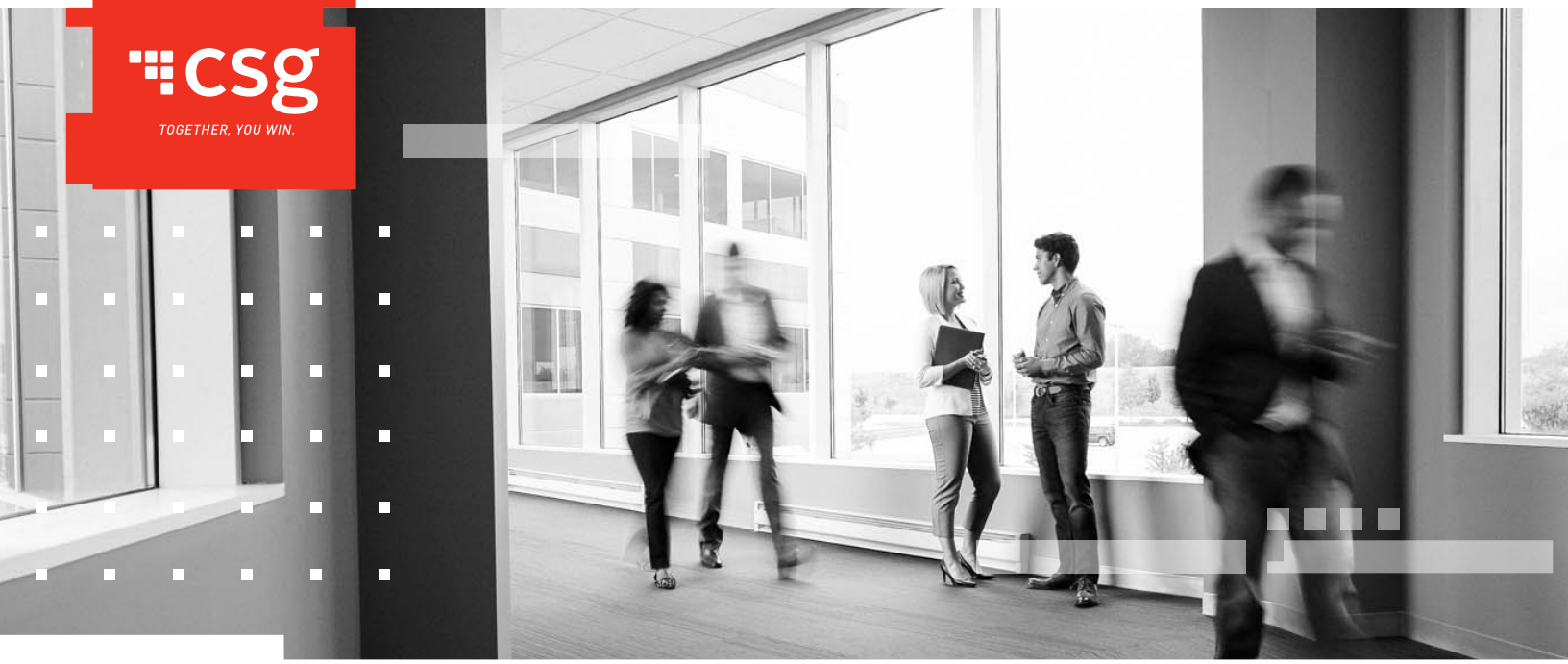
csg

TOGETHER, YOU WIN.

CYBER DATA MANAGEMENT: THE IMPORTANCE OF THE CYBER DATA MANAGEMENT NODE

A WHITE PAPER

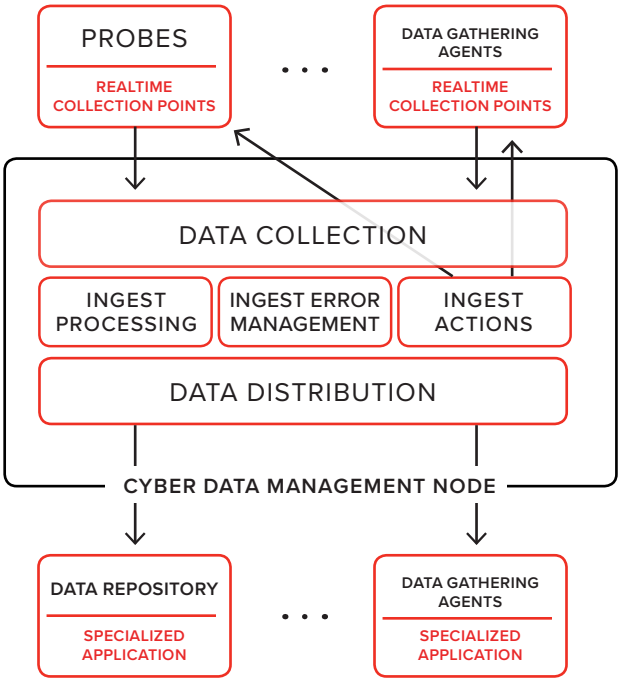


WHAT IS A CYBER DATA MANAGEMENT NODE?

