ASSERTION®
Collaborate Confidently

ASSERTION® SecureVoice™ Data Governance Policies

Document Version: 1.1
Date: 11-Feb-2023
Document ID: PS00P032

Document Revision History

Version	Change Description	Date
1.0	First Public Release	27-Dec-22
1.1	Added generic CDR parameters	11-Feb-23

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Assertion Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

Assertion Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Assertion Inc. Customer and/or End User agree to indemnify and hold harmless Assertion Inc, Assertion Inc' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Assertion Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Assertion Inc does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Assertion Inc support

Assertion Inc (operating as ASSERTION™) provides a channel for you to use to report problems or to ask questions about your product. For support information, see the ASSERTION™ Web site: https://assertion.cloud/support

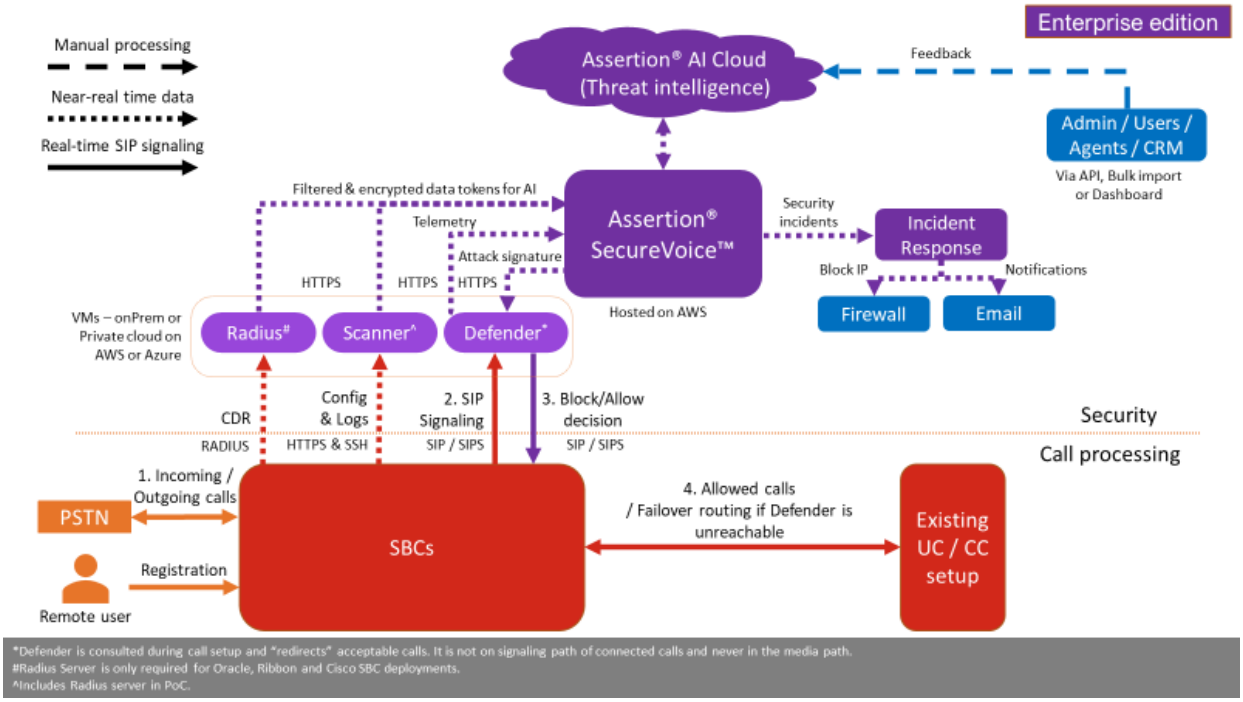
ASSERTION® is a registered trademark of Assertion Inc.

