Your Guide to Data Resilience and SIEM Solutions

Contents

Introduction	3
What is SIEM?	3
SIEM Solutions Enhanced with AI and ML	4
Benefits of SIEM solutions	4
How does Veeam Data Platform Integrate with SIEM Solutions?	7
Which SIEM Solutions Does Veeam Data Platform Integrate With?	9
CrowdStrike	9
Splunk	10
Palo Alto Networks	11
Microsoft Sentinel	12
Sophos MDR and XDR	13
Veeam Incident API	14
Five Benefits of Integrating Veeam Data Platform with SIEM Solutions	15
Conclusion	16

Introduction

In today's rapidly evolving digital landscape, ensuring the security and resilience of data is key for organizations of all sizes. The integration of Security Information and Event Management (SIEM) solutions with data protection platforms like Veeam has become a critical strategy for enhancing security operations and safeguarding valuable information.

This e-book begins by establishing the fundamental concepts of SIEM and its importance in the modern security landscape. It delves into the key functionalities of SIEM solutions, followed by detailed insights into integration options, and how Veeam's integration with various SIEM solutions can streamline security operations, automate incident responses, and ensure the integrity and security of backup data.

Through practical examples and use cases, this e-book demonstrates the value of integrating with SIEM solutions and Veeam for a robust and resilient data protection strategy.

What is SIEM?

A SIEM solution serves as a highly configurable security system of record solution that aggregates and analyzes security event data. By leveraging SIEM, organizations can effectively respond to threats, mitigate potential damage, all while meeting regulatory compliance and reporting requirements.

SIEM tools offer several key functionalities:

1. **Data aggregation and normalization:** Collecting and standardizing data from diverse IT and operational systems, whether on-premises or in the cloud.
2. **Event identification and investigation:** Providing detailed insights for investigating security events.
3. **Real-time and historical event management and reporting:** Facilitating the management and reporting of both current and past security events.

Modern SIEM solutions now use artificial intelligence (AI) and machine learning (ML) to enhance their analytical and predictive capabilities. Additionally, SIEM solutions integrate with security orchestration, automation, and response (SOAR) solutions, enabling teams to automate tasks and streamline incident response actions.

SIEM Solutions Enhanced with AI and ML

Due to the scale of data handled by SIEM solutions, AI and ML functionality significantly enhance SIEM.

Improved Threat Detection:

AI and ML can analyze vast amounts of data in real-time, identifying patterns and anomalies that might indicate security threats.

Reduced False Positives:

SIEM solutions often generate numerous false positives, overwhelming security teams. AI and ML algorithms learn from historical data to better distinguish between genuine threats and benign activities, reducing the number of false alerts.

Behavioral Analysis:

ML algorithms can continuously monitor user and network behavior to detect unusual activities. This helps in identifying inside threats and threats that bypass security measures.

Proactive Security Measures:

By leveraging predictive analytics, AI and ML can anticipate potential threats based on historical data and emerging trends, allowing organizations to take proactive measures to safeguard their systems.

Benefits of SIEM solutions

SIEM solutions are valuable for organizations of all sizes, among their top benefits include:

- **A single pane of glass:** Gain visibility in one place by centralizing and analyzing data from disparate data sources.
- **Real-time threat detection:** Detect and identify potential security breaches and threats in real time, minimizing the risk of compromise.
- **Improved incident response:** Investigate and triage security events efficiently, reducing the time and resources required for research and resolution.
- **Compliance:** Reports and audit trails to comply with regulatory and industry-specific security standards, frameworks, and compliance.
- **Enhanced Forensics:** Historical data allows detailed forensic investigations to identify attack vectors and causes of security incidents.

Integrating with SOAR solutions allows triggering of predefined actions in response to detected threats closing the loop from detection to correction. Finally integrating with data platforms such as Veeam allows for clean system recoveries without risk of reinfection and many more capabilities that we'll discuss in the next few sections.

