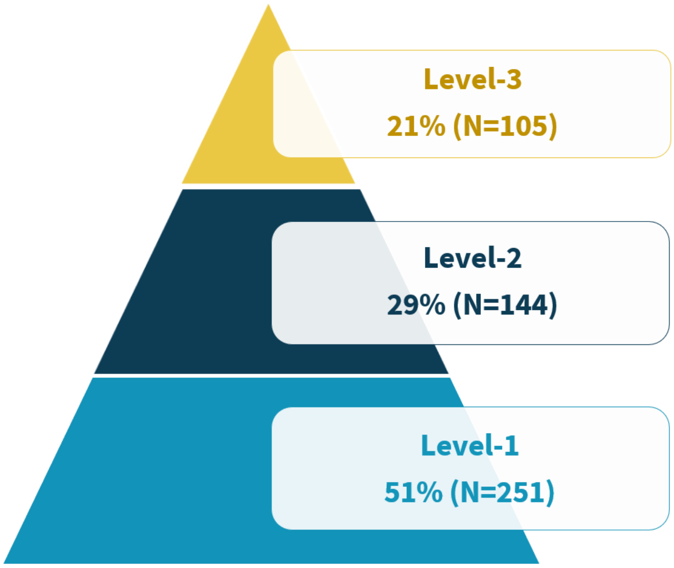
Figure 3. XDR Alignment Maturity Model Distribution

Based on responses, ESG observed the following distribution of organizations. It is important to note the distribution **is consistent across company sizes**:

Level-3 (High Level of Alignment):
- Aggregate data from across controls in an automated way
- 21% of the market today

Level-2 (Medium Level of Alignment):
- Mostly siloed data across security controls with some automated aggregation processes **OR**
- Aggregated data across security controls, but with many manual processes
- 29% of the market today

Level-1 (Low Level of Alignment):
- Mostly/completely siloed data in TDR controls with only manual data aggregation
- 50% of the market today

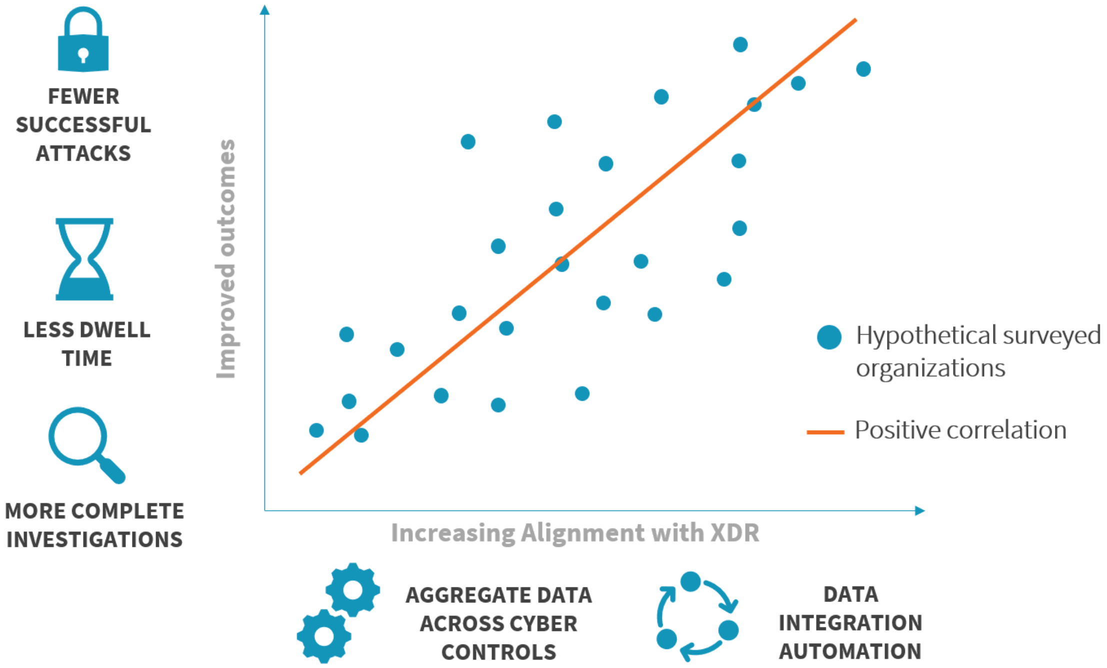


Source: Enterprise Strategy Group

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Our hypothesis going into the survey was that organizations with more automated aggregation, correlation, and analysis of security data would experience less dwell time and fewer successful attacks.

Figure 4. ESG's XDR Alignment Maturity Hypothesis Visualized


FEWER SUCCESSFUL ATTACKS
LESS DWELL TIME
MORE COMPLETE INVESTIGATIONS
Improved outcomes
Increasing Alignment with XDR
● Hypothetical surveyed organizations
Positive correlation
AGGREGATE DATA ACROSS CYBER CONTROLS
DATA INTEGRATION AUTOMATION

Source: Enterprise Strategy Group

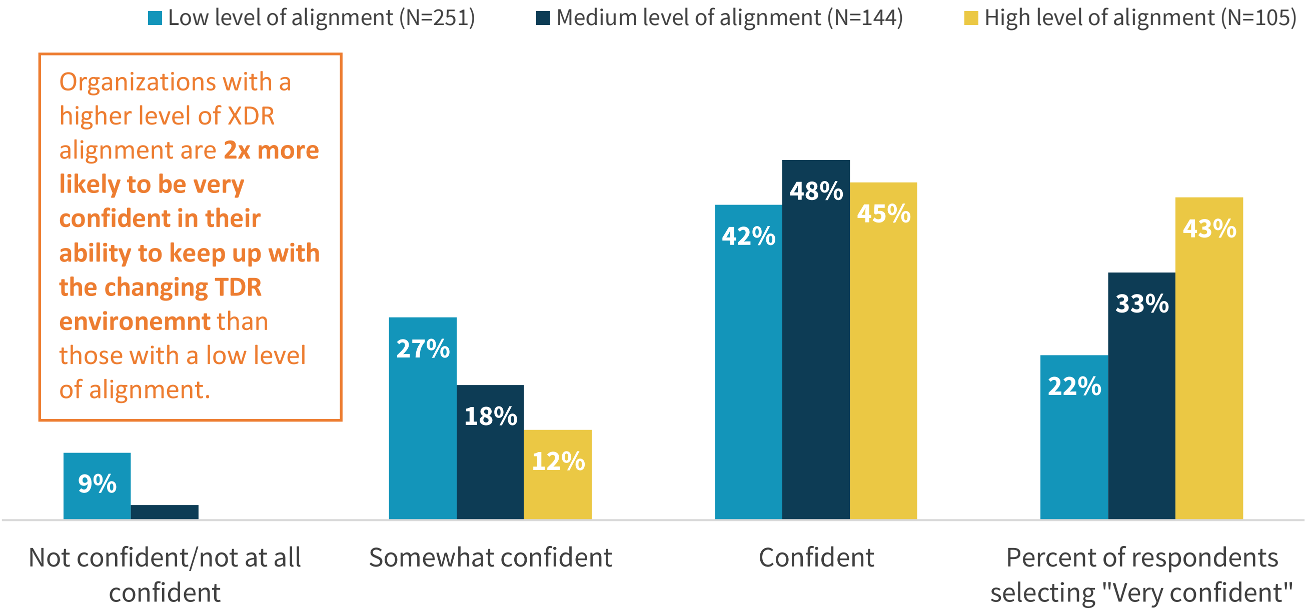
Level-3 Organizations Experienced Half as Many Successful Attacks

As suspected, level-3 organizations with high levels of alignment to XDR reported experiencing significantly fewer successful attacks. They also felt like they were holding their own in the TDR battle, and that they are stretched less thin than level-1 and level-2 organizations. Level-3 organizations also felt that data correlation across multiple security controls is more effective, driving numerous operational and security advantages.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 5. Higher Alignment Means More Confidence in the TDR Function

Thinking of the next 12-24 months, how confident are you that your organization's detection and response function can move at the speed needed to keep pace with threats and not negatively impact the business?