Contents

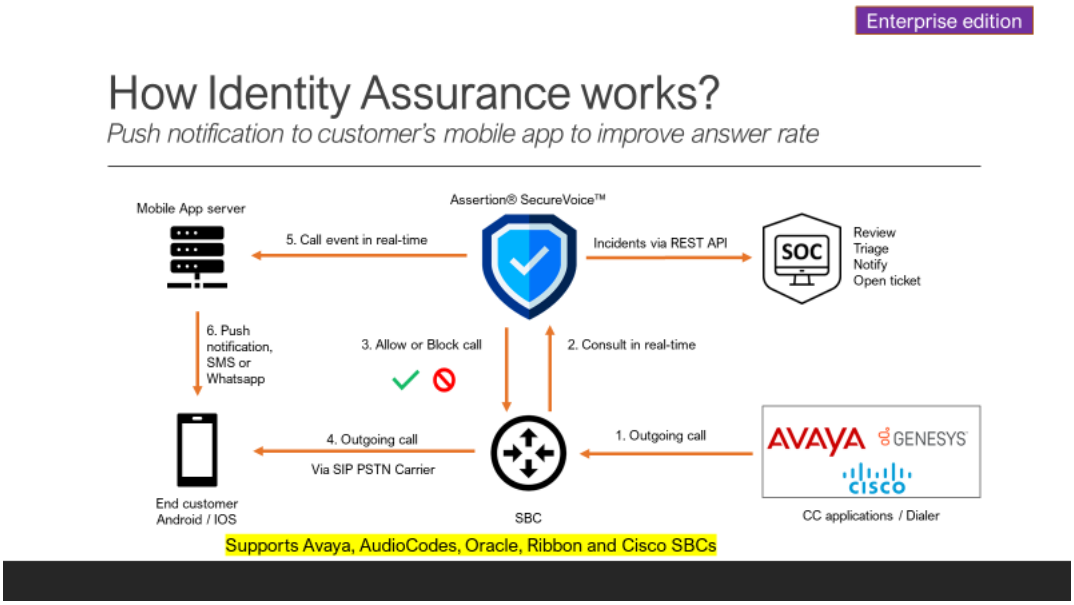
Solution Overview: How SecureVoice™ Works

SecureVoice™ has two key components:

- A Defender collects only SIP Signaling data: It studies every SIP message in real time and analyzes it individually as well as in relation with previous SIP traffic to make Block/Allow decisions. The Defender is only concerned with SIP signaling and is never in the media path once the call is established.
- A Scanner that collects configuration and SIP trace log data, or syslog, or CDR from the SBC to understand how the SBC appears to a public or private network attacker.



The system is also capable of sending notifications to registered clients when an outbound call from an enterprise is made. This is called as Identity Assurance. The following diagram explains how it works.



Data Privacy and Security

Assertion does not collect or store credentials to access your SBC (or any other network device) on its cloud. We do not share the customer data with any third party except with you (the Partner who has rights to the Customer data).

Data collected is encrypted at the Scanner before it is uploaded to Assertion cloud. Uploaded data is always kept encrypted at the cloud end except when required for analysis.

Any anonymized data fragments that are used for ML purposes will not have any reference to the customer and cannot be used to reverse engineer or identify the customer/SBC/the network or the users involved.

Encryption and Security

The service uses TLS 1.2 with ECDSA 256 (RSA 3072 equivalent) encryption for the highest security of data during transit. Data at rest is encrypted using AES-128 encryption. All connections between components are via secure channels – SSH, HTTPS and SIPS.

Access Restrictions and Audit Trail

Data stored on Assertion cloud is encrypted and under access control. Only authorized service staff can access the detailed reports, evidence trail and raw data. All accesses made by our services and support staff to read sensitive data will be logged in the Audit trail system.

Data Localization

Data will be stored in cloud servers, currently in the AWS US East Virginia data center, which is our default location.

Data Storage

Assertion follows a data-walled garden approach where each customer's data is stored in a separate area on the Cloud. This ensures that there is no chance of data from two or more customers being mixed up or incorrectly accessed, thereby ensuring utmost confidentiality and privacy.

On explicit request from you for data deletion, all the collected data and reports will be deleted forever from the cloud servers for a particular SBC.

Data Categorization and Retention

The data used for threat analysis and prevention is categorized as below:

- **Raw Data:** Data sent to the defender for analysis
- **Processed/ Intermediate Data (tokenized):** This data is required for analyzing calling patterns, detecting toll fraud attacks, and detecting rogue traffic that may cause service disruption attacks. Encrypted and stored in a separate bin for each customer.
  The data collected as tokens (or parts of) logs, SIP signaling, and CDR may include
  - IP address of SBC, network components and endpoints
  - Phone numbers
  - Date and Time when phone calls are made
  - Endpoint type used to make calls
  - Transport type used to establish the session
  - Audio/video encryption indicators (only for remote worker protection)

  The above data is required for analyzing calling patterns, detecting toll fraud attacks, and detecting rogue traffic that may cause service disruption attacks.
- **Findings & Report Data:** Encrypted and stored in a separate bin for each customer.

