A GUIDE TO NEXT-GEN SIEM

Why the Future of Cybersecurity is Proactive

E-BOOK

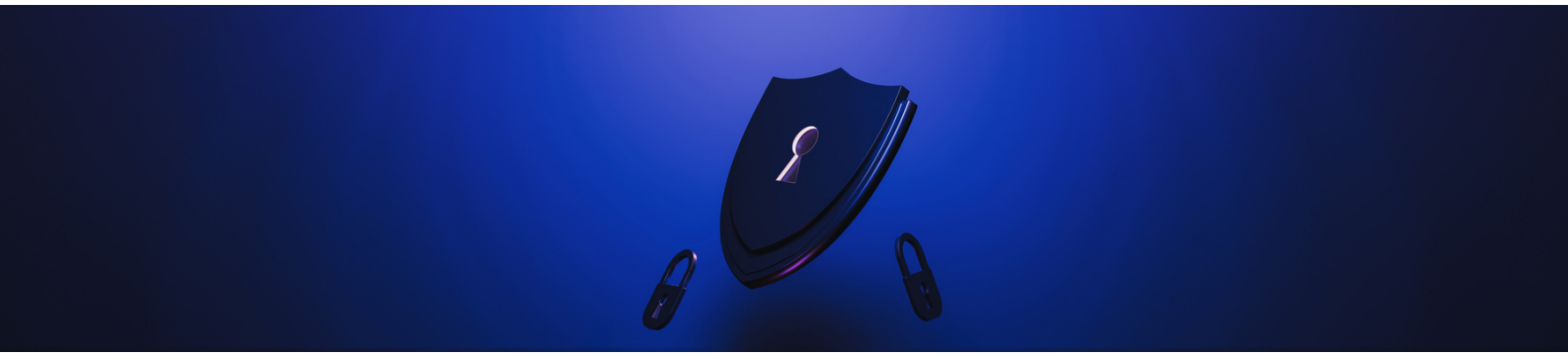
Blacklight

Table of Contents

Introduction

Security Information and Event Management (SIEM) represents a crucial toolset in cybersecurity. At its core, it is a log event collection and management tool. Through the analysis of log events and other data across an organisation's IT infrastructure, SIEM supports threat detection, compliance, and security incident management.

The evolution and significance of SIEM in the contemporary cybersecurity landscape can not be overstated, as it has become a critical tool for organisations aiming to bolster their defence against an increasingly sophisticated array of cyber threats. However, with an ever-evolving threat landscape, legacy SIEMs can no longer keep up with advanced threats or guarantee security managers real-time clarity needed to make effective data-driven decisions. Additionally, given high costs and increasingly complex cyber-attacks, SIEMs have shown to be incapable of generating value or providing a consistent solution to threats and breaches in real-time.



Challenges of Legacy SIEMs

What is a legacy SIEM and how do they compare with next-gen SIEM platforms? Legacy SIEM systems represent the first generation of SIEM solutions and have been a staple in the cybersecurity landscape for decades. They were designed to help organisations collect, store, analyse, and correlate security-related data from various sources such as firewalls, antivirus software, and network devices. The key characteristic of legacy SIEM systems is their reliance on ***rule-based detection***, hence their reliance on predefined rules and signatures to detect security incidents. These rules apply to known attack patterns and vulnerabilities, limiting their effectiveness to only known threats and not the identification of novel or sophisticated attacks.

Additionally, legacy SIEMs primarily provide ***historical analysis*** of security events. At the time, they were effective for analysts and cyber professionals in log management and reporting, allowing for valuable compliance and post-incident investigations. However, such historical focus makes real-time threat detection and response almost impossible. Threat detection and response are also greatly affected by the high volume of ***false positives*** that are generated due to their rule-based nature. Security teams often spend significant time investigating false alarms, which leads to alert fatigue and reduced efficiency.

On top of this, ***limited User and Entity Behaviour Analysis (UEBA)*** makes legacy SIEMs less effective in identifying abnormal user or entity behaviour patterns, which are critical features for detecting insider threats and advanced attacks. The lack of contextual analysis and the inability to understand the context in which actions are

taken make it difficult to identify and differentiate between normal and suspicious behaviours. Legacy SIEMs may also lack the machine learning algorithms required to adaptively learn and detect anomalous behaviours over time. Without having a wide range of data sources, comprehensive UEBA may not be performed as it requires large data sets from various system applications and network activities.