The National Cybersecurity Initiative is an effort to develop a strategy to protect the nation's government-run and private computer networks. The Initiative is all-inclusive; there will be real-time and offline capabilities to detect, investigate, and manage intrusions into U.S. government networks. CSG believes the Cyber Data Management Node (CDMN) is a vital component in the Cybersecurity solution architecture.

The Cybersecurity solution architecture will inevitably contain collection points of information throughout the nation's networks. Some collection points will be real time (intrusive probes) and others will be offline (data gathering agents). The Cybersecurity solution architecture will also contain repositories of information that hold the details of network usage for statistical and investigative analysis. The CSG CDMN functions in the middle, accepting information from the collection points, interpreting the data with conditioning processes, and finally, providing the results to the data repositories.

The interpretation of information related to the use of communication networks is complex. Sources of information vary widely, as does the form of the information and its content. Viewed singularly, the information does not specify intent and is void of human meaning. The rules with which to analyze the information must be flexible and receptive to managing unexpected content.



While the goal is to analyze information and make informed decisions, the task first becomes one of data processing and computer science. The data must be organized and cleansed after gathering, after which it can be effectively used to draw inferences as to human intent.

The mission of the CDMN is to remove the complexities so that meaningful and accurate data sets can be made available for analysis. The CSG Cyber Data Management Node is specifically designed and built as a framework for dealing with disparate data and transforming it into an understandable and meaningful dataset for logical analysis. CDMN provides:

- **Ingestion** – Gathering and processing information towards a single objective: the creation of a clean data set for human or automated analytic consumption. Ingestion includes data collection from any source, data validation, aggregation, correlation, error suppression and correction, and preparation for population of one or more analytic or forensic databases
- **Enrichment** – Blending referential data with ingested information to increase its value. Referential data can be names, addresses, coordinates, adjective text, or any other additive value. The objective of enrichment is to remove the private nature of raw data and enhance its meaning. Many such attributes of the raw data are slowly changing in nature (e.g. DHCP assignments, domain assignments) – resolving these attributes close to the time of ingest and before commitment to a repository avoids extensive post-processing "joins" and permits early and rapid analysis using these attributes
- **Attribution** – Matching data from various sources for the purpose of assigning the intent to the action. Attribution is achieved by correlating multiple streams of data-phone records with network access records, for example—to obtain the broad picture of network usage rather than just snapshots
- **Reporting** – Providing a dynamic window into the ingested data. Reporting is a method of interrogating the ingested data set with logical, rational, and substantive queries to produce a revealing view of the content based on summarization and aggregation over multiple attributes
- **Dissemination and Collaboration** – The business rules implemented by the CSG solution have a transient nature; they change over time. New processing algorithms (configuration) are created when more knowledge is gained or when new information is introduced. Dissemination is the process of ensuring the new configuration and rules are applied to the different instances of the solution
- **Action** – Besides passive collection of data, the CDMN can respond actively to recognized events, or by manual direction to control and manage the collection points to affect an active response to a recognized event

THE BUSINESS RULES IMPLEMENTED BY THE CSG SOLUTION HAVE A TRANSIENT NATURE; THEY CHANGE OVER TIME.

WHY CSG FOR CDMN?

CSG is unique in its ability to provide large data management solutions. We presently provide data management solutions to Government organizations and commercial companies in telecommunications, finance, and logistics. We do this on a global basis managing significantly large volumes of source data, preparing it for specialized use by various applications in the enterprise. We offer the CSG Cyber Data Management Node (CDMN) as your best choice to fulfill the ingest requirements for the National Cybersecurity Initiative.

CSG believes that the value and significance of any long-term collection of cyber data will be enhanced by our approach to structured management of the ingest process. CDMN will eliminate unwanted or redundant information ("filtering"), assemble related data ("correlation"), and resolve cross-references ("enrichment") prior to committing any data to a repository. This approach is especially important in today's world of very large repositories implemented with technologies which are typically write-once, read many; where updates to existing data is both costly and time-consuming.

THE CSG CYBER DATA MANAGEMENT NODE (CDMN) PROVIDES THE FOLLOWING CAPABILITIES:

- Enrichment of the ingested cyber traffic data feeding existing or newly planned data warehouses through the use of referential information which itself can be the result of ingested information—for instance from the network providers (e.g. DNS, user information, geo-location information)
- Distributed deployment options allowing the CDMN to be deployed as a centralized system and/or a remote system. The centralized model acts as the primary concentrator of cyber data prior to population of the repository. The remote model allows the CDMN to be deployed in close proximity of the data source (probe). The intent is to process the collected data at the source and reduce the volume to that set of information required by the specialized applications
- Distributed configuration – Rules for ingest collection, ingest processing, and ingest actions can be centrally built and tested. The centralized CDMN can then distribute the configurations to the remote CDMN locations for auto loading and execution
- A proven and auditable data collection function.
- Rapid reaction to new and/or unexpected data types. The CDMN has integrated tools that allow fast creation of new data types and the corresponding processing rules
- An integrated ability to interact with the data sources (probes) for re-configuration or filtering of input data. For example, if the CDMN detects a particular pattern of data types it can send commands to the data gathering agent (probe) to change its behavior in collection
- An integrated error processing system to manage out-of-band situations or data anomalies. The CSG data management experience is such that no planning exercise can foresee all processing scenarios

