binalyze!

Strategies for Minimizing Investigation Time and Complexity

Empowering Cyber Resilience: Streamlining Digital Forensics and Incident Response

Introduction

Cybercriminals are always changing their tactics, putting organizations at constant risk. . Security leaders know that the ability to swiftly detect, investigate, and respond to security incidents is paramount today. Although we've gotten better at detecting threats early, we struggle with investigating them effectively.

Reducing the time between threat detection and response to an incident is an ongoing issue that must be addressed for modern security and risk mitigation. Traditional methods are no longer sufficient to tackle the complex threats and challenges security teams face today.

Digital forensics emerges as a cornerstone of comprehensive incident response strategies. By meticulously analyzing digital evidence, digital forensics enables organizations to uncover the full scope of an attack, identify the perpetrators, and understand the methods employed. This depth of insight is crucial for not only resolving the immediate incident but also for fortifying defenses against future threats.

In this report, we first examine the hurdles in using digital forensic methods for incident response investigations. Then, we discuss strategies that can speed up these investigations. Our goal is to help teams achieve quicker response times, leading to stronger outcomes and increased cyber resilience for organizations.

Investigation Challenges Today

Multiple challenges slow down investigations today.

Skills Shortage

A critical challenge faced by organizations is the shortage of skilled professionals capable of navigating cyber investigations using digital forensics. The specialized knowledge required to analyze digital evidence, understand sophisticated threat actors, and manage complex tools creates a bottleneck in the investigation process. Existing security solutions often rely heavily on manual effort and expertise, exacerbating the skills gap issue and hindering the timely resolution of security incidents.

What is the extent of the disparity? Data from CyberSeek reveals that while approximately 1.1 million individuals are currently employed in cybersecurity roles in the U.S., there are over 500,000 vacant positions in the field. Looking globally, projections from Cybersecurity Ventures suggest that the deficit in the cyber workforce could reach around 3.5 million individuals by 2025.

Regulatory Obligations and Compliance

The need to comply with a myriad of regulatory requirements adds another layer of complexity to investigations. Traditional tools may lack the necessary documentation or workflow automation to ensure compliance efficiently. This deficiency can lead to potential delays in response times and increase the risk of non-compliance, further complicating the investigation process.

Integration and Automation Challenges

To comprehensively investigate and respond to escalated cybersecurity incidents, incident responders typically complement existing SOC monitoring and detection solutions with DFIR tools. These are necessary to provide forensic visibility and capabilities. Many traditional solutions operate in silos and lack integration capabilities, making it difficult to automate processes across different tools and platforms. This lack of integration and automation slows down the response time and increases the workload on analysts and responders. Without seamless integration, security teams struggle to streamline workflows and achieve comprehensive threat detection and response.

Volume and Complexity of Data

The sheer volume and complexity of data present in modern cybersecurity environments pose significant challenges for security teams. With data scattered across various sources such as cloud, on-premises, and hybrid environments, managing, let alone analyzing this data required for granular investigations becomes incredibly challenging. Existing SOC monitoring and detection solutions, meanwhile, have limited storage capacity suited for their detection and monitoring needs but are unable to store forensic-level detail needed for investigations. Investigations may require teams to gather additional evidence but traditional DFIR tools that provide deep investigation capability, may struggle to scale effectively or integrate smoothly across diverse data sources, resulting in delays and inefficiencies in the investigation process.

Collection from Remote Assets

One of the primary challenges in incident response investigations is collecting evidence from remote assets. Traditionally, access to remote assets would involve travel time to get boots on the ground which significantly slows down the start of any investigation. Add to that obstacles related to collecting evidence from remote assets, including:

- **Access to Logs and Data:** Remote assets may lack comprehensive logging capabilities, making it challenging to gather relevant evidence to understand the scope and impact of the incident.
- **Bandwidth Constraints:** Data transfer from remote locations to centralized storage for analysis is often slowed by limited bandwidth.
- **Diverse IT Environments:** Remote assets often operate in heterogeneous environments with varying configurations, complicating the standardization of data collection methods and analysis.
- **Security Concerns:** Ensuring the secure transmission of data from remote assets is crucial to prevent interception or tampering during investigations, adding a layer of complexity to evidence collection efforts.

Implementing a rigorous investigation framework is indispensable for uncovering the intricacies of each threat, enabling timely interventions, and fostering an environment of continuous improvement in security practices. By prioritizing comprehensive investigations, organizations can enhance their ability to withstand and recover from cyber incidents, ensuring long-term security and building cyber resilience.