SIEM Integrations

SIEM solutions are versatile and designed to integrate with a wide range of systems to collect, analyze, and correlate security data. Below is a categorized list of systems SIEM solutions typically integrate with, along with how integration is achieved.

Network Devices

Network devices including firewalls, routers, switches, web application firewalls, and VPNs are key data sources to have visibility of potential malicious activity.

Common integration methods: Log collection via Syslog, SNMP, or API-based integration.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) Solutions are tools designed to continuously monitor and respond to threats on endpoint devices, such as computers, laptops, servers (Windows, Linux, macOS), and mobile devices. EDR solutions provide real-time visibility into endpoint activities when integrated with SIEM. They provide a central point for security teams to detect, investigate, and mitigate potential threats like ransomware and malware.

Common integration methods: Endpoint agents or log collectors installed on devices, or through APIs.

Identity and Access Management (IAM)

Identity and Access Management (IAM) solutions are comprehensive security solutions designed to manage and control authentication, authorization and user management across systems. Examples of IAM systems include Active Directory (AD), Entra ID, and a variety of commercial and open-source Single Sign-On (SSO) solutions.

Common integration methods: APIs, log ingestion, or through security logs.

IT Service Management (ITSM)

IT Service Management (ITSM) solutions ensure that the right processes, people, and technology are in place so that organizations can meet their business goals. ITSM is often associated with frameworks like ITIL (Information Technology Infrastructure Library), which provides best practices for IT service management. Examples of ITSMs include ServiceNow and Jira Service Management.

Common integration methods: APIs, log ingestion, endpoint agents, or file-based imports.

Log Management

Log Management solutions are tools designed to collect, store, and analyze log data generated by various systems and applications within an IT infrastructure. They provide insights into system performance and security events.

Common integration methods: Log forwarding using Syslog, Rsyslog, or log collectors.

Security Tools

Practically all security tools provide data that can be centralized in a SIEM solution, including EDRs, threat feeds, vulnerability scanners, SOAR platforms, and even anti-virus or malware detection tools.

Common integration methods: API-based integration, direct log ingestion, or file-based imports (e.g., CSV, JSON).

SIEM can integrate and receive data from practically any other software or system, even databases and data protection platforms where the initial thought might be that they do not relate to security. The fact that they manage data and backups makes them even more critical to make available security related data visible to IT and security teams.

How does Veeam Data Platform Integrate with SIEM Solutions?

Veeam Administration

Veeam Data Platform users know that monitoring backups and the operation of the data protection platform is crucial for maintaining the integrity and security of systems and data. Veeam administrators play an important role in managing and maintaining Veeam environments including backup repositories and the Backup & Replication environment.

Some of the primary tasks for Veeam administrators include, configuration, scheduling, and execution of backup jobs. They also handle data recovery processes, ensuring that data can be restored quickly and accurately in case of data loss or corruption.

Other data protection tasks not frequently discussed include continuously monitoring backup environments for any issues or anomalies and — more importantly — security measures to protect backup data from malware and cyberattacks. Other responsibilities include access controls, backup encryption, and compliance with relevant regulations and best practices.

In essence, Veeam administrators ensure the organization's data is securely backed up, stored, and constantly validated.

Veeam's integration with SIEM solutions enhances the surveillance of the organization's data.

Veeam + SIEM solutions

When Veeam Data Platform integrates with a SIEM solution, the goal is to automate security alerts and monitoring, providing rapid feedback on potential changes to backup environments and backup data. This allows for more proactive and efficient detection and incident responses. Integration is essential because it enables the SIEM to monitor and analyze backup activities continuously. If abnormal changes or suspicious activities within the backup environment are detected, the SIEM promptly alerts the security team. This early detection of anomalies can serve as a vital defense against cyberattacks, ensuring the security of the backup environments.

Integrating Veeam with a SIEM solution enhances visibility to security teams by combining data resilience capabilities including Veeam threat detection with SIEM capabilities. This integration helps prevent or minimize the business impact of cyber incidents in data environments.

