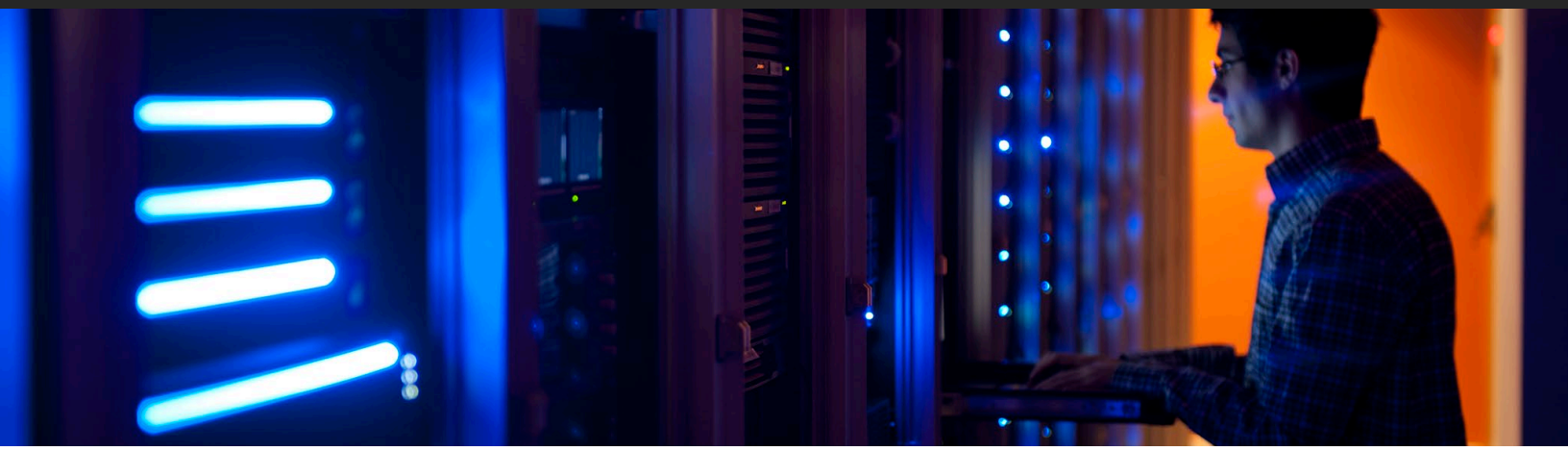
Enterprise Strategy Group by TechTarget



RESEARCH INSIGHTS REPORT

The XDR Payoff: Better Security Posture

Organizations that employ strategies aligned with XDR experience fewer successful attacks, have a better overall security posture, and live with less daily stress on their teams.

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

January 2023

This Enterprise Strategy Group Research Insights Report was commissioned by Trend Micro and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

The advent of extended detection and response (known as XDR) has provided a meaningful path for security teams to modernize security operations and gain leverage. Building on the learnings from both endpoint detection and response (EDR) and security information and event management (SIEM) solutions, XDR aggregates, correlates, and analyzes security telemetry across endpoint, network, email, and cloud security controls to automate the detection, investigation, and response of advanced 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 continues building 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 TechTarget's Enterprise Strategy Group (ESG) 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 strategies aligned with XDR 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. 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 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 they can investigate and respond to threats faster and ignore much 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.

Further research from ESG reinforced these findings, with respondents citing the importance of expanding attack surface coverage, simplifying alert triage and response, and centralizing security operations functions as the top desired XDR outcomes related to security efficacy.[1]

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 leveraging SIEM solutions, more than half say they are frustrated with the level of complexity, redundancy, and expert resources required to operate their SIEM.

[1] Source: Enterprise Strategy Group Complete Survey Results, *SOC Modernization and the Role of XDR*, September 2022.

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.

XDR is helping organizations automate the aggregation, correlation, and analysis of security data, delivering increased fidelity and efficiency for security teams that are struggling to keep up with the detection and investigation of advanced threats. With no end in sight for the cybersecurity skills 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.

Current Situation

Security teams are facing unprecedented change, with more than half reporting that security operations are more difficult today than two years ago.[2] Five key macro-trends are influencing this change:

- The attack surface in most organizations is rapidly expanding, and current tools are failing to support it, while introducing more vulnerabilities to manage.
- The threat landscape continues to become more sophisticated, as adversaries leverage advanced attack strategies to evade security controls.
- Continued investment in cloud applications and services challenges existing tools to keep up, while many organizations lack the people and skills needed to secure cloud resources.
- The move to cloud, together with ongoing defense-in-depth security strategies, is producing massive amounts of alerts, telemetry, and noise, making it challenging for security teams to triage and prioritize where to focus.
- Reactive, firefighting activities are consuming security resources, leaving no time to improve security programs.

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.

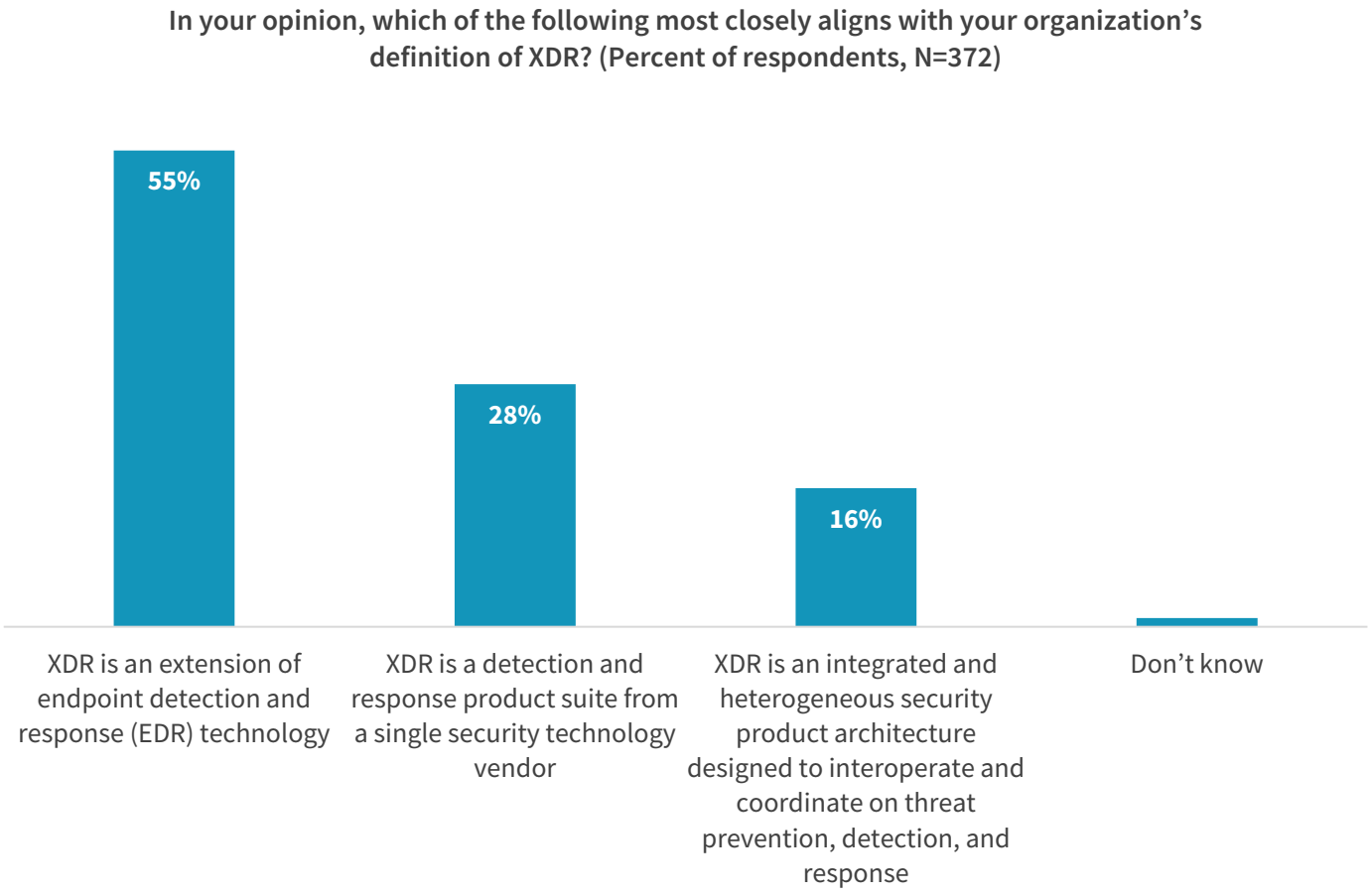
Introducing XDR

XDR is the next step in the evolution of detection and response automation. It builds on the proven concepts that come from both EDR and SIEM solutions, enabling security analysts to detect and respond to all types of threats that make it past traditional security controls.

[2] Ibid.

The industry continues to be confused about what XDR is, with 55% believing that XDR is an extension of EDR, and 44% believing XDR is either a detection and response product from a single security technology vendor or an integrated and heterogeneous security product architecture designed to interoperate and coordinate on threat prevention, detection, and response (see Figure 1 below).[3]

Figure 1. Multiple Definitions of XDR Add Confusion



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Despite these differences in definition, most XDR solutions are capable of ingesting security telemetry from multiple security controls out-of-the-box and are able to correlate and analyze signals to identify and isolate threats. XDR removes much of the "heavy lifting" that is often required to assemble this data in SIEMs and data lakes, allowing security teams to focus on detection and investigation activities instead of building and managing custom aggregation and analysis tools.

While XDR offerings are still evolving, 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 offerings have become a primary incident response tool for security teams, delivering new levels of automation and visibility, and supporting the detection, investigation, and response of more advanced attacks.

How EDR Investments Have Influenced the Road to XDR

Security architects work tirelessly to assemble and maintain a collection of security controls aimed to protect users, data, applications, and infrastructure. Defense-in-depth strategies have become commonplace for many organizations,

[3] Ibid.

