DECODING SIEM DECEPTIONS

panther

INTRODUCTION

In this eBook, we will delve into the deceptive claims and limitations of legacy and other SIEM solutions.

By understanding these common pitfalls, you will gain the knowledge and confidence to choose a modern SIEM that truly empowers your security operations. From debunking cloud-native myths to unraveling the hidden costs, each chapter explores a specific deception and provides actionable insights on how to avoid them.

Through this comprehensive guide, you will discover the importance of transparency and flexibility in a modern SIEM. We will explore how a cloud-native architecture ensures seamless scalability, resilience, and adaptability to changing infrastructures. You will learn about the risks associated with legacy SIEMs that hinder effective threat detection and response.

Furthermore, we will uncover the truth behind pricing models and highlight the advantages of a modern SIEM's transparent pricing structure. With a focus on operational efficiency, we will demonstrate how a modern SIEM eliminates the need for dedicated specialists and empowers engineers to take control of their security processes.

Finally, we will emphasize the significance of Detection-as-Code, breaking down the complexities of legacy SIEMs and enabling you to customize detection strategies based on your unique requirements. By leveraging the power of a modern SIEM, you can overcome the limitations of legacy solutions and empower your security team to tackle evolving threats effectively.

DECEPTION #1

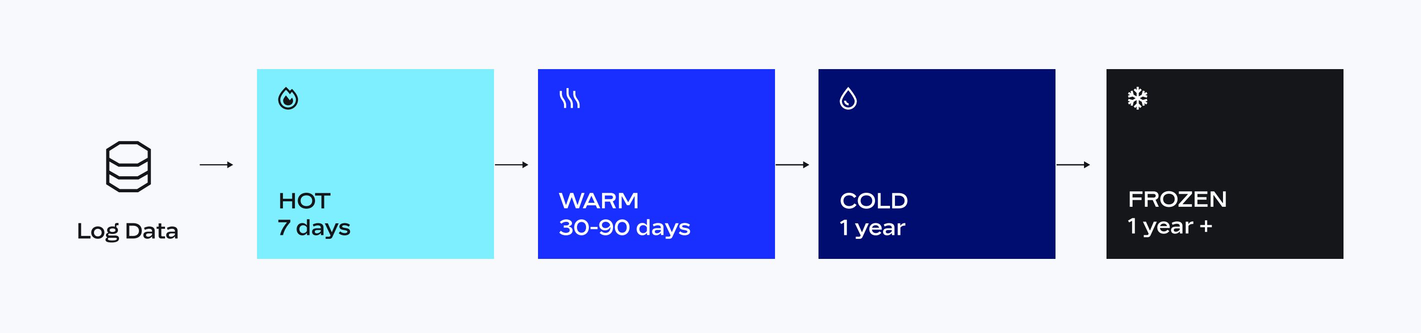
“We’re Cloud Native”

When considering a SIEM solution, it is crucial to differentiate between true cloud-native solutions and those that have been retrofitted and re-architected for cloud deployment. In this section, we will discuss the significance of a SIEM solution being built in the cloud from the ground up and explore the limitations of legacy SIEMs designed for traditional infrastructures, such as corporate networks and perimeter security.

Designed for Traditional Infrastructures

Legacy SIEMs were originally designed to focus on corporate networks and traditional perimeter security. These legacy solutions often struggle to adapt to the complexities and scale of modern cloud environments. They may lack the necessary integrations with cloud-native services, resulting in limited visibility and reduced effectiveness in monitoring cloud-based applications and resources. Legacy SIEMs may rely on outdated data collection and storage methods, making it difficult to capture and analyze security events from distributed cloud environments effectively.

As organizations embrace cloud computing and migrate their infrastructure and applications to the cloud, it becomes essential for their SIEM solutions to adapt accordingly. Legacy SIEMs designed for traditional on-premise networks often face challenges when operating in cloud environments. They may lack native integrations with cloud platforms, hindering their ability to collect and analyze security data effectively. Additionally, legacy SIEMs may require extensive customization, reconfiguration, and constant rearchitecting to accommodate cloud-native technologies such as microservices, containers, and serverless architectures.



