SANS | Research Program

Survey

SANS 2024 Detection and Response Survey

Transforming Cybersecurity Operations: AI, Automation, and Integration in Detection and Response

Written by **Josh Lemon**

November 2024

[P] | Prelude

Executive Summary

This is SANS's inaugural year conducting our Detection and Response Survey, which aimed to gather insights on how organizations around the globe manage cybersecurity threats. Our goal was to interpret the raw data from respondents and offer insights and guidance to help other professionals in the field enhance their detection and response strategies.

One main objective was to explore how organizations detect and respond to cyber threats. As we analyzed the state of detection and response in 2024, it became evident that these capabilities are central to an organization's cybersecurity strategy, but may be left behind when it comes time to build cybersecurity budgets.

In examining the organizational structures for detection and response, we found an almost even split between those using integrated teams and those employing separate specialized teams. This suggests no clear consensus in the industry on the best approach, highlighting diverse strategies based on organizational needs, resources, and priorities. The data also sheds light on the specific challenges organizations face, such as budget constraints.

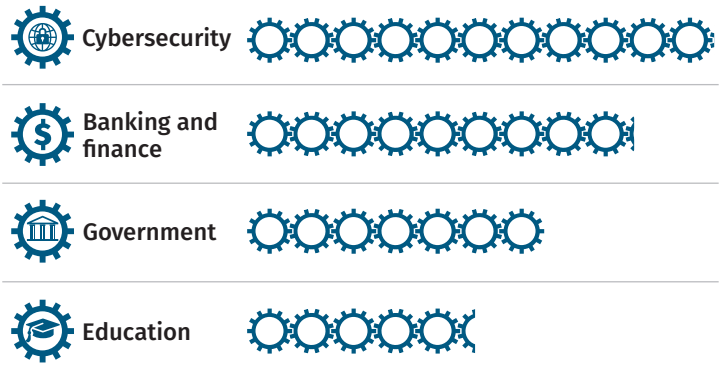
Our findings highlight the complex landscape of modern cybersecurity detection and response, where the interplay between human expertise and automated tools is crucial for staying ahead of threats. The survey revealed that:

- A significant majority of organizations (64%) are integrating automated response mechanisms into their operations.
- Only 16% of respondents report having fully automated their response processes.
- At 59%, the need for skilled personnel was the top obstacle to implementation.
- A full 47% of respondents reported that budget constraints were a top concern.
- About two-thirds of respondents (67%) indicated they plan to expand their use of artificial intelligence (AI) and machine learning for threat detection and response.

As we look toward the future, the survey indicates a trend toward increasing the use of AI and machine learning for threat detection and response. This focus on advanced technology reflects a proactive stance against the evolving threat landscape, aiming to automate threat detection and enhance the accuracy of responses. However, as organizations adopt these technologies, the need for skilled personnel to manage and interpret AI-driven insights remains paramount. The 2024 survey provides a detailed view of the current state of detection and response in cybersecurity, offering a valuable benchmark for organizations to refine and advance their defense strategies.

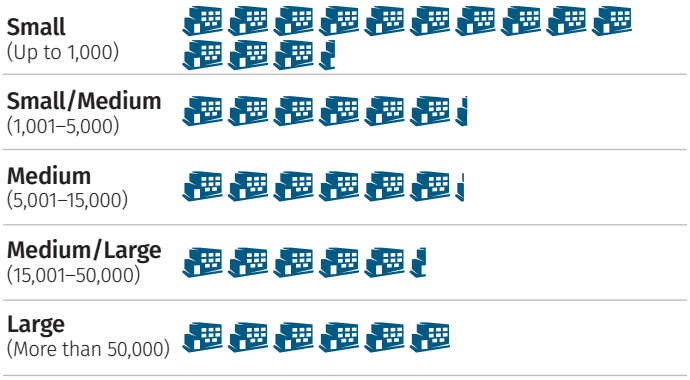
Despite this being the first year for the SANS Detection and Response survey, we were pleased to have almost 400 respondents. Figure 1 provides a snapshot of respondents' demographics.

Top 4 Industries Represented



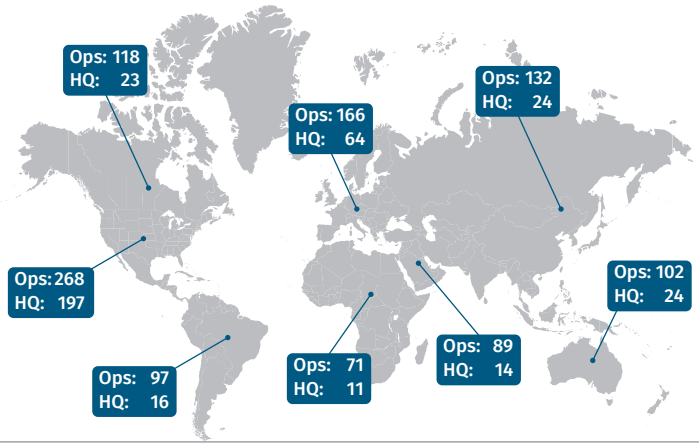
Each gear represents 5 respondents.

Organizational Size

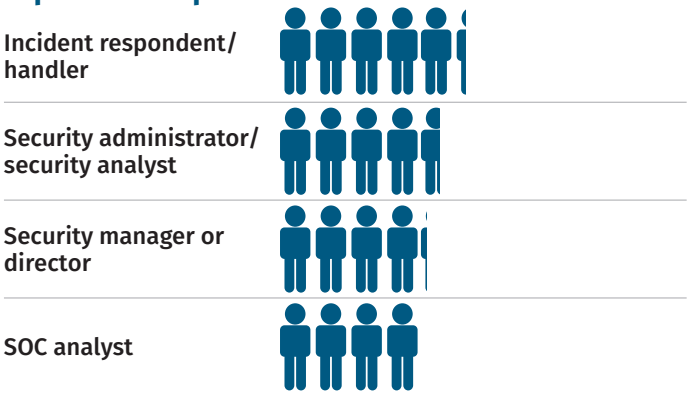


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Survey Demographics

Threat Detection: Are You Playing with the Right Deck?

Most respondents (87%) said they are using automated or assisted tooling to detect threats. This can give organizations a significant advantage early in the Cyber Kill Chain[1] in the hope of reducing damage or destruction posed by threat actors. However, a significant number of respondents (66%) are still using manual monitoring. (See Figure 2.) This is somewhat concerning, given the speed at which threat actors move as well as the dwell time it can take for organizations to detect a threat inside the network. This could mean that some organizations are performing more manual monitoring and struggling to deal with the current threat landscape. Yet another sizable proportion of respondents (39%) indicated that they are using AI- and machine learning (ML)–based technologies to detect threats.

