# Gigamon and Sumo Logic Partner to Drive Deep Observability into Cloud Environments

## A New Breed of Security for the Hybrid Cloud

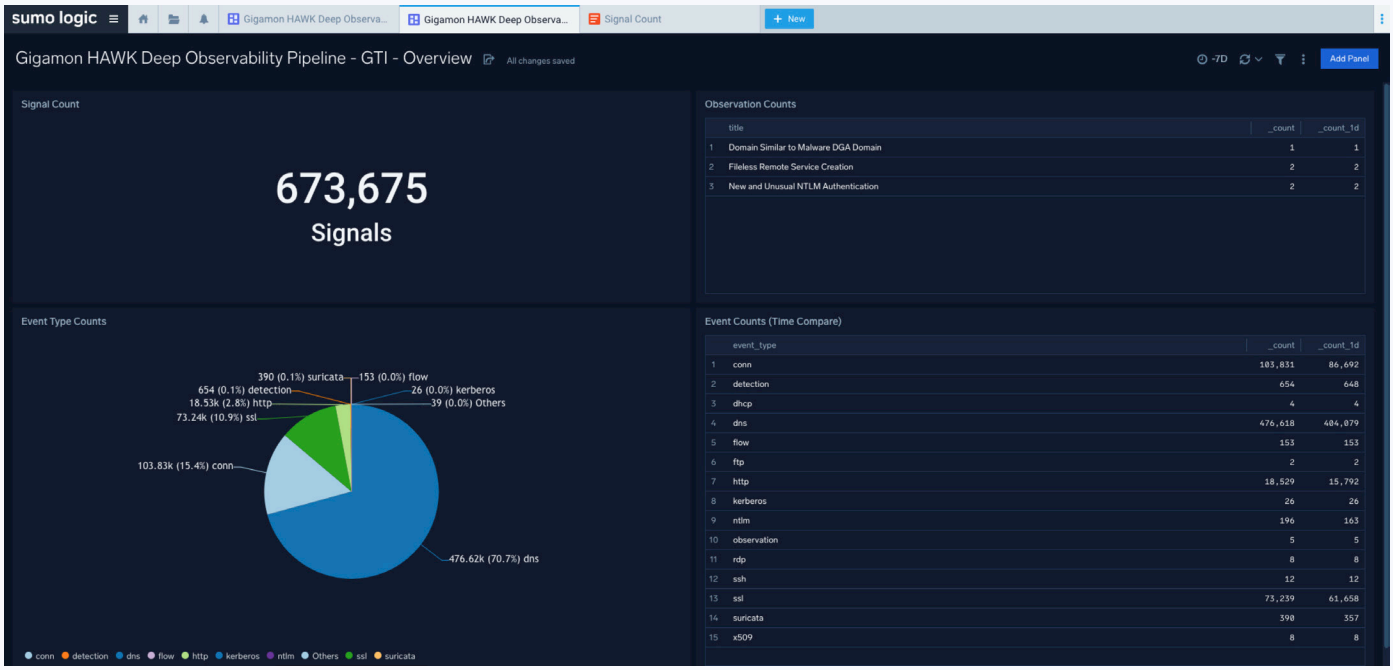
Security teams rely on tool integrations so the right data is available at the right time to the right people. Often these integrations suffer because too much of the wrong data gets delivered, driving up storage costs and making correlations impossible. Ideally, integrations should focus on exchanging only relevant, rich contextual data between products. Gigamon MetaStream with Signals is optimized by Gigamon's Applied Threat Research (ATR) team to deliver relevant data from Gigamon ThreatINSIGHT NDR to Sumo Logic's Cloud-native Security Monitoring and Analytics Platform.

### KEY JOINT SOLUTION FEATURES

- Delivery of Detections and Observations of adversary network activity identified by ThreatINSIGHT
- Delivery of ATR-defined network metadata aggregations rather than full network events
- N | S | E | W network visibility for core, cloud networks (AWS, Azure, GCP)
- Secure, easy data exchange via simple, cloud-based self-provisioned Gigamon hosted AWS S3 bucket

### KEY JOINT SOLUTION BENEFITS

- Rapid threat discovery within CSE via ThreatINSIGHT detections and observations
- Fast triage and investigation efforts with ThreatINSIGHT network metadata to reduce dwell time
- Hi-fidelity signals of adversary behavior mapped to MITRE ATT&CK framework available within SCE
- Low storage costs with network metadata aggregations only 2-5% the size of full network events




## The Problem and Solution

The goal of security integrations is to ensure security teams are never without the information they need to detect, investigate, and respond to threats. Integrations fall short when solutions exchange too little or too much data. Security alerts without context are useless and too many irrelevant events clog impede processes resulting in security teams waiting for results.