Operational Configuration and the Importance of Serverless

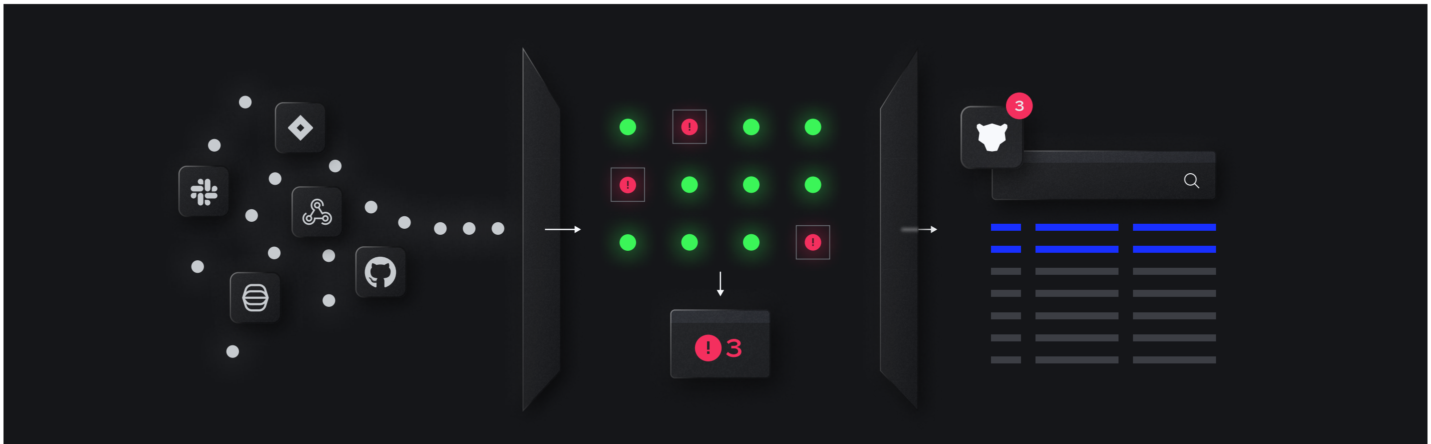
Legacy SIEM solutions often require complex operational configurations, involving the setup and maintenance of dedicated servers. In contrast, a modern SIEM embraces serverless architectures and a modern security data lake, which eliminate the overhead and complexities associated with infrastructure management.

Serverless SIEM solutions provide significant advantages, including reduced maintenance efforts, improved scalability, and the ability to focus on security operations rather than infrastructure management. By eliminating the need for server provisioning and maintenance, security teams can dedicate their resources to proactive threat detection and incident response. Leveraging the scalability offered by cloud providers, serverless SIEM solutions can handle high volumes of security data without compromising performance. This enables organizations to maintain real-time monitoring capabilities while freeing up their security professionals to focus on critical security tasks. The flexibility and agility of serverless architectures also allow for rapid adaptation to changing requirements, ensuring optimal performance and cost efficiency in dynamic cloud environments.

The Risk of Downtime in a Dynamic Cloud Environment

In a dynamic cloud environment, the risk of downtime is a significant concern as legacy SIEM solutions struggle to keep pace with rapid changes, leading to disruptions in security monitoring and alerting. Such downtime can have detrimental effects on security operations, causing real-time visibility gaps and delays in detecting and responding to security incidents, giving attackers more time to cause damage.

