cloudera

SOLUTION BRIEF

Security

CYBERSECURITY TURNKEY SOLUTION

The hyper-connected digital world produces cybersecurity data at a volume and rate that surpass the capability of manual processes and traditional security tools. Enterprises are challenged to find an economical way to effectively detect cyber threats and comply with data governance requirements. Available tools often require lengthy setup and configuration to unique technical environments and business objectives. They also bring a steep learning curve to achieve tangible results.

To meet these demands, you need a best-of-breed approach that brings together the best modern technologies in big data, advanced analytics, machine learning, and more. Moreover, this solution must be future proof — able to grow to match the elevating sophistication of cyberattacks.

Cybersecurity Turnkey Solution (CTS) — a multi-partner solution from Cloudera, System Soft Technologies, and Zoomdata built on a reference hardware platform from PSSC Labs — provides the functionality and performance you need: quick time to business impact, powerful analytics, low cost-to-performance ratio, out-of-the-box compliance, and flexible expansion options.

BENEFITS OF THE CYBERSECURITY TURNKEY SOLUTION

Designed, architected, integrated, and tested with precision, the Cybersecurity Turnkey Solution provides the following benefits:

Immediate time-to-value

- Fast-start turnkey solution bypasses lengthy setup and configuration.
- Performance-optimized appliance hardware is uniquely designed and architected for cybersecurity.

Ease and convenience meeting compliance requirements

- Out-of-the-box compliance frameworks, including the popular NIST framework for cybersecurity, enable fast startup.
- Massive scalability and storage of big data Hadoop eliminate data loss.
- Long-term data retention enhances compliance and threat detection.
- Comprehensive datasets increase visibility of risks.

Accelerated threat detection with precision

- Advanced user and entity behavior analytics (UEBA) and statistical and data science models speed detection.
- Real-time ingestion and stream processing enable rapid threat analysis.
- Advanced visualization and situational awareness foster efficient threat hunting.

Streamlined security operations to overcome talent shortage

- Integrated single view of risks eliminates swivel chair analytics.
- Alert triage reduces manual processes and prioritizes response.
- Machine learning models automate threat detection.

Flexible and extensible next-gen cybersecurity platform

- Seamless integration with existing SIEM protects investments.
- Optimal price-to-performance ratio to start and low-cost option for expansion keep costs low.
- Pluggable model-as-a-service extends platform with add-on features.
- 100% open source atthe core assures continuous enhancement and innovation.

PARTNER ECOSYSTEM COMPONENTS OF THE CYBERSECURITY TURNKEY SOLUTION

Cloudera Cybersecurity Platform (CCP), powered by Apache Metron, is precisely engineered to visualize diverse, streaming security data at scale to aid in real-time detection and response to threats. The following components are incorporated:

- **Apache Metron** — A next-generation security operations center (SOC) data analytics and response application integrates multiple open source big data technologies into a centralized tool for security monitoring and analysis. It is a threat detection platform based on machine learning algorithms and anomaly detection that can be applied in real time as events are streaming in. It includes capabilities for log aggregation, full packet capture indexing, advanced behavioral analytics, and data enrichment. It applies current threat intelligence information to security telemetry within a single platform.
- **Cloudera Data Platform (CDP)** — Powered by Apache Hadoop, CDP is a secured, enterprise-grade big data platform that provides a cost-effective way to store enriched telemetry data for long periods of time along with the corpus of data required to do the feature engineering that powers discovery analytics.
- **Cloudera DataFlow (CDF)** — CDF is a full featured data collection solution that is streaming-data agnostic and integrated with hundreds of processors. With ingestion flows customized for the security platform, HDF enables Metron to ingest and process diverse streaming data feeds at scale, including security data feeds, logs, network metadata, and more.

Zoomdata is a modern business intelligence platform for visualization that allows regular business users to visually interact with and analyze high-volume, fast-moving, mission-critical data. It offers:

- **Modern, responsive Web front end** — Zoomdata provides a single, unified Web user interface that is compatible with modern browsers. While data rolls in, users can filter, sort, drill down, reformat, and create or change chart types. This “non-blocking” data exploration experience allows users to engage in speed-of-thought analysis against massive live data sources.
- **Intelligent BI engine** — Zoomdata’s scalable in-memory business intelligence (BI) engine applies built-in multisource analytics to correlate data from hot, warm, and cold storage on the same dashboard and even in the same frame. Zoomdata’s patented Data Sharpening™ streams predictive results, so analysts can interact with data immediately — even while long-running queries take shape.
- **Enterprise-ready architecture** — The Zoomdata platform is architected as a set of loosely coupled microservices. This enables faster integration of new functionality, optimal resource management, faster recovery in some failure scenarios, and greater deployment flexibility. Zoomdata offers robust application security and can delegate data authorization privileges to Apache Ranger for centralized control, ease of administration, and greater peace of mind.

Elysium Analytics, the security analytics solution from System Soft Technologies, uses open source machine learning technologies to solve real-world security issues that other SIEM and security analytics solutions struggle to solve. Elysium offers intuitive analytics for cloud security, compliance reporting, endpoint protection, user and entity baselining to identify anomalous behavior, and vulnerability detection on enterprise assets. Features include:

- **User and entity behavior analytics (UEBA)** — Rather than relying on rules like legacy SIEM systems, Elysium UEBA applies powerful, sophisticated machine learning algorithms to yield actionable insights into user and entity activities within the network. This reduces false positives and gives analysts actionable information.
- **Threat hunting** — Interactive security notebooks (based on open source solutions such as Zeppelin and Jupyter) provide insight and action on anomalies within your environment. Each notebook is purpose built with a self-contained workflow for a specific use case. These are powered by Zoomdata visualization tool for faster data exploration.
- **Insider threat detection** — Some users are being compromised without their knowledge, while others might be acting deliberately. Elysium keeps a baseline for every user in the organization and calculates the deviation from the baseline to each user's own history and to the rest of the community.
- **Compliance reporting** — A pre-tuned set of reports and rules enable quick rollout and provide fast access to non-compliant systems through interactive notebooks (playbooks) with adaptive workflow.
- **Cloud access security broker (CASB)** — User-created shadow IT solutions are exploited by attackers. Elysium monitors cloud resources to detect shadow IT, penetration, and suspicious activity.