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 anomalous behaviors, forensic teams still needed to access endpoint data to understand the impact and methods of attacks. This realization precipitated the invention of 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 quickly realized that core security controls, such as antivirus, firewalls, email security, and others, have logical limits to their abilities to prevent attacks, resulting in a small number of attacks successfully compromising infrastructure. This realization led security teams to adopt a "prevent what you can and detect and respond to what you cannot" approach, elevating EDR into a mainstream tool for the modern SOC. Yet, as more organizations invested in EDR, attackers employed more sophisticated attack techniques, leveraging multiple vectors to evade EDR solutions, which alone lack sufficient context into advanced, persistent threats and other stealthy attacks.

More mature, well-funded security teams have overcome this challenge by aggregating and correlating security signals from multiple security controls, combined with advanced analytics, to provide rapid, high-fidelity visibility into advanced attacks. While this strategy required significant engineering investment in the past, the new approach to threat detection and response offered by XDR solutions is simplifying and strengthening security processes with greater visibility across all data sources, therefore achieving more out of strategic security investment for organizations of all sizes. In addition to upgrading detection capabilities, 44% of surveyed security teams reported that they expect XDR solutions will help them consolidate current security operations technologies into a common platform.[4]

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 several 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, Enterprise Strategy Group research shows that few organizations feel that their SIEM has fully 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, hard-to-find experts are required to achieve these results.

[4] Ibid.

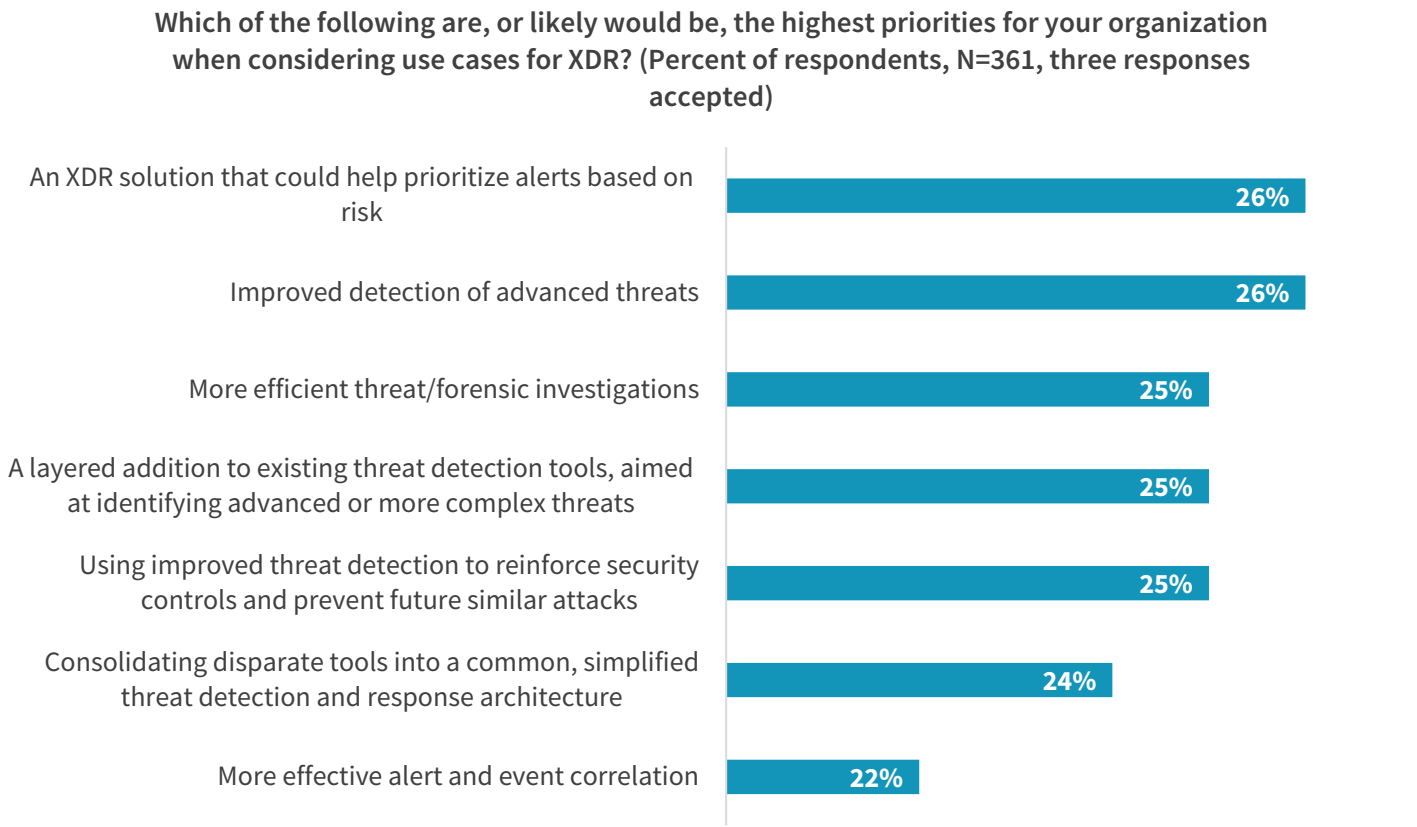
New strategies involving both SIEM and XDR are emerging, reassigning more advanced detection and response use cases from SIEM to XDR. Research shows that, while many believe that XDR solutions may be capable of replacing some or all SIEM use cases over time, most plan to continue SIEM usage for the near future in support of forensics and compliance use cases, among others.[5]

Understanding the Value of XDR

As XDR solutions continue to mature and find a place in security operations strategies, top priorities are centered around advanced threat detection. However, many aspire to achieve additional benefits from XDR implementations (see Figure 2), including:[6]

- Consolidation of disparate tools into a common threat detection and response architecture.
- More effective alert and event correlation. Less specialized skills needed to perform security operations tasks.
- Prioritization of alerts based on risk.
- Reinforce security controls and prevent future similar attacks.
- More efficient threat/forensic investigations.

Figure 2. Top 7 XDR Use Case Priorities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

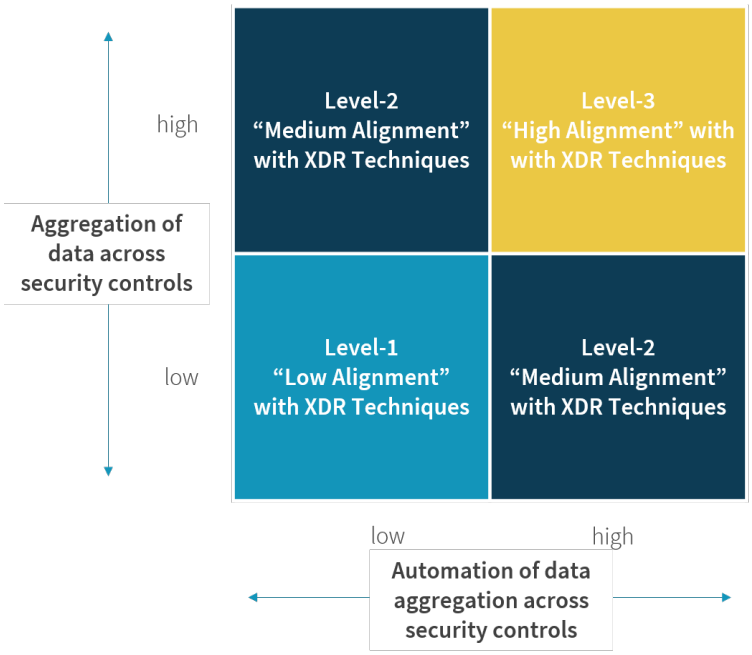
[5] Source: Enterprise Strategy Group Research Report, *The Impact of XDR in the Modern SOC*, March 2021.
[6] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

Organizations Aligning with XDR Approaches Report Better Overall Security Posture

To gather data for this report, Enterprise Strategy Group (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.

With all the confusion around the formal definition of XDR, ESG research established three cohorts representing levels of XDR alignment, with Level-3 representing those companies that were most aligned with XDR techniques. As we see from the model in Figure 3, 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.

Figure 3. ESG's XDR Value Assessment Model



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, a division of TechTarget, Inc.

As demonstrated in Figure 4, 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.

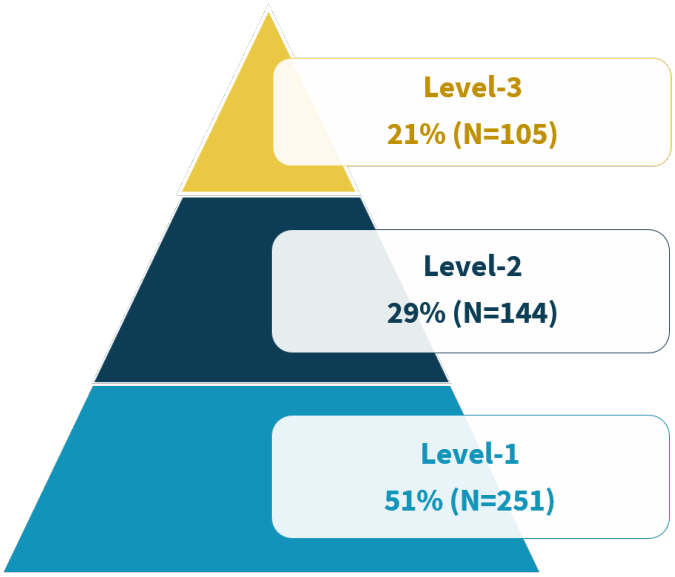
Figure 4. XDR Alignment Maturity Model Distribution