Extended downtime can also impact compliance and regulatory obligations, exposing organizations to legal and financial risks. To mitigate these risks, organizations need a modern SIEM solution that seamlessly adapts to the dynamic cloud environment. A modern SIEM leverages cloud-native architectures and technologies, integrating with cloud services like auto-scaling groups and load balancers to ensure uninterrupted availability and performance. With its scalable and resilient design, a modern SIEM minimizes downtime, maintains continuous security monitoring and alerting, and dynamically adjusts resources to handle spikes in data volume and changes in the cloud environment, all while preserving the effectiveness of security operations.



EMBRACING THE CLOUD: BENEFITS OF A CLOUD-NATIVE SIEM

A SIEM solution built in the cloud from the ground up is designed with the cloud environment's unique characteristics in mind.

Being Truly Cloud-Native Offers the Following Benefits:

Scalability

One of the primary advantages of a cloud-native SIEM is its inherent scalability. Traditional SIEM solutions often struggle to handle high volumes of security data generated by modern applications and diverse log sources. In contrast, a cloud-native SIEM is designed to scale dynamically to accommodate fluctuating data volumes and meet the needs of rapidly growing organizations. By leveraging cloud resources and distributed architectures, a cloud-native SIEM can seamlessly scale its processing capabilities, ensuring that no security event or log entry goes unnoticed.

Resilience

Maintaining an always-available and resilient SIEM infrastructure is essential for effective security operations. Cloud-native SIEM solutions excel in providing high levels of resilience. By leveraging the cloud's redundant and fault-tolerant infrastructure, a cloud-native SIEM can withstand failures or disruptions without impacting security operations. This resilience allows security teams to rely on a consistent and uninterrupted flow of security data, ensuring that threats are promptly detected and mitigated.

Adaptability to Changing Infrastructure

In today's dynamic IT environments, infrastructures are continuously evolving. Legacy SIEM solutions, designed for traditional corporate networks and perimeter security, often struggle to adapt to these changes. However, a cloud-native SIEM embraces the dynamic nature of modern infrastructures, including cloud environments, microservices, and containers. It can seamlessly integrate with diverse systems, applications, and log sources, providing comprehensive visibility and monitoring capabilities. This adaptability enables security teams to keep pace with the evolving threat landscape and ensure effective security monitoring across the entire infrastructure.

Leveraging Cloud-Native Services

Cloud-native SIEM solutions also leverage the benefits of cloud-native services, such as serverless computing. Serverless architectures eliminate the need for managing operational components like servers, allowing security teams to focus on their core responsibilities rather than infrastructure maintenance. With serverless computing, the SIEM solution automatically scales resources based on demand, reducing operational overhead and improving cost efficiency. This enables security teams to allocate their resources more effectively towards threat detection, incident response, and proactive security measures.

DECEPTION #2

“No Overhead Necessary”

Legacy SIEM solutions often demand extensive resources, including personnel, time, and expertise, to manage and maintain them. We will discuss the challenges associated with legacy SIEMs that require a dedicated team of specialists to oversee their operations. The resource-intensive nature of legacy SIEMs can divert valuable resources away from managing actual security threats, impacting an organization’s overall security posture.

Pitfalls of Proprietary Query Languages

Legacy SIEM solutions often rely on proprietary query languages that require specialized knowledge and training. This reliance on proprietary languages can limit the accessibility and flexibility of the SIEM solution, making it challenging for security teams to customize and optimize the system. We will delve into the drawbacks of proprietary languages and the potential barriers they create for effective SIEM management.

A Modern SIEM: No Dedicated Infrastructure Team Required

Contrary to the deceptive notion of requiring a team of specialists, a modern SIEM solution is designed to be managed without the need for a dedicated team. Modern SIEM solutions provide a “set it and forget it” approach, enabling security teams to focus on managing threats rather than spending extensive resources on SIEM maintenance. Modern SIEMs leverage user-friendly interfaces, intuitive workflows, and automation to simplify SIEM management tasks, empowering security professionals without requiring specialized expertise.