The Multi-Tool Challenge in Managing Investigations

Security analysts interact with 6 tools to investigate an alert[1], while DFIR professionals use 11-15 paid or open source tools for investigations[2]. In addition to the integration issues highlighted above, there are additional hurdles to consider that can slow down the investigation process:

- **Complex User Interfaces:** Each tool may have its interface and learning curve, slowing down investigations as analysts navigate between multiple platforms to gather information and perform analysis.
- **Data Overload:** The proliferation of security tools can result in information overload, overwhelming analysts with vast amounts of data and making it challenging to identify relevant insights efficiently.
- **Costly Tool Sprawl:** A multitude of tools increases licensing and training expenses, impacting budgets.

Repetitive and Time-Consuming Tasks

DFIR processes involve numerous tasks, such as evidence collection and analysis, documentation, and reporting. Analysts are forced to spend valuable time on manual, repetitive tasks that could be automated, resulting in inefficiencies and delays in incident resolution.

1 SOC Market Trends Report, ESG, Oct 2023
2 The State of Digital Forensics and Incident Response, IDC, Sept 2023

Why Existing Tools and Approaches Don't Work

Traditional forensic tools and methods present significant challenges in meeting the needs of cybersecurity environments. These tools are often complex and not well-suited to the speed, scale, and agility required for modern investigations. Additionally, they typically specialize in specific platforms or parts of the investigation process, leading to fragmentation in the investigative workflow. On the other hand, existing monitoring and detection tools like EDR, XDR, and SIEM provide some level of alert investigation capability but lack the comprehensive forensic visibility necessary for thorough investigations. This gap highlights the need for a more integrated and streamlined approach to incident response.

Amid This Difficult Landscape, Shrinking the Time to Investigate is Essential

The importance of shrinking the investigation window cannot be overstated. By expediting the detection, investigation, and mitigation of security incidents, organizations can effectively minimize the potential impact of breaches, safeguard sensitive data, and uphold business continuity. However, achieving this goal is not without its challenges, as the process of conducting thorough investigations is riddled with complexities and obstacles.

Consider the following data points:

Average Time for Incident Investigation and Resolution

The process of incident response, from detection to resolution, is critical for organizations to maintain their cybersecurity posture and mitigate risks effectively. However, the average time taken for incident investigation and resolution can vary significantly, impacting the overall security and operational continuity of businesses.

Investigation Time: Based on a recent IDC report, the average time to investigate an incident stands at approximately 26.1 days. This duration encompasses various activities, including initial detection, analysis of evidence, identification of the root cause, and assessment of the incident's impact.

Bridging the Gap between Detection and Investigation

The adoption of non-traditional digital forensic technologies for incident response investigations has become essential due to dispersed data across regions and platforms and the nature of the threats being investigated. Manual processes to gather and process data required for detailed investigations can delay the start of investigations by days or even weeks. However, leveraging cloud-based platforms enables efficient investigation of assets regardless of their physical location. This enhances investigation efficiency, mirroring the depth of on-premises investigations without the hassle of collecting, and then analyzing evidence from remote and spread-out digital estates.

Automation and Integration

Implementing automation streamlines the collection and analysis of data by reducing manual, repetitive tasks. Integration with SIEM, EDR and XDR solutions automates data collection, analysis, and response to common threats. This approach accelerates investigations and minimizes human errors, enabling organizations to respond to incidents promptly and effectively.

Instead of requiring analysts and responders to manually collect data and perform initial analyses upon receiving an alert, investigation and response automation solutions seamlessly kick-off the process. Upon detecting a potential threat, alerts trigger automatic evidence collection from affected assets, delivering crucial data even before analysts start their work. This preemptive action ensures that critical analysis is already in progress, greatly reducing both the time to initiate an investigation and the overall response time to security incidents.

Enhanced Forensic Visibility

Solutions providing comprehensive visibility into an organization's digital environment enable quicker, more informed decision-making. Emphasizing and enabling forensic-level visibility over alert-level visibility ensures that responders have all the necessary information to understand and counteract threats effectively.

User Experience and Operational Speed

Improving the user experience and enabling analysts and responders to use forensic capabilities facilitates quicker adoption and more efficient use by analysts and responders alike. Emphasizing speed ensures that investigations can keep pace with the rapidly evolving threat landscape. This enables organizations to respond to incidents with increased agility, enhancing overall operational speed and effectiveness.

Get Together: How to Foster Collaboration

The adoption of platforms that facilitate real-time collaboration among investigators can break down geographical barriers. Tools that offer secure communication channels, shared workspaces, and real-time data analysis can foster a "borderless investigation" environment, crucial for timely and effective incident response.

