>SOLUTION BRIEF_

AI-Powered SOC Transformation: Cortex XSIAM and Cribl's solutions for unparalleled security insights.

THE CHALLENGES

Organizations are struggling with tool sprawl and alert overload, leading to slow detection and response times. With dozens of disconnected tools generating thousands of alerts daily, SOC teams face significant challenges in quickly identifying and mitigating threats.

THE SOLUTION

Cortex XSIAM and Cribl empower security teams to modernize their SOCs by ensuring the data collected and routed to XSIAM's AI models operate with the most accurate and complete information, enabling more precise and proactive threat detection.

THE BENEFITS

- Accelerated time-to-value.
- Enhanced visibility.
- Future-proof security architecture.
- Protect your environment at scale with AI/ML.

The challenge.

Organizations often struggle with their legacy security operations center (SOC) and data management tools because each solution provides a unique type of data. Normalizing and aggregating this data can result in losing important context and nuance. The security analyst must stitch the data from all the tools together to identify an attack in progress, making it difficult to quickly detect and remediate an attack. Additionally, many find their data locked in proprietary formats, limiting their control and flexibility.

Companies are looking to modernize and transform their SOC. This requires replacing both their legacy SOC products with best-in-class security tools and their old data collection and data management tools with a data processing engine.

The solution.

Cortex XSIAM and Cribl empower security teams to modernize their SOCs by ensuring the data collected and routed to XSIAM's AI models operate with the most accurate and complete information, enabling more precise and proactive threat detection. Together, delivering faster time-to-value, enhanced visibility, and a future-proof security architecture that adapts to evolving needs and threats.