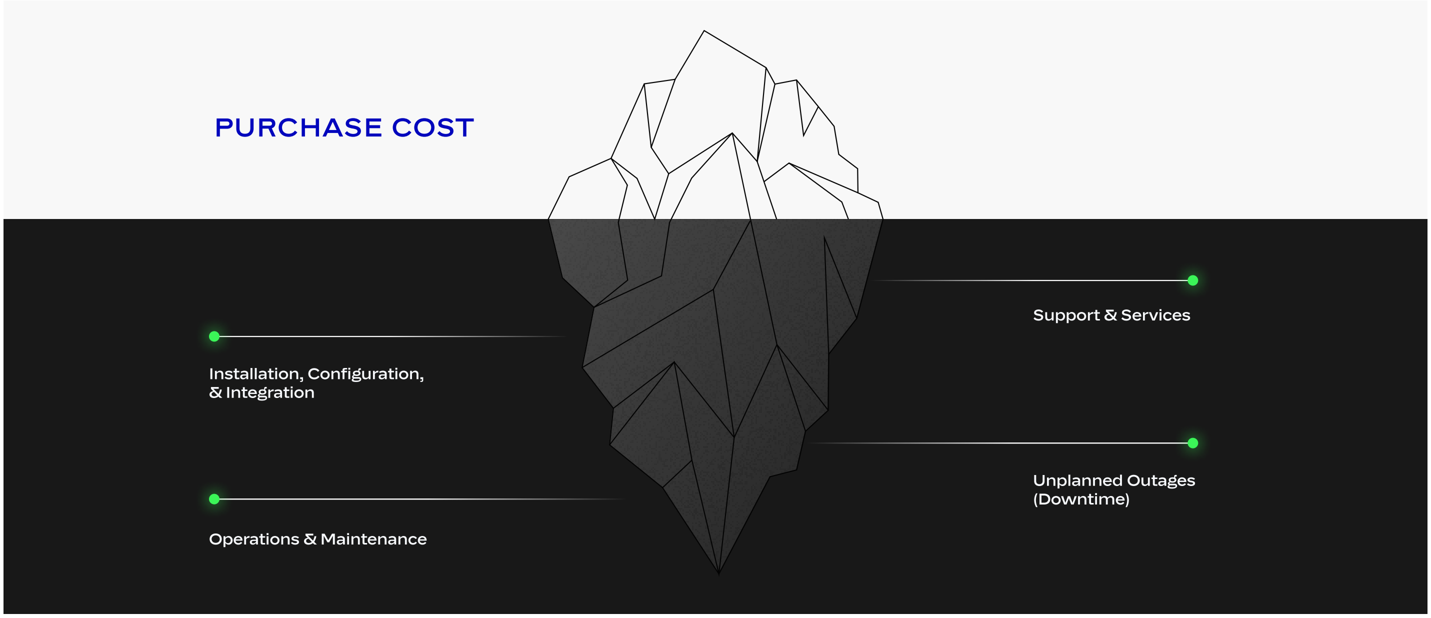
DECEPTION #3

“We Start at 20 Cents”

Legacy SIEM solutions often employ a ransomware-like pricing model, initially luring organizations with seemingly low costs but quickly escalating charges for essential functionalities. We will discuss how legacy SIEM vendors position themselves as budget-friendly options, only to impose additional fees for necessary features and capabilities. By exposing this deceptive pricing tactic, organizations can make informed decisions when evaluating SIEM solutions.

The True Costs Behind the Pricing Structure

In this section, we will unravel the true costs behind the pricing structure of legacy SIEM solutions. We will examine the hidden fees associated with essential features, such as advanced threat detection, incident response, and compliance reporting. By understanding the full extent of the costs involved, organizations can avoid unexpected expenses and accurately assess the value proposition of legacy SIEMs.


