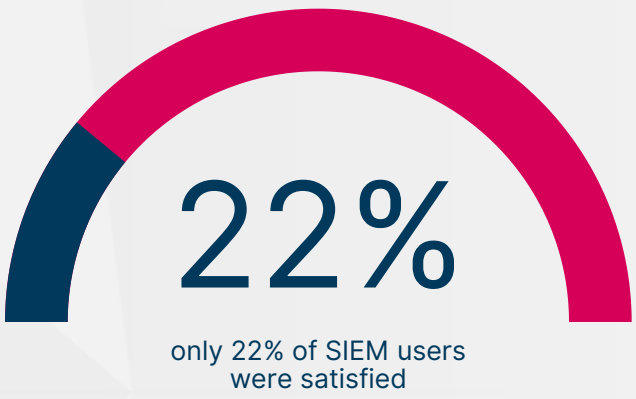
LOG MANAGEMENT BEST PRACTICES FOR YOUR SIEM

SIEMS ARE UNDERUTILIZED

No other detection technology collects and processes data in as versatile a way as **SIEM platforms** can. However, despite heavy investments made to SIEM solutions, these platforms are significantly **underutilized** due to log collection challenges and running with **outdated detection rules.**

*Based on one of the surveys published by **SANS, only 22% of SIEM users** were very satisfied with their solutions**

**Common and Best Practices for Security Operations Centers: Results of the 2019 Survey*

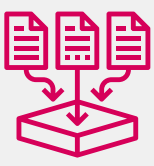


only 22% of SIEM users were satisfied

WHY SHOULD WE START WITH SIEM LOG MANAGEMENT?

It is crucial to have a good log collection system to ensure that all subsequent processes run smoothly. Efficient log management guarantees that SIEMs consistently receive logs from the right log sources with the right detail at the right time.

CHALLENGES OF LOG MANAGEMENT



Do we collect **right log sources?**

Do we collect logs with **the right level of detail?**

Are we collecting logs with **no delay** after events?

BREACH & ATTACK SIMULATION FOR ENHANCED LOG MANAGEMENT

Gartner lists Breach and Attack Simulation (BAS) among the top eight security and risk trends for 2021. An integrated and TTP-centric log validation helps SIEM practitioners keep up with the changes, consistently identify the right sources, define the right detail, and ensure timely delivery.

PICUS

www.picussecurity.com