CDAP for Cybersecurity

Cloudwick Data Analytics Platform for Cybersecurity

Cloudwick Data Analytics Platform (CDAP) is a managed cybersecurity data lake platform that ingests and stores trillions of events from PCAP, Netflow, Proxy, IDS/IPS logs, syslog and firewall logs for advanced cybersecurity. CDAP is the first big data cybersecurity platform to provide complete threat visibility, replay and analysis for the Security Operations Center (SOC) analyst, forensic analyst and data scientist. CDAP is offered as both a data center and cloud cybersecurity solution.

Built on Cloudera's industry leading distribution, CDAP provides a turnkey cybersecurity data lake platform that provides new cybersecurity capabilities from leading advanced analytic vendors like Cybraics, H2O and Dataiku, open source machine learning projects like Apache Spot, and enhances and extends the capabilities of SIEMs, IDS, IPS, Snort and other traditional tools.

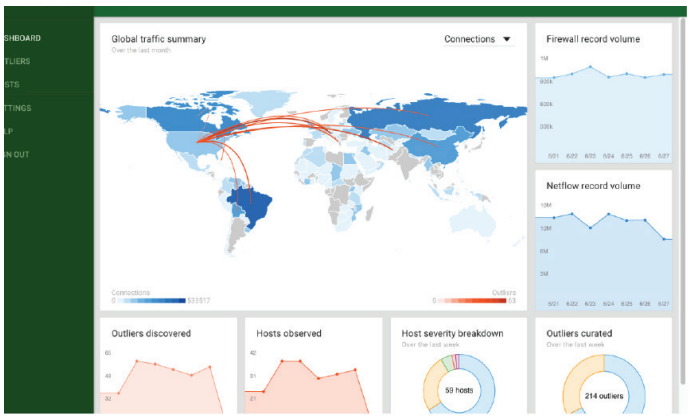
CDAP COMPONENTS

- **CDAP Data Agent (CDA)** collects logs, alerts and events from SIEMs, PCAP, Netflow, firewalls, IDS, IPS, Active Directory and other data sources at wirespeed.
- **CDAP Data Ingestion & CDAP Data Catalog (CDI/CDC)**, which ingests and catalogs packets, alerts, logs and netflows, making it extensible for data scientists and SOC analysts.
- **CDAP Data Hub (CDH)** is the secure data lake that processes and stores petabytes of data for SOC analysts and data scientists to perform advanced analytics.
- **CDAP SOC Connector (CSC)** provides a connector layer for integrating traditional tools like Wireshark, Snort, IDS, IPS and SIEMs with CDAP for data replay, faster correlation and complete threat visibility and analytics.
- **CDAP Data Science (CDS)** provides the data scientist and advanced analytic vendors with secure and auditable access to CDAP for running machine learning and advanced analytics.

Cybraics powered by CDAP

Traditional security tools only detect what they know, making it impossible for them to discover sophisticated and targeted attacks. On the other hand, manually identifying these attacks in the billions of log files generated each day is an impossible task, even for a team of the best cyber hunters. Cybraics both finds the unknown threats that others miss, and reduces the workload of your cyber team. Fueled by over 10 years of research from government and commercial partners, Cybraics algorithms can analyze virtually any data, combining multiple techniques across network, user and entity behavioral analytics with a proprietary active learning system that categorizes and prioritizes anomalies. This combination provides the greatest coverage of the threat landscape possible, while reducing the false positive rate to nearly zero.

Cybraics identifies behaviors, generates a complete evidence bundle, and presents the SOC analyst with full situational awareness of the threat landscape inside the network. Every threat passed through to the analyst includes a comprehensive evidence bundle with all of the information necessary to take immediate action, so adversaries are recognized immediately and action can be taken quickly.



CDAP

- Democratizes enterprise and service provider cybersecurity data by collecting and storing all cybersecurity data for the enterprise SOC and data scientist, providing complete visibility.
- Capable of ingesting more than 100 million events per second from PCAP, Netflow, IDS, IPS, syslogs, firewalls and log files - all at wirespeed.
- Fully managed big data advanced analytics platform for cybersecurity - in the data center or cloud.
- Simplifies and enhances traditional IDS, IPS, SIEM, Wireshark and traditional cybersecurity tools while providing next-generation machine learning and advanced analytics for the SOC and data scientist.

Cybraics

- Full threat coverage – Our unique analytic pluralist approach and multi-modal learning techniques provide the broadest coverage of the threat landscape, from unknown and insider threats to vulnerabilities.
- Near-zero false positives – By layering a combination of an active learning system and human curation on top of the analytics, we are able to triage every alert, reducing the false positive rate to almost zero, ensuring every result you receive is important.
- Analytics-as-a-Service - our AaaS provides an uncompromising end-to-end advanced analytics cybersecurity solution that scales to support any data type and/or volume.
- Deployed in the cloud or on-premise, our service for actionable intelligence is the most powerful way to detect and respond to threats and secure your assets.

Cloudwick

cloudera

CYBRAICS