PURCHASE COST
Support & Services
Installation, Configuration, & Integration
Unplanned Outages (Downtime)
Operations & Maintenance

Limited Data Retention Versus the Benefits of a Security Data Lake

Legacy SIEMs often offer limited data retention periods, typically around 30 days, which can hinder investigations and compliance efforts. The benefits of a security data lake, provides extended data retention capabilities, allowing organizations to retain security logs and events for longer periods, often up to 365 days. The advantages of longer data retention periods contributes to effective threat hunting, incident response, and forensic investigations.

Additional and Hidden Costs to Consider

Beyond the upfront pricing, legacy SIEM solutions come with additional costs that organizations need to consider. These costs may include staffing requirements to manage the SIEM, ongoing software licenses, and potential expenses related to customization and integration with other security tools. Shedding light on these hidden costs, enables organizations to make a comprehensive evaluation of the total cost of ownership of legacy SIEMs.

Transparent Pricing of Modern SIEMs

Modern SIEM solutions differentiate themselves by offering transparent pricing models. They provide clear and upfront pricing structures, without hidden fees or unexpected charges for essential functionalities. Modern SIEM solutions empower organizations by providing transparent pricing, allowing them to accurately assess the costs and make informed decisions based on their specific security requirements.

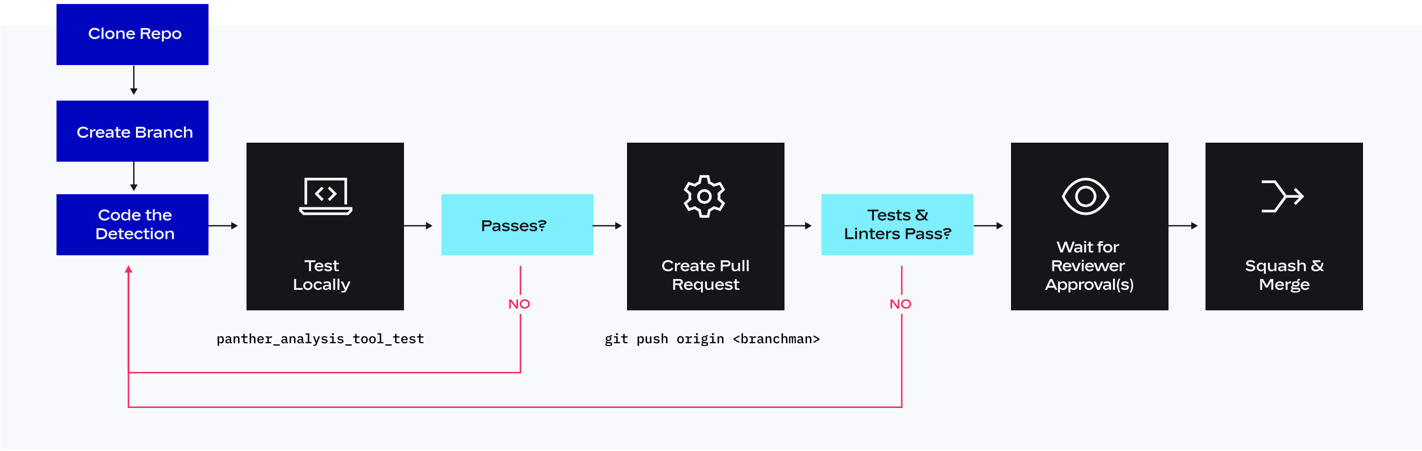
Set It and Forget It: Focus on Managing Threats

By adopting a modern SIEM solution, organizations can shift their focus from managing the SIEM system to managing actual security threats. Modern SIEMs allow security teams to spend more time on proactive threat hunting, incident response, and other crucial security operations, rather than dealing with the complexities of SIEM administration. This approach maximizes the efficiency and effectiveness of security teams, enhancing an organization's overall security posture.

DECEPTION #4

“Easily Customizable Detections”

Legacy SIEM solutions often operate as black box environments, making it challenging for organizations to understand the inner workings and underlying detection mechanisms. The limitations of proprietary or overly complex legacy SIEM systems, can hinder transparency and hinder the ability to tailor detection capabilities to specific security needs. This lack of visibility and control can undermine the effectiveness of security monitoring and threat detection efforts.