Veeam event data includes Veeam security and environmental events, enabling organizations to detect threats, eliminate blind spots, and address potential risks within backup environments. Integrations can be rapidly installed, giving immediate visibility of events from Veeam Data Platform in the SIEM without access or required expertise with Veeam Data Platform.

With Veeam Data Platform, security teams can detect threats before an attack occurs with inline entropy analysis to identify potential encryption attempts, YARA scanning for recognizing complex threats, indicators of compromise tools detection, and other security features. Veeam Data Platform data is sent to rapidly centralize events and alerts through the SIEM enhancing overall cybersecurity effectiveness.

There are over 300 events that Veeam Data Platform can send to SIEM products, these are just a few examples:

- Backup Jobs (completed, successful, failed)
- SureBackup Jobs
- Backup Copy Jobs
- VM Backup and Copy Jobs
- File Backup and Copy Jobs
- Backup Jobs for Microsoft EntraID
- Log Backup Jobs for Microsoft EntraID
- Backup Jobs for Enterprise plug-ins
- Log Backup Jobs for Enterprise plug-ins
- Replication jobs
- Veeam Backup & Replication security events by severity level
- Veeam ONE alarms by severity level
- Objects marked as infected
- Objects marked as suspicious
- Four-eyes authorization events

If an incident does occur, the SIEM visibility and Veeam's recovery capabilities ensure fast data restoration.

Which SIEM Solutions Does Veeam Data Platform Integrate With?

Several integrations already exist for Veeam Data Platform, these fully supported integrations not only visualize the status of the backup environment in dashboards but also offer advanced reporting and automation playbooks. Let's review some of the existing integrations:

CrowdStrike

The Veeam App for CrowdStrike Falcon LogScale offers pre-defined dashboards, proactive alerting, and scheduled searches allowing customers to set up automated searches that run at specific times or intervals to help monitor the logs and generate alerts. For CrowdStrike Next-Gen SIEM, a Veeam Data Platform Data Connector is also available.

Falcon LogScale has an index-free architecture that allows scalability for organizations to log all their data and retain it for years while avoiding ingestion bottlenecks. With more data collected from multiple sources including Veeam Data Platform, security teams can conduct investigations, threat hunt, and scale to over 1 PB of data ingestion per day with negligible performance impact. Live and historical dashboards let users instantly prioritize threats, monitor trends, and troubleshoot issues. Easily drill down from charts to search results. Build and share custom dashboards or use pre-built dashboards.

In turn, CrowdStrike Next-Gen SIEM leverages AI-powered detections, blazing-fast search capabilities, and workflow automation to rapidly identify and mitigate threats. It provides real-time visibility across all data sources, enabling organizations to detect and respond to security incidents more efficiently.

With CrowdStrike + Veeam, organizations enhance visibility and reduce complexity to immediately identify compromised data or cyberattacks. Veeam integrates data events and malware detection information directly into CrowdStrike products, enabling faster threat prioritization and response.

If you are already a Veeam Data Platform Advanced or Premium customer, click here to download The Veeam App for CrowdStrike Falcon LogScale connector.

If you are already a Veeam Data Platform Essentials or Foundation customer, you will need to upgrade to Veeam Data Platform Advanced or Premium to utilize the connector. Click here to speak with our team about upgrading today.

If you are not a Veeam customer, sign up for a FREE Veeam Data Platform trial today. After downloading your trial, click here to download and connect the The Veeam App for CrowdStrike Falcon LogScale solution.