Benefits of Collaboration

Collaboration in incident response investigations offers numerous advantages, transforming the process into a team sport where every member contributes to a more comprehensive investigation. By bringing together cross-functional and regionally distributed teams in a shared workspace, collaboration fosters seamless teamwork regardless of physical location. This shared environment allows for the exchange of insights and findings in real time, leading to enhanced decision-making, faster response times, and increased accuracy. Moreover, collaboration promotes learning and skill development among team members, strengthening organizational resilience against future threats.

Contribution of Shared Tooling and Technologies

Shared tooling and technologies play a pivotal role in standardizing and streamlining incident response processes, leading to greater efficiency and effectiveness. Solutions that can provide a single view of the investigation and evidence, enabling teams to work on a consolidated view of information, insights, and analysis findings. By integrating capabilities for data collection, analysis, timeline creation, and reporting, shared technologies ensure that all team members operate using the same data and insights, reducing response times and improving overall security posture. Furthermore, shared technologies facilitate automated workflows, ensuring consistency in response, and compliance with regulatory requirements. Ultimately, investing in shared tools and technologies enhances collaboration, promotes standardization, and contributes to cost efficiency in incident response investigations.

The Role of Proactive Response

Proactive response strategies enable organizations to stay one step ahead of potential threats, reducing the time and resources required for investigations and enhancing overall security posture. The sooner a potential threat is detected, the simpler and shorter the subsequent investigation typically becomes. Identifying a single compromised asset promptly can prevent the more significant challenge of remediating an entire environment later on, after the threat has escalated and spread.

Organizations must adopt proactive response strategies to reduce investigation time and complexity. These include regular security drills and exercises that not only test the resilience of security controls but also fine-tune detection capabilities. By continuously improving these processes, organizations can respond more effectively to incidents.

Another vital component of a proactive response is compromise assessments. Traditional detection tools are limited to recognizing known threats, leaving organizations vulnerable to zero-day attacks and other novel exploits. By conducting compromise assessments, organizations can uncover undetected threats, including those that have bypassed existing security measures.

The integration of compromise assessment as a continuous process is gaining traction. Leveraging investigation and response automation technologies enables organizations to perform forensic-level assessments rapidly and at scale. This continuous assessment ensures that threats are identified and mitigated with minimal delay, thereby reducing the time and complexity of investigations.

Lastly, Proactive threat hunting is also critical. Skilled analysts use their knowledge of adversary tactics and threat intelligence to seek out and neutralize threats before they manifest into full-scale attacks. This hypothesis-driven approach ensures that potential threats are addressed promptly and decisively.

Case Studies

Case Study 1: Demonstrating the Effectiveness of Remote Investigations and Shrinking the Investigation Window