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

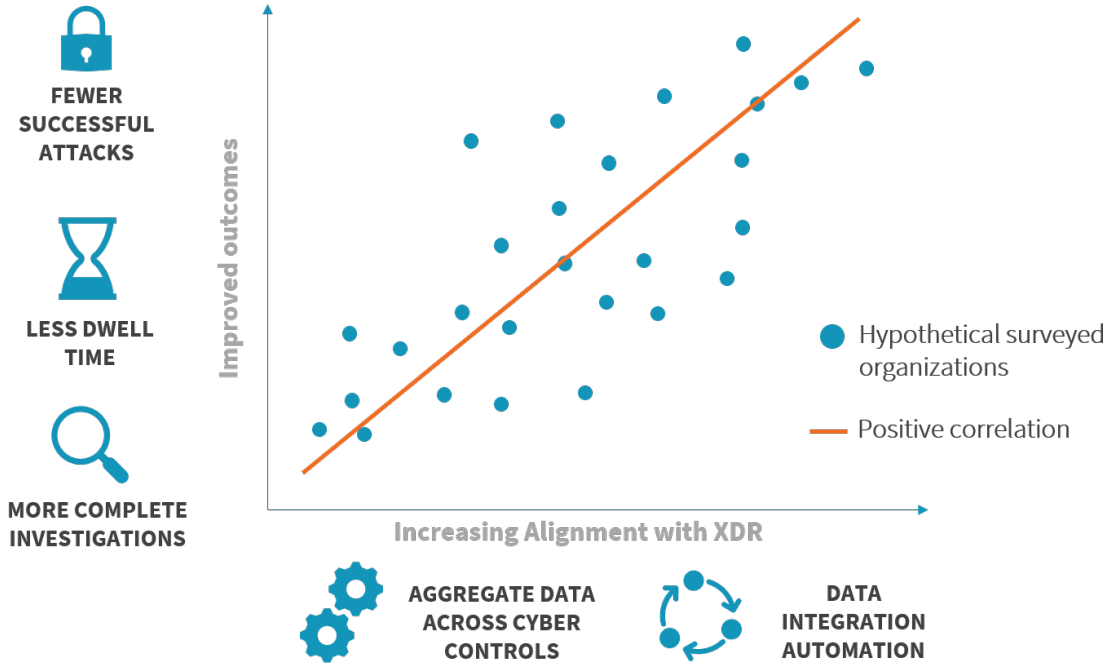
Level-1 (Low Level of Alignment):
- Mostly/completely siloed data in TDR controls with only manual data aggregation
- 50% of the market today



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 5. ESG's XDR Alignment Maturity Hypothesis Visualized

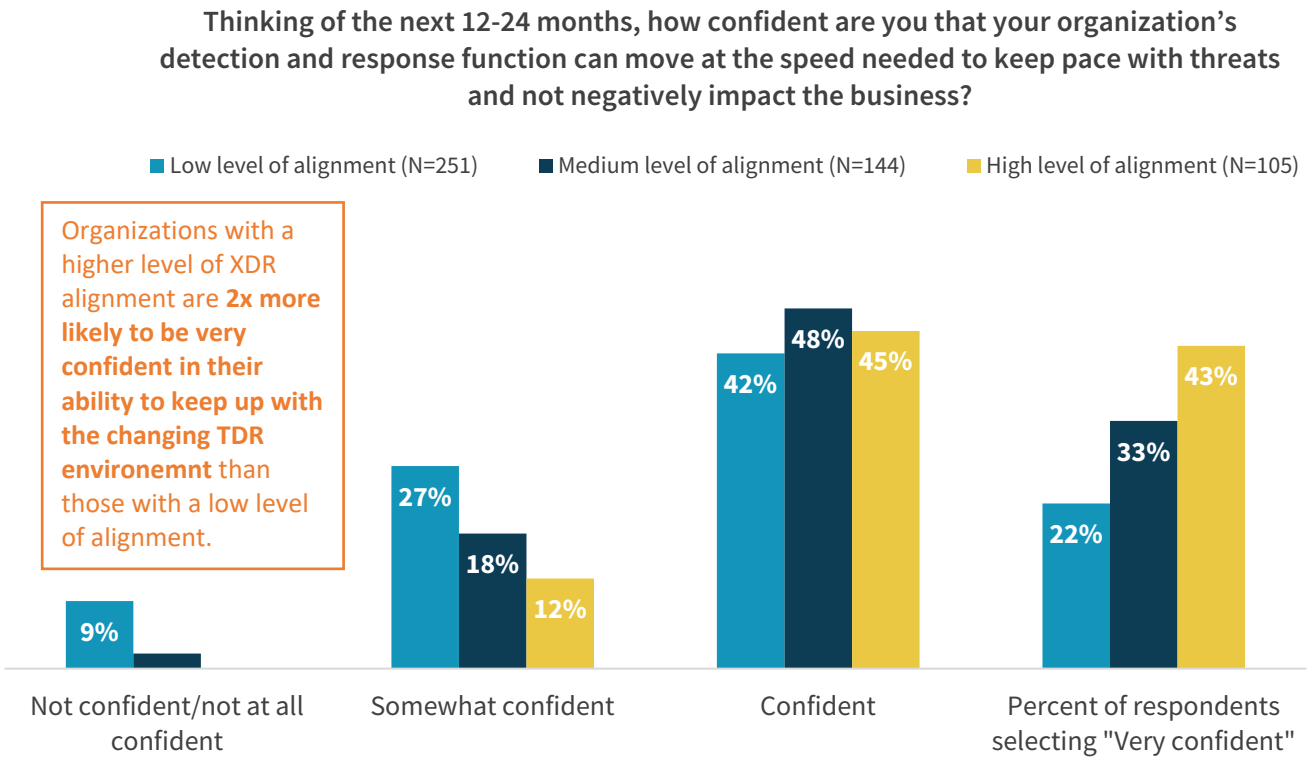


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 threat detection and response battle and that they were 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.

Figure 6. Higher Alignment Means More Confidence in the TDR Function



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

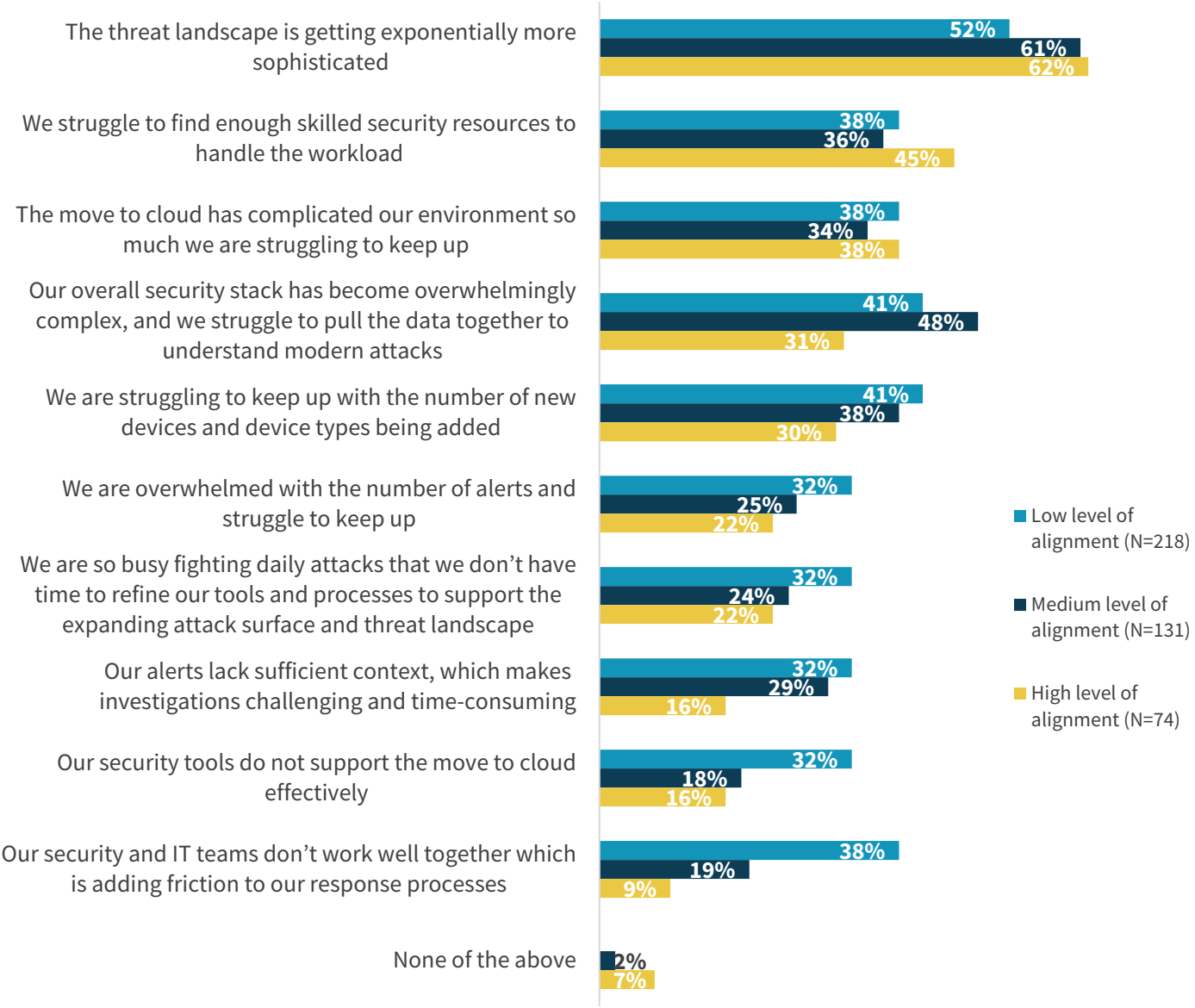
Quantitatively speaking, Level-3 organizations with high levels of alignment to XDR experienced only half as many successful attacks over the past 12 months. When asked how many FTEs it would take to replace their automated systems, organizations reported an average of 8 FTEs, which is an untenable additional investment for most organizations. Further, Level-1 organizations 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 FTEs 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 7).