Splunk

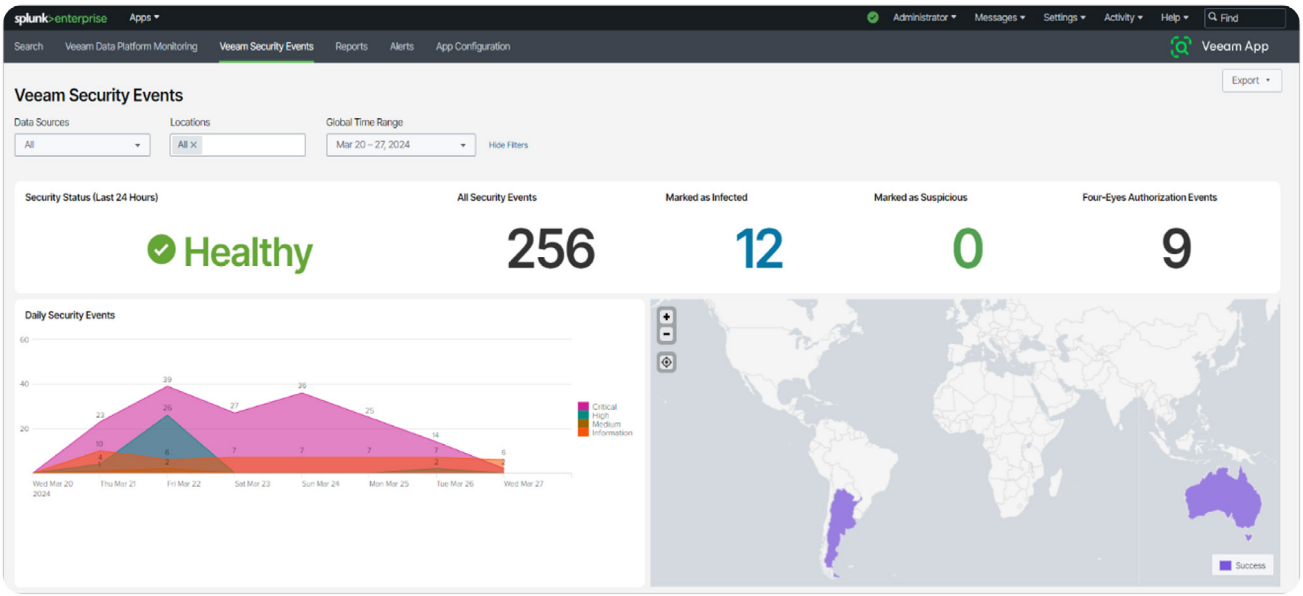
Utilizing Veeam event forwarding capabilities, the Veeam App for Splunk offers Veeam Data Platform data in a comprehensive suite of monitoring and security tools within Splunk, including dashboards, alerts, and reports. This app integrates seamlessly with Splunk user roles and location management. Available for Veeam Data Platform Advanced and Premium customers, the app enables health and security status monitoring of Veeam backup infrastructure using Splunk's capabilities.

The Veeam App for Splunk processes events sent by Veeam Backup & Replication via syslog. This integration allows users to gain real-time insights into job statuses and security events, thanks to the built-in dashboards. Additionally, the app includes built-in reports and alerts, severity level management for events and alerts, and supports multiple Veeam Backup & Replication servers and data source locations.

Veeam's integrates with both Splunk Enterprise and Splunk Cloud Platform, ensuring that IT and Security users can effectively monitor and secure their backup infrastructure, regardless of their deployment environment.

If you are already a Veeam Data Platform Advanced or Premium customer, click here to download The Veeam App for Splunk connector.

If you are already a Veeam Data Platform Essentials or Foundation customer, you will need to upgrade to Veeam Data Platform Advanced or



Premium to utilize the connector. Click here to speak with our team about upgrading today.

If you are not a Veeam customer, sign up for a FREE Veeam Data Platform trial today. After downloading your trial, click here to download and connect The Veeam App for Splunk solution.

Palo Alto Networks

A complementary technology to SIEM solutions are Security Orchestration, Automation, and Response (SOAR) platforms which are designed to streamline and automate security incident response processes, creating standardized workflows, and enabling rapid, coordinated actions against detected threats.