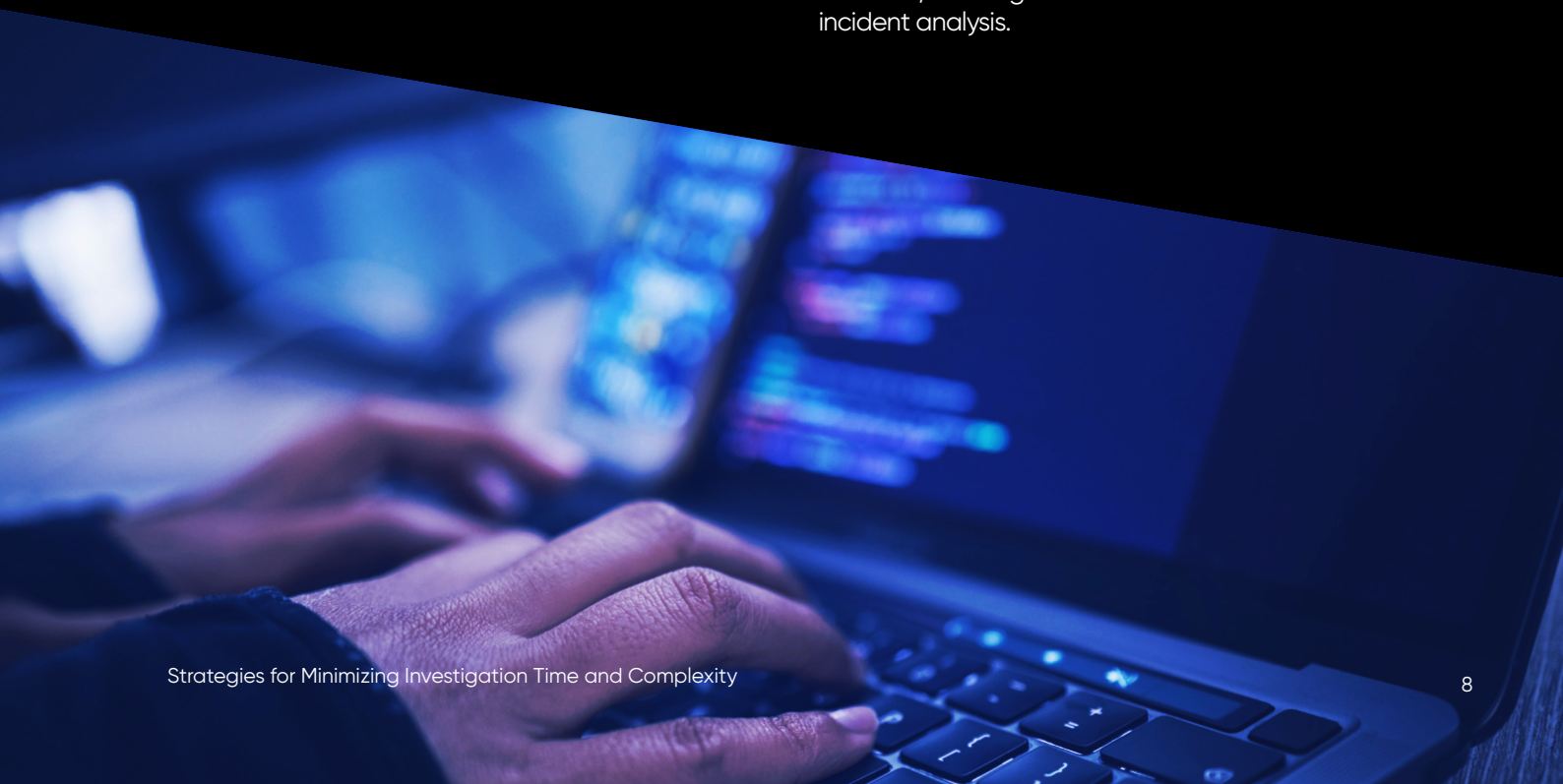
A prominent European cybersecurity firm faced the challenge of expediting investigations and evidence collection across diverse digital environments. Seeking to enhance their incident response capabilities, they aimed to remotely identify critical assets and streamline reporting for prompt client insights.

Adopting the Binalyze AIR solution yielded significant success for the security firm. They witnessed a drastic reduction in evidence collection times, from days to mere minutes, thereby accelerating investigation workflows. Leveraging Binalyze AIR's remote evidence collection and automation capabilities, the organization achieved greater efficiency, collaborated seamlessly, and experienced a notable 30% increase in case investigation speed. Binalyze AIR facilitated triage at scale, empowering the security firm to swiftly identify affected assets and prioritize high-priority investigations. Additionally, automation and collaboration features enabled the organization's teams to work together seamlessly, further boosting overall efficiency. With Binalyze AIR's user-friendly interface, the firm reduced onboarding times to under 30 minutes, facilitating swift implementation and immediate focus on client service delivery.

Case Study 2: Enhancing Incident Response Efficiency at a Leading Telecommunication Company

A prominent telecommunication company faced the challenge of optimizing its Digital Forensics and Incident Response (DFIR) processes. With the increasing complexity and volume of data, the company's incident response teams needed an effective suite to swiftly collect, investigate, and analyze evidence, assess compromises, generate reports, and take remediation actions promptly. As a leading telecommunications provider with operations in multiple countries and millions of subscribers, the company faced challenges in managing the influx of data, exacerbated by the shift to remote work during the pandemic. With over 550 data sources and eight billion raw data logs processed daily, the Cyber Defence Center grappled with over 300 daily alerts. To address these challenges and comply with stringent data privacy regulations, the company developed the BOZOK Cyber Threat Intelligence (CTI) platform, including data leakage, brand protection, and vulnerability modules.

The company achieved significant efficiency gains after implementing Binalyze AIR, experiencing a significant reduction in evidence collection times from days to mere minutes. The solution's remote evidence collection and automation capabilities led to improved efficiency, eliminating human errors and saving 49% of full-time equivalent (FTE) time and effort. Moreover, Binalyze AIR facilitated collaboration among team members, providing a central hub for analysts to work on cases from a single interface, resulting in faster and more accurate incident analysis.