Organizations with a higher level of XDR alignment are **2x more likely to be very confident in their ability to keep up with the changing TDR environemnt** than those with a low level of alignment.

Source: Enterprise Strategy Group

Quantitatively speaking, level-3 organizations with high levels of alignment to XDR experienced only half as many successful attacks over the past 12 months. When asked how many full-time equivalent (FTE) people it would take to replace their automated systems, organizations reported an average of 8 FTEs, which is an untenable additional investment for most organizations. Further, Level-1 orgs said that they ignore nearly twice the number of alerts as level-3 organizations, effectively creating a blind spot and ongoing unknown/unaddressed risk.

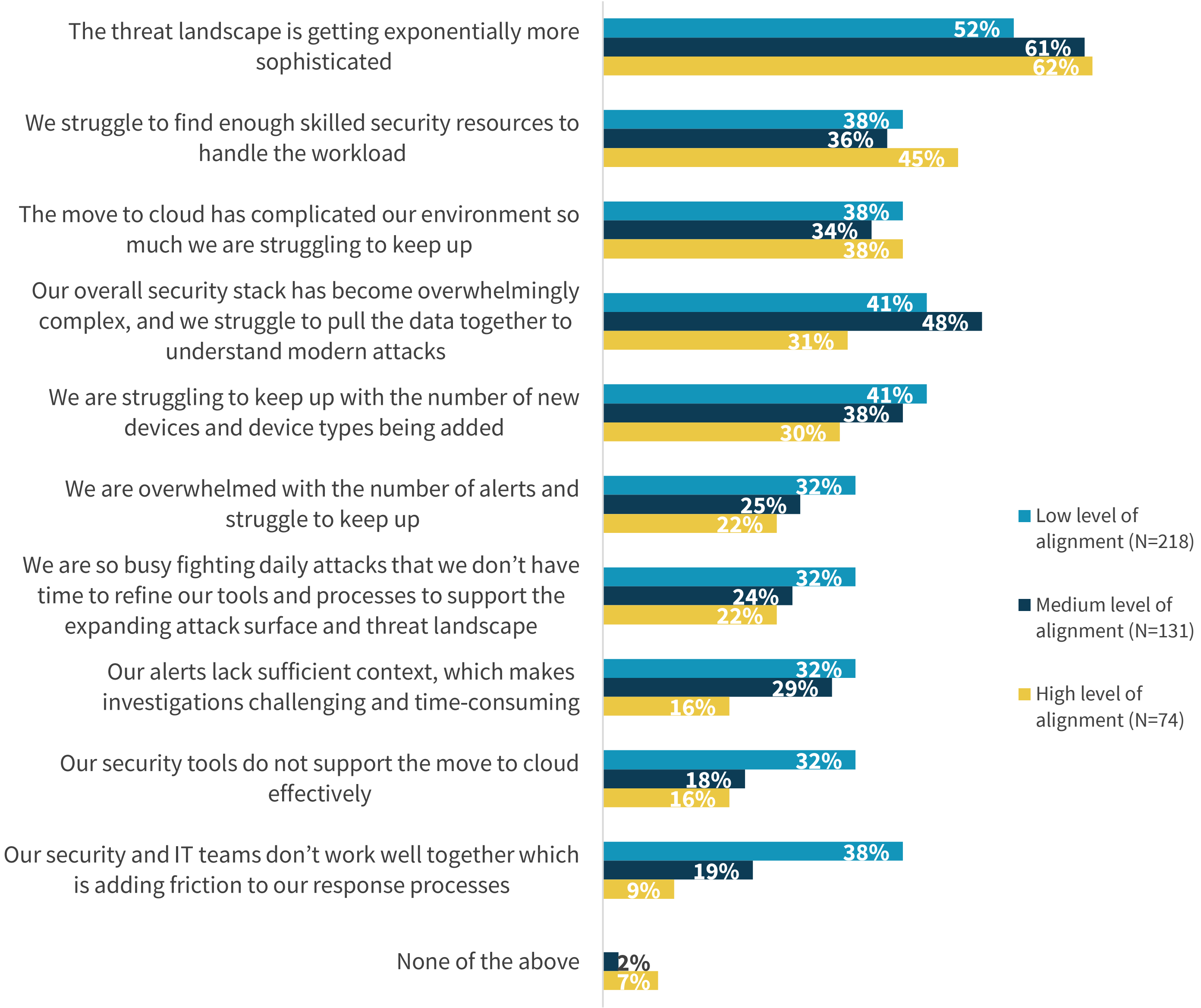
When asked how many full-time equivalent (FTE) people it would take to replace their automated systems, organizations reported an average of 8 FTEs.

Note that the sophistication of the threat landscape was the most-cited primary challenge regarding TDR for all levels of organizations surveyed; level-1 organizations reported struggling more than their counterparts with keeping up with new devices, cloud applications, and the number of alerts and lack of alert context (see Figure 6).

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 6. Those in Alignment Struggle Less with Operational Challenges

You indicated that threat detection and response has become more challenging over the past two years. Which of the following are the primary challenges your organization is facing regarding threat detection and response? (Percent of respondents)