Integrating Veeam with Palo Alto Networks Cortex XSIAM and Cortex XSOAR products significantly enhances security operations by centralizing the view of security-related activities within your backup environment. This seamless integration allows users to combine Palo Alto Networks security tools with Veeam's trusted data protection platform.

Veeam Apps for integration with Palo Alto Networks Cortex XSIAM and Cortex XSOAR tools provide real-time insights into your Veeam environment and immediate notifications for potential security-related activities, all within a single, centralized platform. Benefits of the integration include reducing the risk of data loss due to malware, accidental deletion, internal security threats, and other data loss scenarios.

Scalability is another key feature, as these Veeam apps allow the monitoring of enterprise-scale environments for security activities without the burden of excessive alerts or manual processes. The Palo Alto Networks AI-powered monitoring and incident response capabilities enable faster investigation and response to cyberthreats, enhancing the overall speed and efficiency of your security operations.

Veeam App for Palo Alto Networks XSIAM leverages the event data of Veeam Backup & Replication and Veeam ONE, integrating the latest security features including in-line malware detection. If malware is detected, the details of the security event are sent to Cortex XSIAM via syslog, where data is automatically correlated with other security events, then security teams are alerted and can view the activity in the same single pane-of-glass as their other source environments, ultimately expediting response times.

The Veeam App for Palo Alto Networks XSOAR enables regular API queries against Veeam Backup & Replication and Veeam ONE to monitor for significant security events or alerts. Besides incident creation within Cortex XSOAR, the integrated app also provides a dashboard for deeper insights into the customer's backup environment and pre-defined playbooks to automate incident response, ensuring efficient and effective incident management. An essential tool for SOC centers and security analysts.

If you are already a Veeam Data Platform Advanced or Premium customer, click here to download The Veeam App for Palo Alto Networks Cortex XSIAM and Cortex XSOAR connector.

If you are already a Veeam Data Platform Essentials or Foundation customer, you will need to upgrade to Veeam Data Platform Advanced or Premium to utilize the connector. Click here to speak with our team about upgrading today.

If you are not a Veeam customer, sign up for a FREE Veeam Data Platform trial today. After downloading your trial, click here to download and connect The Veeam App for Palo Alto Networks Cortex XSIAM and Cortex XSOAR solution.

Microsoft Sentinel

The Veeam App for Microsoft Sentinel helps security teams detect threats earlier, accelerate investigations, and strengthen response by incorporating backup and security data into existing workflows. By enriching security operations with Veeam data resilience context, organizations can close critical visibility gaps and respond faster to attacks that target the backup environment.

This is Veeam's first SIEM integration to surface adversary TTPs detected by Veeam Recon Scanner, providing early visibility into behaviors commonly seen in ransomware attacks and mapped to the MITRE ATT&CK framework. These early warning signals, coupled with suspicious activity monitoring and ransomware detection events help analysts spot threats before they escalate. The integration also includes dashboards that visualize backup and security data alongside endpoint, network, and identity signals for a centralized, holistic view of risk.

Bi-directional automation takes it a step further. Analysts can use built-in playbooks or create

their own to enrich Microsoft Sentinel incidents with Veeam context such as affected workloads, restore point history, and repository health. They can trigger actions like verifying restore integrity or initiating a backup directly from Microsoft Sentinel. Together, Veeam and Microsoft empower security teams to act faster, collaborate better, and ensure a clean recovery.

If you are already a Veeam Data Platform Advanced or Premium customer, click here to download The Veeam App for Microsoft Sentinel connector.

If you are already a Veeam Data Platform Essentials or Foundation customer, you will need to upgrade to Veeam Data Platform Advanced or Premium to utilize the connector. Click here to speak with our team about upgrading today.

