imperva

SOLUTION BRIEF

Imperva SIEM Integration

What is SIEM?

Security Information and Event Management (SIEM) is a comprehensive approach to managing security incidents and events in an organization's IT infrastructure. It involves the collection, analysis, and correlation of log data from various sources to provide actionable insights into potential security threats and incidents. SIEM solutions act as a central nerve center for security operations, enabling organizations to proactively monitor and respond to security events in real-time.

SIEM with Imperva

Implementing a SIEM solution with Imperva Cloud WAF offers several significant benefits for organizations, including:

1. Query and Customize Dashboards Across Accounts and Websites

One of the primary advantages of SIEM is its ability to consolidate logs and security events from multiple accounts and websites protected by Imperva within an organization. This centralization allows security analysts to query and analyze data holistically, gaining a comprehensive understanding of the entire environment. With centralized dashboards, security teams can quickly detect anomalies, identify potential threats, and respond promptly to security incidents.

2. Cross-Information Between Other Security Appliances and Services

SIEM solutions can integrate with various security appliances and services, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and more. By correlating data from these different sources, SIEM provides a more comprehensive view of the security landscape. This cross-information allows security analysts to identify patterns and potential threats that may go unnoticed when analyzing individual data sources.

3. Log Completeness Beyond Imperva Cloud WAF

Imperva offers a range of security solutions beyond just WAF. To ensure comprehensive protection, it's crucial to monitor logs from all our products, including ABP, ATO, and DDoS protection. With SIEM integration, you can centralize these logs, making it easier to review and respond to threats effectively. Imperva's multi-layered approach ensures your security remains robust and adaptable.

Imperva Connector Types and Choosing Between Them

Imperva offers multiple connector types for integrating with SIEM solutions. The choice of connector depends on the specific needs, infrastructure, and SIEM application of choice. The main connector types are:

1. S3 Connector

The S3 connector allows customers to maintain their data and store a large volume of data before it is ingested by the SIEM. This method is usually more expensive but provides greater control over the data. Organizations with complex compliance requirements or specific data retention policies may prefer the S3 connector. Most SIEMs have pre-built functionality to pull S3 logs when needed.

2. Imperva API

The Imperva API connector is ideal for on-premises and cloud-based SIEMs. It provides a secure and efficient way to transmit data from Imperva solutions to the SIEM. Additionally, the Imperva API is the default method for some pre-built integrations, such as with Azure Sentinel, Microsoft's SIEM solution.

3. SFTP Connector

The SFTP (Secure File Transfer Protocol) connector is an older technology and offers partial support for only some of the data sets. While it can still be used, it may not be the most efficient or recommended choice compared to the other connectors mentioned above.

After Integration Accomplished

Once the integration between Imperva and the chosen SIEM solution is accomplished, organizations can take advantage of additional functionalities and benefits:

1. SIEM Vendors' Own Applications with Imperva Logs

SIEM vendors often develop their own applications specifically designed to leverage the rich log data provided by Imperva. These applications enhance the SIEM's capabilities, enabling advanced threat detection, visualization, and reporting. Integration with Imperva logs allows SIEM users to extract valuable insights and context from the application-layer security events.

2. Going Beyond With Azure Sentinel and Imperva Integration

Azure Sentinel, Microsoft's cloud-native SIEM solution, offers seamless integration with Imperva's log data. Organizations using Azure Sentinel can benefit from advanced threat intelligence and incident management capabilities, all backed by Microsoft's expertise in cloud security. With Azure Sentinel, security teams gain access to actionable insights and customizable dashboards for real-time monitoring and response.

3. Imperva-supported applications for Major SIEM Vendors

Imperva provides out-of-the-box support for major SIEM vendors, ensuring a smooth integration experience. This support simplifies the setup process and allows organizations to quickly harness the power of SIEM solutions while leveraging Imperva's robust security capabilities. As a result, security teams can focus on analyzing threats and responding to incidents, rather than spending time on complex integration tasks.

Monitoring Your Application Security

Once the integration is in place, organizations can monitor the application-layer security events effectively using their SIEM solution. Two essential monitoring aspects are:

1. Spike in Security Events Across All Traffic

To detect unusual activity, security analysts can create rules or alerts based on spikes in security events across all traffic. SIEM solutions provide flexible rule-creation options, allowing security teams to tailor alerts to their specific needs. By identifying and investigating unusual spikes in real-time, organizations can respond proactively to potential threats.

2. Traffic from Different Countries

Monitoring the countries from which traffic originates is vital to detect abnormal attacks from non-legitimate countries. Imperva Cloud WAF and some SIEM solutions can provide geographic visualization, making it easier for security teams to identify suspicious traffic patterns and potential threat sources. After detecting such an anomaly, the customer can create an access rule in the Imperva console that will block the suspicious patterns.

In conclusion, SIEM plays a crucial role in modern cybersecurity by providing organizations with the tools to centralize and analyze security events across accounts and websites. Imperva's flexible connector types offer options for integrating with various SIEM solutions, making it easier for organizations to enhance their security posture. By effectively monitoring and responding to security incidents, organizations can stay one step ahead of cyber threats and safeguard their critical assets and data.