gravwell

SECURITY DATA PLATFORM VS. SIEM:

CHOOSING THE RIGHT TOOL FOR MODERN SECURITY CHALLENGES

As cybersecurity threats evolve, organizations must choose the right security tools to protect their digital assets. Traditional Security Information and Event Management (SIEM) solutions have long been the cornerstone of security operations, providing centralized log collection, correlation, and incident response. However, as data volumes grow and threats become more sophisticated, Security Data Platforms (SDPs) have emerged as a powerful alternative, offering advanced analytics, scalability, and flexibility.

This white paper explores the key differences between SIEM and Security Data Platforms, highlighting their respective strengths, challenges, and ideal use cases. By understanding these distinctions, security leaders can make informed decisions that align with their organization's needs and ensure robust cyber resilience. We also delve into future trends, best practices, and considerations to guide organizations in their security evolution.

INTRODUCTION

- SIEM solutions aggregate and analyze security data from multiple sources to detect potential threats. They provide centralized logging, real-time monitoring, and compliance reporting.

  Security Data Platforms, on the other hand offer the same functionality as a SIEM but a less rigid structure. Specifically there is less structure around the formatting of data at ingestion, scalable data ingestion/performance at scale, flexible querying, often leveraging modern big data technologies but can also be built on a custom data structure. These platforms allow security teams to analyze raw security data dynamically, Offering a richer, more flexible and more thorough approach to security analytics, enabling deeper threat detection and investigation.

WHY THIS COMPARISON MATTERS

- Organizations today face increasingly complex security landscapes. Legacy SIEMs often struggle with scalability and cost issues, while Security Data Platforms provide a more agile approach to handling security data. Understanding when to use each solution—or a combination of both—is crucial for effective cybersecurity operations.

gravwell

WHAT IS SIEM?

SIEM solutions were designed to centralize security event data and provide real-time threat detection. Their primary functionalities include:

- Log Collection and Management: Aggregating logs from network devices, servers, and applications.
- Correlation and Analysis: Identifying patterns and anomalies that may indicate security incidents.
- Alerting and Incident Response: Automating threat detection and generating alerts.
- Compliance Reporting: Helping organizations meet regulatory requirements.

STRENGTHS OF SIEM

- Centralized security visibility
- Automated alerting and incident response
- Compliance and audit readiness
- Established vendor support and ecosystem
- Integrated threat intelligence feeds

LIMITATIONS OF SIEM

- High cost of implementation and maintenance
- Performance degradation with large-scale data
- Limited flexibility in querying raw security data
- Out of the box rules may miss sophisticated threats

gravwell

WHAT IS A SECURITY DATA PLATFORM?

Security Data Platforms provide a modern, scalable approach to security data management. These platforms enable security teams to analyze data on demand, using a piped query language and analytics.

KEY FEATURES

- **Structure on Read**: Unlike SIEMs, which structure data upon ingestion, SDPs allow for flexible querying without predefined schemas.
- **Piped Query Language**: Advanced filtering and analytics capabilities for rapid threat detection.
- **Scalability**: SDPs can ingest and query large volumes of data.
- **Enhanced Threat Hunting**: Enables security analysts to conduct deeper investigations without pre-configured rules.
- **Open Data Model**: Ensures interoperability with various security tools and sources.
- **Deployment**: Operates in cloud, on prem and in air gapped environments

HOW SDPS COMPLEMENT SIEMS

While SDPs can function independently, they also enhance SIEM capabilities by providing deeper analysis, improved performance, and cost-effective data retention. Many organizations use SDPs as a secondary layer of security intelligence to refine SIEM-generated alerts.

gravwell

COMPARISON: SIEM VS. SECURITY DATA PLATFORM

FEATURE	SIEM	SECURITY DATA PLATFORM
Architecture & Scalability	Centralized, structured data	Distributed, scalable processing
Analytics & Intelligence	Pre-built out of the box rule-based detection	Rule based detection with advanced pipeline query language.
Use Cases	Compliance, basic threat detection	Large-scale analytics, hunting
Performance	Can lag with large datasets	Optimized for real-time analysis
Cost & Maintenance	Expensive licensing and storage costs with pay by the pound pricing models	Lower storage costs. Stepped pricing or credit models to put the user in control.
Integration & Flexibility	Fixed integrations, difficult scaling	Open data models, cloud-native adaptability

gravwell

CHALLENGES AND CONSIDERATIONS

SIEM CHALLENGES

- Expensive licensing and storage
- Performance degradation with large datasets
- Limited flexibility for deep threat hunting
- High operational overhead for managing out of the box rules that are not customized to the users environment

SDP CHALLENGES

- Requires skilled analysts to maximize potential
- Can be complex to implement alongside legacy systems
- Less focus on compliance out-of-the-box
- Need for significant data engineering expertise

KEY CONSIDERATIONS

- **Data Volume:** If handling petabytes of data, an SDP may be more effective.
- **Security Maturity:** Organizations with advanced security teams may benefit more from an SDP's flexibility.
- **Budget Constraints:** Organizations with limited budgets may struggle with SIEM licensing fees.

gravwell

CONCLUSION

Both SIEM and Security Data Platforms serve critical roles in modern security operations. SIEM remains essential for compliance and centralized monitoring, while SDPs offer scalability, flexibility, and advanced analytics. The choice between the two depends on an organization's security needs, regulatory requirements, and operational capabilities.

Organizations should assess their security landscape and consider a hybrid approach where applicable. By aligning security tools with business objectives, companies can build a resilient and future-proof cybersecurity strategy.

NEXT STEPS

- Evaluate current security operations and pain points.
- Determine the data volume and analytics requirements.
- Consider a phased approach to integrating a Security Data Platform alongside an existing SIEM.
- Consult with security professionals to ensure optimal implementation.

By making informed decisions, organizations can enhance their security posture and better protect against evolving threats.

gravwell

RECOMMENDATIONS AND BEST PRACTICES

WHEN TO CHOOSE SIEM

- Regulatory compliance is a primary concern.
- Centralized logging and automated incident response are key requirements.
- The organization has a dedicated SIEM team to manage and maintain the system.
- A structured event-driven security framework is needed.

WHEN A SECURITY DATA PLATFORM IS MORE APPROPRIATE

- The organization needs real-time, high-speed data analysis.
- Large-scale data ingestion and scalability are major concerns.
- Advanced analytics and threat hunting are priorities.
- Security teams need more flexible, exploratory data analysis capabilities.

HYBRID APPROACHES

Many organizations benefit from a hybrid approach, leveraging SIEM for compliance and incident response while using an SDP for advanced threat detection and analytics. Integration best practices include:

- **Using SDPs to pre-filter data** before sending it to a SIEM to reduce costs
- **Deploying machine learning models** within an SDP to refine SIEM alert accuracy

FUTURE TRENDS IN SECURITY OPERATIONS

- Increased adoption of cloud-based security platforms
- Greater reliance on AI-driven security analytics
- Convergence of SIEM and SDP capabilities into unified security platforms
- Growth in zero-trust architecture models leveraging security analytics