Retention Period

- Raw Data: 1 day.
- Processed Data: 30 days
- Findings: 1 year
  (Reports, generated from Findings, are available for a period of 1 year)

What data is collected and why

If you own an Avaya SBC

Use case: Call screening, Active defense

Data collected from SIP signaling, SIP trace logs

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
IP address	SIP trace logs	IP address where the SIP message is sent or received from	Required to label the attacker and for collective learning	Yes	Yes	Yes
Calling party(inbound calls)	SIP Signaling, SIP trace logs	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling, SIP trace logs	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling, SIP trace logs	The From header of the SIP message. It includes the display name and number of	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes

		the calling party				
Called party (outbound calls)	SIP Signaling, SIP trace logs	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilizatio n attack, E911 abuse etc.	Yes	Yes	Yes
Contact information	SIP trace logs	The contact header of the SIP message. It includes the IP address and port where the calling party can be reached.	Required to track organized criminals and inside attacker	Yes	Yes	No
Call ID	SIP signaling, SIP trace logs	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required to correlate the request and responses	Yes	Yes	No
Endpoint type	SIP trace logs	The user-agent header of the SIP message. It includes the endpoint type used by the users	Required to determine unauthorize d endpoint types and categorize known cyber criminals	Yes	Yes	Yes

Config Data Collected

Retention period: 1 day

Data field collected	Description	Reason for Collection
Access configuration	This includes the user created on SBC, login restrictions, password policies, radius and ldap list	Required to check configuration against NIST cyber security framework
Backup configuration	This includes the backup and backup schedule settings	Required to check configuration against OEM security guidelines
DoS/DDoS setting	This includes Single source DDoS, Stealth DDoS, Call walking, DoS whitelisting, scrubber list and rules, domain DoS	Required to check configuration against NIST cyber security framework
TLS setting	TLS server profile list, TLS client profile list, certificate metadata	Required to check configuration against OEM security guidelines and best practices
Remote worker	Subscriber flow, endpoint flow, application rule list, border rule list, Media rule list, Security rule list, Endpoint policy group list, routing policy list, signaling interface, interworking list	Required to check configuration against OEM security guidelines and best practices
Trunk gateway	Server flow, endpoint flow, application rule list, border rule list, Media rule list, Security rule list, Endpoint policy group list, routing policy list, signaling interface	Required to check configuration against OEM security guidelines and best practices
Reverse proxy	Reverse proxy list, replay service list, PPM mapping profile list	Required to check configuration against NIST cyber security framework
Monitoring and advanced features	SNMP user list, SNMP trap severity list, Advance rule list, E911 options, Advanced features options	Required to check configuration against NIST cyber security framework

Use case: Remote worker add-on

Data collected from SIP signaling, SIP trace logs

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
IP address	SIP trace log	IP address where the SIP message is sent or received from	Required to label the attacker and for collective learning	Yes	Yes	Yes
Calling party(inbound calls)	SIP trace log	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP trace log	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP trace log	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (outbound calls)	SIP trace log	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Contact information	SIP trace log	The contact header of the SIP message. It includes the IP address and port where the calling party can be reached.	Required to track organized criminals and inside attacker	Yes	Yes	No
Media parameters	SIP trace log	The media lines from the SIP message. It	Required to determine potential man in	Yes	Yes	No

		includes the IP and port to send and receive media and the codecs to be used for this call	middle attacks via unsecured media			
Call ID	SIP trace log	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required correlate the request and responses	Yes	Yes	Yes
Endpoint type	SIP trace log	The user-agent header of the SIP message. It includes the endpoint type used by the users	Required to determine unauthorized endpoint types and categorize known cyber criminals	Yes	Yes	Yes

If you own an AudioCodes SBC

Use case: Call screening, Active defense

Data collected from SIP signaling, SIP trace logs, and CDR

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
IP address	SIP trace logs	IP address where the SIP message is sent or received from	Required to label the attacker and for collective learning	Yes	Yes	Yes
Calling party(inbound calls)	SIP Signaling, CDR	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling, CDR	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling, CDR	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes

Called party (outbound calls)	SIP Signaling, CDR	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Contact information	SIP trace logs	The contact header of the SIP message. It includes the IP address and port where the calling party can be reached.	Required to track organized criminals and inside attacker	Yes	Yes	No
Call ID	SIP signaling, SIP trace logs	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required to correlate the request and responses	Yes	Yes	No
Endpoint type	SIP trace logs	The user-agent header of the SIP message. It includes the endpoint type used by the users	Required to determine unauthorized endpoint types and categorize known cyber criminals	Yes	Yes	Yes

