

State of SIEM 2022

We surveyed hundreds of SecOps professionals who currently use a SIEM solution. This report summarizes their challenges, frustrations, and areas of improvement.

Key Areas of Frustration



77% said receiving high-value alerts took longer than a month.



49% believe their SIEM covers less than half of their security data.



40% suffer from poor alerts, such as false positives, and a large volume of alerts.

Based on this data, we can conclude **many existing SIEM solutions are complex to deploy, provide patchy coverage, and reduce SecOps productivity.**

But on a Brighter Note

21%

say they are using a cloud-native SIEM.

Cloud-native SIEMs help security practitioners reduce the operational burden of managing a SIEM and increase focus on threat detection and response.

This year's State of SIEM report indicates that existing SIEM solutions are unable to keep up with modern cloud environments. **Security teams expect faster time-to-value, greater customization for their detection logic, and higher quality alerts from their SIEMs.**

FOR MORE FINDINGS

Read the Full Report

[Download Now](#)

