csg

TOGETHER, YOU WIN.

SECURITY DATA ORCHESTRATOR

SUPERCHARGE YOUR SECURITY MONITORING

csg
TOGETHER, YOU WIN.

MORE DATA, MORE CHALLENGES

As communication service providers, networks and systems intake more and more data, they're challenged to efficiently filter, normalize and transport high volumes from many varied sources. A data scaling problem quickly emerges when incoming security events and logs from disparate platforms rapidly overwhelm SIEM consoles and storage subsystems.

The traditional solution to managing increasing event volumes and the corresponding increased strain on security analysts required for monitoring is to continually grow capacity. More network bandwidth, more data storage and more people to monitor the events.

Additionally, current technologies are creating challenges related to accessing and sharing of security data in real time such as:

- Security event data stored in multiple locations, often duplicated
- Security event data not easily parsed for specific purposes, requiring all data to be stored
- Multiple solutions providing fragmented and scattered data that reduces the operational efficiency of security analysts
- Storage requirements inflated by data redundancy and irrelevance

IMPROVING PERFORMANCE AT REDUCED COSTS

CSG Security Data Orchestrator enables you to streamline the handling of alert and log information and strengthen your security operations. The solution helps ingest, filter, cleanse, and correlate massive amounts of data at machine speed.

Security Data Orchestrator easily handles the tasks of high volume data normalization and transmission to the monitoring layer, thereby reducing the impact on large existing investments.

The result? Greatly improved performance from business, operations and security analytics—and much lower storage costs and bandwidth utilization.

KEY SOLUTION BENEFITS

- High Volume Ingest
- Filtering
- Normalization
- Compression
- Encryption
- Priority Transmission

MAINTAIN AND FEED EXISTING SOLUTIONS

- SIEM
- Log Aggregation
- Physical Security
- Other SOC Tools
- Other NOC Tools
- External Feeds

RAPID, SECURE DEPLOYMENT

- Installation services available for system deployment
- Dedicated professional services team
- Cleared personnel available for government installations

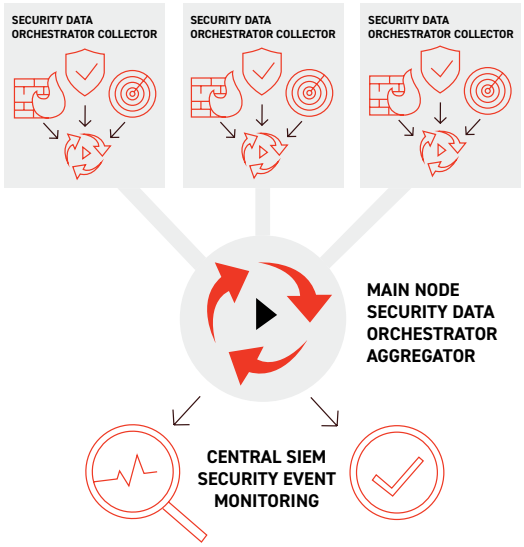
The solution adapts to accommodate non-standard data formats and transmission methods, ensuring format and transmit protocol of inbound data is never an issue.

THE COLLECTOR

Security Data Orchestrator is comprised of two main components: Security Data Orchestrator Collector and Security Data Orchestrator Aggregator.

The Security Data Orchestrator Collector software is co-located with the data sources in a distributed enterprise network to capture security event and log data from disparate technologies. Configure the Collector to filter unwanted data records; enrich useful records with a unique record identifier; resolve and augment records with local origin information; and apply priority designations to the records.

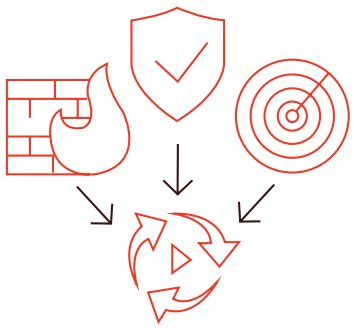
DISTRIBUTED SECURITY DATA ORCHESTRATORS



The enriched records are then transmitted to one of more defined destinations in priority order.

- Transmission options permit different (or the same) subsets of the records to be transmitted to each destination, on different schedules, with data packaging optimized for the destination
- Data records are safely stored on the Collector until they have been delivered to all configured destinations
- The Collector performs encryption and compression prior to transmission to the destination ensuring the security of the data and minimizing the amount of data being transmitted

SECURITY DATA ORCHESTRATOR COLLECTOR



THE CONNECTORS

Device connectors are software modules residing in the Security Data Orchestrator that interface to the devices where data is sourced. The Connectors transfer the data and monitor all data acquisition processes, register the data files with the Data Management subsystem and restarts any failed input sessions, when possible.

The device connectors also connect to the systems receiving data distribution. Custom connectors can be created for new devices or proprietary data formats.

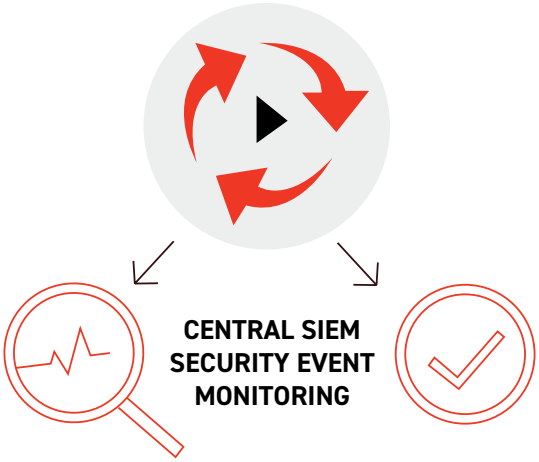
THE AGGREGATOR

The Security Data Orchestrator Aggregator is an enterprise-grade software application designed to reliably and efficiently ingest large volumes of data, typically from a distributed network of Security Data Orchestrator Collectors. The Aggregator performs advanced data operations, to complement the initial Collector processing, including correlation of records across multiple record streams, further elimination of unwanted records, detection and elimination of duplicate event reports, and enrichment of the data with enterprise information:

- User credentials
- IP reputational information
- IP geospatial infromation

Higher levels of error checking can be configured for the data at this time, along with other data normalization:

- Upper/lower normalization
- Data/timestamp normalization



Data deemed to be in error may be sidelined within the Aggregator for inspection by skilled data flow analysts. The Aggregator solution permits such data to be recovered and corrected in bulk.

RAPID, SECURE DEPLOYMENT

Installation services are available for deployment of the Security Data Orchestrator system. Our dedicated professional services team has cleared personnel available for government-related

TALK TO OUR EXPERTS ABOUT HOW SECURITY DATA ORCHESTRATOR CAN SUPERCHARGE YOUR SECURITY MONITORING TODAY. VISIT CSGI.COM FOR MORE INFORMATION.