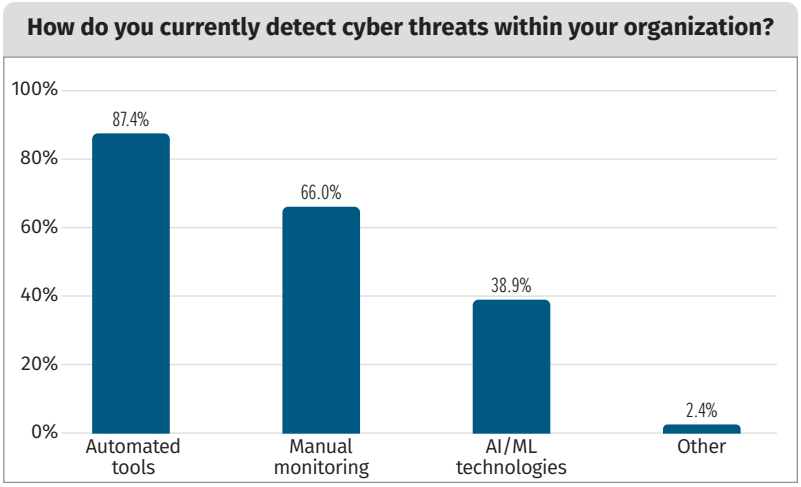


Figure 2. Threat Detection Methods

It is essential to understand how organizations are performing detections as well as the types of tools they are using and how useful they are. We asked respondents how effective various threat detection tools are—with no limit placed on how many tools they could select. We discovered that organizations are leveraging a range of technologies to enhance their detection capabilities. At 42%, extended/endpoint detection and response (X/EDR) tools are perceived as the most effective, indicating a growing reliance on X/EDR solutions. This is likely due to their capability to provide comprehensive visibility across endpoints—both within a corporate network boundary and outside of it—and their capacity to respond swiftly to emerging threats. We've also seen the industry significantly move toward detection on endpoints, which aligns closely with the outcome for this type of tooling.

At a relatively close second (30%), the involvement of a dedicated threat hunting team was considered "extremely effective." This suggests that, although automated tools are crucial, a human hunter remains a key requirement for successful threat detection. The ability of threat hunters to not only apply contextual understanding of evidence or indicators, but also think creatively, might explain why this approach remains highly valued along with technological solutions.

[1] "The Cyber Kill Chain," www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Regarding tool efficacy, there was an even spread across all tool types (see Figure 3). At 67%, network detection and response (NDR) topped respondents' lists, indicating a strong need for monitoring and threat detection at the network layer. NDR also acts as a valuable backup, particularly in environments that do not have EDR tools deployed to endpoints, including ICS-related or legacy systems that fall outside vendor support agreements—which is another risk altogether.

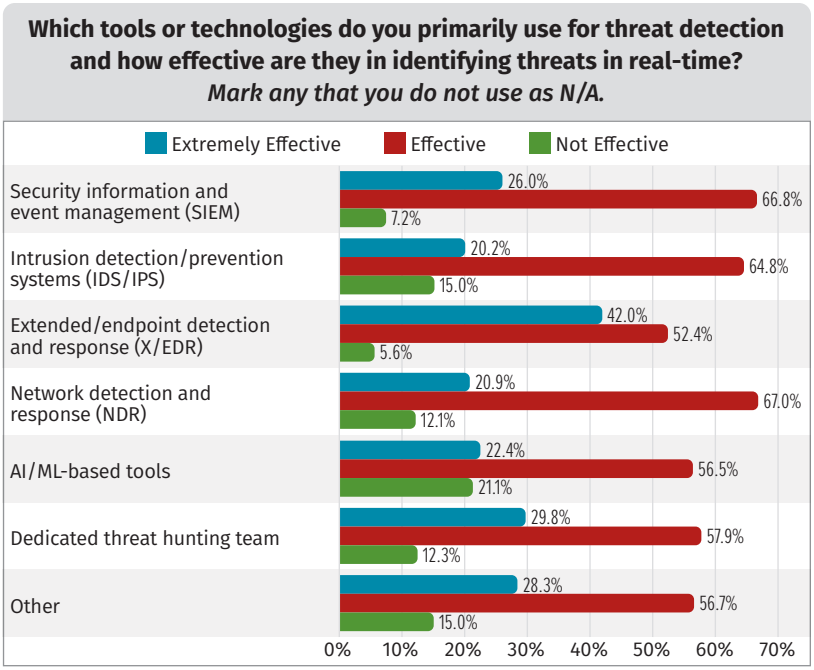


Figure 3. Use and Efficacy of Tools

Detection by the Living Machine

In contrast, respondents had mixed opinions about how useful AI/ML-based tools are for performing detection. Only 22% of respondents rated these tools as extremely effective; another 57% deemed them effective, while 21% found them ineffective. Overall, AI/ML-based tools are ranked roughly in the middle at being extremely effective and ranked the most ineffective for detecting threats. This doesn't necessarily mean AI- and ML-based tools should not be used for threat detection. It just means tools in this category need to become more effective at catching threat actors.

We also asked organizations if they currently use machine learning algorithms for threat detection, and found that a little more than 51% do so (see Figure 4). This could reflect a growing trend toward adopting technologies within this category quickly, although the industry still seems somewhat undecided. It is worth noting that 22% of respondents were unsure whether their organization was using machine learning algorithms for threat detection.

Of the organizations using machine learning for threat detection, only a quarter were using it extensively. The majority (51%) use it on a moderate basis, while an additional 22% use machine learning on a fairly minimal basis, possibly indicating that experimentation and tuning are still ongoing.

