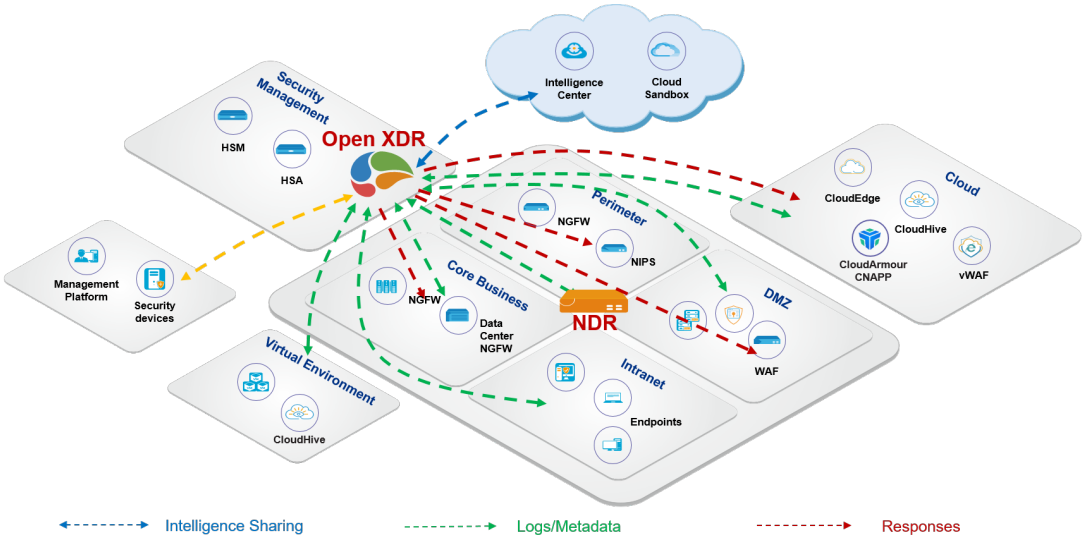
Hillstone Open XDR (Extended Detection and Response) Solution

Hillstone Open XDR (iSource) is a AI-powered, open extended detection and response (XDR) platform designed for modern security operations. It unifies threat logs, network traffic, and endpoint telemetry from across the security infrastructure, delivers intelligent threat detection and investigation through advanced ML-driven analytics and correlation, and automates response across heterogeneous security ecosystems. Hillstone Open XDR introduces a unified operational workflow spanning asset risk management, multi-source data ingestion, threat detection and analysis, case-based investigation, and coordinated response — giving security teams complete visibility, accurate threat identification, and swift containment and mitigation.



Product Highlights

Unified Data Collection from Multiple security Products with Full Visibility

Hillstone iSource Open XDR consolidates threat logs, network traffic, and endpoint telemetry from virtually any source — across Hillstone and third-party security products — through an open data ingestion architecture supporting a broad range of protocols and data formats. Built-in and customizable parsing templates enable rapid onboarding of new data sources, while a real-time management console provides continuous visibility into device connectivity and ingestion health. It not only brings full security visibility with far fewer blind spots, but also improves detection accuracy and provides effective and efficient defense against threats.

Advanced ML-driven Analytics and Detection

By synergizing the data and logs collected across the entire security infrastructure, as well as threat intelligence from top threat intelligence sources, Hillstone Open XDR can discover even stealthy and evasive threats, and attribute the attacks.

Hillstone Open XDR applies behavior analytics and ML-driven analysis to distinguish genuine threats from noise and correlates individual alerts into high-fidelity, prioritized security cases. Continuously analyzing the intricate relationships between incidents and alerts, it merges relevant events and generates a detailed Attack Story that traces the attack's origin, progression, and scope — mapped against the MITRE ATT&CK framework. This empowers security teams with in-depth insights, reducing investigation time and enabling swift, confident assessments of an incident's full impact.