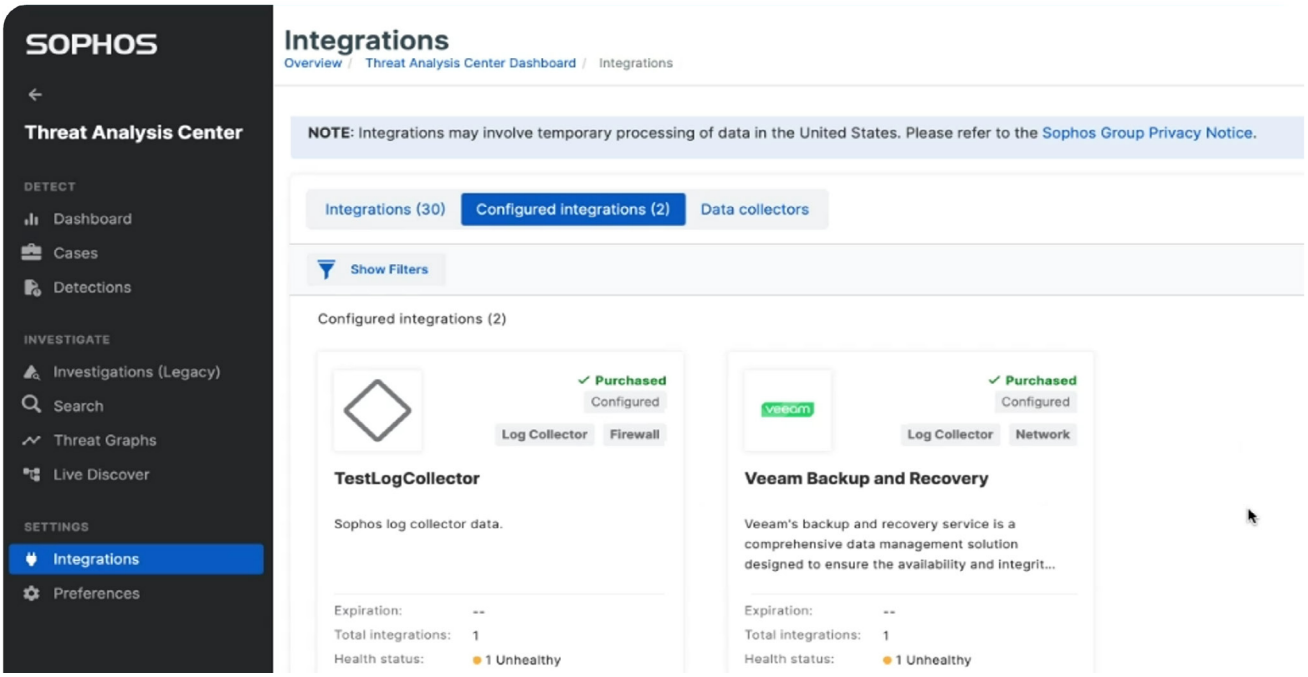
If you are not a Veeam customer, sign up for a FREE Veeam Data Platform trial today. After downloading your trial, click here to download and connect The Veeam App for Microsoft Sentinel solution.

Sophos MDR and XDR

Closely related to SIEM solutions, managed detection and response (MDR) and extended detection and response (XDR) are technologies that help detect and respond to cyberthreats. Sophos MDR and XDR are integrated into Veeam Backup & Replication so events can be sent to Sophos.

The Sophos MDR service provides 24/7 security. The MDR service provides 24/7 security monitoring, filters out redundant alerts, and investigates threats to Veeam environments. It investigates attempts to delete backup repositories, disable multi-factor authentication, delete encryption passwords, and more.

Organizations using the Sophos XDR solution for in-house investigation and response can also integrate Veeam events to identify potentially malicious activity, combined with threat detections from other sources in a single unified platform and console.



Events are forwarded from Veeam Data Platform through syslog, ensuring that all relevant data is captured and analyzed in real-time. This seamless integration enables security teams to monitor and respond to potential threats more effectively, leveraging the advanced capabilities of Sophos MDR and XDR.