PSSC Labs provides a tightly integrated, turnkey appliance platform that is configured to support 150TB of data, 240 processor cores, and a high speed network topology. This enables you to gain further insight into the real-time cybersecurity threat landscape across your network. Some of the benefits include:

- **Turnkey appliance-level solution** — All necessary components are integrated including compute, storage, networking, and software. This enables simple deployment and fast time to production.
- **Highest performance enterprise platform** — This proven enterprise-ready platform builds on high performance hardware with complete redundancy for optimal reliability.
- **Full support package** — The complete platform includes a one year service level agreement for all system hardware and integrated software components.

CYBERSECURITY TURNKEY SOLUTION BENEFITS EVERYONE IN YOUR SECURITY ORGANIZATION

For CISO and security executives

Cybersecurity Turnkey Solution helps senior executives assure the security the business needs efficiently and economically.

- CTS consolidates multiple SIEM products to one platform that serves many enterprise needs: compliance, UEBA, network traffic monitoring, machine learning, end point protection, vulnerability management, and log management and search.
- It reduces false positives by 70-80%, allowing analysts to focus on real issues.
- It reduces the mean time to repair (MTTR) by up to 75% to reduce risks.
- CTS enables a virtual SOC that addresses most tier-1 tasks through automation, increasing productivity.
- It provides 360 degree user and entity views to detect anomalous behavior in near real time.
- It enables 100% agility by leveraging open source software and providing the ability to capture all data sources at scale.
- CTS delivers proven value—10 times the value of existing solutions with only 20% of the implementation and support costs. Average implementation and time-to-value is less than 6 weeks.

For the security operations center

The solution goes far beyond dashboards by giving SOC analysts a holistic view of distributed cybersecurity threats. When they don't know what they don't know, analysts can ask new questions in new ways to identify and neutralize threats quickly.

- CTS fosters independent analysis and insights. All data can be visualized and interrogated through live network maps, geographic maps, heat maps, and other charts and tables. Advanced filtering, automatic time bucketing, and custom fields and calculations allow analysts to work independently of IT to contain and resolve threats. Analysts can explore and isolate suspicious activity in real time on one dashboard frame and replay the historical record on another for broader, deeper understanding.

  It's optimized for big data. Traditional BI tools can't handle massive or fast-moving data. Zoomdata provides the following unique features that make it easier to analyze data when the pressure is on:

  - Push-down processing optimizes query response times.
  - Data Sharpening™ streams predictive results.
  - Data DVR allows analysts to see how threats change and migrate over time.

  - Timebar slider simplifies time-based analysis.
  - Live Mode delivers near-real-time data.
  - Search box and facets support let you get the most out of hot-storage search engine data.

- It saves time during crises. During a cyberattack, time is the enemy. Powered by Zoomdata, CTS can stream updates as frequently as once a second. Analysts never have to force expensive full-query refreshes, so network and computing resources are conserved for high-value analytic processing and exploration.
- It enables SIEM augmentation or migration. The solution can replace or complement a SIEM. Apache Metron offloads data from a SIEM to increase retention and provide faster search or analytics. Moreover, Metron can preprocess or filter high-throughput logs that are not feasible in the SIEM including PCAP, firewall, DNS, windows events, and audit logs.
- CTS can provide real time automated responses. Pairing real-time data ingest with automated response orchestration enables organizations to minimize exposure and improve SOC efficiency.
- It uses user and entity behavior analytics (UEBA) to detect anomalous behavior. The solution captures baseline behavior using efficient algorithms. Profile retrieval supports time aggregations as well as seasonal trends.

For security data scientists

With Cloudera Cybersecurity Platform at the core, the solution ingests, normalizes, enriches, triages, and manages applications and security data at scale and in real time. That provides the following benefits to data scientists:

- It eliminates data silos. A pre-built state-of-the-art security data lake, the solution provides a single repository for all the enterprise's security telemetry data. This helps security data scientists find the data required to train and evaluate models.
- It prioritizes on high-value creation. The solution offers pre-prepared data and a number of algorithms ready to implement streaming use cases, such as the Apache Metron profiler feature. This liberates data scientists from the heavy lifting of data gathering and cleaning, so they can focus on differentiated data modeling or data science initiatives.
- It's flexible and extensible. The solution is ideal for organizations that want to go beyond out-of-the-box solutions and incorporate custom dashboards, notebooks, triaging, and data storage to optimize their SOC processes. For example, it offers the extensibility for data scientists to bring their own models (model-as-a-service) and a notebook environment.

For IT infrastructure teams

CTS is enterprise ready. Turnkey deployment enables fast time to production, and it's easily scalable as needs grow. Benefits for IT administration include:

- It's enterprise grade. Only the highest quality, enterprise components are included in the solution. It offers redundant power at both the rack and server level. Each server includes redundant operating system hard drives for an extra layer of protection. The out-of-band management network is preconfigured for easy monitoring and maintenance.
- It offers turnkey deployment. All necessary hardware, software, and network components are preconfigured, allowing for easy deployment and faster time to production.
- It scales easily. The high-density server platform lets you scale from 150 TB to multiple petabytes without significant additional infrastructure costs.