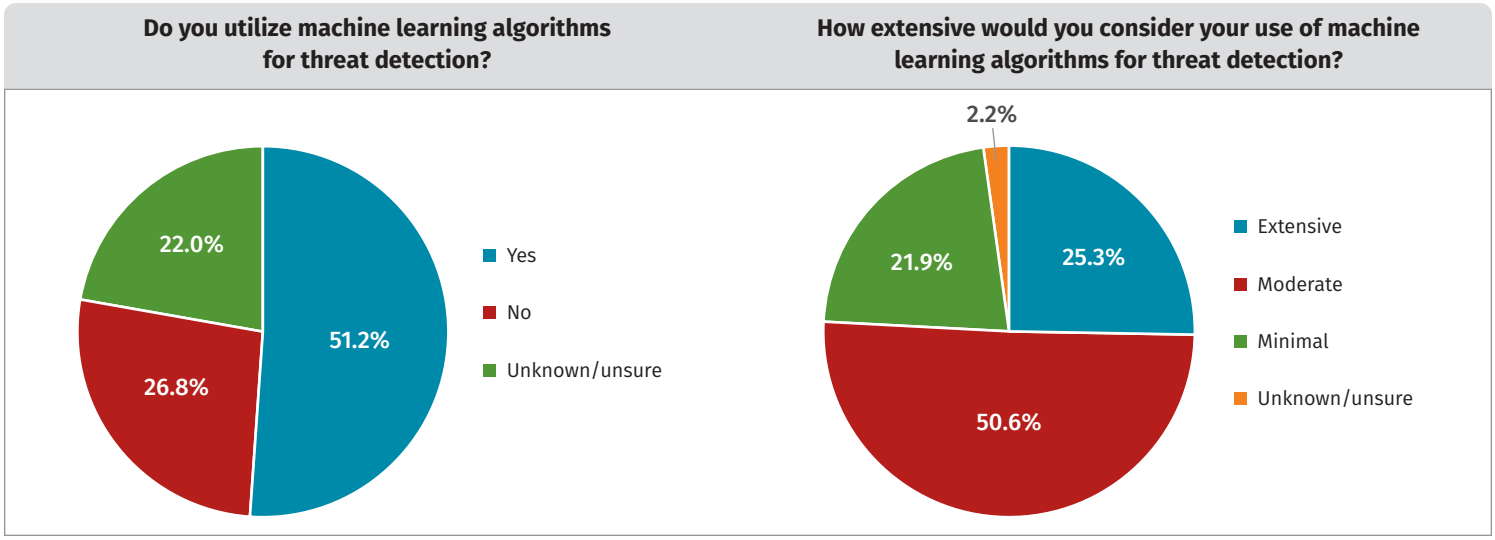


Figure 4. Utilization of Machine Learning

Detection in the Clouds

One of the more interesting findings was regarding respondents' capabilities and effectiveness in detecting cloud-based threats. This included infrastructure as a service (IaaS), software as a service (SaaS), and functions as a service (FaaS). All these cloud-based technologies form part of an organization's attack surface and need to be monitored for malicious actors. Very few organizations felt they were extremely effective in using either cloud-native tools (21%), third-party tools (17%), or in-house developed tools (19%) to conduct threat detection. Most respondents, however, felt they were effective at using all these tools, with cloud-native tools (67%) receiving the highest effectiveness rating.

Crafting Detections and Sharing Them

Understanding how organizations source their detection rules is important to get a better picture of how the industry is detecting actors. Most respondents use industry threat intelligence platforms (65%) as their primary source, followed by internal teams that develop rules for them (62%). There is also a strong preference for using security vendors (59%) and government or regulatory agencies (57%), with open-source communities (46%) being the least-used source of detection rules. That open-source communities have such a low priority is somewhat surprising, given a lot of the technology used to craft and share rules has come from the open-source community. But it is also unsurprising in that organizations are more willing to trust industry-based threat intelligence platforms that have curated rules ready for use.

It was also important to understand what format organizations prefer for their threat detection rules. In order of priority, machine-readable formats such as YARA[2] and STIX[3] are the most preferred, followed by rules that have already been integrated with security tools; human-readable detections and email notifications were the least desirable formats for receiving detection rules. The biggest challenge organizations face when receiving detection rules is the rules' quality and reliability—73% of respondents see this as a challenge. This is closely followed by compatibility issues with existing tools (55%), the sheer volume of information (54%), and the lack of context or relevance for the detection (50%).

As children we're taught that "sharing is caring." How much does this apply to sharing useful detection rules with other entities? Only 39% of respondents are sharing detection rules or indicators of compromise with other entities. Those who are sharing strongly prefer sharing daily with internal teams (35%), back to industry-specific threat intelligence platforms (27%), or with government or regulatory agencies (19%). Very few organizations are sharing their threat detection intelligence with the open-source community. The primary motivation for organizations to share their threat detection intelligence is reciprocating information sharing (68% of respondents)—sharing information so similar information is shared back with them. Sixty-five percent of respondents are keen to enhance the overall security posture of their organization, and 58% are doing it for community-based contributions, which is commendable given that's how a lot of threat intelligence for the wider cybersecurity community originated.

[2] "YARA," https://virustotal.github.io/yara/

[3] "Introduction to STIX," https://oasis-open.github.io/cti-documentation/stix/intro

Automation in Action: The Future of Incident Response

This section takes a deeper dive into how organizations respond to detected threats. Most respondents (68%) say that they perform a semi-automatic response; however, a large proportion use manual response techniques (23%). (See Figure 5.) It is not just smaller organizations that respond manually; it varies from organizations that have fewer than 100 employees up to larger multinational organizations.

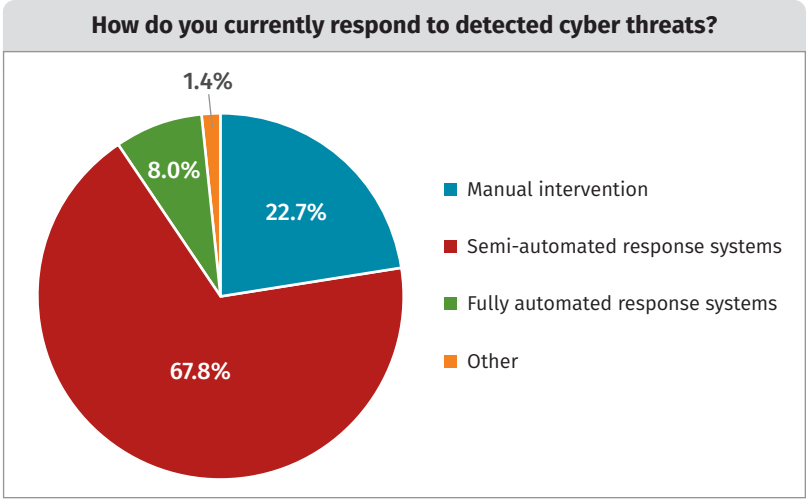


Figure 5. Threat Response Methods

When examining the tools and technologies organizations use for threat response, endpoint detection and response (EDR) emerges as the predominant choice, with 82% of respondents relying on it (see Figure 6). This closely aligns with the trends observed in threat detection, where endpoint visibility and rapid response capabilities are crucial. EDR's ability to observe, detect, and respond to threats at the endpoint level makes it a vital tool for many organizations, particularly given that threat actors generally start their attacks at endpoints or use them as a "beachhead"[4] while conducting an attack within an organization. It's not surprising for EDR to be such a heavily relied-on technology, given that it covers organizations not only for detection but also for response, while also being an effective way to consolidate tooling costs.

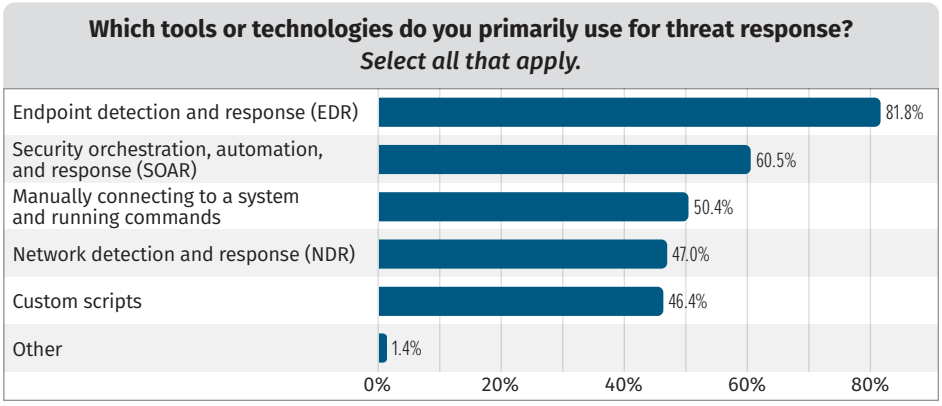


Figure 6. Threat Response Tools

The survey also reveals a notable reliance on security orchestration, automation, and response (SOAR) platforms—61% of respondents incorporate these tools into their threat response strategies. SOAR's capability to automate routine tasks and integrate various security tools enables organizations to streamline their response processes in an attempt to reduce the time it takes to address incidents. Interestingly, despite the advances in automation and tooling (both commercial and open-source) available for endpoints, 50% of respondents still manually connect to systems and run commands, indicating that hands-on, human-led response remains a significant component of threat response activities. The use of custom scripts is closely related to performing manual tasks, so it is unsurprising that 46% of respondents also use them. It also shows that although a large selection of off-the-shelf tools are available today, there are still gaps between what responders need and what's available.