Sophos has officially supported this integration, ensuring that customers receive reliable and consistent performance.

If you are already a Veeam Data Platform Advanced or Premium customer, click here to download The Veeam App for Sophos MDR and Sophos XDR connector.

If you are already a Veeam Data Platform Essentials or Foundation customer, you will need to upgrade to Veeam Data Platform Advanced or Premium to utilize the connector. Click here to speak with our team about upgrading today.

If you are not a Veeam customer, sign up for a FREE Veeam Data Platform trial today. After downloading your trial, click here to download and connect The Veeam App for Sophos MDR and Sophos XDR solution.

Veeam Incident API

In addition to the previously described supported integrations, Veeam offers an Incident API for third-party integrations. A common use case is when, via the API, information about threats is sent to Veeam Data Platform which then creates a restore point for the affected environments based on the information coming from the third-party security solution. With this Incident API, other threat related information from cyber security tools can notify the Veeam Backup & Replication server of infections such as malware, ensuring all restore points created after the corresponding incident for the affected environment are marked as infected.

Five Benefits of Integrating Veeam Data Platform with SIEM Solutions

1. Enhanced Security Monitoring

Integrating Veeam Data Platform with a SIEM solution enables comprehensive security monitoring. The SIEM can ingest and analyze backup server and data backup-related events in real time, offering insights into potential security threats such as unauthorized access attempts, unusual data modifications, malware, or failed backup jobs. This proactive approach allows organizations to detect and mitigate security incidents early, it also brings together IT operations and backup admins with Security teams.

2. Incident Response

This integration facilitates incident response workflows. When the SIEM solution reports anomalies or suspicious activities coming from the backup environments, it alerts security teams about threats in Veeam Data Platform and backup environments. In the case of SOAR systems, it can trigger automated actions such as isolating affected systems, notifying security teams, or initiating predefined remediation processes. Automation reduces response times, minimizing the impact of security incidents.

3. Compliance and Audit Reporting

By combining Veeam Data Platform with SIEM, organizations can streamline compliance and audit reporting. The SIEM generates detailed reports on backup activities, access logs, and security events. This helps organizations meet regulatory requirements and maintain comprehensive audit trails. The integration simplifies the process of demonstrating compliance with data protection regulations.

4. Unified Threat Detection

Unified threat detection in a solution correlates data protection platform events and backup data events with other security events across the organization. Threats can be detected by different security systems at different segments or layers of the overall organizations digital environments. This holistic approach helps identify complex attack patterns and coordinated threats targeting both production and backup data. By consolidating security information, organizations can significantly improve their threat detection and incident response capabilities.

5. Operational Efficiency

Integrating Veeam Data Platform with SIEM enhances operational efficiency by reducing alert fatigue and simplifying security management. The SIEM solution can filter and prioritize alerts based on severity, ensuring security teams focus on the most critical issues. Centralized monitoring and management of security events further streamline operations and reduce the workload for IT staff.

Conclusion

Overall, integrating Veeam Data Platform with SIEM and SOAR solutions enhances security monitoring, automates incident response, simplifies compliance, improves threat detection, and boosts operational efficiency. By leveraging these capabilities, organizations can enhance their overall security posture, extending beyond current network and system defenses to include data protection and backup environments — critical components for recovery from natural disasters and increasingly frequent cyberattacks.

If you are already a Veeam Data Platform Essentials or Foundation customer, you will need to upgrade to Veeam Data Platform Advanced or Premium to utilize these SIEM integrations. Click here to speak with our team about upgrading today.

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes businesses should control all their data whenever and wherever they need it. Veeam provides data resilience through data backup, data recovery, data portability, data security, and data intelligence. Based in Seattle, Veeam protects over 550,000 customers worldwide who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

→ Learn more: veeam.com

See our SIEM integrations in action with this demo

Not a Veeam customer? Sign up for a FREE trial today to test our SIEM integrations