Representing the first generation of SIEM solutions, legacy SIEMs struggle with scalability due to the way they were initially architected, designed, and developed. Traditional SIEM solutions are often deployed on dedicated hardware infrastructure (i.e. on-premise) within an organisation's data centre. As the volume of security data grows, scaling up hardware resources can be costly and time-consuming. Moreover, hardware-based scaling may not provide the agility needed to adapt to sudden increases in data volume during security incidents or as the organisation grows. As they were not designed to seamlessly integrate with cloud-based or hybrid IT infrastructures, legacy SIEMs struggle to collect and analyse security from diverse sources that organisations may be adopting in an increasingly digital and cloud-based business environment.

Evolve or Be Replaced: The Rise of Next-Gen SIEM

Next-gen SIEM solutions represent a new breed of cybersecurity platforms designed to overcome the limitations of legacy SIEMs. They embrace advanced technologies and methodologies to provide more *proactive, adaptive, and efficient* security operations. There are several ways that they differ from legacy SIEM solutions:

Aspect	Legacy SIEM	Next-Gen SIEM
Approach	Rule-Based Detection.	Based on analytics, statistical models, UEBA and AI for broader detection.
Integrations	Requires advanced customisation and limited out-of-the-box capabilities.	Correlates logs regardless of data source and domain (e.g., on-premise, private/public cloud).
Deployment	On-premise with limited integrations to hybrid eco-systems.	Designed to support hybrid eco-systems and multi-cloud ecosystems.
Scalability	Limited adoption to changing environments or growing business.	Cloud-native – full advantage of the elasticity of the cloud to deliver compute, memory, and storage resources on demand.
Detection	Delayed alerts. Limited real-time detection. Mainly reactive incident investigations.	Utilises AI for threat hunting to increase visibility.
False Positives	High volume – due to manual ad-hoc fine tuning.	Low volume – automated fine tuning and embedded ML.
UEBA	Not applicable.	Robust UEBA capabilities for unusual threat detection.
Cost	Cost-heavy investment required. Hardware and skill dependent, significant administrative overhead with add-on module licenses.	Simple cost structure and predictable. Avoids the modular license approach by including everything part of the SaaS offering.

Approach

Next-Gen SIEM platforms represent a paradigm shift in threat detection. They employ advanced analytics, machine learning, and behavioural analysis to identify both known and unknown threats. In the ever-evolving landscape of cybersecurity, some of these advanced technologies enable Next-Gen SIEM platforms to gain adaptability:

Advanced Analytics: Next-Gen SIEMs harness the power of advanced analytics to process and analyse large volumes of security data rapidly. They can identify patterns, anomalies, and correlations that may indicate security threats. By applying AI models and algorithms, they recognise trends that are not evident in traditional rule-based systems.

Machine Learning: Adaptive learning is at the core of Next-Gen SIEMs. These platforms use machine learning algorithms to continuously learn from historical and real-time data, allowing them to rapidly evolve and improve their threat detection capabilities over time. Even the most subtle changes in data patterns and deviations from normal behaviour can inform the system of a potential threat.

Behavioural Analysis: As a key component of Next-Gen SIEMs' threat detection capabilities, these systems monitor user and asset behaviour to create baselines of what is considered "normal" behaviour. When deviations from these patterns occur, such as unusual access patterns or privilege escalation, the SIEM can trigger alerts. This is an extremely advantageous feature in comparison to legacy SIEMS where insider threats and sophisticated attacks may not trigger traditional rule-based alerts.

Scalability & Flexibility

Scalability and flexibility of Next-Gen SIEM platforms are paramount in addressing some of the limitations of traditional SIEMs.

Cloud-Native Architecture:
Next-Gen SIEM solutions are designed with cloud-native architectures. This means they are inherently scalable and can adapt to changing workloads and data volumes. Organisations can take advantage of cloud resources to handle spikes in data traffic during security incidents or as they grow.

Elastic Scaling:
Elastic scaling is a hallmark of Next-Gen SIEMs. It allows the platform to dynamically allocate and release computing resources based on demand. During periods of increased activity, such as a DDoS attack or a surge in log data, the SIEM can automatically scale up to handle the load. When the demand decreases, resources are scaled down, optimizing cost-efficiency.

Integration Capabilities:
Next-Gen SIEMs are often designed to seamlessly integrate with a wide range of data sources, including cloud services, on-premises systems, OT systems, IoT devices, and third-party security tools. This integration flexibility ensures that organisations can consolidate their security data and monitor all aspects of their digital environment, regardless of where the data resides.

Reduced False Positives

False positives can overwhelm security teams and diminish their ability to respond effectively to real threats. Next-Gen SIEM platforms are engineered to minimise false positives through advanced methods:

Machine Learning Algorithms:
Next-Gen SIEM platforms leverage machine learning algorithms and advanced analytics to continuously refine their threat detection capabilities. These algorithms are trained on large datasets of historical security events and incidents, allowing the SIEM to learn what constitutes normal behaviour within an organisation. As the SIEM learns, it becomes better at distinguishing between genuine security threats and benign activities. It recognises subtle patterns, trends, and anomalies in data that traditional rule-based systems can't detect. This adaptability means that over time, false positives are significantly reduced, and the SIEM becomes more precise in alerting security teams to actual threats.