Config Data Collected

Retention period: 1 day

Data field collected	Description	Reason for Collection
Access configuration	This includes the user created on SBC, login restrictions, password policies, radius and ldap list	Required to check configuration against NIST cyber security framework
CLI settings	This includes the ssh, login restrictions settings	Required to check configuration against OEM security guidelines
Media Security setting	This includes media authentication and encryption protocols	Required to check configuration against OEM security guidelines
Message manipulation setting	TLS server profile list, TLS client profile list, certificate metadata	Required to check configuration against OEM security guidelines and best practices
Remote worker	Classification, message condition, IP Group config, CAC rule, proxy set	Required to check configuration against OEM security guidelines and best practices
Intrusion Detection	IDS settings	Required to check configuration against OEM security guidelines and best practices
Firewall	Firewall config	Required to check configuration against NIST cyber security framework
TLS settings	SBC's TLS setting	Required to check configuration against NIST cyber security framework

Use case: Remote worker add-on

Data collected from SIP signaling, SIP trace logs,

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
IP address	SIP trace log	IP address where the SIP message is sent or received from	Required to label the attacker and for collective learning	Yes	Yes	Yes
Calling party(inbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (outbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Contact information	SIP Signaling	The contact header of the SIP message. It includes the IP address and port where the calling party can be reached.	Required to track organized criminals and inside attacker	Yes	Yes	No
Media parameters	SIP Signaling	The media lines from the SIP message. It includes the IP and port to send	Required to determine potential man in middle attacks	Yes	Yes	No

		and receive media and the codecs to be used for this call	via unsecured media			
Call ID	SIP Signaling	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required correlate the request and responses	Yes	Yes	Yes
Endpoint type	SIP Signaling	The user-agent header of the SIP message. It includes the endpoint type used by the users	Required to determine unauthorized endpoint types and categorize known cyber criminals	Yes	Yes	Yes

If you own an Oracle SBC

Use case: Call screening, Active defense

Data collected from SIP signaling and CDR

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
Calling party(inbound calls)	SIP Signaling, CDR	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling, CDR	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling, CDR	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (outbound calls)	SIP Signaling, CDR	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Call ID	SIP Signaling, CDR	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required to correlate the request and responses	Yes	Yes	No
PAI	CDR	P-Asserted Identity that contains the caller id information for the call on the	Required to correlate spoofing activities	Yes	Yes	No

		INVITE SIP packet.				
Realms	CDR	Realms are used when an Oracle SBC communicates with multiple network elements over a shared intermediate connection.	Required to determine the external call leg. Used in determining call direction.	Yes	Yes	No
Accounting Session Time	CDR	Length of session (time in seconds, or milliseconds if so configured)	Required for anomaly detection	Yes	Yes	No
Call Start time	CDR	IP address of the SIP proxy or the H.323 stack'sIP address of the SIP proxy or the H.323 stack's call signal address	Required for anomaly detection	Yes	Yes	No
Accounting status	CDR	SIP proxy port or the H.323 stack's call signaling RAS port	Required for anomaly detection	Yes	Yes	No
NAS IP Address	CDR	IP address of the SIP proxy or the H.323 stack'sIP address of the SIP proxy or the H.323 stack's call signal address	Required for anomaly detection	Yes	Yes	No
NAS Port	CDR	SIP proxy port or the H.323 stack's call signaling RAS port	Required for anomaly detection	Yes	Yes	No
Accounting Session ID	CDR	Call-ID field value of the SIP INVITE message, the call Identifier of the H.323 message, or RADIUS	Required for anomaly detection	Yes	Yes	No

