ThreatStream AirGap Deployment

Some enterprise organizations or government entities require the maximum possible security when running third party platforms. This means disconnecting it from all other systems to ensure the environment is secure.

Many organizations struggle to use threat intelligence effectively in an air-gapped environment because most threat intligence platforms need connectivity to be effective because of the real-time collection of raw data.

For those organizations requiring maximum security, Anomali ThreatStream AirGap can be deployed as a completely standalone private instance, delivering full functionality without connecting to the Internet or any other threat intelligence service.

ThreatStream AirGap delivers complete functionality of Anomali's market leading cloud-native threat intelligence management solution in a secure, on prem solution.

ThreatStream AirGap can be deployed as a completely standalone private instance in an air-gapped / non-Internet aware environment. Intelligence can be developed locally or loaded via a supported air-gapped data synchronization method.

Where full air-gap deployments are not a requirement, the application can be made Internet aware in order to make direct use of third party intelligence services to support real-time investigation and analysis for the creation of local intelligence.

KEY HIGHLIGHTS:

- Support for fully air-gapped environments, through third party data diode solutions
- Capability to host large volumes of intelligence data for utilization by local users
- Support for many simultaneous local users
- Optional enrichment capabilities to third party intelligence sources to augment research
- Integration with upstream and downstream data sources to ensure the solution can be a single aggregation point for all intelligence for an organization or enterprise

Key Capabilities:

- Feeds sources are provisioned and stored in SaaS and then synced via Anomali SyncApp to pull this dataset down from SaaS to my AirGap appliance
- Updates or changes I make to my OSINT, Commercial or Custom feeds from SaaS are never pushed back upstream
- Local data is created on the AirGap appliance and is never pushed upstream
- SaaS content is scored through Macula on ingest, but local data is not scored by Macula
- All searches and queries are against local data enrichments are executed locally directly to enrichment sources sandbox is not available

Key Differentiators:

Integrated automation that supports the re-deployment of many instances reducing overhead and producing predictable results, including:

- AirGap appliances - including hot-cloning of the dataset for redeployment in the field
- SyncApp - used for data sync from the field back into the environment
- Integrator - for distribution of MRTI to security controls, such as proxies, firewalls, elasticsearch
- Trusted Circles / data sharing structures - to support integration between CVAH & CS&D

In addition, ThreatStream can:

- Run in full AirGap or Internet-aware modes depending on the customer requirements
- Be supplied as a STIG Compliant deployment to provide improved assurance for customers
- Optionally make use of both Anomali Cloud hosted services or 3rd party intelligence sources to assist with local research
- Support large datasets and user communities

KEY USE CASES

- Meet regulatory requirements, or Federal/ National Government Standards to ensure the sovereignty of your dataset and the privacy of your content
- I have large amounts of externally sourced data; I have multiple data sources; commercial, private, public
- I have medium to large amounts of internally sourced data which remains local at all times
- Push data directly into security appliance via API
- Utilize the Feeds SDK to ingest data
- Provision a local TAXII client or server to pull or push collections

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI