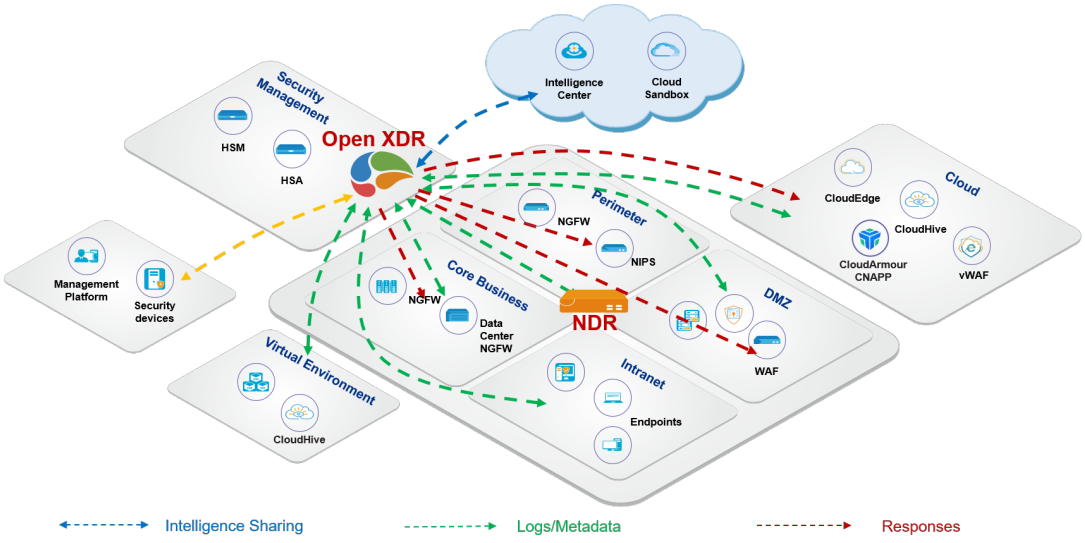
Hillstone Open XDR (Extended Detection and Response) Solution

Hillstone Open XDR (iSource) is a data-driven, AI-powered, extended detection and response (XDR) platform built for openness and interoperability. It unifies massive security data, investigates correlations of incidents, identifies potential threats, and automates security orchestration across diverse security products and ecosystems. With both northbound and southbound integration, it seamlessly connects with external security devices and threat intellgence feeds, enabling cohesive collaboration and response across the security stack. Hillstone Open XDR brings a radical new approach to cybersecurity with complete visibility, highly accurate threats identification and swift containment and mitigation for unrivaled security operation efficiency.



Product Highlights

Unified Data Collection from Multiple security Products with Full Visibility

Hillstone iSource features an open architecture that collects various types of data, such as threat logs, traffic data, and incident reports, from almost any source across Hillstone's product stack and as well as 3rd party products. By standardizing and integrating heterogeneous data across components, including cloud, network and endpoints, iSource breaks down security information silos. It not only brings full security visibility with far fewer blind spots, but also improves detection accuracy and provides effective andefficient defense against threats.

Advanced ML-driven Analytics and Detection

By synergizing the data and logs collected across the entire security fabric, as well as threat intelligence from top threat intelligence sources, Hillstone iSource can discover even stealthy and evasive threats, and attribute

the attacks. Powered by machine learning technology and statistical algorithms, its behavior analytics engine helps distinguish anomalous activities among a large amount of integrated data. Its correlation analysis engine consolidates individual incidents for context awareness, and applies analysis to correlated data to identify high-fidelity incidents. By continuously analyzing the intricate relationships between incidents and alerts, it merges relevant incidents and generates a detailed incident graph that traces the attack's origin, progression, and scope. This empowers security operation teams with in-depth insights, reducing investigation time and enabling swift assessments of an incident's full impact. Its powerful log analysis has built in threshold- and status-based detection and correlation analysis capability that allows security analysts to define customizable rules to identify key threats via artifacts. The Search Processing Language (SPL)-based log search engine also alleviates the pain of searching and analyzing massive logs.

Comprehensive Vulnerability and Risk Management

Hillstone vulnerability management helps identify and present vulnerabilities by leveraging the industry's leading vulnerability assessment solution. It also supports adding new scanners for customization or even manually importing a vulnerability report file for further containment of threats. Assets are the core for risk management. Hillstone iSource provides comprehensive risk management to assets like servers, endpoints, or even applications and services, from multiple dimensions including risks, vulnerabilities and threat events. It presents statistical data, such as distribution and trends of threats and vulnerabilities, along with detailed information of individual assets. This holistic approach protects assets by identifying and mitigating potential exposures to threats.

Automated Security Orchestration and Cohesive Response

Hillstone iSource offers automated security orchestration and response capability with built-in playbooks, integrated interactions with Hillstone security products and the ability to assign tasks for collaborative ticket management. Besides predefined playbooks that offer optimized workflows and responses, Hillstone iSource also offers the agility and flexibility to define automated workflows visually in playbooks based upon ingested incidents or alerts, intelligence queries and actions of response. These playbook-driven responses combine automated tasks that can span multiple Hillstone devices, such as Hillstone NGFW, NIPS, CloudEdge, CloudHive, etc., with manual tasks handled respectively through incident ticket management. Certain 3rd-party devices can also be supported in playbooks via RESTful APIs or SSH connection. This enables swift incident triage and attack containment before damage can be done.

Unified Management and Reporting with Intuitive and Customizable Console

The customizable dashboard allows simple and rapid access to the organization's security posture with comprehensive statistical information such as rankings and counters, as well as incident summarization and security trends with graphical charts and lists. The intuitive design provides an optimized user experience for management and operations. Hillstone iSource also supports template-based or customizable reports that can be generated on schedule or on demand. Public APIs enable integration with third-party tools or security products to inject security data generated across the entire security fabric and perform interactions to contain threats.

Features

Data Collection

- Support Support collecting data via TCP, UDP, Kafka , JDBC, and Beats protocols
- Support collecting data in formats including Syslog, NetFlow, Metadata, Sysmon, and Linux Syslog
- Support parsing data using built-in templates for AVRO, Grok, Key-Value, JSON, and JsonPath
- Support online or offline updates to data parsing templates
- Support custom data type configurations
- Support configuring data filtering and aggregation rules
- Support forwarding Syslog logs and threat event logs to third-party platforms
- Support encrypted log access and forwarding protocols
- Support configuring data forwarding types and intervals
- Support threat log reporting via plugin integration
- Support log backup
- Support log backup to third-party servers via FTP

Full Visibility

- Support threat hunting
- Support threat events monitoring, and visualization of risky assets and risk trends
- Support distributed display of threat geographic connections
- Support threat landscape monitoring dashboard
- Single sign-on (SSO) support for security monitoring dashboards
- Support custom monitoring dashboard
- Support full-screen display of stats and information on overall security, servers' security, endpoints security, vulnerabilities, areas security, threat events, and hierarchical management
- Support establishing the insight topology of network flow by collecting and analyzing the traffic
- Key threat events overview
- Support listing threat events of individual BDS

Detection Rules

- Support rule configuration of threat detection for scanning, file, HTTP detection, suspicious protocol, brute force, DNS, ransomware, mining, USB behavior, violating access, weak password, and user-defined threats

Threat Analysis

- Rule-based threat detection
- Threat log analysis
- Behavior analysis
- Correlation Analysis
- Statistics and analysis of risky servers, risky endpoints, and threat events
- Support the evidencecollection, processing and status marking of threat events
- Threat evidence information supports multiple decoding types, such as URL, Base64, Unicode, UTF-8, HEX, etc.
- Support MITRE ATT&CK® Matrix mapping
- Support threat aggregation and reconstruction of the attack chain

Assets Management

- Support management of serverassets, endpoint assets and unclassified assets
- Support collection and management of CloudArmour assets
- Support IoT asset discovery
- Support assets overview
- Support favorite assets management
- Support asset classification
- Support asset fingerprint extraction
- Support custom asset label
- Support grouping management of servers, endpoints and various server services
- Support automatic discovery of assets, including active scanning and manual importing of assets
- Support asset inventory management
- Support asset source priority configuration
- Support display of users' status
- Support centralized management of assets to be imported and assets to be updated
- Support extracting asset fingerprints from vulnerability reports
- Support asset segmentation

