CYBERSECURITY AND INFRASTRUCTURE SECURITY (CISA) TERMS OF USE FOR MALCOLM, VERSION 1.0

This Terms of Use addresses MALCOLM Version 1.0. Should CISA subsequently alter the software, CISA will update the version number and any other provisions of this Terms of Use impacted by the change.

1. DEVELOPMENT OF MALCOLM.

The Cybersecurity and Infrastructure Agency (CISA) of the U.S. Department of Homeland Security developed a network traffic analytic tool called MALCOLM that is easy to use, provides powerful traffic analysis, allows for streamlined deployment, provides secure communications, and expands visibility of control systems. MALCOLM accepts network traffic data in the form of full packet capture (PCAP) files and Zeek (formerly Bro) logs. An analyst can upload these artifacts via a simple browser-based interface or captured live and forward them to MALCOLM using lightweight forwarders. MALCOLM will automatically normalize, enrich and correlate the data for analysis.

2. WHAT IS MALCOLM?

(a) MALCOLM is a powerful network traffic analytic tool that provides a robust analysis of network traffic with better visibility and usability than other network traffic analyzers currently available. MALCOLM provides visibility into network communications through two intuitive interfaces: **Kibana**, a flexible data visualization plugin with dozens of prebuilt dashboards providing an at-a-glance overview of network protocols; and **Moloch**, a powerful tool for finding and identifying the network sessions comprising suspected security incidents.

(b) MALCOLM offers streamlined deployment by operating as a cluster of Docker containers, isolated sandboxes that each serve a dedicated function of the system. This Docker-based deployment model, combined with a few simple scripts for setup and run-time management, makes Malcolm suitable to quick deployment across a variety of platforms and use cases, whether it be for long-term deployment on a Linux server in a security operations center (SOC) or for incident response on a MacBook for an individual engagement.

(c) MALCOLM offers secure communication by securing all communication within MALCOLM from both the user interface and remote log forwarders with industry standard encryption protocols.

(d) MALCOLM is not only great for general-purpose network traffic analysis; it provides insight into protocols used in the industrial control systems (ICS) environments. CISA will continue to develop MALCOLM to provide additional parsers for common ICS protocols.

(e) MALCOLM is comprised of several widely used open source tools, all with permissive copy-left license terms and conditions thereby providing a security solution that does not require a paid license. The open source tools include:

- **Moloch PCAP**, which binds capture and viewer tools for PCAP file processing, browsing, searching, analysis, and carving/exporting.
- **Nginx**, which uses HTTP and reverse proxy server to provide TLS encryption and HTTP authentication for the user-facing MALCOLM components.
- **Elastic Stack**, which has several components:
  - **Elasticsearch**, a search and analytics engine for indexing and querying the metadata from network traffic sessions;
  - **Logstash**, a data processing pipeline for transforming Bro logs into the format used by Moloch and inserting them into Elasticsearch;
  - **Beats**, lightweight log file shippers for sending Bro log files to Logstash for parsing; and,
  - **Kibana**, a general-purpose data visualization tool.
- **Elastalert**, which is an alerting framework for Elasticsearch.
- **BitSensor's ElastAlert Fork and Kibana Plugin**, which comprises the REST APIs, Docker image and Kibana plugin for use with ElastAlert.
- **CyberChef**, which is a "swiss-army knife" data conversion tool.
- **Zeek (formerly Bro)**, which is the network analysis framework and IDS.
- **Docker and Docker Compose**, which is the containerization platform for simple, reproducible build and deployment of the MALCOLM appliance across environments and coordination of communication between its various components.

(f) Although all of the open source tools, which make up MALCOLM, are already available and in general use, MALCOLM provides a framework of interconnectivity that makes it greater than the sum of its parts. While there are many other solutions for network traffic analysis readily available, such as complete Linux distributions like Security Onion or licensed products like Splunk Enterprise Security, MALCOLM's easy deployment and robust combination of open source tools fill a void in the network security space that will make network traffic analysis accessible to many in both the public and private sectors as well as individual enthusiasts.

3. OPEN SOURCE DISTRIBUTION OF MALCOLM.

CISA desires to distribute MALCOLM to the public through an open source platform to allow users to have access to software in source code and binary format. CISA also believes the open source distribution of MALCOLM will make network traffic analysis accessible to many in both the public and private sectors as well as individual enthusiasts. Accordingly, CISA provides MALCOLM to you, the user, under the conditions contained in this Terms of Use.

4. LICENSE GRANTED IN MALCOLM.

A U.S. Government contractor developed MALCOLM for the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security and therefore MALCOLM is subject to United States copyright law. The United States Government has unlimited rights in the

copyright in MALCOLM, which is sufficient to allow end users to download, access, install, copy, modify, and otherwise use MALCOLM for its intended purpose. Specifically, the U.S. Government is providing MALCOLM to Users with a royalty-free, irrevocable, worldwide license to use, disclose, reproduce, prepare derivative works, distribute copies to the public, including by electronic means, and perform publicly and display publicly MALCOLM, in any manner, including by electronic means, and for any purpose whatsoever.