		client information				
Ingress Session ID	CDR	Call ID generated by the originating device	Required for anomaly detection	Yes	Yes	No
Egress Session ID	CDR	Call ID generated by the SBC to represent a two-way transaction	Required for anomaly detection	Yes	Yes	No
Accounting Termination Cause	CDR	Reason for session ending	Required for anomaly detection	Yes	Yes	No
Cisco Setup Time	CDR	The setup time	Required for anomaly detection	Yes	Yes	No
Cisco Connect Time	CDR	The connect time	Required for anomaly detection	Yes	Yes	No
Cisco Disconnect Time	CDR	The disconnect time	Required for anomaly detection	Yes	Yes	No
Cisco Disconnect Cause	CDR	The reason for session disconnection	Required for anomaly detection	Yes	Yes	No
Firmware Version	CDR	Firmware version on the SBC	Required for anomaly detection	Yes	Yes	No
Local time zone	CDR	Timezone of the SBC	Required for anomaly detection	Yes	Yes	No
Session Disposition	CDR	Status of the session attempt as it progresses from being initiated	Required for anomaly detection	Yes	Yes	No
Disconnect Initiator	CDR	Identifies how the initiator session is closed	Required for anomaly detection	Yes	Yes	No
Disconnect Cause	CDR	The reason for session disconnection	Required for anomaly detection	Yes	Yes	No
SIP Status Code	CDR	The status code for the session	Required for anomaly detection	Yes	Yes	No

CDR Sequence Number	CDR	The sequence number of this record relative to other records in the file	Required for anomaly detection	Yes	Yes	No

If you own a Ribbon SBC

Use case: Call screening, Active defense

Data collected from SIP signaling, SIP trace logs, and CDR

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data (Y/N)	Part of Processed Data (Y/N)	Part of Findings (Y/N)
Calling party(inbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (outbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Call ID	SIP Signaling,	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required to correlate the request and responses	Yes	Yes	No

Data collected from CDR

Raw data

This includes all the fields that are part of the CDR as mentioned by Ribbon here.
However, this data is purged in a day.

Processed data (purged in 30 days)

Of all the data fields collected from the CDR, only the below are part of processed data, and are therefore, purged in 30 days.

- CDR Field
- Record Type
- Accounting ID
- Start Time (system ticks)
- Start Time (MM/DD/YYYY)
- Start Time (HH/MM/SS
- Call Direction
- Calling Number
- Called Number
- Egress Local Signaling IP Address
- Egress Remote Signaling IP Address
- Call ID
- From Field
- To Field
- Display name of SIP URI PAI header
- User Parameter of P-K-CallForwardingLast Header
- Userinfo and Hostname of SIP Request URI Header
- Userinfo and Hostname of SIP URI PAI header
- Displayname of Tel URI PAI header
- Userinfo of Tel URI PAI header

If you own a Cisco CUBE

Use case: Call screening, Active defense

Data collected from SIP signaling, SIP trace logs, and CDR

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
Calling party(inbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (outbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Call ID	SIP Signaling,	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required to correlate the request and responses	Yes	Yes	No

Data Collected from CDR

Raw Data

This includes all the fields that are part of the CDR as mentioned by Cisco here.
However, this data is purged in a day.

Processed Data (purged in 30 days)

Of all the data fields collected from the CDR, only the below are part of processed data, and are therefore, purged in 30 days.

- cgn
- cdn
- disconnect-text
- tx-duration
- release-source
- h323-setup-time
- Acct-Unique-Session-Id
- h323-remote-address
- h323-disconnect-time

If you own any other SBC

Use case: Call screening, Active defense

Data collected from SIP signaling, SIP trace logs, and CDR

Data Fields Collected	Data Source	Description	Reason for Collection	Part of Raw Data?	Part of Processed Data?	Part of Findings?
Calling party(inbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (inbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine the toll-free numbers of the customer	Yes	Yes	Yes
Calling party (outbound calls)	SIP Signaling	The From header of the SIP message. It includes the display name and number of the calling party	Required to determine the historical behavior of the caller and anomaly detection	Yes	Yes	Yes
Called party (outbound calls)	SIP Signaling	The To header of the SIP message. It includes the display name and number of the called party	Required to determine toll fraud attack, resource misutilization attack, E911 abuse etc.	Yes	Yes	Yes
Call ID	SIP Signaling,	The call-id header of the SIP message. It is the identifier string of the call and is unique for a call	Required to correlate the request and responses	Yes	Yes	No

Data Collected from CDR

Raw Data

This includes all the fields that are part of the CDR as mentioned by your SBC OEM.
However, this data is purged in a day.

Processed Data (purged in 30 days)

Of all the data fields collected from the CDR, only the below are part of processed data, and are therefore, purged in 30 days.

- Source realm
- Destination realm
- From user
- To user
- Call ID
- Unique call id
- Setup time
- Connect time
- Disconnect time
- Call Duration
- Call setup duration
- Call bill duration (if applicable)
- Disconnect reason code.
- Disconnect initiator