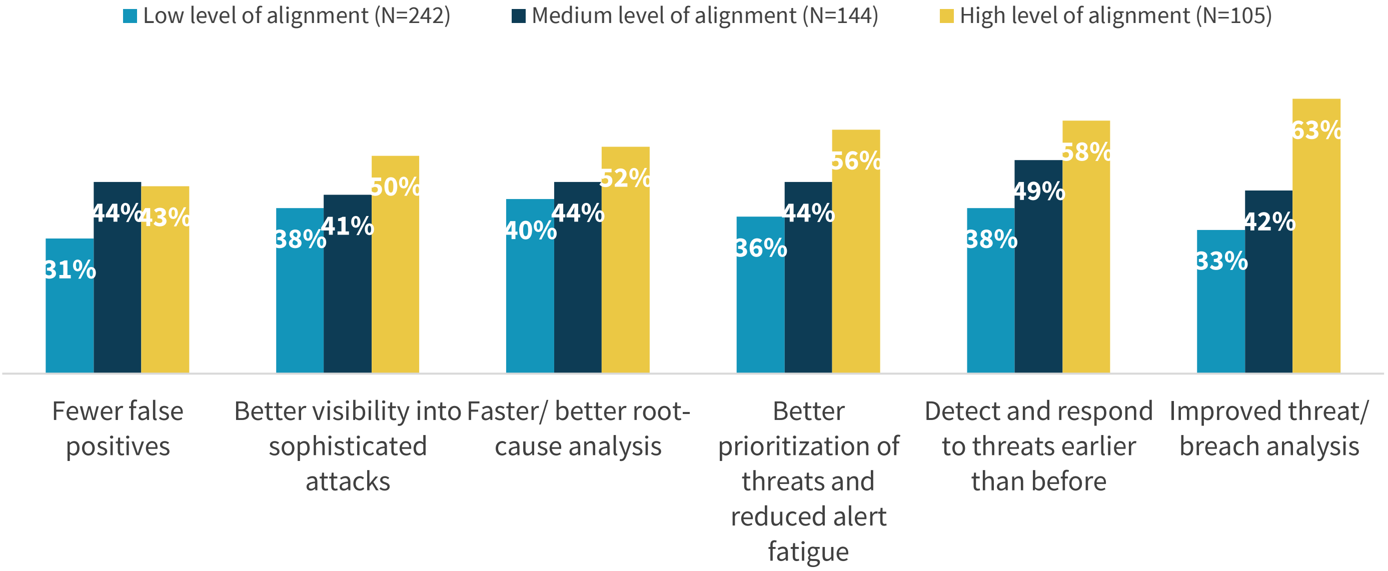
Source: Enterprise Strategy Group

As we explored specific areas of improvement, we saw that level-3 organizations with high levels of alignment to XDR achieved better results almost entirely across all areas, with significant improvement in threat/breach analysis, prioritization of threats and alert fatigue, visibility into sophisticated attacks, and detection and response times. Also notable was the fact that level-2 organizations consistently performed better than level-1 orgs as well.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 7. Organizations in Higher Alignment Are More Likely to Achieve Greater Improvements

You indicated your organization is at least somewhat effective correlating threat data for detection/response. Have you achieved any of the following security improvements as a result? (Percent of respondents, "Yes, significant improvement achieved")



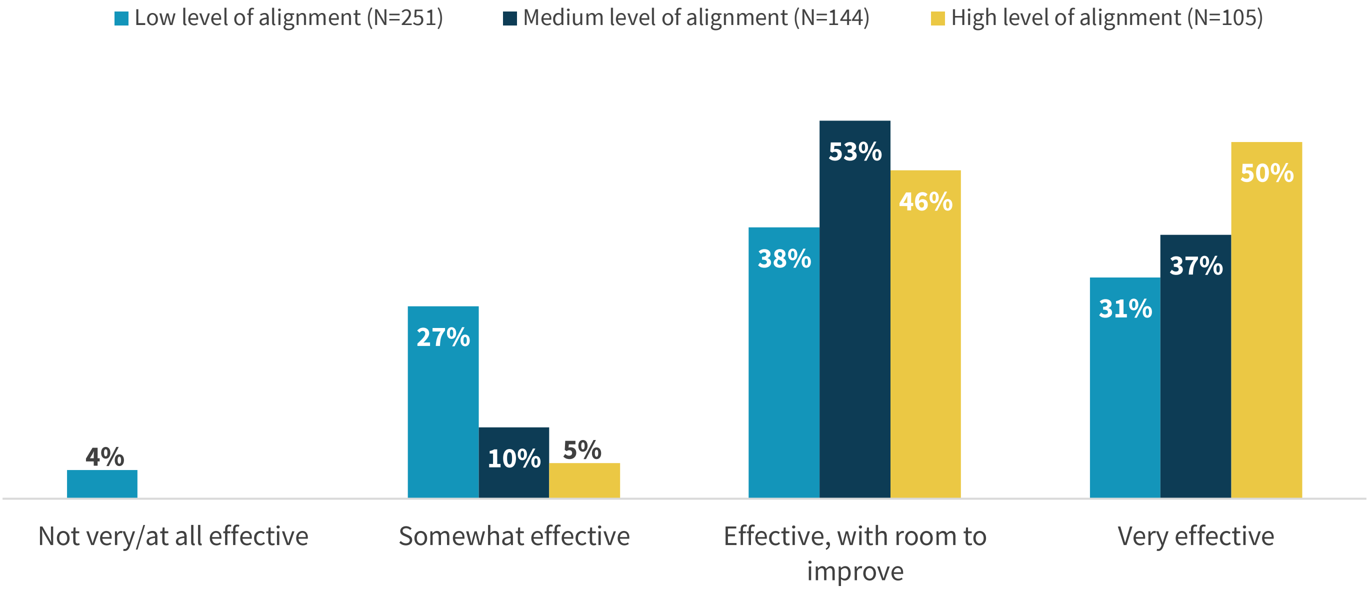
Source: Enterprise Strategy Group

Better Correlation = Better Results

Level-3 organizations with high levels of alignment to XDR are 61% more likely to be very effective at correlating data from different security controls than level-1 and level-2 orgs, with 50% of level-3 orgs reporting that they are very effective (see Figure 8). Even with those results, 63% of all respondents say that they can see room for improvement in overall data correlation (see Figure 9). The quest to sharpen detection of modern complex attacks requires an ongoing investment in correlation rules for most, even when automation is applied. Many new XDR solutions promise to close this gap through continuous, automated rules refinement based on extensive, ongoing threat intelligence provided by the solution provider.

Figure 8. Threat Data Correlation Effectiveness, by Alignment Level

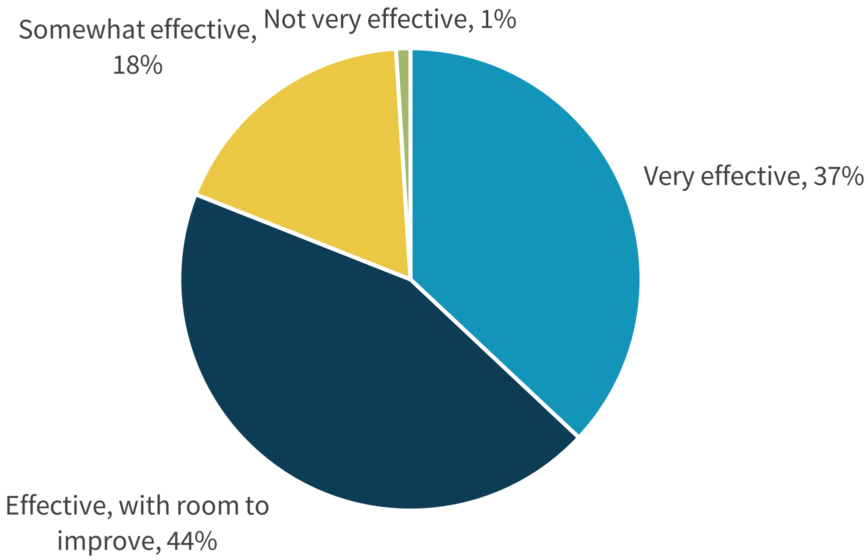
How effective is your organization at correlating threat data from different security controls to improve threat detection and response? (Percent of respondents)



Source: Enterprise Strategy Group

Figure 9. Threat Data Correlation Effectiveness, All Respondents

How effective is your organization at correlating threat data from different security controls to improve threat detection and response? (Percent of respondents, N=500)