5. ADDITIONAL LICENSE TERMS. The above grant of license is conditioned on the user's compliance with each of the following:

(a) User will ensure compliance with, and provide continued notice of this license, and any open sources licenses identified in Section 6 of this Terms of Use.

(b) To the extent practicable, User will acknowledge the contribution of DHS/CISA in the development of the MALCOLM by the following statement in a readme text file of the tool: *MALCOLM is developed with funds from the Cyber Security and Infrastructure Security Agency of the U.S. Department of Homeland Security*.

(c) This Terms of Use does not constitute, in any matter, an endorsement by CISA, DHS, or the U.S. Government of any information, plans, or actions resulting from use of MALCOLM.

(d) This Terms of Use does not, in any manner, constitute the grant of a license to the public of any CISA or DHS, or third party patent, patent application, copyright or trademark, except as provided by this Terms of Use, or other intellectual property of CISA and DHS.

(e) CISA denies any, and all, liability, as discussed in Section 7 of this Terms of Use, associated with or resulting from the use of MALCOLM.

(f) This Terms of Use and the legal relations between the Users and CISA shall be determined in accordance with United States Federal law.

6. NOTICE OF THIRD PARTY SOFTWARE.

(a) MALCOLM is comprised of proprietary or open source software. The list of open source software is included in Attachment A of this Terms of Use. All components of MALCOLM, individually and as a combined work are subject to United States Copyright law.

(b) All third party software necessary for operation of the MALCOLM are subject to copyright licenses. DHS has identified all the third party copyright licenses needed to operate MALCOLM and conducted a good faith analysis to determine that the third party library dependencies allow users to download, access, install, copy, modify, distribute and otherwise use the third party library dependencies for operation of MALCOLM.

(c) Identified in Attachment A, are the third party library dependencies and links to the specific terms and conditions, not under CISA or DHS control, but that are applicable to the above referenced third party software.

7. DISCLAIMER OF LIABILITY.

The United States Government shall be not be liable or responsible for any maintenance or updating of MALCOLM, nor for correction of any errors in MALCOLM.

THE MALCOLM IS PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THE MALCOLM WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR FREEDOM FROM INFRINGEMENT, ANY WARRANTY THAT THE MALCOLM WILL BE ERROR FREE. IN NO EVENT SHALL THE UNITED STATES GOVERNMENT OR ITS CONTRACTORS OR SUBCONTRACTORS BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THE MALCOLM, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE MALCOLM. THE UNITED STATES GOVERNMENT DISCLAIMS ALL WARRANTIES AND LIABILITIES REGARDING THIRD PARTY SOFTWARE, IF PRESENT IN THE MALCOLM, AND DISTRIBUTES IT "AS IS".

ATTACHMENT A
Open Source Dependencies

BSD License For:

Nginx: Uses HTTP and reverse proxy server to provide TLS encryption and HTTP authentication for the user-facing MALCOLM components
https://nginx.org/en/; https://nginx.org/LICENSE

BitSensor's ElastAlert Fork and Kibana Plugin: Comprised of the REST APIs, Docker image and Kibana plugin for use with ElastAlert
https://github.com/bitsensor/elastalert-kibana-plugin; https://github.com/bitsensor/elastalert-kibana-plugin/blob/master/LICENSE.md

Zeek (formerly Bro): Provides the network analysis framework and IDS
https://www.zeek.org/download/index.html; https://opensource.org/licenses/BSD-2-Clause

---

Apache License, Version 2.0 For:

Moloch PCAP: Binds capture and viewer tools for PCAP file processing, browsing, searching, analysis, and carving/exporting
https://github.com/aol/moloch; https://github.com/aol/moloch/blob/master/LICENSE

*Elastic Stack**: Comprising of several components that perform search and analysis, data processing, log shipper, and data visualization. These components are Elasticsearch, a search and analytics engine for indexing and querying the metadata from network traffic sessions; Logstash, a data processing pipeline for transforming Bro logs into the format used by Moloch and inserting them into Elasticsearch; Beats, a lightweight log file shippers for sending Bro log files to Logstash for parsing; and Kibana, a general-purpose data visualization tool
*The Elasticsearch binaries used in MALCOLM are tagged with "-oss" in the package, which are distributed under the Apache License Version 2.0
https://www.elastic.co/downloads/; https://www.elastic.co/subscriptions;
https://github.com/elastic/elasticsearch/blob/master/LICENSE.txt

Elastalert: An alerting framework for Elasticsearch
https://github.com/Yelp/elastalert; https://github.com/Yelp/elastalert/blob/master/LICENSE

CyberChef: A "swiss-army knife" data conversion tool
https://github.com/gchq/CyberChef; https://github.com/gchq/CyberChef/blob/master/LICENSE

Docker and Docker Compose: The containerization platform for simple, reproducible build and

deployment of the MALCOLM appliance across environments and coordination of communication between its various components.
https://github.com/docker/compose; https://github.com/docker/compose/blob/master/LICENSE

End of Open Source Dependencies Legal information