Risk Management:

- Unified management of risk assets/service
- Analysis of asset compromise states
- Asset risk reports

Vulnerability Management

- Support statistical and detailed information of vulnerabilities
- Support import of third-party vulnerability reports
- Support vulnerability scanning with built-in and third-party scanners
- Support management of scanning tasks

Information Management

- CVE hotspot threat information notification
- Support intelligence database of DNS domains, malicious codes, IP, vulnerabilities, intrusion detections, geo-location, URL and MITRE ATT&CK® knowledge base
- Support intrusion detection and web attack detection signature database
- Support abnormal behavior and malware behavior model database, and honeypot knowledge base
- Comprehensive intelligence with other relevant threats
- Support manual and periodic offline/online intelligence database upgrades
- Support whitelist of global, DNS, and file
- Support blacklist of DNS, malicious code, and IP

Correlation Analysis

- Support correlation analysis of massive data and detection of kill chain
- Support centralized and classified search of global threat events
- Support searching by keywords, SPL, and pre-defined conditions
- Support online/offline updates of the Syslog parsing rule and threat correlation analysis rule database

Case-Based Investigation

- Support case analysis for entities including assets, IPs, domains and identities
- Support multi-source event case rules
- Support visualizing causal relationships between entities in the case topology
- Support case topology pruning and event timeline trimming
- Support displaying the attack timeline within the attack gragh
- Support playing the attack graph in chronological order
- Support automatic and manual creation of cases
- Support merging related cases and alerts

Incident Response

- Support ticket management system
- Support ticket workflow with different privileges for roles
- Support integration with Hillstone NGFW, CloudEdge, CloudHive, and NIPS for policy deployment and IP blocking
- Support integration with Hillstone CloudArmour for host isolation, process termination, and file removal
- Support integration with NSFOCUS Anti-DDoS system for IP blacklisting
- Support integration with VirusTotal for IP/domain/file intelligence validation
- Support integration with third-party security devices from vendors such as Huawei, Fortinet, etc.
- Support third-party device integration over RESTful APIs, SSH or custom plugins
- Playbook-based auto or semi-auto(with double confirmation) orchestration and response, with support of pre-defined playbooks and validity period setting
- Support email notification to administrators for secondary confirmation of firewall policy deployment
- Support policy aggregation
- Support marking event status within the playbook
- Support manually reissuing unsuccessful playbook-driven automated response
- Support agile threat management for weak password, ransomware, mining attacks, favorite assets and threats

Alerts

- Support custom alert rules
- Support alert notification of SMS, email and WebUI
- Support integration with WeCom, DingTalk, and Feishu bots for sending alerts

Reporting

- Support four report templates including overall security risk, endpoints security risk, server security risk, and incident response report
- Support optional function of report task
- Support periodic or on-demand report
- Support online preview
- Support export reports in PDF/WORD format
- Support custom logo
- Support email notification of report generation
- Support management of classified protection

System Configuration

- Support management of user authority, Syslog,

Features

Netflow, logs storage, evidence information, network configuration, mail configuration, and license configuration
- Support assigning user roles with access privileges (administrator, operator and auditor) for different features and data
- Support trusted host configuration
- Support two-factor authentication with email and SMS verification
- Supports authentication for administrators via local servers, RADIUS, and TACACS+
- Support integration with Hillstone WAF, ADC and HSM
- Record of system logs
- Sync up with BDS rules
- Support HA and clustering up to 5 nodes
- Support hierarchical management
- Support system logo and title customization

Supported Platforms
- Linux: CentOS 7
- Windows: Microsoft Windows 10
- VMware: VMware EXSi 6.7

Specifications

Models		SG-6000-ISC6305	SG-6000-ISC6310	SG-6000-ISC6320
Performance	Throughput	3Gbps	6Gbps	15Gbps
	Event Processing	5000EPS	8000EPS	15000EPS

Version: EX-08.01-iSource-2.0R14-0925-EN-01