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 Open XDR 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 Open XDR offers automated security orchestration and response capability with built-in playbooks, integrated interactions with Hillstone and 3rd-party security products and the ability to assign tasks for collaborative ticket management. Besides predefined playbooks that offer optimized workflows and responses, Hillstone Open XDR 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 devices, such as Hillstone NGFW, NIPS, CloudEdge, CloudArmour, etc., with manual tasks handled respectively through ticket management. 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

Hillstone Open XDR's role-based access control and asset domain segmentation enable data isolation, delegated administration, and tiered ticketing workflows across teams and branches — all within a single platform. Configurable dashboards give every stakeholder the right view of security posture, and template-based or on-demand reporting makes audit and compliance preparation straightforward. Open APIs extend the platform into existing SIEM and management system investments, maximizing the value of what organizations have already built.

Features

Data Collection

- Support data ingestion via TCP, UDP, Kafka , JDBC, and Beats protocols
- Support Syslog, NetFlow, Metadata, Sysmon, and Linux Syslog formats
- Support parsing data using built-in templates for AVRO, Grok, Key-Value, JSON, and JsonPath
- Support online/offline updates to data parsing templates
- Support real-time monitoring of data source connectivity and ingestion rate
- Support custom data type configurations
- Support configuring data filtering and aggregation rules
- Support Syslog and threat event log forwarding to third-party platforms
- Support encrypted log access and forwarding protocols
- Support configurable data forwarding types and intervals
- Support plugin-based threat log reporting
- 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 geographic threat distribution visualization
- 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

Detection Rules

- Scanning, file, HTTP, suspicious protocol, b rute force, DNS
- Ransomware and cryptomining detection
- USB behavior, unauthorized access, weak password
- User-defined threat detection rules

Threat Analysis

- Rule-based threat detection
- Threat log analysis
- Behavior analysis
- Correlation Analysis
- Statistics and analysis of risky servers, risky endpoints, and threat events
- Business Baseline Learning for false positive suppression
- Attacker and victim perspective aggregation analysis
- X-Forwarded-For chain analysis for true attacker IP tracing
- Threat process details
- Support PCAP download
- Support raw threat log search
- Threat evidence collection with multi-format decoding (URL, Base64, Unicode, UTF-8, HEX)
- Support MITRE ATT&CK® Matrix mapping
- Support threat aggregation and reconstruction of the attack chain

Assets Management

- Support active scanning and passive discovery of assets
- Support manual asset import
- Support IoT asset discovery
- Support assets overview
- Support favorite assets management
- Support asset classification
- Support asset fingerprint extraction
- Support asset onboarding, update, and retirement workflow management
- Support asset change tracking
- Support custom asset groups and labels
- Support grouping management of servers, endpoints and various server services
- Support asset inventory management
- Support asset source priority configuration
- 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 host vulnerability analysis
- Support host weak credential analysis
- Support Windows missing patch analysis
- Support built-in weakness scanner
- Support import of third-party vulnerability reports
- Support third-party scanner integration
- Support vulnerability scanning with built-in and third-party scanners
- Support periodic scanning task configuration
- Support management of scanning tasks
- Support third-party vulnerability report import and analysis

Information Management

- CVE hotspot threat intelligence 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 multi-source alert auto-correlation into unified security cases
- Support case priority scoring
- Support case summary with ATT&CK tactic chain overview
- Support attack impact scope analysis
- Support case analysis for entities including assets, IPs, domains and identities
- Support case topology: causal relationship visualization (public/internal network perspectives)
- Support multi-source event case rules
- Support case topology pruning and event timeline trimming
- Support attack topology playback in chronological order
- Support automatic and manual creation of cases
- Support merging related cases
- Support cross-component advanced forensic search
- Support case lifecycle management
- Support audit trail of case lifecycle: automated and manual actions recorded chronologically within each case

Incident Response

- Support playbook management
- Support ticket management system with role-based workflow
- Support integration with Hillstone NGFW, CloudEdge, CloudHive, and NIPS for policy deployment and IP blocking
- Support audit log export for Hillstone NGFW policy deployment and IP blocking actions
- 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 workbenches for weak password, ransomware, mining attacks, favorite assets and threats
- Support pending playbook and ticket reminders

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/

Features

endpoint/server security risk, and incident response report
- Support periodic/on-demand report generation
- Support online preview
- Support export reports in PDF/WORD format
- Support custom logo
- Support email notification of report generation

System Configuration

- Support management of user authority, Syslog, 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+
- 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-2.0R15-046-EN-01