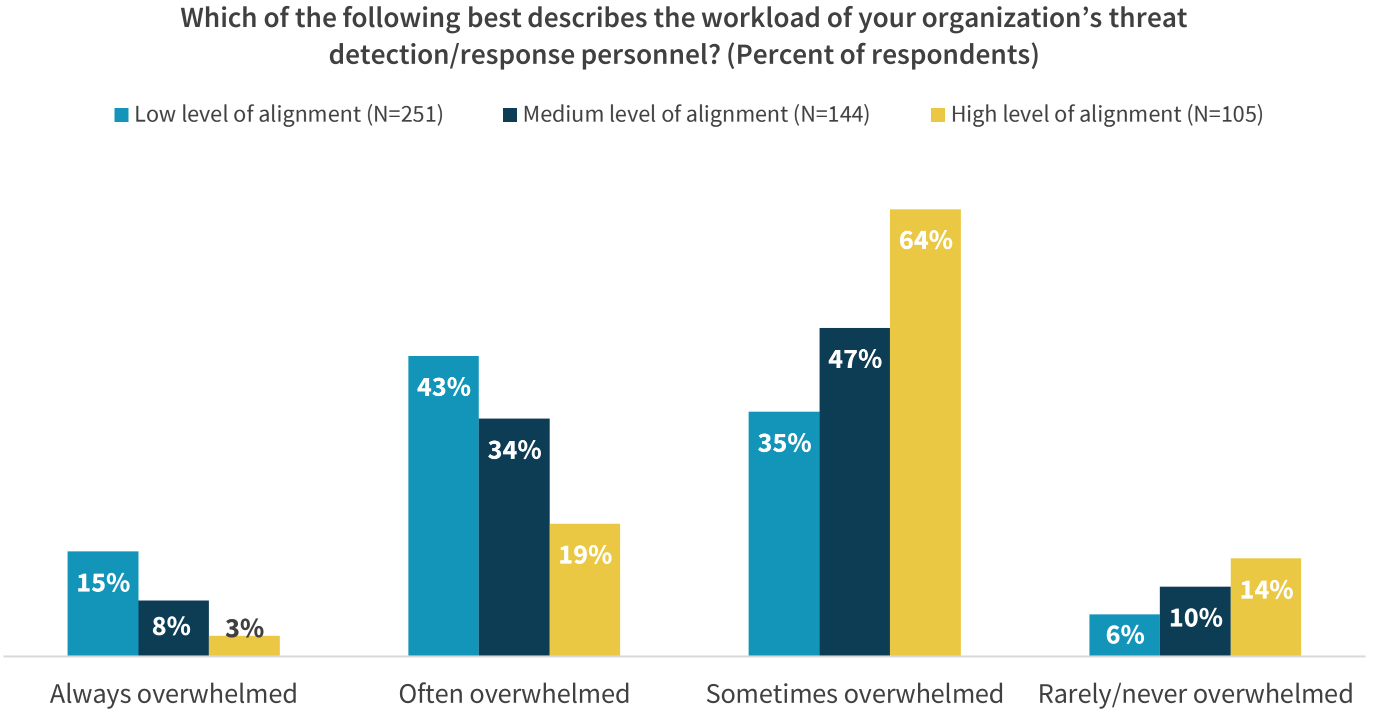


Source: Enterprise Strategy Group

Lower alignment, level-1 orgs are 2.6x more likely than level-3 orgs to describe their detection and response teams as always or often overwhelmed (see Figure 10). Manually correlating data is both time-consuming and labor-intensive, leaving level-1 analysts with less time to focus on true threat investigation. This hurts teams already facing skills shortages, stressing them even more.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

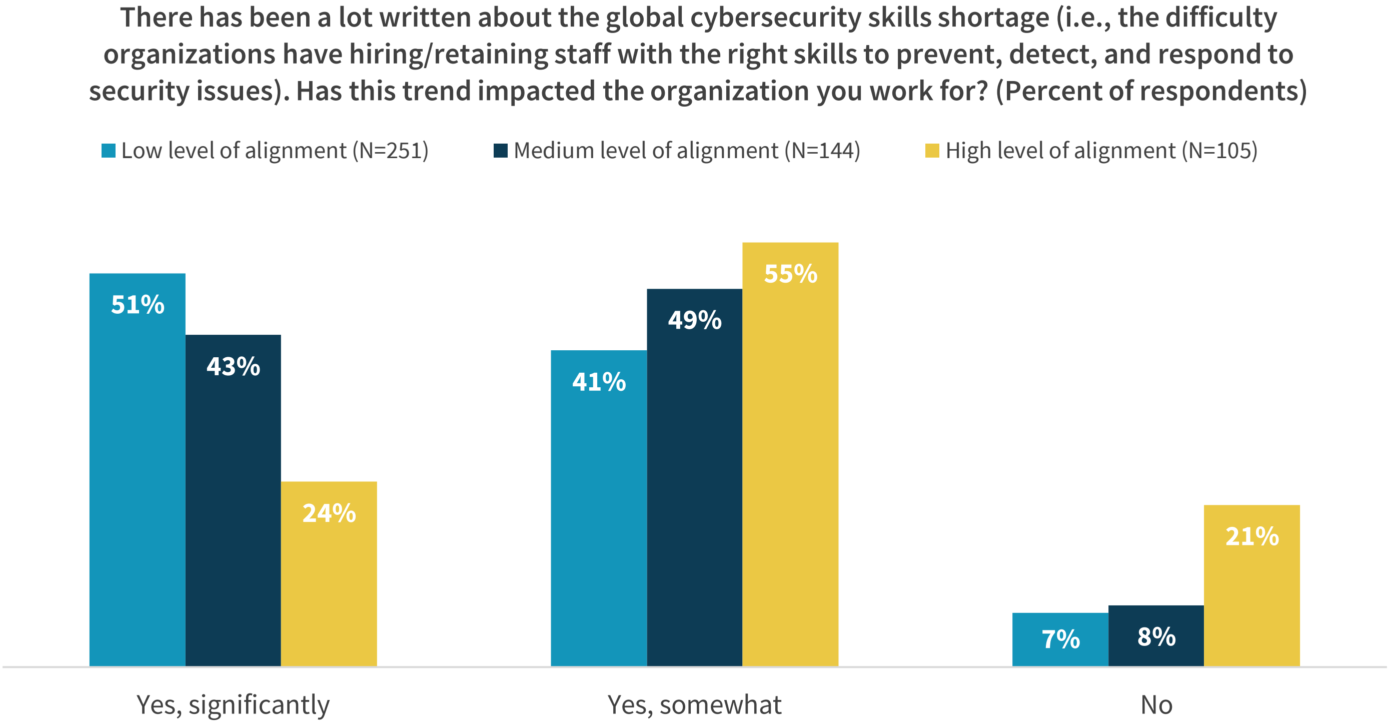
Figure 10. Threat Detection/Response Personnel Workload, by Level of Alignment



Source: Enterprise Strategy Group

This is demonstrated in Figure 11 as we see that level-1 orgs tend to report more significant issues with cybersecurity skills shortages.

Figure 11. Impact of Global Cybersecurity Skills Shortage, by Level of Alignment



Source: Enterprise Strategy Group

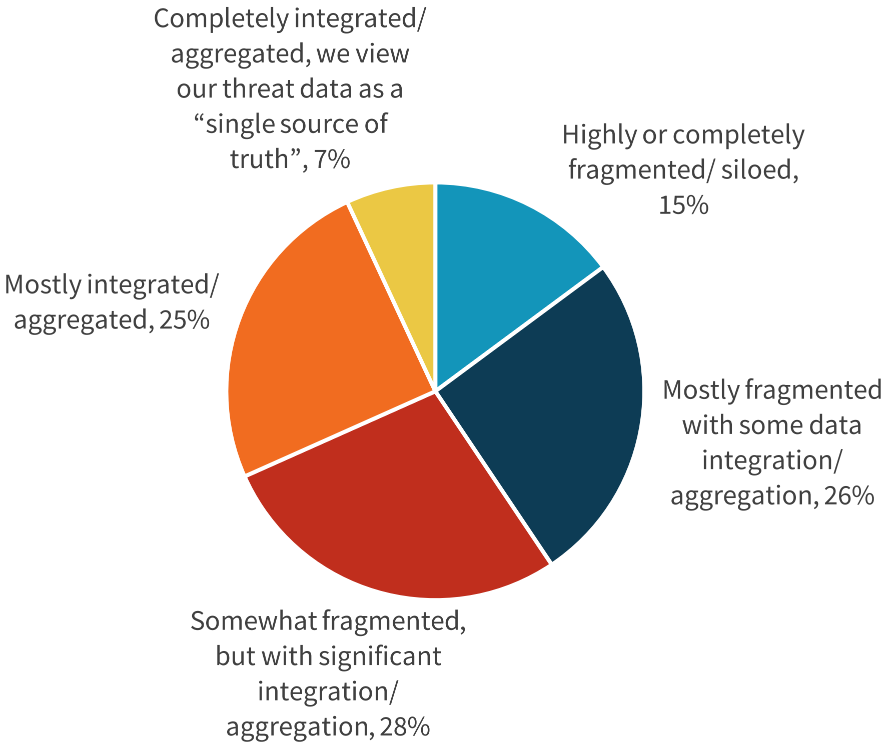
© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Siloed Data for Most