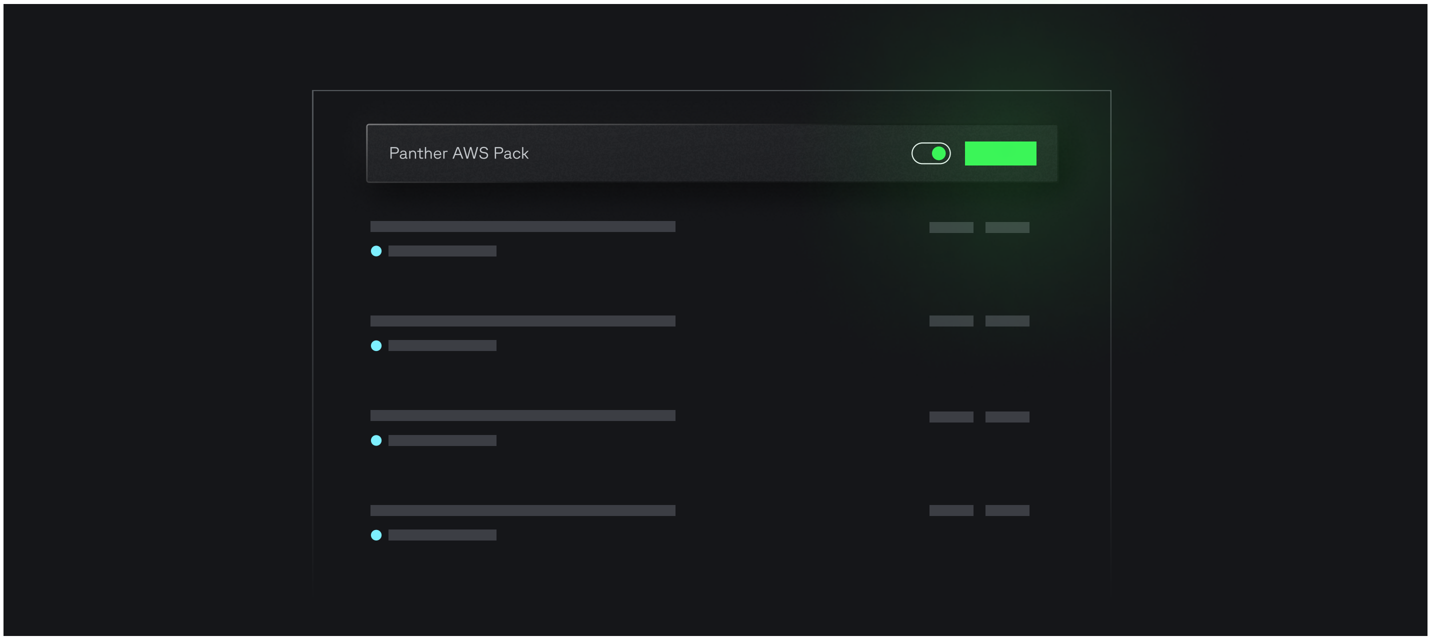


The Power of Detection-as-Code

Detection-as-Code is a key feature of modern SIEM solutions, allowing security teams to define and customize detection rules and logic using programming languages and frameworks. Detection-as-Code follows the principles of the software development lifecycle, providing transparency, flexibility, and repeatability. By leveraging Detection-as-Code, organizations gain visibility into detection mechanisms, enabling customization, and facilitating collaboration between security and engineering teams.

Customization and Flexibility with a Detection Toolkit

A detection toolkit is an essential component of a modern SIEM solution, providing pre-built detection rules, playbooks, and analytics templates that organizations can customize to suit their specific needs. A detection toolkit empowers security teams to go beyond out-of-the-box detections, tailoring detection capabilities to their unique environments and threat landscape. This customization and flexibility enhance the accuracy and relevance of security monitoring, enabling organizations to detect and respond to threats effectively.