Figure 7. Those in Alignment Struggle Less with Operational Challenges

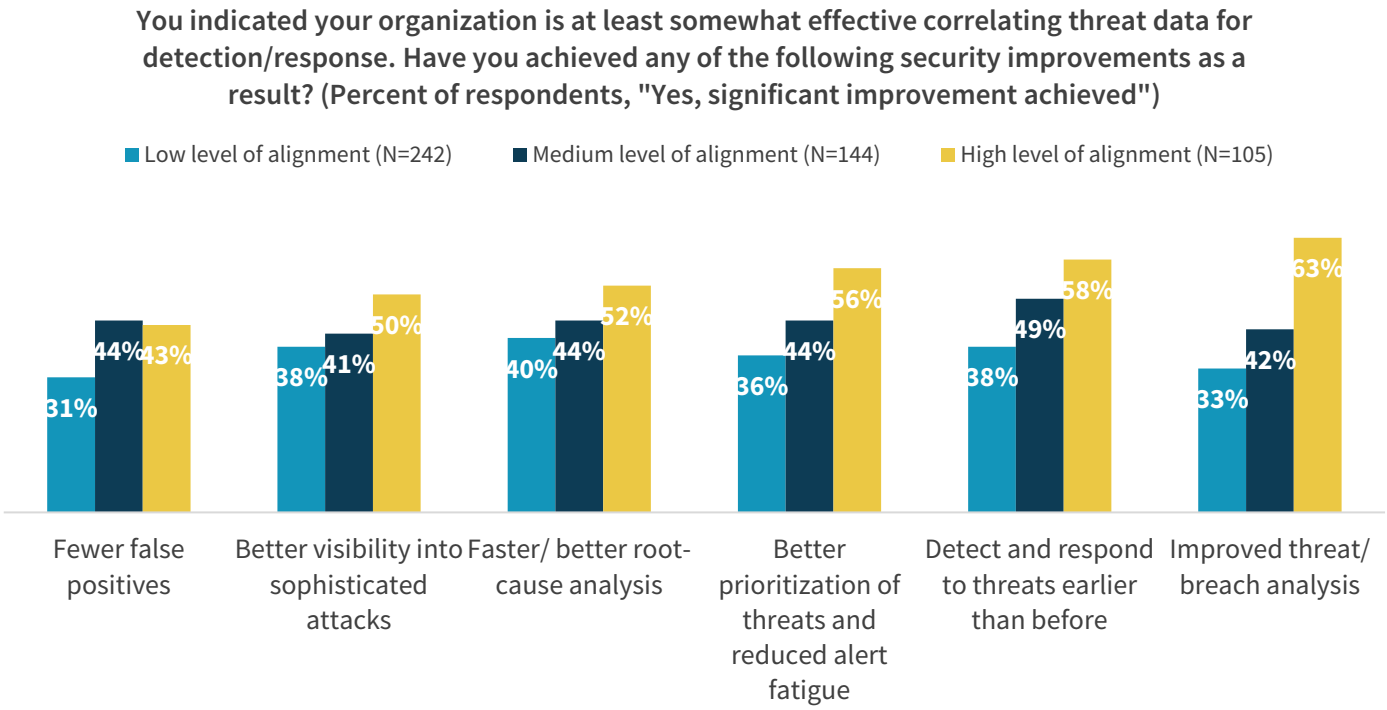
You indicated that threat detection and response has become more challenging over the past two years. Which of the following are the primary challenges your organization is facing regarding threat detection and response? (Percent of respondents)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 organizations, as well.

Figure 8. Organizations in Higher Alignment Are More Likely to Achieve Greater Improvements

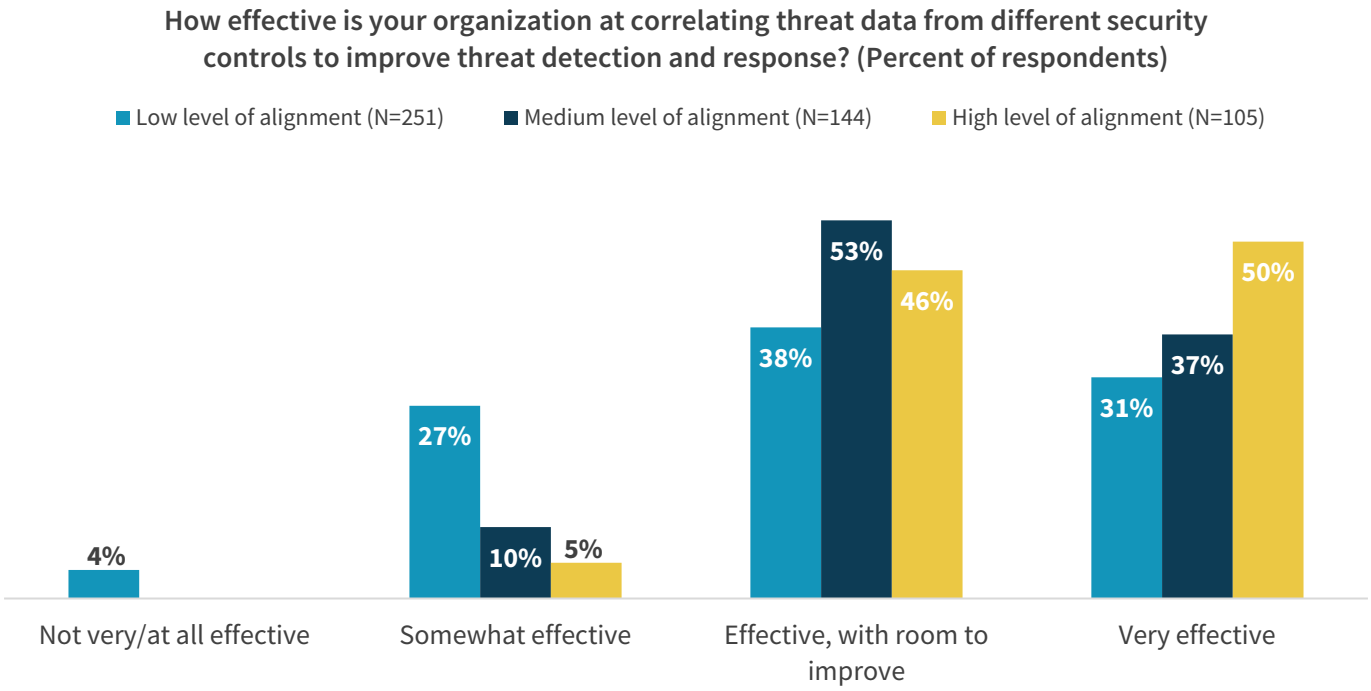


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Better Correlation = Better Results

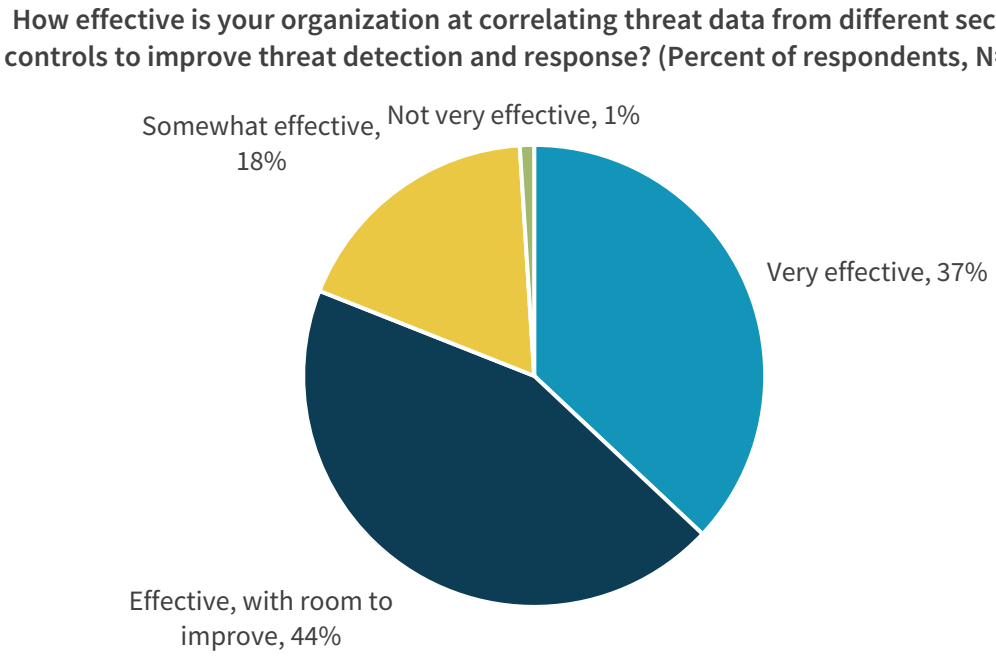
Level-3 organizations with high levels of alignment to XDR are 61% more likely to be highly effective at correlating data from different security controls than Level-1 and Level-2 organizations, with 50% of Level-3 organizations reporting that they are highly effective (see Figure 9). Even with those results, 63% of all respondents say that they can see room for improvement in overall data correlation (see Figure 10). The quest to sharpen detection of modern complex attacks requires an ongoing investment in correlation rules for most, even when automation is applied. Many XDR solutions promise to close this gap through continuous, automated rules refinement based on extensive, ongoing threat intelligence provided by the solution provider. Enterprise Strategy Group favors XDR solutions with this type of continuous, dynamic update of detection rules and threat intelligence.

