cybereason® | SOLUTIONS

CYBEREASON SDR

SIEM Detection and Response (SDR) is an Open security observability and AI-driven analytics platform enabling data consolidation across the enterprise to gain meaningful visibility and reduce time to detect, investigate and remediate attacks.

KEY BENEFITS

- Drive down data costs by consolidating your enterprise security data lakes
- Full observability across the existing IT and security estate by Ingesting almost any IT data in any format
- Enhance Analyst productivity and visibility by removing security data silos
- Simplify Threat Detection and Response with Automated Triage and Investigation

As enterprises continue to invest into digitalisation, they are increasingly encountering an evolving threat landscape and complex security challenges. With workloads spread across multiple cloud environments, workforces operating in hybrid setups, and an increasing number of intelligent devices connected in critical operations, the attack surface has expanded significantly. This growth is exacerbated by the exponential increase in data volumes, driving up the cost of storing, managing, and analyzing this data for security purposes.

Attackers are taking advantage of organizations' complex environments and leveraging creative, modern techniques to evade detection. Threats can lurk and move stealthily between security data silos, making them hard to detect and eradicate. This forces security teams to scramble to triage and investigate incidents as they impact different parts of their IT estates.

Traditional security tools like SIEMs are limited in their effectiveness. They often operate with narrow log aggregation and correlation capabilities, relying on predefined thresholds for alerting. This approach makes it challenging to gain deep insights for root cause analysis and investigation of security threats and vulnerabilities. Analysts are often left manually retrieving data from disparate tools in order to build the true picture of a malicious operation, causing delay in detection and response times and increasing the risk and cost of a breach.

REIMAGINE SOC OPERATIONS BY TRANSFORMING YOUR DATA STRATEGY

Cybereason SDR, or SIEM Detection and Response, is a cybersecurity solution that transforms security operations by solving the big limitations of some of the core technologies used by security analysts today SDR takes a new architectural approach to address the same use-cases and business outcomes that these technologies were intended to deliver.

Built with an open architecture in mind, Cybereason SDR includes an extremely scalable data lake that is designed to take in data across all IT & Security tools of an enterprise's existing ecosystem. SDR is able to ingest both structured and unstructured raw trace and metrics data from across the enterprise without the data ingest cost and quality problems of SIEMs. Combined with a unique observability layer, SDR leverages AI-driven analytics and automation to provide security operations teams with more comprehensive threat detection, and much faster response and remediation times across this unified security data lake.

Cybereason SDR is the culmination of over 10 years experience of providing market leading prevention, detection and response technologies and services with the unique ability to allow analyst to stop chasing alerts to uncovering and ending malicious operations with the MalOp™ detection engine.

Unlike the closed proprietary SOC ecosystems from other Cyber security vendors, Cybereason SDR is designed to drive down data consumption and processing costs by integrating with existing enterprise data lake consolidation projects currently underway in many enterprises today.

Cybereason SDR is **the culmination of over 10 years experience of providing market leading prevention, detection and response technologies and services** with the unique ability to allow analyst to stop chasing alerts to uncovering and ending malicious operations with the MalOp™ detection engine.

KEY CAPABILITIES

UNCOMPROMISING ENTERPRISE SECURITY DATA STRATEGY

Drive down data costs and improve analytics performance by consolidating your enterprise security data lakes and addressing fundamental cost and data quality issues with a SIEM-based architecture. This consolidation eliminates data silos and streamlines data management processes, enabling more comprehensive, efficient and cost-effective data analysis.

Removing the cost barrier to ingesting all security data means enterprises gain meaningful visibility across the entire IT and security estate. This strategy enables businesses to consolidate their cybersecurity tools raw data and enhance security posture by providing comprehensive insights into potential threats and vulnerabilities to stop breach earlier and assure business resilience.

AI-DRIVEN, REAL-TIME ANALYTICS ACROSS ALL SECURITY DATA

Extending Real-time Analysis to the entire IT estate: The Cybereason core technology , powered by the MalOp™ AI-Driven Detection Engine, analyzes the raw trace and metrics data across the enterprise security data lake in real-time.

Automated Triage and Investigation in one UI: Automated triage and investigation workflows build the full narrative of the attack, including root cause, attack timeline, and affected devices, users, and other assets.his AI-assisted approach significantly reduces Mean Time to Detection (MTTD) and Cybereason's Unified Portal enables faster response, including guided remediation.

OPEN ARCHITECTURE. ONE UNIFIED PORTAL

Ingest any structured and unstructured data, gaining critical insights across all existing enterprise IT and security stacks. This approach ensures seamless integration into existing infrastructure, maximizing return on investment and minimizing disruption.

Stop Cyber Attacks that get lost in the noise: *Cybereason SDR ingests and automates the enrichment of an organization's entire IT estate data to uncover threats that would have been missed with siloed solutions. The Cybereason MalOp creates actionable attack stories of an attacker's malicious operation in a single correlated view.*

ABOUT CYBEREASON

Cybereason is a leader in future-ready attack protection, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in La Jolla California with customers in more than 40 countries.