Siloed data is the norm for most organizations. With almost 41% reporting highly or mostly fragmented data (see Figure 12), and 61% reporting manual approaches to integrating and aggregating data from various security controls, keeping up with the growing sophistication of modern attacks is challenging.

Figure 12. Most Security, Threat Detection, and Response Control Information Is Fragmented

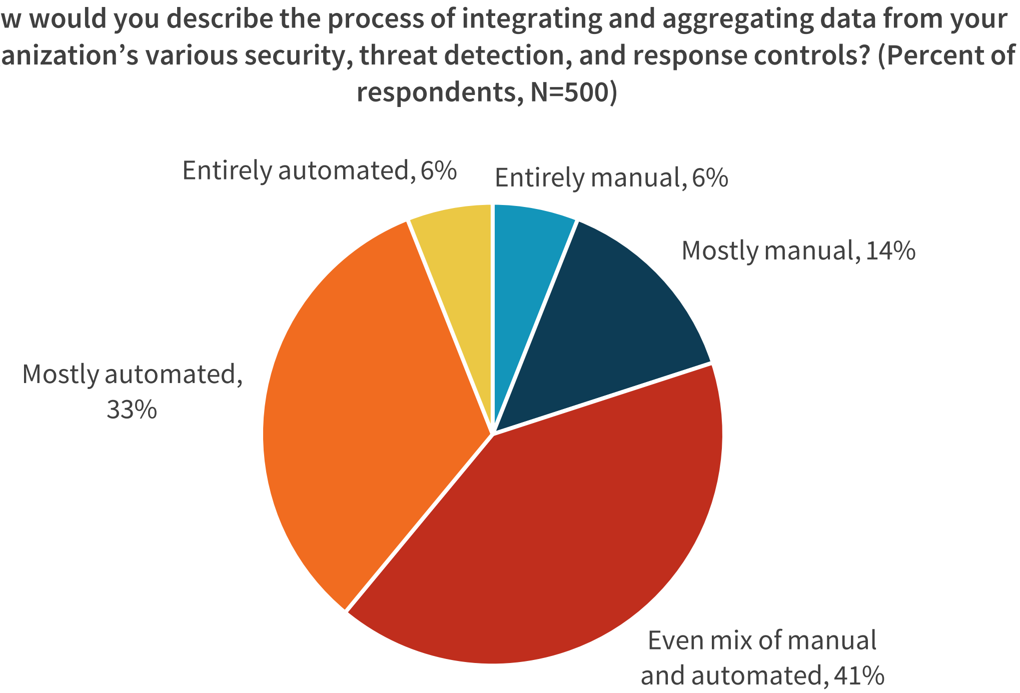
How would you describe the information/data in your organization's various security, threat detection, and response controls? (Percent of respondents, N=500)



Source: Enterprise Strategy Group

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

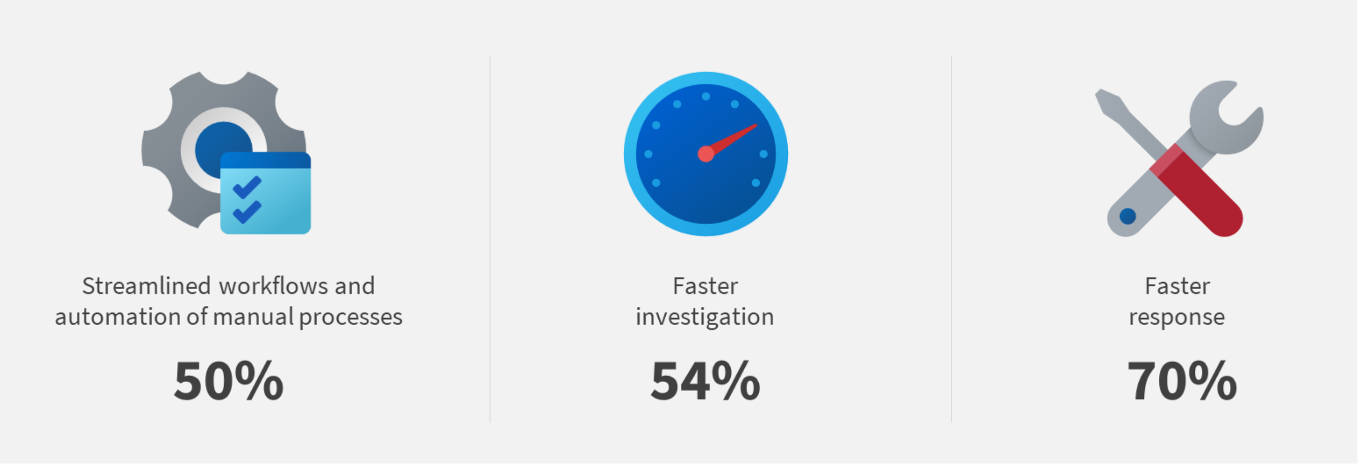
Figure 13. Integration and Aggregation Process for Security, Threat Detection, and Response Controls Data



Source: Enterprise Strategy Group

Yet those who report more effective data correlation experience operational improvements, including faster investigations, faster response, and streamlined workflows of manual processes. Level-3 organizations with high levels of alignment to XDR were 46% more likely than those with low levels of alignment to have achieved accelerated response times.

Figure 14. Operational Improvements Achieved from Effective Threat Data Correlation