Figure 9. Threat Data Correlation Effectiveness, by Alignment Level



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

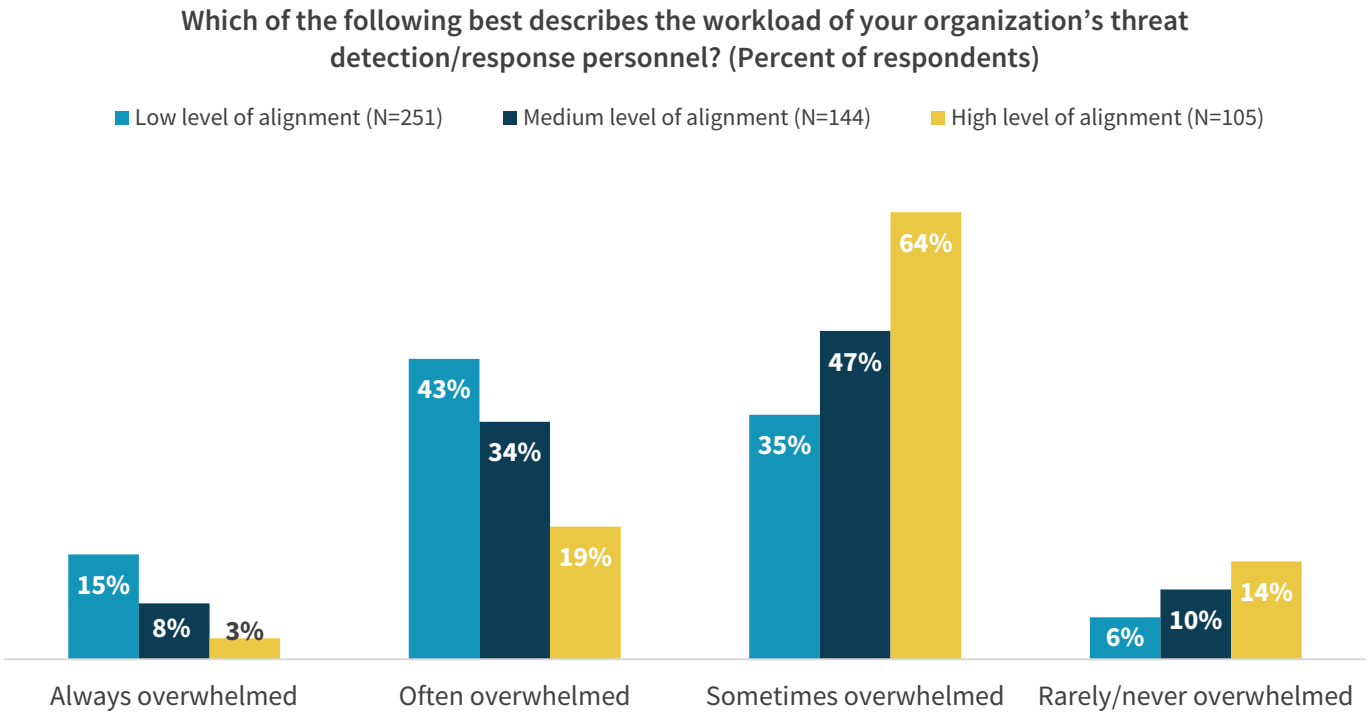
Figure 10. Threat Data Correlation Effectiveness, All Respondents



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 11). 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.

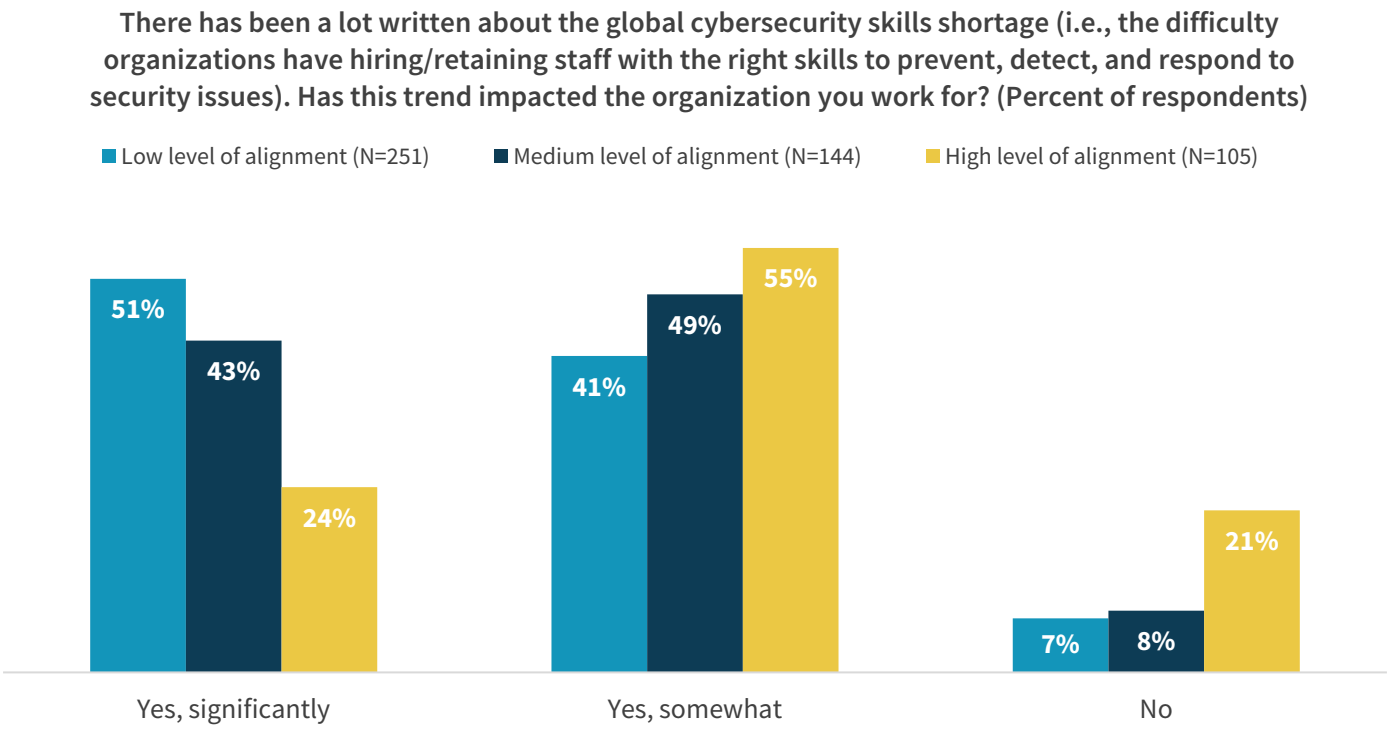
Figure 11. Threat Detection/Response Personnel Workload, by Level of Alignment



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

This is demonstrated in Figure 12, as we see that Level-1 orgs tend to report more significant issues with cybersecurity skills shortages.

Figure 12. Impact of Global Cybersecurity Skills Shortage, by Level of Alignment



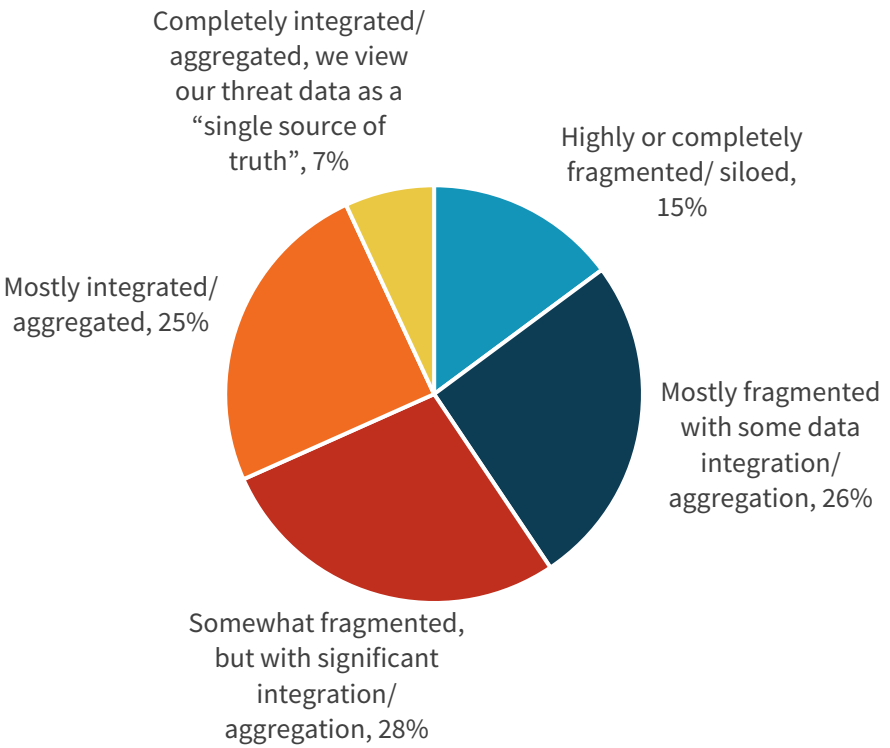
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Siloed Data for Most

Siloed data is the norm for most organizations. With almost 41% reporting highly or mostly fragmented data (see Figure 13), 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. XDR solutions to bring together siloed data, providing an out-of-the-box, automated mechanism to correlate and analyze related security signals, simplifying the upfront work required during investigations in a siloed environment.

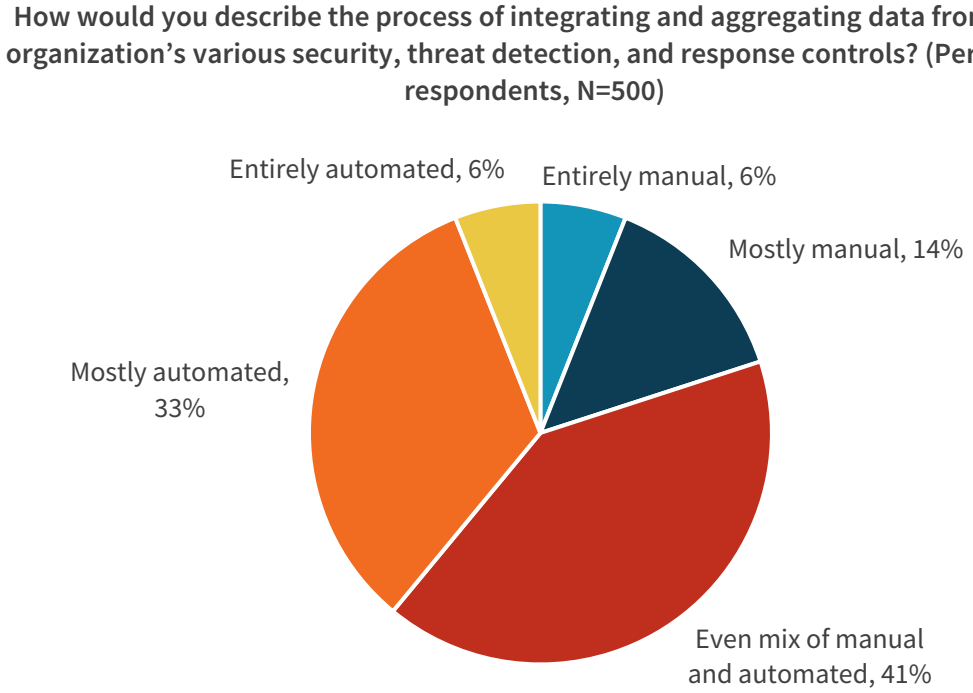
Figure 13. Most Security, Threat Detection, and Response Control Information Is Fragmented

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, a division of TechTarget, Inc.

