Grow Your Data Management, Storage and Processing Capabilities

A basic law of Big Data in cybersecurity: the more data you use, the more data you find you’ll need. Ingestion rates tend to rise.

Where to cap your data capacity is a strategic decision, and not an easy one. Processing, moving, and storing daily logs adds up, especially when you’re scanning hundreds of thousands of events per second. That’s terabytes of log data per day.

Modern Big Data solutions provide tremendous value – they allow near-real-time streaming analysis and deep historical querying, which is hugely important for fast, effective security. But successful data programs must balance the value-add of new sources and use cases. Data architectures should anticipate growth – otherwise costs can skyrocket and analysis can slow to a crawl.

Optiv Solutions

**PRIORITIZATION**
Optiv’s Big Data & Analytics team works with clients to prioritize data for analysis or storage, optimizing system flow. We review all sources and filter redundant information. Often, data details can be removed, as they’re not relevant to the SOC. High-value data should move to processing. Raw logs should flow to low-cost repositories for longer term retention and ad hoc queries.

**TIERED STORAGE**
Tiered storage drives additional efficiencies. High-performance computing components supercharge ingestion and searches of frequently accessed data, while lower cost computing machines have higher storage capacity. Older, rarely accessed data doesn’t require high-performance (nor the high cost that goes with it).

**DATA AGGREGATION**
A final source of efficiency: aggregate data as it begins to age. Summary log information can fuel long-term analysis and comparison, further increasing the system’s capacity (without the need to retain the full history). Example: retain every instance of a failed log-in attempt. Or, you might find value in aggregating how many times each month users access data past a certain age. These capabilities would dramatically reduce the amount of stored data and the cost of performing analysis.
How We Do It

• Align with your business and understand your objectives and priorities
• Assess your environment, sources and use cases to identify top ROI initiatives
• Prioritize and tune data inputs source-by-source
• Build or enhance data pipelines to enable enrichment, tiered storage and aggregation
• Configure monitoring and alerting to manage volume and spend
• Share knowledge by training, documenting and phasing out support to client stakeholders

Why Clients Choose Optiv

Augment your security team with data science, data engineering and cybersecurity expertise by working alongside our team

Accelerate time to insight for reliable, current data by unifying batch and streaming pipelines at massive scale

Build outcomes specific to your business’s problem domain

Access all your data in one place and automate the most complex data pipelines

Create a seamless workflow from data ingestion to deployment of models into production

Establish comprehensive security model featuring fine-grained controls, data encryption, identity management, rigorous auditing and support for compliance standards

Reduce operational complexity while increasing performance and ensuring reliability and cost efficiency at scale

Secure greatness™

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2021 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.