[4] A beachhead is a staging location for a threat actor to operate from within an organization. It is also used often for staging collected information from a victim before exfiltration or as a staging location to access multiple systems.

The fact that 47% of respondents use NDR was a positive finding, given this is a very effective way of responding to a threat without threat actors being able to detect it, unlike a threat actor being able to see the actions of responders on endpoints when they are using EDR tools. The only significant difference between NDR-type tools and EDR-type tools is that NDR tools require more foresight and planning to get network taps in place and access to network infrastructure; in contrast, EDR tools can be pushed out while an incident is still unfolding.

The Fast and the Furious for Response

Analyzing how quickly organizations can respond to confirmed threats provides valuable insight into the maturity and effectiveness of their threat response capabilities. A significant portion of organizations (41%) say they can respond to confirmed threats within minutes, which is impressive (see Figure 7). This promising trend suggests that many organizations have established well-integrated and responsive systems, likely utilizing tools such as SOAR platforms and X/EDR solutions to facilitate rapid detection and immediate response. Additionally, 8% of organizations report being able to respond within seconds! Once a threat detection has been triggered, the ability to rapidly move and respond is a critical capability for organizations today. Based on statistics from the Google Cloud Security team,[5] often the challenge is detecting threat actors early enough—their statistics show a threat actor has at least a 10-day lead time on response, so being able to respond quickly is one way to slowly make up lost ground on threat actors that have been in an environment for some time.

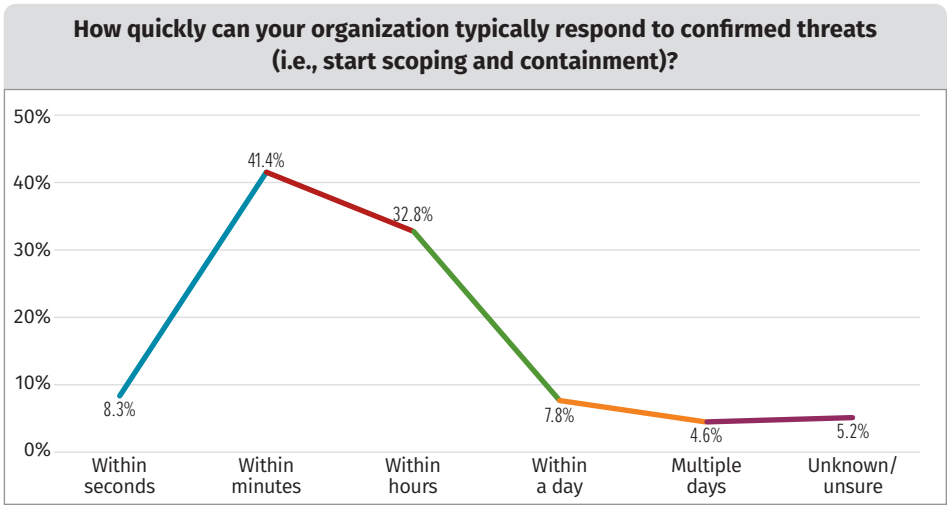


Figure 7. Speed of Threat Response

However, it is also important to note that 33% of respondents indicate their organizations typically respond within hours, and 12% take anywhere from a day to multiple days, which could imply varying levels of preparedness or resource allocation across different organizations. These response times, although still proactive, suggest there may be challenges such as slower internal processes, limited automation, or resource constraints that can delay immediate action. Although it is reassuring to see 83% of respondents can respond to a threat within seconds to hours, it appears that a portion of organizations are still struggling to get from that initial response stage to understand how embedded an actor might be, all the way through to understanding how they might go about evicting a threat actor from their environment.

[5] "M-Trends 2024 Special Report," https://cloud.google.com/security/resources/m-trends

The adoption of automated response mechanisms is becoming increasingly prevalent among organizations, with a significant 64% of respondents indicating that they have partially integrated these systems into their cybersecurity operations. This suggests a growing recognition of the benefits that automation can bring, such as faster response times and more efficient threat management. However, only 16% have fully implemented automated response mechanisms, indicating that there is still a lot of room for growth in this area. Of the remaining respondents, 15% have not adopted any automation and 5% are unsure. These may represent organizations that are either cautious about implementing automation or facing barriers such as budget constraints, skill shortages, or concerns about over-reliance on automated systems.

The most commonly employed strategies for automating detection-to-response workflows are predefined playbooks—74% of respondents are using them to standardize and streamline response actions. This reliance on playbooks highlights the value of having clear, structured, and repeatable processes in place, which can help reduce response times and ensure consistency. Additionally, this can help organizations when recruiting new staff members, ensuring there is a structure to how incoming security operations team members respond when a threat actor is within an environment. Custom integration and automation scripts are also widely used, cited by 64% of respondents, reflecting the need for tailored solutions that can fit specific organizational needs and environments. This may be for environments that are more nuanced in nature or simply that existing tools, be they commercial or open source, just don't provide the automation that some organizations require. Integration with SOAR tools is similarly popular, utilized by 62% of respondents. Interestingly, machine learning models are used by only 35% of organizations, suggesting that although AI is a growing area, it is still being explored and integrated cautiously. These results show that operations staff want tighter integration and fewer "button clicks" to achieve response tasks, which makes sense when a threat actor has at least a 10-day head start, and correlates with some of the staffing challenges we'll dive into shortly.

Where to Respond First

It is crucial to respond rapidly to threats, but it's equally important to prioritize which threats demand immediate attention. We asked respondents to identify which types of threats they consider the most severe. By understanding how organizations rank the severity of different threats, we can gain insights into how they prioritize their response efforts, ensuring that the most critical threats are addressed first.

When multiple threats are detected, a weighted average of respondents (41%) agree that prioritizing response primarily based on the severity of the threat is the most critical factor to prevent significant harm to an organization. The potential impact on business is the next key factor, with 29% indicating a focus on protecting operations and minimizing disruptions. The type of asset affected is considered the third highest priority, and is likely related to assets crucial to the organization's function, such as customer data, intellectual property, or business-critical resources. The most agreed-on factor for respondents (71%) is that resource availability is the lowest priority of the options provided.

Cybersecurity Dream Team: To Integrate or Separate?

How organizations' detection and response functions are structured not only affects the dynamics of a detection and response function, but also can have both positive and negative side effects on cybersecurity operations. When asked whether these functions are integrated within a single team or managed by separate teams, the survey results revealed an almost even split: 48% of respondents indicated that they manage these functions within separate teams, while 48% reported operating as a single, integrated team. (The remaining 4% of respondents were unsure about their organizational structure.) This near-even[6] division, although unexpected, suggests that there is no clear consensus across the industry on the best approach to organizing detection and response activities. It also may reflect differing organizational needs, resource availability, and strategic priorities. These insights will help clarify the varying approaches organizations take to balance specialized expertise and integrated operations in their cybersecurity defense efforts.

When it comes to structuring detection and response teams, organizations appear to be guided primarily by the need for specialized skills, with 68% of respondents highlighting this. This emphasis on specialization might reflect the increasing complexity of cyber operations, where having experts focused on specific aspects of security can lead to more effective detection and response. Efficiency in operations was also a significant factor, cited by 56% of respondents, indicating that many organizations believe that the right team structure can streamline processes and reduce response times. Additionally, 40% of respondents pointed to organizational policies as influencing their team structures, suggesting that internal regulations and guidelines often play a role in how these critical functions are organized. It is somewhat disappointing to see that such a large percentage of respondents are dictated to by organizational policies on how best to detect and respond to cyber threats, instead of relying on the experience and skills of their security operations staff.

In examining how these structures impact overall security posture, 48% of respondents expressed either a positive (29%) or very positive (19%) view of their current setup. This indicates that many organizations feel confident that their chosen approach, whether integrated or separated, effectively enhances their security capabilities. A significant portion of respondents (33%) held a neutral view, suggesting that although their current structure works, they might be open to improvements or adjustments. Interestingly, only a small percentage (14%) felt negatively or very negatively about their organization's team structure. It will be interesting to see how this develops over future surveys to understand if organizations find a more predominant way of structuring their detection and response teams.

[6] The numbers appear even due to rounding. The actual numbers show a 0.3% swing toward separate teams; however, for the purposes of this report, this small amount is negligible.

Looking ahead, organizations are considering various strategies to structure their detection and response teams to enhance efficiency. The most popular approach, chosen by nearly 50% of respondents, is a hybrid structure. This suggests that many organizations see value in blending elements of both integration and specialization, aiming to leverage the benefits of each approach. Such a hybrid model may provide the flexibility to adapt to different types of threats while still allowing for focused expertise where needed. Meanwhile, 44% of respondents plan to maintain specialized separate teams, indicating a continued belief in the importance of deep, focused knowledge areas for both detection and response.

Interestingly, 32% of organizations want to move toward an integrated single team, which may reflect a desire for more cohesive operations or a move for further consolidation with headcount. The small percentage (3%) choosing other approaches suggests that organizations could be looking at other structures not considered in the survey, although none were expressed in any of the free text sections of the survey. Given that respondents currently have an almost even split between a single team and separate teams, it looks like there may be a swing in the future to more hybrid or separate teams on the horizon.

Battling Cloud Threats from Below

Cloud detection and response present unique challenges and opportunities compared to traditional endpoint detection and response, primarily due to cloud environments' dynamic nature and scale. Organizations face significant challenges, with 56% citing limited expertise in cloud security as a major hurdle. This underscores the critical need for specialized knowledge to manage cloud threats effectively. The complexity of managing multicloud setups and integration with existing security tools are also prominent challenges, affecting 51% and 49% of respondents, respectively, highlighting the technical and operational difficulties inherent in cloud security.

When it comes to detecting threats, cloud-native security tools are seen as the most effective, with 21% of respondents rating them as extremely effective and 67% as effective. This suggests that leveraging security tools designed specifically for cloud environments is providing benefit to those using them. However, 13% still find cloud-native tools not effective, indicating room for improvement. Third-party and in-house-developed tools also show moderate effectiveness, but a concerning 19% and 21%, respectively, find these tools needing improvement. This may simply be because of how rapidly the cloud environment evolves, making these tools hard to maintain over time. Although 59% of respondents find manual monitoring effective, only 15% consider it extremely effective, and 26% find it ineffective. This likely reflects the limitations that manual processes may present in large-scale cloud environments.

To address these challenges, 71% of organizations plan to enhance training for security teams on cloud-specific threats, clearly recognizing the need to build internal expertise. Additionally, 53% are looking to adopt more advanced cloud-native security tools, and 52% aim to integrate AI/ML for threat detection and response; however, given the outcomes provided by organizations in previous responses to AI/ML, this may prove insignificant. The focus on training, technology adoption, and increased collaboration with cloud service providers (40%) suggests that organizations see a clear need to evolve their cloud detection and response strategies.

Investing in Talent for Detection and Response Success

When discussing the building and effective utilization of automation tools for detection and response, the importance of skilled staff cannot be overstated. As organizations increasingly rely on automated systems to manage the growing volume and complexity of cyber threats, having a team equipped with the necessary skills becomes essential. The survey data shows that you cannot simply drop in a "cool new tool" and expect it to find "all the bad things." Nearly 77% of organizations are addressing skill gaps through training programs, which is a clear indicator that organizations and their staff recognize that defending their environment requires specialized knowledge from others outside their organization. This commitment to training aligns with the plans of 71% of respondents to enhance training for cloud-specific threats, further emphasizing the need for specialized knowledge in managing the unique challenges posed by cloud environments.

Hiring skilled personnel is another critical strategy, with 61% of respondents bringing in external expertise to strengthen their detection and response teams. This approach complements internal training efforts, providing immediate access to advanced skills that can accelerate the detection and response capabilities, at least for the short term; however, this may not be a sustainable approach over time to build skills internally. This type of strategy could decrease the number of new graduates or junior staff entering the cyber defense area within our industry. Although it could be more of a strategic plan for the current state of the economy, it will be an interesting trend to watch over time.

Outsourcing, used by 40% of organizations, can offer a flexible solution to access specialized skills and knowledge without the long-term investment of hiring full-time staff. This approach can be particularly valuable for smaller organizations or those with budget constraints, enabling them to benefit from expert insights and capabilities as needed. Just over 30% use internal rotations, suggesting that some organizations are also exploring ways to diversify their existing talent, ensuring that team members gain experience across different cybersecurity areas.

Organizations appear to be taking a multifaceted approach to improving detection and response to threats within cloud infrastructure. Beyond training, 53% of respondents plan to adopt more advanced cloud-native security tools, and another 53% are looking to integrate AI and ML for enhanced threat detection and response. Although crucial, these technological improvements require staff adept at managing and optimizing these tools to ensure they deliver their full potential and accurately detect and enable response functions for threats. The data shows that organizations recognize this need, as evidenced by the high percentage focusing on training and hiring skilled personnel. The survey results for training and education highlight a clear recognition of the need for trained staff to build and maintain automation tools and uplift capabilities for protecting cloud environments. Just remember that the expensive AI or ML tool sold to you needs an experienced operator to interpret what it is doing and ensure it is defending your organization correctly.

Pay Now or Pay Later: The Cost of Cybersecurity

Many organizations operate under budget constraints regarding detection and response activities. A significant portion of respondents (42%) describe their budget allocation as adequate but limited, and another 22% find it outright insufficient (see Figure 8). This suggests that although organizations are aware of the importance of investing in detection and response, they are often forced to make do with limited resources. Only 26% of respondents consider their budget sufficient, and a mere 5% view it as more than sufficient, highlighting a general sense of financial strain within this critical area of cybersecurity. These limitations could impact the effectiveness of threat detection and response, because financial resources are crucial for acquiring and maintaining advanced tools and training, and retaining skilled personnel.

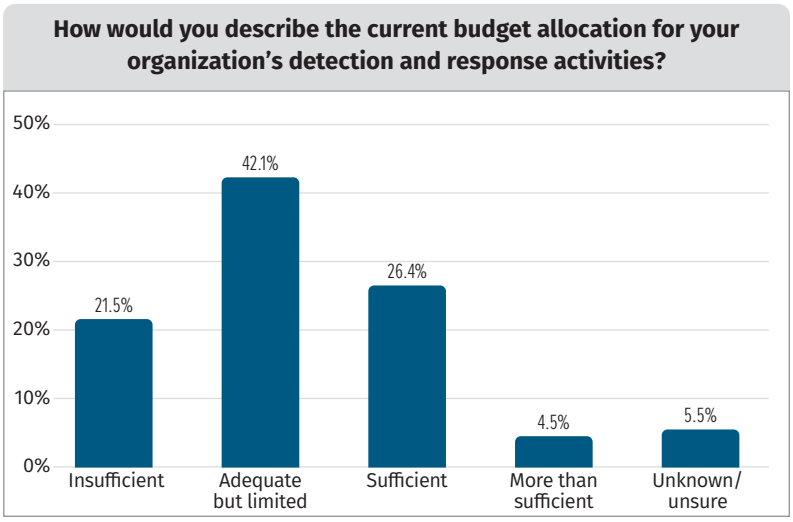


Figure 8. Adequacy of Detection and Response Budget

Looking to the future, there appears to be some optimism, albeit cautious, regarding budget increases for detection and response departments. About 42% of respondents anticipate a moderate budget increase, indicating that some organizations are beginning to recognize the need for more significant investment to enhance their cybersecurity posture. However, this optimism is tempered by the fact that only 7% foresee a significant increase, whereas 25% expect no change at all. Furthermore, 9% anticipate a moderate budget decrease, and 2% expect a significant decrease. These findings suggest that although there is awareness of the need for increased investment, financial constraints and competing priorities limit the extent to which budgets can be expanded.

The current and projected budget scenarios present challenges for organizations aiming to improve their detection and response capabilities. The fact that a substantial number of organizations are working with insufficient or limited budgets could hinder their ability to adopt new technologies, hire additional skilled personnel, and invest in necessary training programs. As the threat landscape continues to evolve and become more sophisticated, these budget limitations could make it increasingly difficult for organizations to keep pace with emerging threats. It is ironic that a lot of the countries represented in the survey this year impose significant fines for data breaches. Given that the detection response teams within an organization are directly related to preventing a data breach, it may be that an organization pays for investment in their detection response team or pays a data breach fine if they don't—either way, the funding for this would have to come from somewhere.

Metrics That Matter in Threat Response

Measuring the performance of detection and response teams is critical to demonstrating the value and effectiveness of cybersecurity efforts to leadership and the broader organization. Most organizations use key performance indicators (KPIs) that focus on the speed and efficiency of their response, with 67% tracking mean time to respond (MTTR) and 52% monitoring mean time to detect (MTTD). These metrics are crucial because they highlight how quickly a team can react to and identify threats, which is vital in minimizing potential damage. Other common KPIs include the number of incidents detected (64%) and resolved (58%), though these counts can sometimes be misleading. As detection capabilities and automation improve, the volume of incidents may increase, which does not necessarily correlate with an increased threat level but rather an enhanced ability to uncover and address potential issues.

Despite the importance of these metrics, the effectiveness of current measurement practices is mixed. Only about 26% of respondents believe their metrics are very or extremely effective in clearly understanding their team's performance; a larger portion (39%) finds them only moderately effective. This suggests that although metrics are being tracked, they may not always provide the comprehensive insights needed to fully gauge the performance of the detection or response team members. A notable challenge highlighted by 51% of respondents is the difficulty in data collection, compounded by a lack of skilled personnel (49%) and standardized metrics (45%). Although metrics are on the minds of detection and response teams, they may be getting neglected due to issues with being able to automate better and track metrics instead of distracting from the operational work of defending a network.

Benchmarking against industry standards can provide valuable context for these metrics, yet only 23% of organizations do so regularly, with 31% doing so occasionally. This indicates a potential area for improvement, because regular benchmarking could help organizations understand their performance in relation to their industry peers. Challenges such as insufficient tools for analysis (42%) and high volumes of incidents (31%) also highlight the need for better resources. The challenge is often taking this data and communicating this challenge to leadership.

Understanding and measuring detection coverage is crucial for organizations aiming to maintain a robust security posture. According to the survey, a significant majority of organizations (64%) actively assess or measure their detection coverage and capabilities, demonstrating a clear commitment to understanding and improving their security effectiveness. However, 23% do not assess or measure their detection coverage, which could leave them vulnerable to gaps in their detection defenses that go unnoticed. Regular assessment is vital. This does not necessarily require adhering to a specific industry standard, but instead applying a consistent methodology that identifies gaps and monitors improvements over time. Without this, organizations risk having blind spots in their defenses, which threat actors will exploit.

Those who measure their detection coverage often use established frameworks and intelligence. The MITRE ATT&CK Matrix, a popular tool used by 74% of respondents, helps organizations track the tactics and techniques used by adversaries and thereby assess their ability to detect those behaviors. Additionally, 72% of organizations rely on threat intelligence reports, giving them insights into current and emerging threats. Red team operations are utilized by 62% of respondents, indicating a proactive approach to testing and validating their detection capabilities. Although these methods are effective, relying solely on vendor tools (35%) or third-party vendors (36%) may limit an organization's ability to fully understand and control its detection capabilities.

The frequency with which organizations review the performance metrics of their detection and response teams varies widely. Nearly a third of respondents (29%) conduct reviews monthly, suggesting that many organizations may need to monitor their performance more closely. Almost 9% do so daily, which is understandable if an organization has the data and the ability to adapt to issues. Some 22% of organizations conduct weekly reviews, offering a more balanced approach to regular performance assessment. Interestingly, 14% review metrics quarterly, and 8% do so annually, which really is too far apart and is likely limiting their ability to identify and adapt to issues. Threat actors do not wait three months to a year to adjust their technique, so neither should organizations when it comes to reviewing their capabilities.

In terms of improving the measurement of detection and response performance, there is no clear standout, indicating organizations realize that they need to use different approaches to tackle various issues. The most frequently cited improvements include real-time monitoring capabilities (54%) and advanced analytics and reporting tools (52%), highlighting the desire for more immediate and insightful data on security performance. Better integration with other security tools (50%) and regular training and skill assessments (49%) are also seen as essential, indicating that organizations understand the importance of having the right tools and ensuring that their teams can use them effectively. Nearly 48% of respondents want more comprehensive metrics, suggesting that many organizations feel their current metrics are not providing a complete picture of their detection and response capabilities.

From False Positives to Real Problems

False positives are a significant challenge for many organizations attempting to detect cyber threats—64% of respondents identified them as a major issue (see Figure 9). Some 42% of respondents encountered false positives frequently (accounting for 41% to 80% of cases), which indicates a substantial area for improvement in detection tools and processes. When detection systems generate a high number of false positives, it can lead to alert fatigue, where security teams become desensitized to alerts, potentially overlooking true threats. Additionally, managing false positives consumes valuable time and resources that could otherwise be devoted to investigating and responding to genuine threats. This issue is exacerbated by the volume of data organizations need to process, a challenge highlighted by 63% of respondents. This increases the likelihood of false positives and further strains security operations.

64% of respondents identified false positives as a major issue.

Figure 9. Cyber Threat Detection Challenges

The sophistication of threats, cited by 45% of respondents, and the lack of skilled personnel, noted by 59%, add to the complexity of the threat detection landscape. Sophisticated attacks can bypass traditional detection methods, making it difficult for teams to differentiate between legitimate threats and benign anomalies. This likely explains why manual threat hunting is the second-most-useful process for detecting threats. Furthermore, the lack of skilled personnel compounds the problem, because experienced security professionals are more capable of fine-tuning detection systems to minimize false positives and accurately identify real threats. With only 10% of respondents indicating they rarely encounter false positives, it is clear that detection tools and techniques still have a long way to go in accurately detecting a real threat.

To address these challenges, organizations need to invest in better training for their staff and take a more in-depth look at the technology and tools they have that are generating false positives. One possible solution is to collect metrics on the false positives generated by commercial tools and drive those vendors to reduce the amount of overhead it causes the detection and response team.

In terms of other challenges and barriers, budget constraints are the most significant obstacle organizations face in maintaining an effective detection and response capability, with 47% of respondents ranking it as their top concern. This finding highlights the financial pressures that many organizations are under, which can limit their ability to invest in advanced tools, technologies, and skilled personnel needed to enhance their cybersecurity posture. Talent acquisition and retention was viewed as the second (weighted) highest obstacle, highlighted by 21% as a primary concern, further underscoring the difficulty in securing and maintaining the skilled professionals necessary to manage sophisticated detection and response operations. Technology limitations were the third (weighted) obstacle, with 36% of respondents ranking it as a significant issue, reflecting the challenges of keeping up with rapidly evolving threat landscapes and the need for constant updates and improvements in detection technologies. Regulatory compliance ranked as the fourth (weighted) obstacle, with 13% of respondents seeing it as a major concern. Although regulatory compliance, weighted against the other options, was the lowest, it still shows the ongoing challenge organizations face in meeting various legal and regulatory requirements, which can sometimes divert resources away from other critical security activities. These challenges illustrate the complex balancing act that organizations must perform when trying to defend their environment, while meeting the needs of the business or regulations at the same time.

The Future of Threat Response Is Automated

The survey data indicates a strong inclination toward increased use of AI and machine learning in threat detection and response, with 67% of respondents planning to expand their use of these technologies. This reflects a growing recognition of AI's potential to enhance cybersecurity efforts by automating and improving the accuracy of threat detection and response. Only 8% of organizations do not plan to increase their use of AI and ML, which could be due to budget constraints or existing investments in other technologies. Given the challenges respondents have with the use of AI and ML technologies, it may make sense that 8% want to hold back and see how AI and ML play out in the industry. The remaining 25% who are unsure or undecided may reflect a wait-and-see approach, as these organizations evaluate the effectiveness of AI in real-world scenarios before committing further resources.

Among those planning to increase the use of AI, the majority (58%) intend to do so moderately, while 29% are planning extensive adoption. This moderate to extensive adoption plan indicates that organizations are aiming to strike a balance between leveraging advanced technologies and maintaining control over their cybersecurity operations. The high interest in advancements like behavioral analysis (83%) and automated threat hunting (64%) highlights the desire to move toward more proactive and sophisticated detection methods. Predictive analytics (60%) and advanced correlation engines (56%) are also on the agenda, suggesting that organizations are looking to anticipate and correlate threats more effectively, rather than simply reacting to them. We'll keep an eye on these technologies as this survey progresses over the coming years. However, these technologies are no silver bullet for catching threats; they require significant watering and feeding to keep them healthy and useful.

In terms of automating detection-to-response workflows, organizations are considering a variety of strategies. Enhanced playbooks (68%) and improved integration with SOAR tools (65%) are top priorities, reflecting the need for structured, automated processes that can streamline responses and reduce the time to mitigate threats. Nearly 52% of respondents are planning to implement custom automation scripts, indicating the need for more manual solutions, likely for very specific requirements; 48% are planning for advanced machine learning models. The plan to purchase new tools with built-in integrations (38%) further shows a trend toward seeking comprehensive, out-of-the-box solutions that can simplify implementation and integration efforts, which feed into the initial requirement of improved integrations.

The future for detection and response still looks a little mixed, with a touch of caution for many respondents. It's clear that respondents want to play in the world of AI and ML, although the technologies still need to mature. Overall, the biggest advancements detection and response teams are crying out for is more automation with the tools they have or intend to purchase. Being able to reduce the number of manual tasks required is a huge win, so it makes sense that this is the driving force for the future—at least for now.

Conclusion

The findings from the first year of the SANS Detection and Response Survey paint a comprehensive picture of how organizations currently handle the complexities of threat detection and response. The data consistently emphasizes the crucial role of human expertise in balancing advanced technology, as evidenced by the widespread use of endpoint detection and response (EDR) tools, which 82% of respondents rely on, and the adoption of semi-automated response systems by 67% of organizations. Despite the increasing role of automation, there remains a critical need for skilled personnel to interpret and act on these technologies, underscored by the 59% of organizations citing a lack of skilled personnel as a significant challenge. The mixed effectiveness of AI- and ML-based tools also points to the need for ongoing development and tuning to fully realize their potential in cybersecurity.