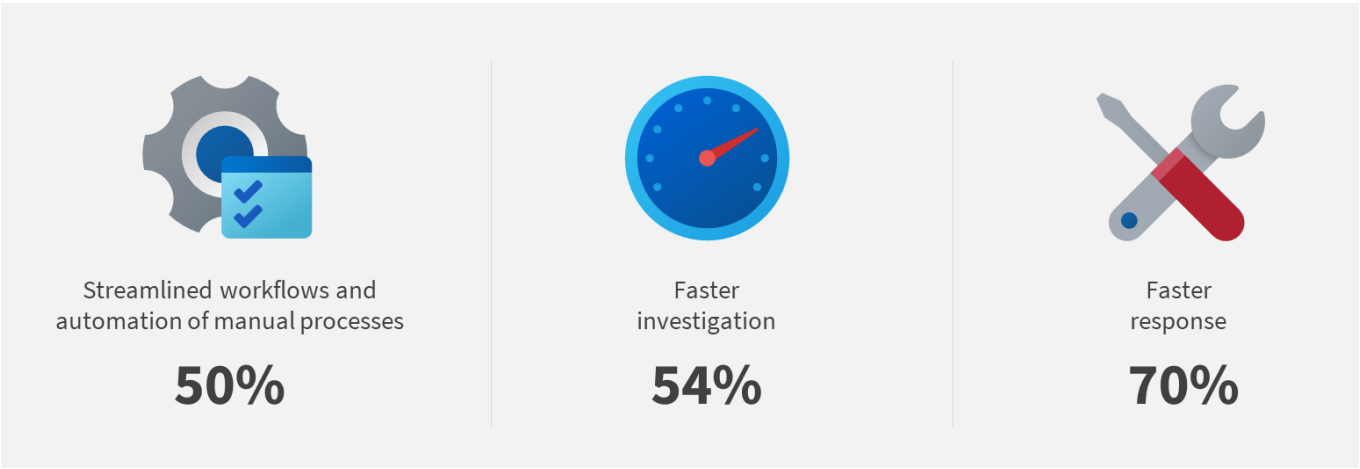
Figure 14. Integration and Aggregation Process for Security, Threat Detection, and Response Controls Data



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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. With XDR solutions tackling this problem, organizations with lower levels of engineering talent can now potentially achieve similar response outcomes.

Figure 15. Operational Improvements Achieved from Effective Threat Data Correlation



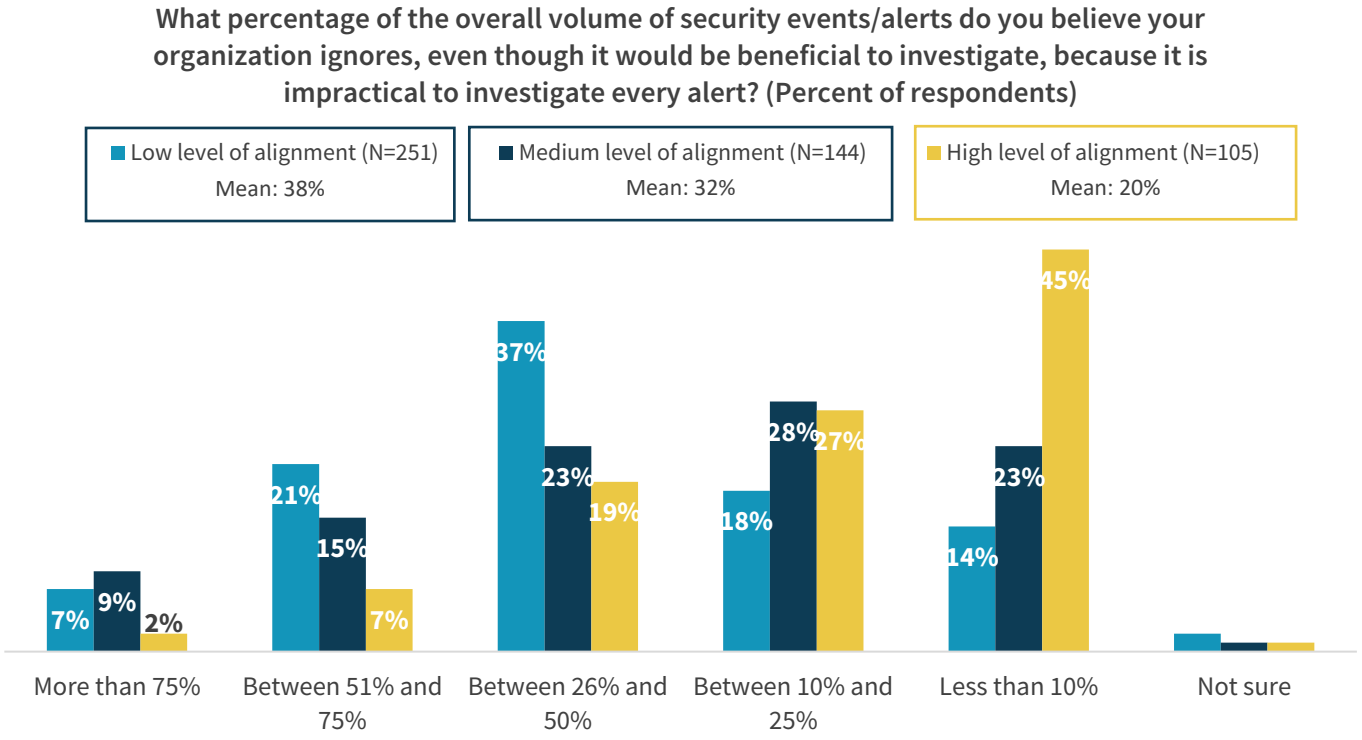
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 16).

This statistic leads to the significant difference we see in the number of breaches experienced by Level-1 and Level-2 organizations. Again, XDR solutions offer a new path for less mature security teams to make a significant impact on the reduction of successful attacks without hiring specialized resources.

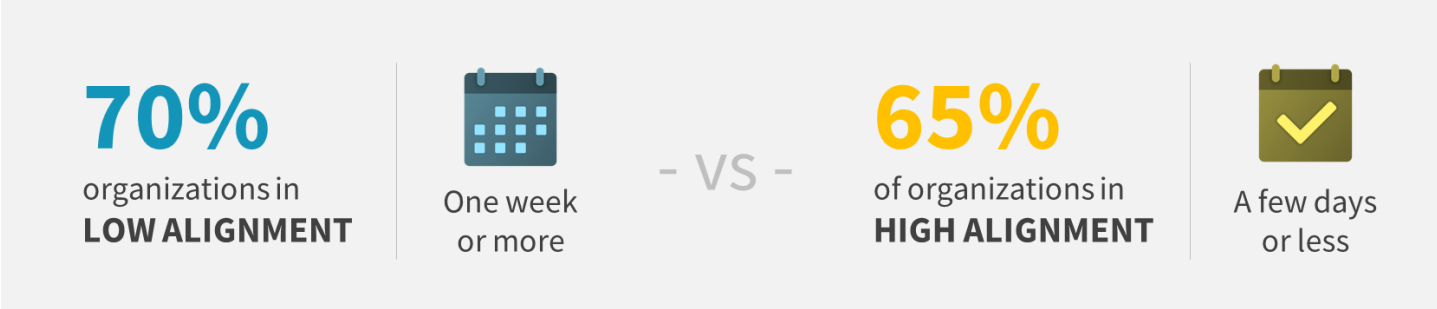
Figure 16. Security Events/Alerts Ignored by Organizations



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 17).