The best practice is to effectively manage the unexpected so that the anomaly can be studied and the processing rules can be enhanced to recognize the situation and provide the data to the repositories for proper intrusion analysis. The error processing system is a collaborative tool providing a UI that is convenient and insightful for problem resolution

→ A reporting and analytical tool to aid data quality management and analysis

The CDMN is available now as COTS software. Its core components are deployed globally to satisfy the data management requirements of market leaders in the telecommunications, financial services, and logistics industries.

The Cyber Data Management Node is based on CSG's pre-integrated Intermediate and Interactivate applications. The interpretation of information related to the use of communication networks is complex. Sources of information vary widely, as does the form of the information and its content. Viewed singularly, the information does not specify intent and is void of human meaning. The rules with which to analyze the information must be flexible and receptive to managing unexpected content.

CSG INTERMEDIATE

CSG Intermediate solution has proven to be the mediation system of choice for many of the world's largest network operators for more than two decades, providing collection and mediation functions for more than 220 customers on six continents. CSG's mediation customer base includes an impressive list of government, financial, wireless, VoIP, local, long distance, and next-generation network providers.

With a powerful yet flexible and easy-to-use processing logic module at its heart, Intermediate can provide complete control over the ingest and enrichment processes, while at the same time providing a platform that enables the rapid introduction of new data sources and ingest rules.

In the CDMN solution, Intermediate serves as the localized ingest and enrichment application. All data collected by or on behalf of the Government is processed through Intermediate.

Intermediate also includes a Rapid Development Environment to ease the task of building processing rules. As much as possible, Intermediate removes the complexities of programming from rules creation. A rich set of tools is provided, enabling users to not only develop new ingest logic independently but to do so in a business-oriented fashion. Using the efficient and intuitive tools, the end user can, with minimal effort and resources, develop the new ingest logic scripts and then run them through the built-in interactive testing facility prior to packaging up for deployment.

Included with Intermediate is the Reporting tool (IRPT), an analytic toolset leveraging Oracle RDBMS technology. This is used to provide advanced, customizable reporting, queries, and analytic functions on the collected cyber data set. The database management routines support high volume summarization, aggregation, presentation and query over any number of data attributes, with drill down to detail records.

CSG INTERACTIVE

To meet the Cyber investigation challenges faced today within the internet world, CSG offers Interactivate, a flow-through "activation" system. "Activation" is the process of managing multiple, disparate collection points with a common, high-level command or API interface.

Interactivate is a flexible application that can allow Government personnel to implement new business rules for network element control as investigations evolve. This system is a fully automated, flow-through activation platform that can accommodate dissimilar networks, technologies, and infrastructures.

The Interactivate architecture is highly scalable and flexible, and supports integration with multiple types of external systems using many types of communications and control protocols.

Interactivate's activation process begins when it receives a request from an external source or application. Interactivate processes these high-level requests using the defined business rules to decompose the requests into separate Activation Actions, which are then directed to a specific device (network element). Each Activation Action identifies the specific device commands and protocol required to complete the request. Once all of the dependent Activation Actions are complete, Interactivate sends an appropriate response back to originator, completing the request process.

Interactivate is a multi-service activation platform that will enable Government officials to build complex triggering rules and decompose them into a series of specific tasks. Interactivate can also provide proactive response to particular thresholds of events which can be pre-defined by the Government. Interactivate also provides alarming, emailing or specific notifications to individuals, groups or devices that require specific and immediate attention.

INTERACTIVATE IS A MULTI-SERVICE ACTIVATION PLATFORM THAT WILL ENABLE GOVERNMENT OFFICIALS TO BUILD COMPLEX TRIGGERING RULES AND DECOMPOSE THEM INTO A SERIES OF SPECIFIC TASKS.

ABOUT CSG

CSG simplifies the complexity of business transformation in the digital age for the most respected communications, media and entertainment service providers worldwide. With over 35 years of experience, CSG delivers revenue management, customer experience and digital monetization solutions for every stage of the customer lifecycle. The company is the trusted partner driving digital transformation for leading global brands, including Arrow, AT&T, Bharti Airtel, Charter Communications, Comcast, DISH, Eastlink, iFlix, MTN, TalkTalk, Telefonica, Telstra and Verizon.

At CSG, we have one vision: flexible, seamless, limitless communications, information and content services for everyone. For more information, visit our website at csgi.com and follow us on LinkedIn, Twitter and Facebook.