Contextual Analysis & Threat Intelligence:
Next-Gen SIEMs excel in contextual analysis. They consider not only the individual security event or alert but also the broader cyber threat intelligence context in which it occurs. This contextual understanding enables the SIEM to make more informed decisions about whether an alert represents a genuine threat and its criticality. For example, an alert triggered by a user, who's credentials have been compromised and leaked, accessing a sensitive file should be considered at a higher criticality. By taking threat intelligence into account as contextual insights, in terms of identities, asset vulnerabilities and industries, Next-Gen SIEM platforms increases the visibility and improves the focus on investigating potential security incidents proactively.

User and Entity Behaviour Analytics (UEBA):
Next-Gen SIEM platforms often incorporate User and Entity Behaviour Analytics (UEBA) capabilities. UEBA allows the SIEM to build behavioural profiles for individual users, assets, and entities within an organisation. It learns the typical behaviour of each user, asset, and entity, including the systems they access, the times they log in, and the data they interact with and much more. When deviations from these established behaviour patterns occur, the SIEM can generate alerts. UEBA helps reduce false positives by providing a baseline for what is considered normal for each user and entity, making it easier to spot abnormal or suspicious activities.

Real-Time Analysis & Analytics

Real-time threat analysis and advanced correlation is a hallmark of Next-Gen SIEM platforms. Unlike traditional SIEMs, which focus on historical analysis and reporting, Next-Gen SIEMs excel in immediate threat detection and response. They achieve this in several ways:

Continuous Monitoring:
Next-Gen SIEM platforms continuously monitor incoming data streams, including but not limited to operating system logs, network traffic, and user activities, in real-time. This constant surveillance ensures that any suspicious or malicious activity is promptly correlated and detected allowing for immediate action.

Automated Incident Response:
Many Next-Gen SIEMs offer automated incident response capabilities. When a threat is detected, predefined response actions can be initiated automatically. To speed up response times but also reduces the risk of human error.

Alerting & Notifications
When a potential security threat is identified, Next-Gen SIEMs generate real-time alerts. These alerts provide security teams with detailed information about the incident, including the affected systems, users and the nature of the threat. Rapid notification enables security personnel to respond swiftly and decisively.

Next-Gen SIEM for Next-Gen Security Teams

What are the benefits of Next-Gen SIEMs for security teams? As organisations face a constant battle against sophisticated threats and malicious actors, security teams must fortify their defences and rely on cutting-edge solutions to go beyond traditional security monitoring. As we described in the previous sections, here are several ways Next-Gen SIEM features can support cybersecurity teams with enhanced incident response, advanced threat hunting, and investigation.

Enhanced Incident Response Capabilities:
Real-time threat intelligence is essential in today's digital landscape, where cyberattacks can unfold in a matter of minutes or even seconds. Next-Gen SIEM platforms empower organisations to proactively defend against threats as they occur, minimizing the potential damage and reducing the mean time to respond (MTTR) significantly. They do so by allowing security teams to define and automate incident response workflows to automatically contain security incidents in real-time. These workflows can include a series of actions and responses to specific types of threats. For instance, when a specific malware behaviour is detected, the SIEM can trigger predefined actions to isolate compromised devices, block malicious activities and notify relevant stakeholders. This orchestration ensures rapid containment and prevents the escalation of security incidents into major breaches.

Behavioural Analytics for Threat Hunting:
Next-Gen SIEMs empower security teams to proactively hunt for threats by using advanced behavioural analytics. These functionalities can identify subtle deviations from normal behaviour patterns within an organiation's network. Security analysts can use behavioural analytics to uncover hidden threats, identify zero-day attacks, and recognise suspicious activities that might not trigger traditional rule-based alerts. This proactive approach helps detect threats at an early stage.

ML-Driven Threat Indicators:
Machine learning algorithms embedded in Next-Gen SIEM platforms continuously analyse and learn from security data. They can identify and highlight unusual patterns or anomalies that may indicate emerging threats. Security teams can leverage these ML-driven threat indicators to stay ahead of adversaries and pre-emptively address potential security risks. These indicators provide actionable insights for threat-hunting efforts.

Introducing Blacklight AI: The Evolution of Next-Gen SIEMs

While cybersecurity players have introduced Next-Gen SIEMs, the market is gasping for a solution that combines timely identification of cybersecurity incidents with a dedicated response team to alleviate the operational pain points businesses face. In an age where many companies operate digitally, the evolution of cyber threats is unprecedented, with the average cost of a data breach reaching an average of USD 4.45 million in 2023.[1] Being able to respond effectively is no longer sufficient. With associated costs reaching highs, a gap must be filled in SIEM solutions that can predict threats and allow organisations to prevent them before they cause significant damage to the core business.