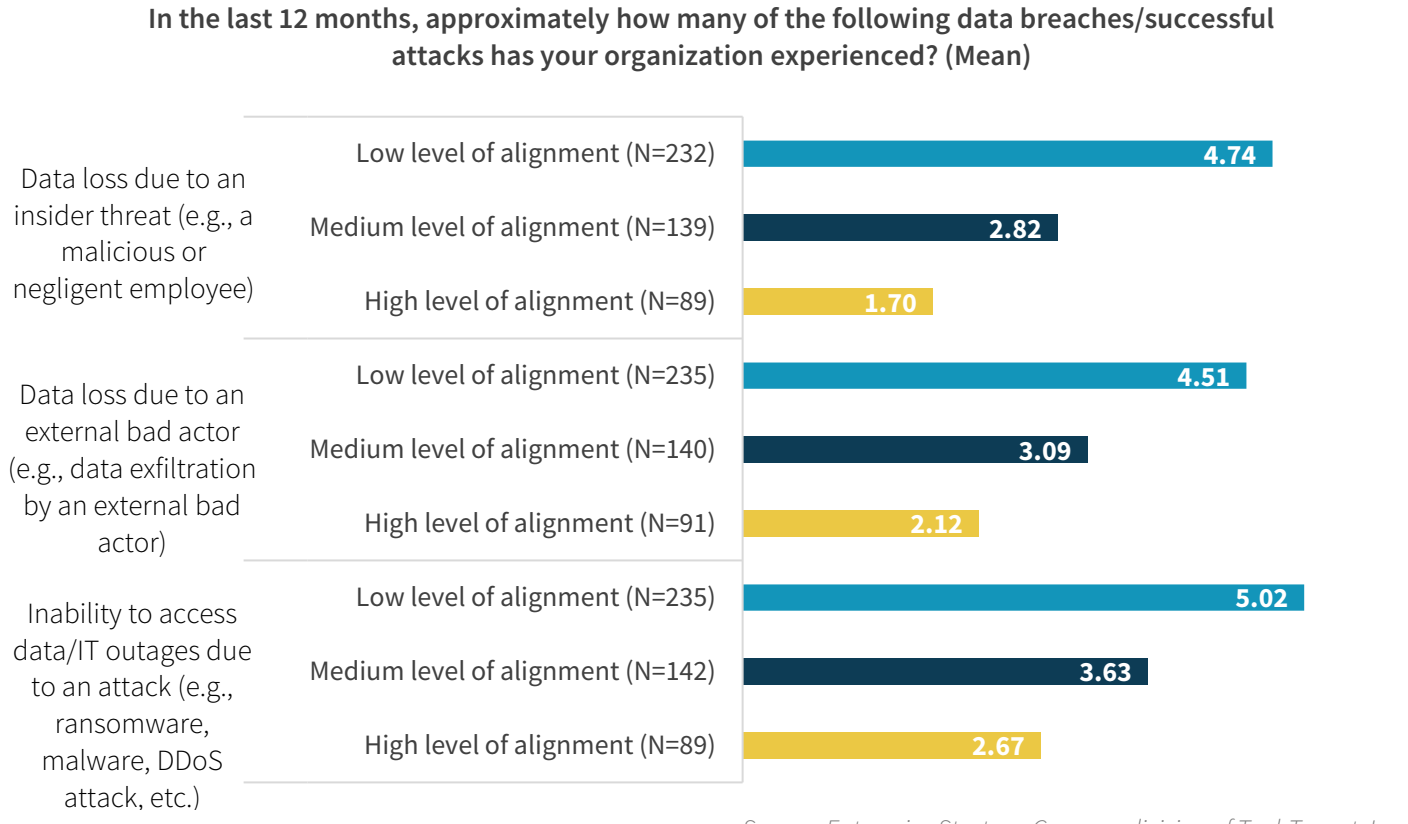
Figure 17. Typical/Average Dwell Time Prior to Data Breach Detection



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 successful attacks.

Figure 18. Average Number of Data Breaches and Attacks



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why Can't My SIEM Solve the Problem?

Seventy-nine percent of today's modern security organizations leverage a 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 that they are very happy with their SIEM's ability to support threat detection and investigations. But why? This is exactly the story that SIEM providers have been pitching for the past few years.

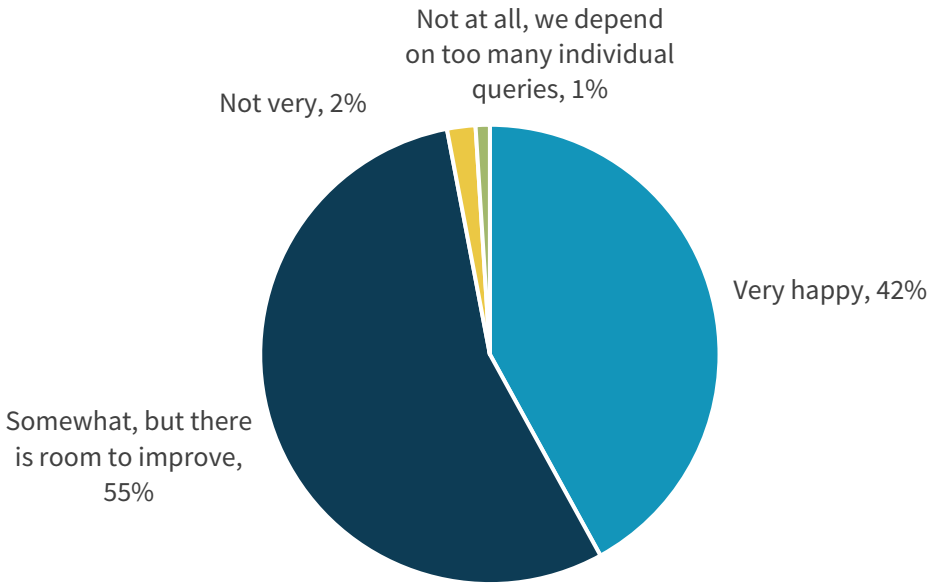
Data ingest is a complex problem, as demonstrated from the statistics below. Eighty-three percent report that they either need ongoing and significant investment to integrate or must be highly customized to effectively aggregate telemetry. Fifty-five percent of organizations see room for improvement when it comes to correlation (see Figure 19).

But these challenges don't stop people from wanting more data. Despite 80% of organizations already using more than ten data sources for their security operations,[7] most see the value in analyzing data from every security control, looking for a more efficient, effective path to do so.

[7] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

Figure 19. 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)

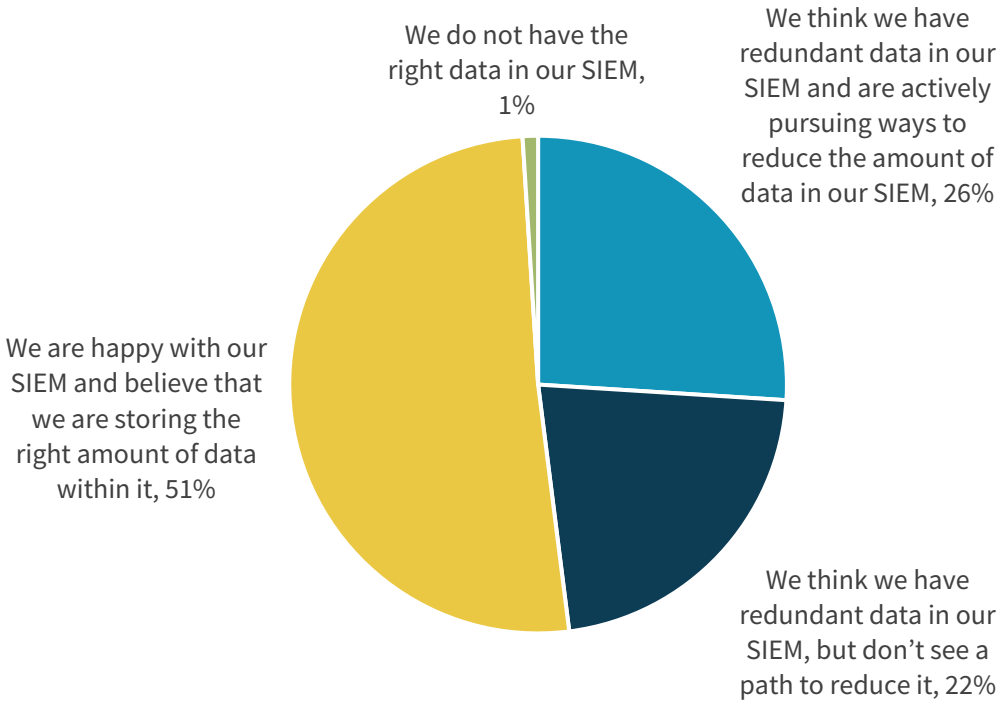


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

For those successfully ingesting data from multiple controls, almost half (48%) struggle with redundant data, inflating the costs associated with SIEM use (see Figure 20). 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.

Figure 20. Organizations' Views on the Amount of Data Ingested into Their SIEMs

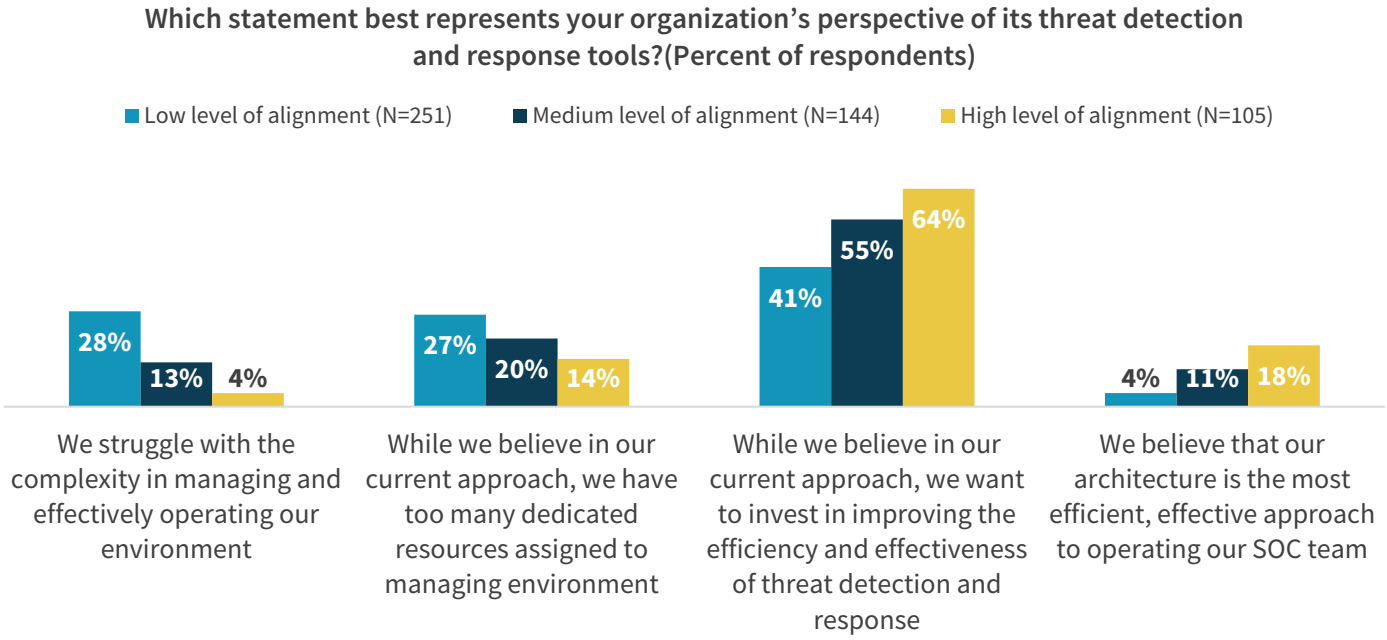
Is your organization happy with the amount of data you are ingesting into its SIEM as it relates to its use of it for threat investigation? (Percent of respondents, N=393)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 21). Better results breed confidence. Note that Level-1 organizations struggle more with the complexity in managing and operating their environments.

