TELESOFT

DATASHEET

400G TRITON

CYBER WARFARE SIMULATION

Prove and enhance your cyber security posture with our Cyber Warfare Simulation tool, our world class SLA and advanced on-site/off-site support.

ATTACK
Replicate attacks, from low and slow password spraying and high rate capacity DDoS to AI poisoning. If you have a PCAP of an attack, this appliance can play it, if you don't have a PCAP then the 400G TRITON CWS can generate it. Spawn malicious traffic at volume to directly test the target, system or team.

DEFEND
SOC and IR teams can be put to the test by attacking the network and infrastructure at high rate with multiple attacks from multiple vectors. Achieve a cutting edge response team to reduce the fallout from an attack by practicing against highly realistic and orchestrated attacks.

INTEL
Strategically located honeypots across the globe glean intelligence directly from the most viable and up to date sources...the attackers. This intelligence is then fed in to the traffic profile database to allow for effortless replication delivery of real-life attacks.

ENTROPY
Overcome traffic replay stagnation through entropy generation by combining direct traffic ingest with source/destination IP randomisation, creating bespoke traffic patterns.

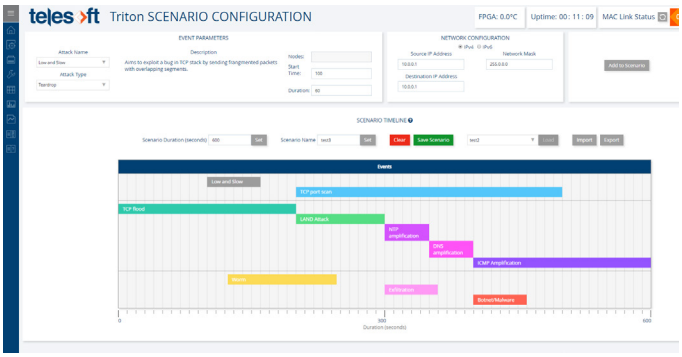
HEADQUARTERS
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
+44 (0)1258 480880
+44 (0)1258 486598
sales@telesoft-technologies.com

AMERICAS
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
salesusa@telesoft-technologies.com

ASIA
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301
+91 120 612 7725
salesindia@telesoft-technologies.com

CYBER WARFARE SIMULATION 400G TRITON

Triton CWS Dashboard



Triton CWS Threat Scenario Configuration

AVAILABLE WITH ON-SITE TECHNICAL SERVICES.

KEY FEATURES

560Mpps traffic generation over 4 x 100GbE ports	Inject threats into background traffic
Amplify and mix PCAP, live traffic streams and synthetic traffic profiles	Open-source TRex support
In-built threat catalogue - one click threat generation	Create DDoS botnets to single flow data exfiltration
Create complex traffic profiles	Multiple traffic profiles and PCAPs per 100GbE port
5s sustained record 100Gb/s line-rate	Real time attack traffic visualisations
Simple or complex threat scenarios supported by embedded VMs for stateful attack capability	Campaign manager enables full control over multiple attack scenarios

TECHNICAL SPECIFICATIONS

Physical	• 1U 19-inch rack mount • 1.7 x 17.2 x 30.6 in (4.3 x 43.7 x 77.7 cm)
Connectivity	4 x 100GBASE-LR4 QSFP28
Performance	• Over 560Mpps spread across 4 x 100GbE ports • Amplify up to 16 million flows per single PCAP file
Control	• Telesoft Triton CWS GUI • TREX interface • RestAPI for integration with automated test
TRex	Supports TRex yaml config file
Power Stats	300W typical, and 400W peak

ORDER OPTIONS

Part Number	Description
500003096	400G Triton CWS, 1U, 4 x 100GbE, QSFP28

TELESOFT

Telesoft Technologies, the Telesoft Technologies logo design, ThinkEngine, Triton, HINTON, OKEFORD, TDAPI, MPAC, MILBORNE, C-CURE and ARNE are trademarks or registered trademarks of Telesoft Technologies Ltd or its subsidiaries. All other brand or product names may be trademarks of their respective companies. All rights reserved.

telesoft-technologies.com
© Copyright 2020 by Telesoft Technologies.
All rights reserved. Commercial in Confidence.