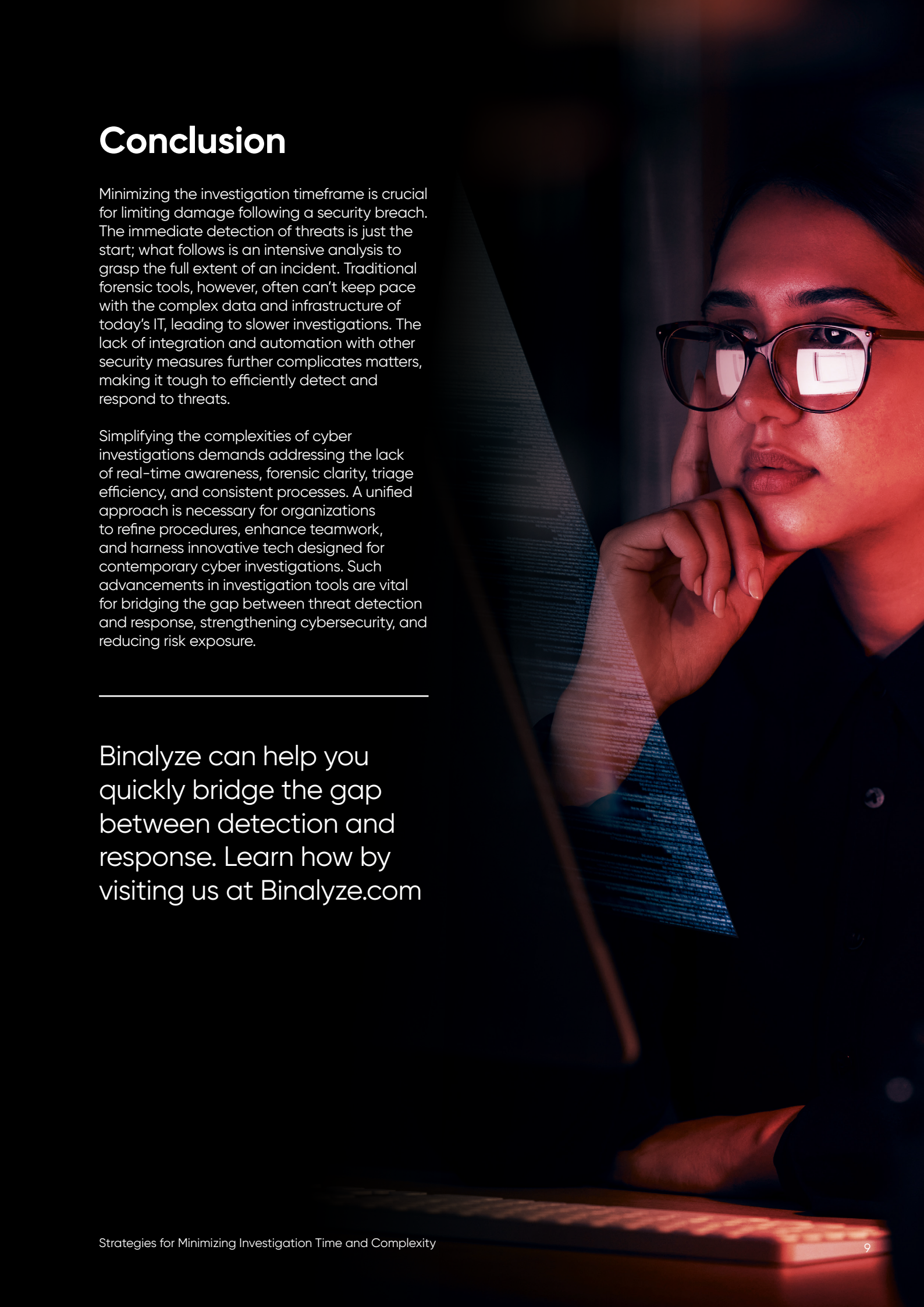


Conclusion

Minimizing the investigation timeframe is crucial for limiting damage following a security breach. The immediate detection of threats is just the start; what follows is an intensive analysis to grasp the full extent of an incident. Traditional forensic tools, however, often can't keep pace with the complex data and infrastructure of today's IT, leading to slower investigations. The lack of integration and automation with other security measures further complicates matters, making it tough to efficiently detect and respond to threats.

Simplifying the complexities of cyber investigations demands addressing the lack of real-time awareness, forensic clarity, triage efficiency, and consistent processes. A unified approach is necessary for organizations to refine procedures, enhance teamwork, and harness innovative tech designed for contemporary cyber investigations. Such advancements in investigation tools are vital for bridging the gap between threat detection and response, strengthening cybersecurity, and reducing risk exposure.

Binalyze can help you quickly bridge the gap between detection and response. Learn how by visiting us at Binalyze.com



binalyze!

To find out more about our next-gen solution, visit us at Binalyze.com or start your free 14-day trial today.

Visit us at www.binalyze.com

Binalyze OÜ
Harju maakond, Tallinn,
Kesklinna linnaosa, Hobujaama
tn 4, 10151, Estonia