Figure 21. Organizations Plan Continued Investment

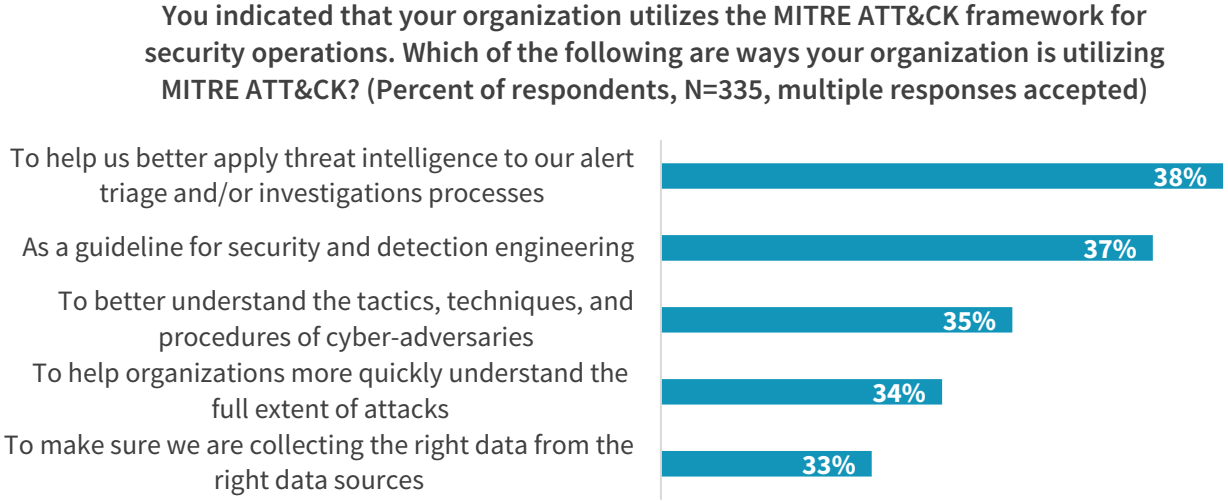


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

MITRE ATT&CK Offers Broad Benefits Across Security Operations

As the XDR movement continues to help security teams modernize security operations, use cases associated with the MITRE ATT&CK framework continue to expand. With almost half (48%) of organizations already extensively using MITRE ATT&CK to inform architecture, investigations, and threat intel strategies, and 96% classifying MITRE ATT&CK as either critical, very important, or important to their overall security operations strategy,[8] this important framework is helping to standardize the way security teams assess, architect, and deploy security strategies. Use cases are quickly expanding to guide investments, in addition to supporting daily security operational processes (see Figure 22).

Figure 22. Top 5 MITRE ATT&CK Use Cases



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[8] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

The Bigger Truth

With no end in sight for the skills shortage, growing attacks surfaces, and accelerating timelines for digital transformation initiatives, security teams need a force multiplier more than ever. XDR solutions are helping security leaders modernize security operations without rearchitecting and engineering custom security tools and integrations. This important advancement offers multiple benefits for security teams, improving both efficacy and efficiency.

As shown in the research contained in this report, organizations that have invested in strategies aligned with XDR are becoming proactive in detecting and responding to attacks faster, handling more alerts, and increasing their overall security posture. Those that do these things experience fewer breaches.

While most organizations still consider their SIEM solution a valuable asset, more than half are frustrated with the level of complexity, redundancy, and expert resources required to operate it and are exploring how XDR can supplement or offset SIEM future investments.

For organizations that are struggling to keep up, XDR offers an accelerant to increase both visibility and throughput. For organizations that have already invested in building custom data pipelines and analysis tools, XDR offers a new path to simplify the process to achieve comparable results, while enabling existing security resources to focus on other strategic initiatives.

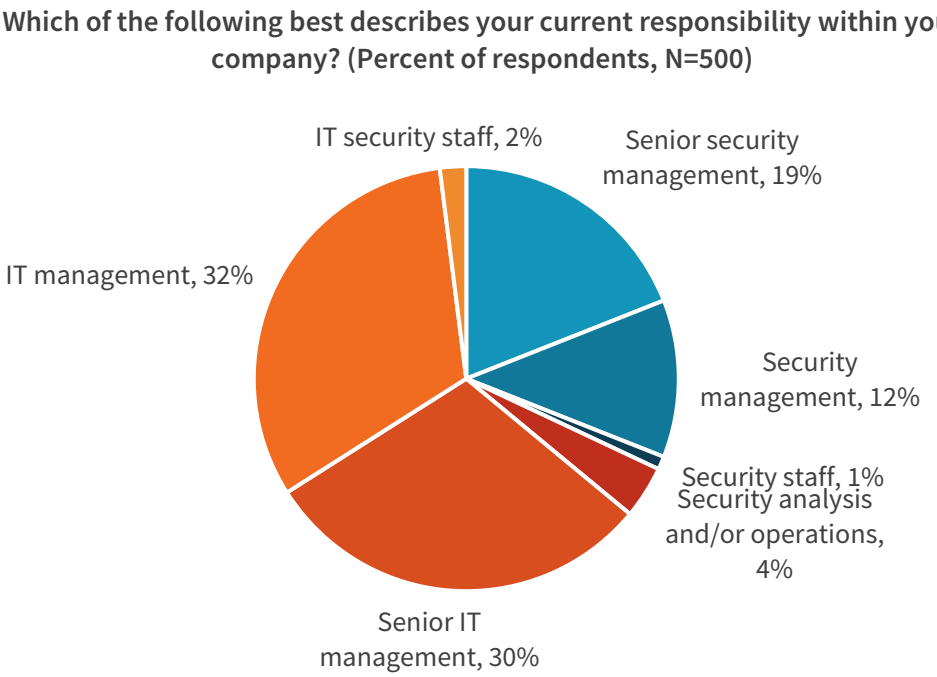
Enterprise Strategy Group strongly recommends that every security leader understand and explore the potential for how XDR can support and accelerate security program objectives by considering XDR solutions from vendors like Trend Micro.

Methodology and Demographics

To gather data for this report, Enterprise Strategy Group 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 filed between June 15, 2020, and June 30, 2020. All respondents were given an incentive to complete the survey in 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 23 - Figure 25 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.

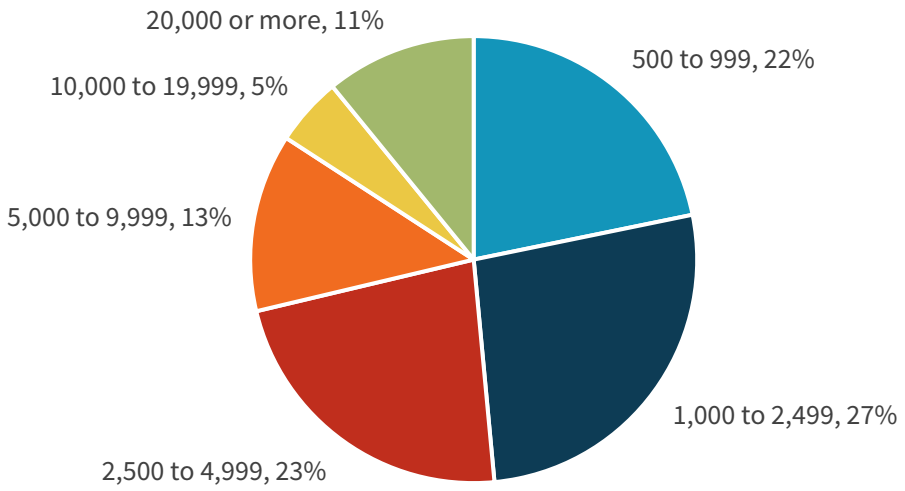
Figure 23. Respondents' Current Responsibility



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 24. Company Size (Number of Employees)

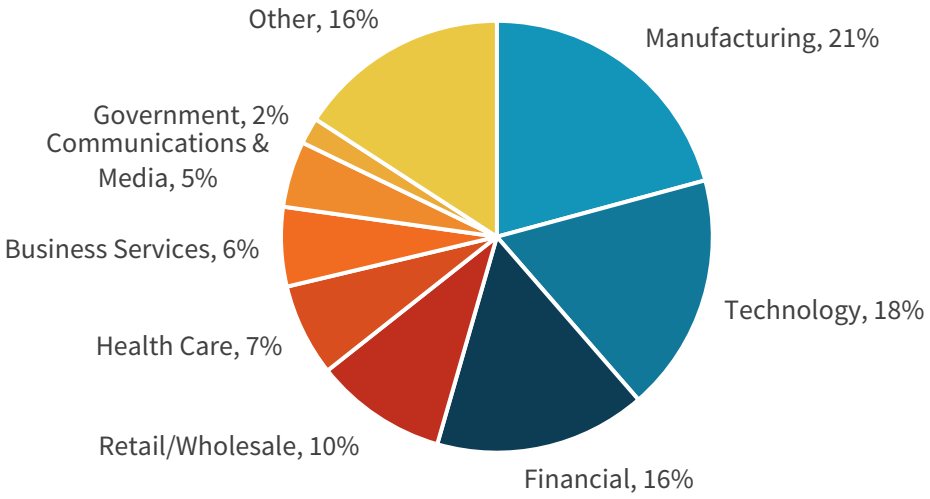
How many total employees does your company have worldwide? (Percent of respondents, N=500)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 25. Respondents' Primary Industries

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



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188