In response to this ever-shifting threat landscape, Blacklight AI represents a groundbreaking leap in cybersecurity technology. At its core, its truly proactive, AI-powered and cloud-native SIEM embodies the fusion of cutting-edge artificial intelligence, machine learning, and advanced analytics with a singular purpose: to empower cybersecurity professionals with the tools they need to **predict, detect, and mitigate** threats effectively.

Blacklight's AI-powered engine learns from the environment of the organisation that adopts it. Gathering and normalising the data from various data sources, the software conveys an easy-to-understand story about the company's cybersecurity posture. Continuously looking for anomalies across different areas, allowing it to detect security incidents, where time is a variable, not a constant. Blacklight uses advanced correlation to predict incidents before they can cause any adverse impact on the enterprise. The core commitment of Blacklight's offering is to alleviate all pain points of customers right from detection down to response.

The Blacklight Advantage

In cybersecurity, in order to identify threats that have yet to make a detrimental impact on businesses, analysts must change how they look for threats. Instead of searching for signals that emulate a threat, any signs of *abnormal behaviour* must be analysed in order for concrete conclusions to be drawn. The differentiator of Blacklight AI lies within the entire SIEM ecosystem.

1. IBM, 2023 – Cost of a Data Breach Report 2023

Blacklight integrates with all cybersecurity solutions and serves as the command centre for any organisation. The solution enables security teams to uncover threats more efficiently, gain better visibility, significantly decrease costs and minimise risk, all from one single platform.

Proactive, Not Reactive

Blacklight is the first ever truly predictive AI-powered detection software. At its core, Blacklight's architecture is rooted in Artificial Intelligence and Machine Learning. The AI engineering behind Blacklight algorithms and models allows the software to use all available data points to perform advanced correlation. For example, among events thought to be exclusive due to geographical or departmental differences.

The AI and ML capabilities continuously identify and detect malicious activities and correlate similar alerts, users and assets, enabling rapid detection for proactive decision-making. Blacklight will prioritise alerts and dynamically update alerts based on new occurrences of events, which will focus the team's efforts on the most critical activities.

SOC Efficiency

Blacklight is designed to do more for security teams, reduce investigation time, and address the cybersecurity skills shortage. It is built to help organisations and managed security providers run lean and efficient SOC teams.

Firstly, with global visibility at your fingertips, Blacklight is built for global correlation while ensuring compliance with data protection and residency regulations. Analysts can detect threats at the highest level in the organisational chart and stop the proliferation of the attack before a new occurrence.

Secondly, the native feedback loops provide insights based on the outcomes of alerts. In addition, embedded machine learning provides continuous and automated awareness of the AI models for continuous fine-tuning. This helps avoid ad-hoc and manual fine-tuning of use cases, leading to reduced noise and alert fatigue.

Thirdly, Blacklight's intuitive interface provides real-time information, dynamic updates, and readily available data for quick and efficient investigations by SOC analysts. All related alerts are aggregated to allow for a more comprehensive view, allowing teams to sift through logs faster and to focus on the most critical threats, with shorter investigation times.

Easy Integration

From IT to OT to Blockchain, and everything in between, Blacklight keeps integrations simple with complete visibility of threats. The software leverages all your security data (and more) for advanced contextual insights with robust integrations. Another big advantage of Blacklight is its ease of integration with other applications, allowing them to share information and functionality with Blacklight without disruptions. Streamlined integration enhances productivity, minimises manual tasks, and optimises overall system performance, ultimately driving more value from the integrated software ecosystem.

Conclusion

With the continued adoption of cloud-based systems, every organisation's attack surface continues to grow. While legacy SIEMs and other solutions can be useful in post-mortem investigation, they won't alert you in real-time to imminent threats. For that, you need a modern solution built for today's digital age. With AI and ML at its core, Blacklight is a truly proactive, Cloud-native, AI-Powered SIEM designed to do more for security teams.

Want To Learn More?

For more information, contact us or request a demo of Blacklight **here**.

OwlGaze | Blacklight

OwlGaze is the cybersecurity software company behind Blacklight SaaS.
Blacklight, our proprietary predictive AI-based SIEM and threat detection software provides first-in-class security.

Blacklight is architected, designed and built using industry best practices, offering the maximum level of flexibility and extensibility. Combined with OwlGaze's SOC services, we help enhance your monitoring, detection and response capabilities using our next-gen software designed for proactive monitoring.

© 2023 OwlGaze. All rights reserved.
info@blacklightai.com