KEYSIGHT TECHNOLOGIES

Breach Defense

Threat Simulator 1.0.4 – SaaS Infrastructure

Release Notes: August 31st, 2020 Issue 02

Deployment Version:	1.0.4.1971
AAM Cluster Version:	1.0.4.1971
Agent Version:	2.4.1-1598902898

Warranty
The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses
The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights
The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula or https://support.ixiacom.com/supportservices/warranty-license-agreements. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Key-sight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Threat Simulator 1.0.4 – SaaS Infrastructure

Document Scope

This document provides information regarding the Threat Simulator 1.0.4, including information about new features, resolved SRs, known defects and workarounds.

Browser Compatibility

Threat Simulator is compatible with the following browsers

- Google Chrome browser 81.0.4044.92
- Firefox browser 75.0

Browser versions that are more current than the versions listed in the table may work but have not been tested at this time.

New Features in Release 1.0.4

Executive Report

This release introduces support for the reporting framework, enabling users to generate and export security assessment reports as portable document files (PDFs). In this release, we are introducing Executive Reports to summarize the security posture across for the last 7 days.

Note, the history data will only be generated starting from the day the update was performed (31st August). Hence it will require 7 days to elapse before a user will see the full history in the report populate.

Agent Management Communication

A new agent has been introduced in this version all management communication between the Agent and the backend is over TLS/443. This means no special network configuration changes should be required to allow Agent Management Communication.

Agents can be updated from the Agents page in the user Interface.

Issues Addressed in 1.0.4

THREATSIM-11614	Addressed issue with Assessment that didn't run any audits if the ports were blocked
THREATSIM-10674	Fixed issue with lateral assessment blocked in Stopping state when running on closed port 443
THREATSIM-10412	Fixed issue with incorrect initialized status on Monero Kill Chain scenario
THREATSIM-11209	Fixed errors when running Demo Web Application Security Assessment
THREATSIM-11071	Addressed issue with skipped audits after first stage failed on WannaCry Kill Chain Assessment
THREATSIM-11188	User is now allowed to assign the same agent name to multiple agents
THREATSIM-11005	Enhanced help for the REST API
THREATSIM-11119	Fixed empty Assessments list issue in REST API
THREATSIM-9113	Enhanced Policy details
THREATSIM-11612	Fixed new insecure deserialization audits issue that were skipped when services were not accessible
THREATSIM-10341	Fixed filtering issue in Agents screen for "Provider:hyperv"
THREATSIM-11524	Corrected issue that caused false positives to be reported when running CISA Top 10, 2016-2019 Server Attacks on a path with SMB access blocked but HTTP port open
THREATSIM-11869	Fixed out of disk space issue on an agent
THREATSIM-11528	User is able to access OVA link from Agent Deployment tutorial
THREATSIM-10795	About now shows email address of user

Limitations and Known Issues

THREATSIM-10840: Docker restarting-loop on Ubuntu 18.04 / 20.04 LTS Desktop/Server

- On Ubuntu-based hosts running 18.04 LTS/20.04 LTS (and probably 16.04 LTS), a fresh Threat Simulator agent installation fails to bring the docker containers up, even though the installation completes without errors. As a result, the agent will show offline in the user interface. The docker container logs command will indicate Permission Denied. This is due to a change that the latest snap docker version has some collateral that seems to be widespread and affects many users on internet.
- If you need to deploy a new Threat Simulator agent on Ubuntu, please pre-install docker container using sudo apt install docker.io command. This docker installation method doesn't have the bug and allows our agent to run properly after install
- For systems where the snap docker version was installed by a prior attempt to deploy our agent, you can correct the issue using the following commands:
  - kill and remove all containers, then remove all container images on host
    - sudo docker kill $(sudo docker ps -a -q)
    - sudo docker container rm $(sudo docker ps -a -q)
    - sudo docker image rmi $(sudo docker images -q)
  - Remove snap docker
    - sudo snap docker remove
  - install docker.io version
    - sudo apt install docker.io
  - Re-install our agent using standard procedure

THREATSIM-10287: Threat Simulator agent supports only IPv4 addresses

- When deploying a Threat Simulator agent on a Linux host with IPv6 address enabled the install may fail. To work around this issue, disable IPv6 and rerun the install script

THREATSIM-10288: Docker Snap may interfere with Agent Installation

- When deploying Threat Simulator on a supported Linux-host that has Docker Snap installed, Docker Snap may conflict with the Docker.io installed by Threat Simulator. To work around this issue, remove Docker Snap and rerun the install script

THREATSIM-10289: UI Response “Serverless Cold Start”

- When unused the services that support the UI are shut down. After logging in the first access to a page in the application may be slow to load time. Subsequent accesses should not experience this lag.

THREATSIM-10290: Assessment complete with Error

- On rare occasions an assessment may complete with an Error. This can be caused by a variety of reasons such as loss of communication with the agent while the assessment is running. If an Assessment Completes with an error, the results of that run will not count in the aggregated results (Health Score), the last successful run will be used. If an error occurred, the user can rerun the Assessment. In future updates we will consider adding the option to automatically rerun on error.

THREATSIM-0385: Audit Reports False Positive (Blocked)

- On rare occasions an Audit may be reported with a false “Pass – Blocked”. This can be caused by a variety of reasons such as loss of communication with the agent while the assessment is running. Typically, there are hundreds of Audits run on a path and a single false positive has little impact on the overall (Health Score).

Operational Notes

THREATSIM-10203: Assessment will run when "Access Control" blocks traffic

- An assessment will run on path regardless of access controls. For example, by default, Web Browser Assessment uses HTTPS: 443. If the network blocks all HTTPS: 443 traffic, the assessment will still run, each audit will report “PASS, BLOCKED, Access Blocked on HTTPS: 443.

THREATSIM-10253: Secondary Management Interface may be Required on Agent

- To operate, a Threat Simulator Agent needs to communicate to the Threat Simulator Manager. This requires the following rules:
  - Outbound, HTTPS: 443, with tar.gz file download
  - Outbound MQTT: 8883
- If required, an Agent can be deployed with a separate interface for "Management Traffic and “Test Traffic”. Refer to "Deployment Tutorials" for more information

THREATSIM-9791: Agent errors with timeout when port 10000 is already in use on the host machine

- When deploying Threat Simulator on a supported Linux-host that has port 10000 already in use, the audits complete with a timeout Error. To work around this issue, stop or remove the application that uses port 10000.

Technical Support

Need help? Connect with us and we will gladly assist you.

You can contact us by email via threatsim-support@keysight.com or using one of the global or regional support emails and/or phone numbers.

Ixia headquarters
26601 West Agoura Road
Calabasas, California 91302
+1 877 367 4942 – Toll-free North America
+1 818 871 1800 – Outside North America
+1.818.871.1805 – Fax
www.ixiacom.com/contact/info

Global Support	+1 818 595 2599	support@ixiacom.com
Regional and local support contacts:		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+656 494 8910	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com