The ThreatINSIGHT integration with Sumo Logic takes a different approach.

ThreatINSIGHT provides nineteen signal types which can be integrated into Sumo Logic. Detections and Observations (anomaly) signals are alert-like in nature providing details on ThreatINSIGHT NDR identified adversary activity. Other signals provide aggregated contextual network event information to be used alongside either ThreatINSIGHT alerts or alerts from other products to facilitate rapid triage, validation, hunting or investigations. These aggregated signals provide the depth of context necessary for security teams to rapidly do their jobs but are a fraction of the size of traditional event data from other network sources.

MetaStream with Signals was designed by our security experts to meet the needs of SOC analysts and incident responders. With Sumo Logic, ThreatINSIGHT's network visibility and advanced adversary identification techniques will help security teams perform threat detection, investigation, and response activities faster and more thoroughly."

– MICHAEL DICKMAN, CHIEF PRODUCT OFFICER – GIGAMON

## MetaStream with Signals Details

MetaStream with Signals provides Detections, Observations, and ATR-defined aggregations from ThreatINSIGHT in a secure AWS S3 bucket managed by Gigamon. This is critical when data is required for further analysis with other datasets within Sumo Logic. Security teams have access to the right data and context to make quick decisions with less pivots.

### RIGHT DATA

Adversary Network Activity and Aggregated Network Events

MetaStream with Signals delivers ThreatINSIGHT NDR identified ad-versary activities and behaviors in the form of Detections, Observa-tions, and ATR-defined aggrega-tions. Aggregations of Network Events provide rich context without the high storage cost of every event.

### RIGHT TIME

Current & Historical Data, For Fast Correlation and Searching

MetaStream with Signals infor-mation is immediately available with access to the past seven days of activity, enabling security teams to investigate both current and histori-cal activities. Data is streamlined to relevant adversary actions to facili-tate both starting points for correla-tions and quick access to network context for validation of other alerts.

### RIGHT PEOPLE

Designed for Analysts, Hunters, and Investigators

Contextual details provided within ATR-defined aggregations provide the right context to quickly validate findings, hunt for actors, and inves-tigate active incidents with speed. Built by responders, for respond-ers... MetaStream with Signals pro-vides your teams the context they desire.

## Conclusion

The ThreatINSIGHT MetaStream with Signals integration with Sumo Logic drives efficiency and effectiveness for your security team while minimizing costs associated with data exchange and storage. Customers can choose to only pull Detections and Observations signals from ThreatINSIGHT initially, but more in-depth context can easily be streamed from the MetaStream with Signals repository hosted by Gigamon. Alternatively, the raw network event data is aggregated and streamlined to a fraction of the size of traditional security event data so customers can efficiently retrieve all MetaStream with Signals data to quickly validated findings, hunt, or investigate an incident.

| Signal Type | Description |
|---|---|
| conn_src_dst | Connection log with aggregation subjects src, dst |
| detection_none | Detection log with no aggregation subject |
| detection_src_sensor | Detection log with aggregation subject src, sensor |
| dns_answer | DNS log with aggregation subject answer |
| dns_host | DNS log with aggregation subject host |
| ftp_username | FTP log with aggregation subject username |
| http_host | HTTP log with aggregation subject host |
| http_src_sensor | HTTP log with aggregation subject src, sensor |
| http_username | http log with aggregation subject username |
| kerberos_username | Kerberos log with aggregation subject username |
| ntlm_username | NTLM log with aggregation subject username |
| observation_none | Observation log with no aggregation |
| rdp_dst | RDP log with aggregation subject dst |
| rdp_src_sensor | RDP log with aggregation subject src, sensor |
| ssh_src_sensor | SSH log with aggregation subject src, sensor |
| ssh_dst | SSH log with aggregation subject dst |
| ssl_host | SSL log with aggregation subject host |
| ssl src sensor | SSL log with aggregation subjects src, sensor |
| suricata_src_dst_sensor | Suricata log with aggregation subjects src, dst, sensor |

MetaStream with Signals supported signal types.

## For more information on Gigamon ThreatINSIGHT and Sumo Logic, please visit: GIGAMON.COM/THREATINSIGHT | SUMO LOGIC

### WHY GIGAMON?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network. The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoy industry-leading customer satisfaction with more than 3,000 organizations around the world.

## Take ThreatINSIGHT for a test drive, visit gigamon.com/demo.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com