Source: Enterprise Strategy Group

Level-3 Organizations Ignore Significantly Fewer Alerts

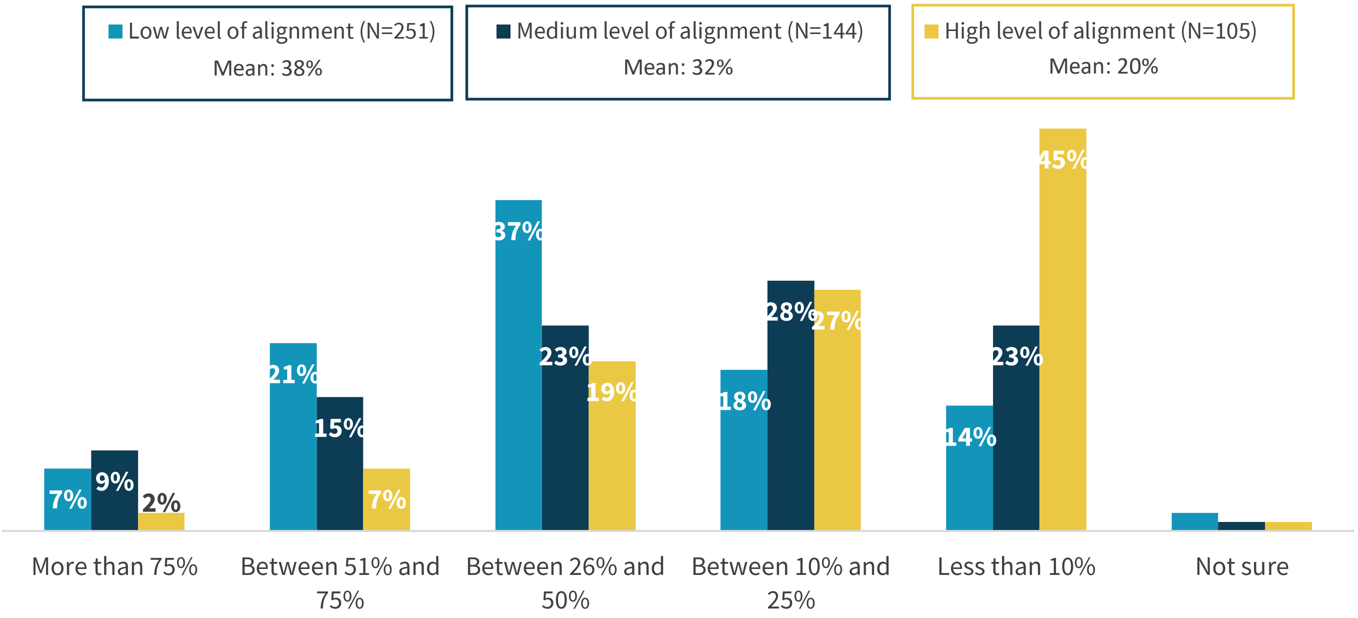
Seventy-two percent of level-3 organizations with high levels of alignment to XDR ignore less than 25% of alerts, compared to 65% of lower level alignment organizations that ignore more than 25% of alerts (see Figure 15).

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

This significant statistic leads to the large difference we see in the number of breaches experienced by level-1 and level-2 organizations.

Figure 15. Security Events/Alerts Ignored by Organizations

What percentage of the overall volume of security events/alerts do you believe your organization ignores, even though it would be beneficial to investigate, because it is impractical to investigate every alert? (Percent of respondents)



Source: Enterprise Strategy Group

Dwell time is a critical metric leading to successful attacks. While 65% of level-3 organizations with high levels of alignment to XDR report average dwell times of a few days or less, 45% of level-1 lower alignment organizations report dwell times of more than one week (see Figure 16).

Figure 16. Typical/Average Dwell Time Prior to Data Breach Detection

70%
organizations in
LOW ALIGNMENT

One week
or more

- VS -

65%
of organizations in
HIGH ALIGNMENT

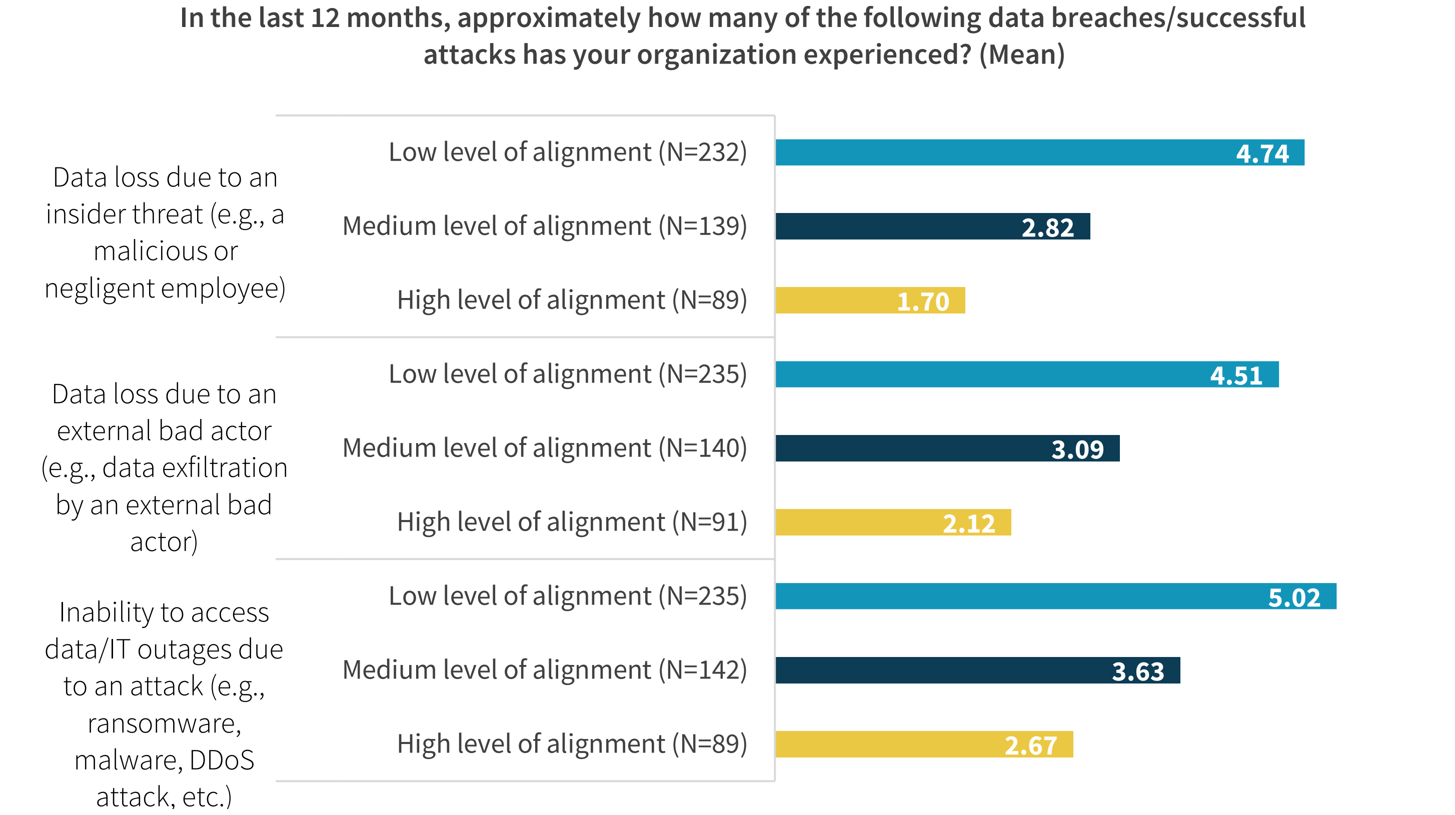
A few days
or less

Source: Enterprise Strategy Group

We can see this impact more clearly when we look at the rates of successful attacks on level-3 organizations with high levels of alignment to XDR versus lower levels. Here we see that level-3 organizations are half as likely to experience success attacks.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 17. Average Number of Data Breaches and Attacks



Source: Enterprise Strategy Group

Why Can’t My SIEM Solve the Problem?

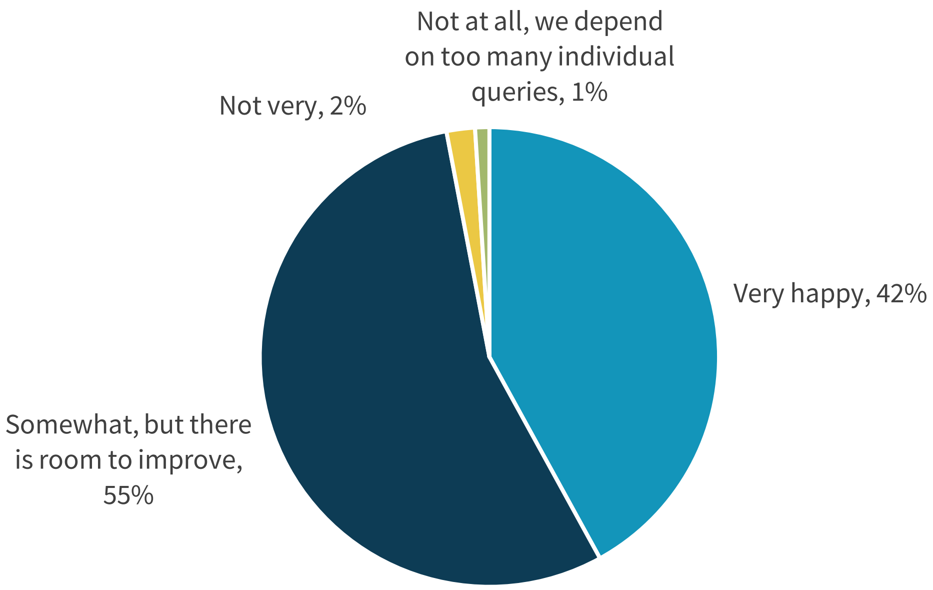
Seventy-nine percent of today’s modern security organizations leverage a security information and event management (SIEM) solution for threat detection and investigation. While SIEMs are widely adopted and have helped significantly, many report their SIEM falls short, with 57% reporting that they are noisy and require expert operators and only 42% reporting their SIEM is a very effective tool to support investigations. But why? This is exactly the story that SIEM providers have been pitching for the past few years.

Data ingest is a complex problem, as demonstrated from the statistics below. Eighty-three percent report that they either require ongoing and significant investment to integrate or need to be highly customized in order to effectively aggregate telemetry. Fifty-five percent of organizations see room for improvement when it comes correlation (see Figure 18).

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 18. Organizations' Satisfaction with Upfront Correlation of SIEMs

How happy is your organization with the amount of upfront correlation your SIEM can do with data to support threat detection and investigation? (Percent of respondents, N=393)



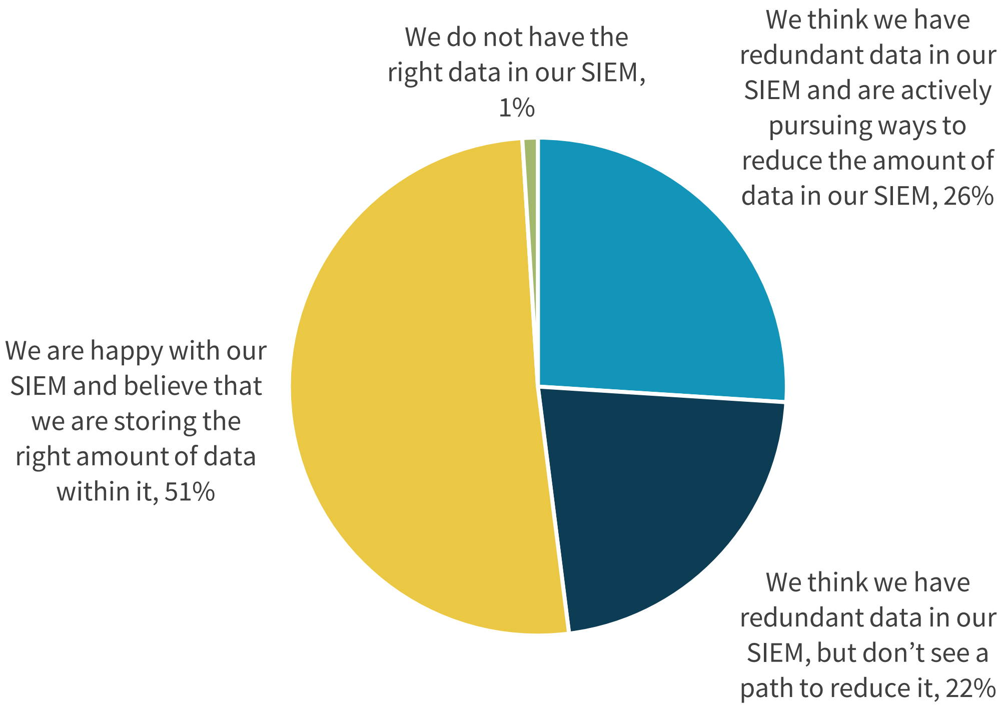
Source: Enterprise Strategy Group

For those successfully ingesting data from multiple controls, half struggle with redundant data, inflating the costs associated with SIEM use (see Figure 19). With the high cost of SIEM and many SIEM vendors charging based on the amount of data in use, reducing the amount of data ingested can make a significant impact on overall operational costs.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 19. Organizations’ Views on the Amount of Data Ingested into Their SIEMs

Is your organization happy with the amount of data you are ingesting into its SIEM as it relates to its use of it for threat investigation? (Percent of respondents, N=393)

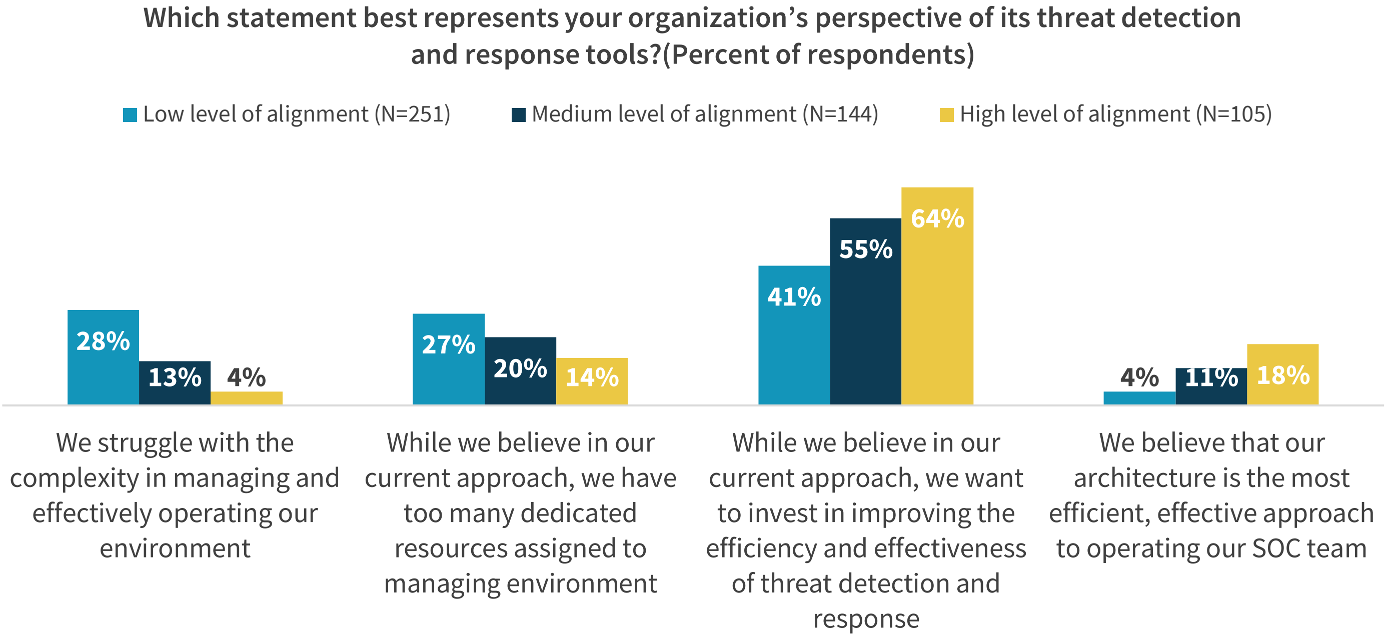


Source: Enterprise Strategy Group

Level-3 organizations with high levels of alignment to XDR not only believe in their approach more strongly, but also plan to invest further in improving the overall efficiency and effectiveness of their TDR programs (see Figure 20). Better results bread confidence. Note that level-1 organizations struggle more with the complexity in managing and operating their environments.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 20. Organizations Plan Continued Investment



