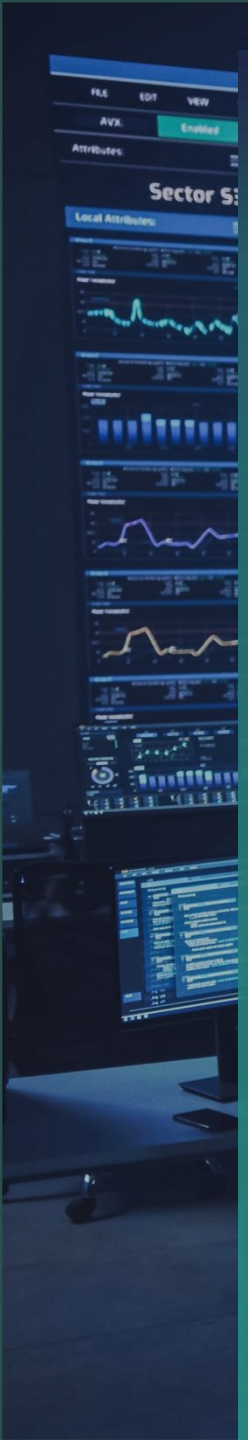
Invisible bits



Event Data Processing

Data Reduction

@ 2025

Invisible bits

What is data reduction?

Data reduction focuses on minimizing logs sizing used in cybersecurity, ensuring that detections and key insights remain intact.

By removing unnecessary information, organizations can substantially cut expenses related to SIEMs costs, data storage, analysis, and management.

This approach is especially beneficial in large-scale data environments, where handling immense volumes can be both financially burdensome and operationally challenging.

Invisible-bits

Real examples of SIEM license cost reduction

Log source	Event average size	Average reduction
Fortinet firewall	890 bytes	54%
Palo Alto firewall	546 bytes	54%
Windows endpoint	2,7 kilobytes	68%
AWS Cloudtrail	2,2 kilobytes	73%
AWS Security hub	17 kilobytes	91%

Total average SIEM license cost reduction: 70%

Suported SIEMs and observability platforms

splunk> LogRhythm now exabeam Radar elasticsearch ArcSight DATADOG

Event Data Processing

SOURCES

Devices
- Fortinet
- Palo Alto
- Active Directory
- ...

SIEMs
- Splunk
- Qradar
- ArcSight
- Azure Sentinel
- ...

Public Clouds
- Azure
- AWS
- Google Cloud Platform

Open formats
- Syslog
- TCP / UDP
- JSON
- HTTP/S
- SNMP Traps
- ...

TRANSFORMATION

ENRICHMENT

DETECTION

REDUCTION

DESTINATIONS

Data Lakes
- ASIP
- Splunk
- Elastic

SIEMs
- Qradar
- ArcSight
- LogRhythm

Public Clouds
- Azure
- AWS
- Google Cloud Platform

Observability
- Datadog
- Coralogix
- Dynatrace
- Graylog

Open formats
- Syslog
- TCP / UDP
- JSON
- HTTP/S
- ...