Budget constraints and resource limitations emerged as recurring themes throughout the survey, with nearly half of the respondents citing budget as their top obstacle in maintaining an effective detection and response capability. These financial challenges are compounded by the need to comply with regulatory requirements and keep pace with technological advancements, which are critical yet resource-intensive. The need for more comprehensive metrics and better integration of security tools also underscores the evolving landscape of the industry, where organizations must continuously adapt their strategies to address internal and external pressures. As organizations look to the future, there is a clear recognition of the importance of investing in advanced detection and response capabilities, with a strong focus on increasing the use of AI and ML, improving integration with SOAR tools, and enhancing training programs to build internal expertise. It is clear that although more advanced technologies are on the horizon and being used by organizations, there is a strong need for skilled staff behind the keyboard to be able to track threat actors within organizations' networks.

Sponsor

SANS would like to thank this paper's sponsor:

[P] | Prelude

[P] | Prelude

SANS | Research Program

Product Briefing

Detection and Response with Prelude Security:

Insights from the SANS 2024 Detection and Response Survey

November 2024

Attacks on organizations are only growing, and most of us in cybersecurity spend significant time and energy detecting and preventing those attacks. Doing it well requires trained and skilled staff, but teams are increasingly able to call on sophisticated AI and machine learning tools to help protect important data.

Prelude Security

You've got detections. You've got playbooks. You've got sensors. You've got dashboards. Do you have any idea how well they're all working?

That's the problem Prelude is here to solve. They start by assuming there's a breach, and work with the mindset of an attacker to find the cracks that can be used to slip malicious code into your systems. The Prelude platform has traditionally focused on the endpoint—the place where most dangerous activities happen—and emulates an adversary to test your system's ability to detect and thwart unwanted activity.

Prior to a testing engagement, Prelude provides foundational monitoring capabilities to make sure all your controls are in place, healthy and configured correctly. It's far too easy for an organization to get complacent and rely on controls that aren't implemented in the right places or configured to get maximum value for the owner. See Figure 1, on the next page.

Key Findings

Most respondents (82%) rely on Endpoint Detection and Response (EDR) as one of their key network security tools.

Many teams (64%) are actively assessing and validating their systems.

More than half of respondents (59%) said the need for skilled personnel was the top obstacle to implementation.

To power its monitoring, Prelude leverages API integrations to make sure everything is in place. But reporting isn't everything—in fact, most SOC analysts would rather look at fewer reports, not more. What makes a report stand out? When it can be used to take immediate action. For many popular security controls, Prelude lets analysts click to fix failures immediately, then deploy new tests via their agent to make sure the fix worked. The probe reports back what each control saw, what it alerted, and what it stopped.

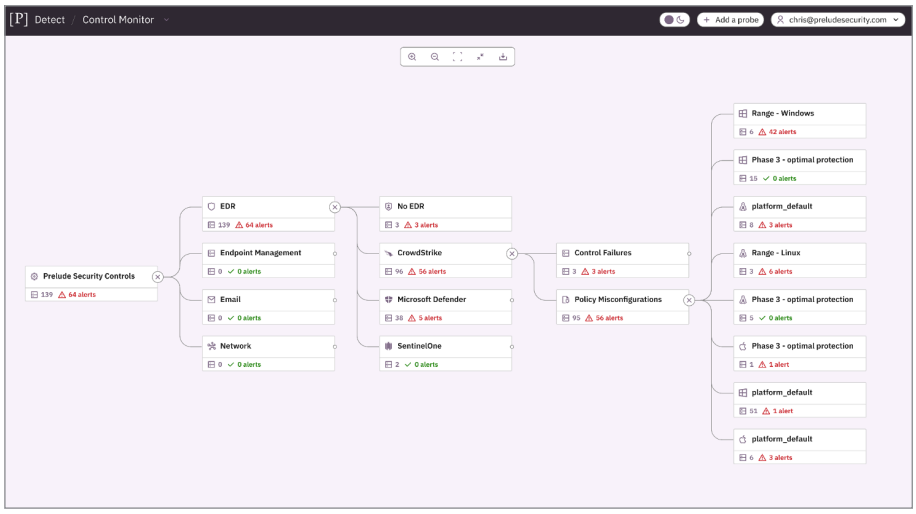


Figure 1. Prelude Detect Control Monitor

Even better, if you expected a detection and didn't see one, Prelude's technology can deploy one on the spot, helping to seal up holes you didn't know you had. Automating this process means you don't have the gap sitting open while you figure out what went wrong. It's all meant to save time for your expert analysts and give you a bit of breathing room to bring less experienced staffers up to speed.

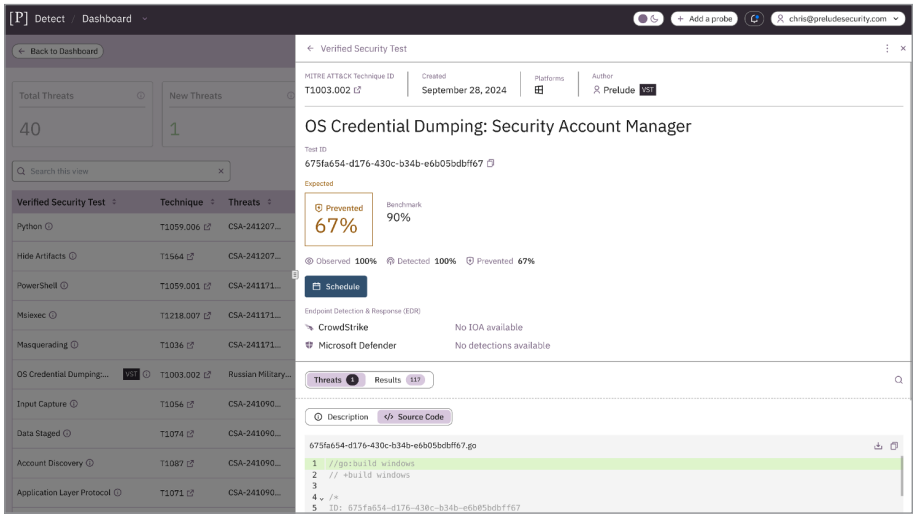


Figure 2. Prelude Detect Dashboard

Prelude's security control first monitors for missing and misconfigured controls. Then, it tests against emulations of adversary behavior. These reduced functionality ("zombie mode") controls are not well documented and very difficult to find using conventional software. Having this level of protection is an extra layer of confidence for your SOC team, who can easily take action to correct misconfigurations and missing controls right in Prelude's dashboard. Customers occasionally say Prelude has found dozens or even hundreds of endpoints the security team didn't even know about.

The SANS Detection and Response survey shows organizations are increasingly moving toward detection on endpoints. Prelude's value lies in being able to demonstrate that investments in detection are optimally configured and protecting the organization. For further validation, tests canemulate a specific set of threat actors, evaluate specific malware tools, or focus on the most mission-critical parts of your systems. Prelude lets you easily initiate tests at your convenience. See Figure 2.

Security analysts are big on visibility, because they need to be able to see—and to show their managers—what specifically is happening on their networks. Prelude shows you what each test is going to do before you start it, and provides examples of expected output and suggestions for remediation if yours is not as expected. Tests are designed to operate on test data only—your information stays intact.

If you want peace of mind that comes with knowing your controls are doing their job, visit **www.preludesecurity.com**