Source: Enterprise Strategy Group

The Bigger Truth

XDR promises a new level of automation and fidelity for security teams that are struggling to keep up with the rapidly expanding and complex threat landscape. With no end in sight for the skills shortage and accelerating timelines for digital transformation initiatives, security teams need a force multiplier more than ever.

As shown in the research contained in this report, organizations that have invested in operationalizing the aggregation and correlation of data across multiple security controls are able to detect and respond faster, handle more alerts, and increase their overall security posture. Those that do these things experience fewer breaches.

While many organizations have attempted to accomplish similar leverage through their SIEMs, more than half are frustrated with the level of complexity, redundancy, and expert resources required to operate it.

XDR brings this proven approach to all security teams, without the high cost and complexity associated with building custom infrastructure to support it. For organizations that are already struggling to keep up, XDR offers an accelerant to increase both visibility and throughput. For organizations that have already invested in building custom data pipeline and analysis tools, XDR offers a new path to simplify the process to achieve similar results.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

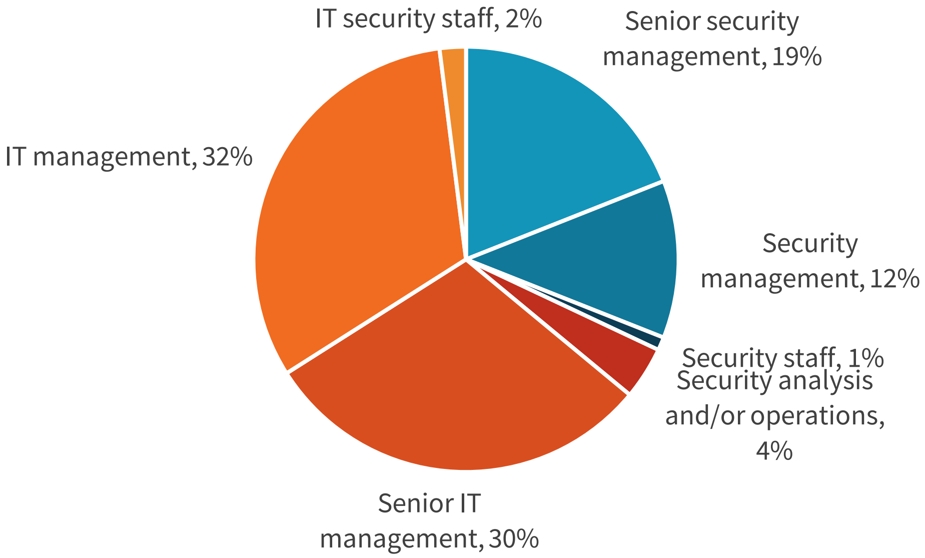
Methodology and Demographics

To gather data for this report, ESG conducted a comprehensive survey of security and IT professionals responsible for their organization's detection and response strategies, processes, and technologies. All respondents were based in North America (US and Canada) and employed at organizations with 500 or more employees. The survey was fielded between June 15, 2020 and June 30, 2020. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After applying data quality control best practices and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 500 respondents remained. Figure 21-Figure 23 detail the demographics and firmographics of the respondent base. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Figure 21. Respondents' Current Responsibility

Which of the following best describes your current responsibility within your company? (Percent of respondents, N=500)

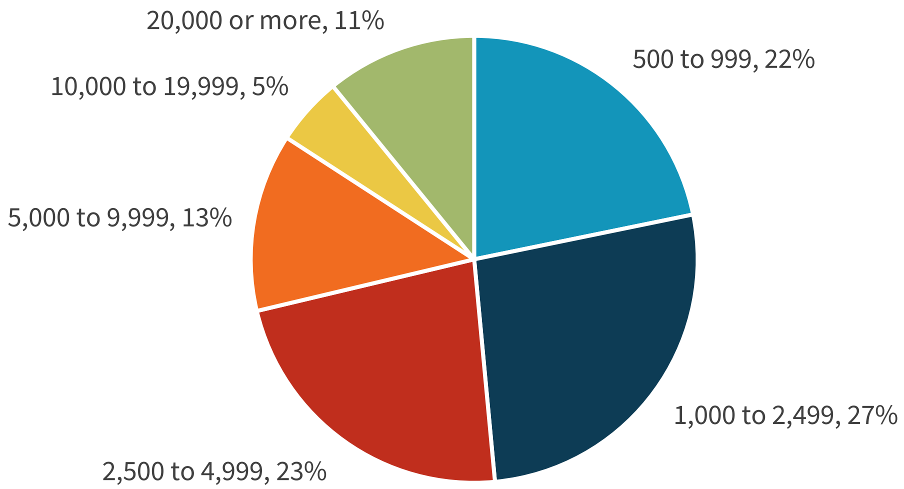


Source: Enterprise Strategy Group

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 22. Company Size (Number of Employees)

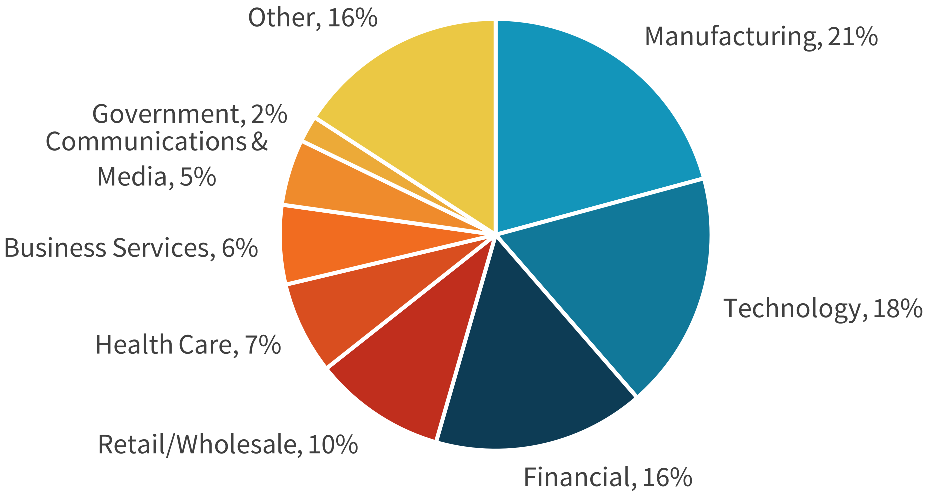
How many total employees does your company have worldwide? (Percent of respondents, N=500)



Source: Enterprise Strategy Group

Figure 23. Respondents' Primary Industries

What is your company's primary industry? (Percent of respondents, N=500)



Source: Enterprise Strategy Group

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.