Breaking Down Silos: Collaboration and Visibility

Legacy SIEM solutions often create silos between security teams, making it challenging to share and collaborate on detection rules and methodologies. Modern SIEM solutions foster collaboration by breaking down these silos. By providing a centralized detection platform, organizations can promote cross-functional collaboration, knowledge sharing, and consistent detection practices across the security team. This collaboration improves the overall effectiveness of threat detection and response.

DECEPTION #5

“Engineering Friendly”

Legacy SIEM solutions often boast being “engineer friendly,” suggesting that they align well with typical developer workflows. However, we will examine the true implications of this claim and uncover the limitations and challenges that engineers face when working with legacy SIEMs.

DevOps Emphasis in Modern SIEMs

Modern SIEM solutions place a strong emphasis on DevOps methodologies, fostering collaboration between security teams and development teams. Modern SIEMs integrate seamlessly into DevOps workflows, allowing engineers to leverage their existing processes, tools, and methodologies. This collaboration enhances the efficiency and effectiveness of security operations, enabling engineers to contribute their expertise while streamlining the overall development and security lifecycle.

Python and Detection-as-Code: Empowering Engineers

A key aspect of engineer friendliness in modern SIEM solutions is the use of Python and Detection-as-Code. Python is a widely adopted programming language, providing engineers with a familiar and versatile tool to customize, extend, and automate SIEM functionalities. Detection-as-Code further empowers engineers by enabling them to write custom detection rules, leverage existing Python libraries, version control, integration with CI/CD pipelines and incorporate advanced analytics and machine learning capabilities into their security operations.

Leveraging Development Lifecycle and Engineering Expertise

Modern SIEM solutions follow the principles of the development lifecycle, aligning security operations with engineering best practices. This approach allows engineers to apply their expertise in building, testing, and deploying detection rules and security analytics. By integrating software development lifecycle principles into SIEM management, engineers can leverage their skills and knowledge effectively, improving the accuracy and efficiency of threat detection and response.

CONCLUSION

Legacy SIEM solutions often fail to meet the needs of modern security teams, who require agility, observability, and the ability to adapt to dynamic cloud environments. The promises of being cloud-native, easy to scale, and cost-effective can be deceptive, as legacy SIEMs struggle to keep up with the ever-increasing volume, velocity, and variety of security data. Their pricing models, hidden costs, and limited data retention can create dependencies and hinder effective security operations.

However, the emergence of modern SIEM solutions brings a fresh perspective to the table. Cloud-native architectures, seamless scalability, transparent pricing, and extended data retention empower organizations to proactively detect and respond to security threats. By leveraging technologies such as serverless computing, Detection-as-Code, and detection toolkits, modern SIEMs empower security teams, eliminate the need for specialized expertise, and foster collaboration between security and engineering functions.

In conclusion, organizations must recognize the importance of choosing a modern SIEM solution that aligns with their evolving security needs. By avoiding the deceptions of legacy SIEMs and embracing a transparent, flexible, and scalable approach, organizations can empower their security teams to stay ahead of emerging threats, detect incidents in real-time, and respond effectively to mitigate risks.

As you embark on your journey to select a modern SIEM solution, consider the challenges and risks we have explored throughout this eBook. Prioritize a solution that offers cloud-native capabilities, seamless scalability, transparent pricing, and customization options. Empower your security teams with Detection-as-Code, detection toolkits, and the ability to collaborate with engineering teams.

Remember, a modern SIEM solution should bring observability into your security operations, allowing you to focus on managing threats rather than worrying about the SIEM's infrastructure. Choose wisely, and may your organization embark on a secure and confident path towards a modern SIEM that truly empowers your security operation .

Learn More About Panther →