

CERNE

100GBPS IDS & EVENT DRIVEN RECORD

100Gbps IDS engine and alert driven packet recorder minimises storage and retrieval latency to rapidly provide context before and after an event

CERNE combines a high rate 100Gbps IDS engine with automated flow processing of relevant network traffic for real-time and historical threat investigation.

Based on Suricata, with Telesoft specific modifications and hardware hooks for accelerated performance, the CERNE is optimised to provide IDS capability at full line rate, processing up to 5 million user defined signatures.

Optional proprietary tags within the signatures enable the user to configure CERNE to process flows associated with an IDS alert. Flows can be buffered and recorded, providing 2.5 seconds back-in-time visibility, giving an analyst rapid access to critical packets prior to an event.

Flow management can be configured for a single IP address, port, protocol or combination providing flexible visibility and context around a potential breach. Automated collection of only relevant traffic by session minimises unnecessary storage, reduces costs and ensures rapid near real-time retrieval.

KEY PERFORMANCE FIGURES*

Line Rate processing

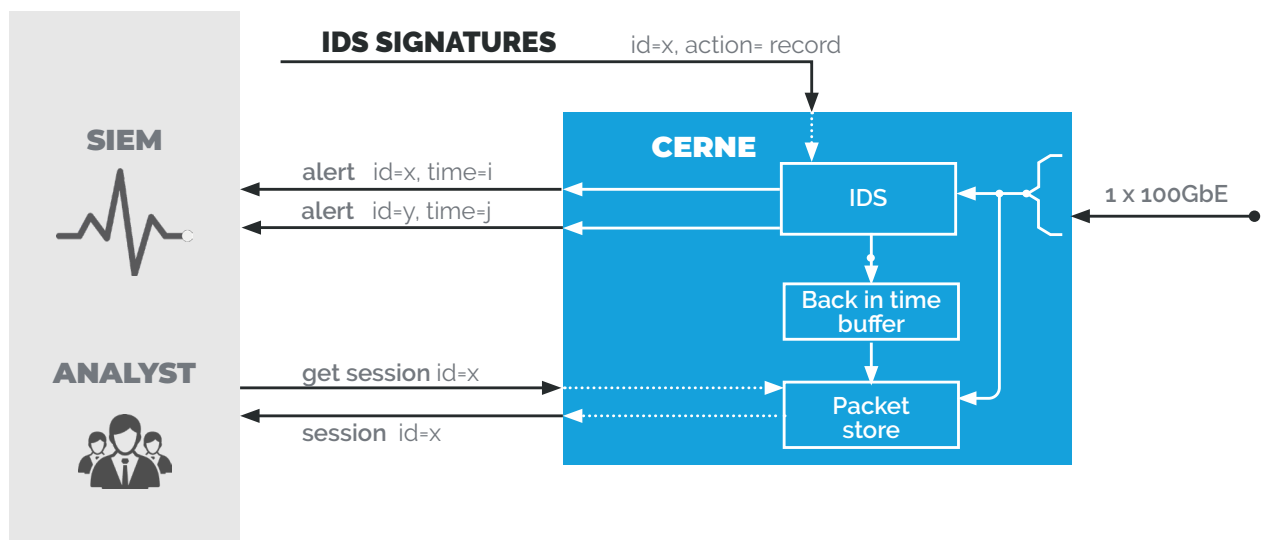
5 million L7 user-defined signatures

250 thousand filters for back in time record

*Performance will be dependent on traffic profile and signatures. See document DX-TTL-GEN-MK-SP-35807 for benchmark figures.

CERNE integrates with existing SIEM architecture for automated threat intelligence configuration, session delivery and storage management.

100GBPS IDS & EVENT DRIVEN RECORD



HEADQUARTERS

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

LONDON

Telesoft Technologies Ltd
The Shard
Floor 25
32 London Bridge Street
London SE1 9SG
sales@telesoft-technologies.com

ASIA

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

AMERICAS

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

KEY FEATURES

Built on hardware accelerated OISF Suricata	Use standard Suricata signature format with optional extensions. Source signatures from existing providers and use existing signature management tools
Alert based flow/session capture	Only export or record relevant data to provide context around an alert. Recorded packets are organised in flows and indexed for rapid retrieval
Live signatures	Update signatures whilst running live traffic without interruption
2.5 second back in time buffer	Capture packets from before and after the event for full context
Controlled via GUI or RestAPI	Integrates with and can be controlled by your SIEM
Full Installation and Commissioning, backed by Engineering experts	Ensure your IDS is tuned specifically for your application and traffic profile, to obtain the best performance results
Tiered support, including Gold and Bespoke options	Spares management, advanced replacements and 24:7 support ensures your IDS down time is minimal

TECHNICAL SPECIFICATIONS

Physical	1U 19-inch rackmount
Interfaces	1 x 100Gb Ethernet QSFP28
Interface Specification	1 x 100GBASE-LR4, 1 x 100GBASE-SR4 OR 1 x DAC (direct-attach copper)
IDS Engine	Modified Suricata v6.0
Storage Capacity	2 x 4TB NVMe SSD
Operating Temperature	10°C to 40°C (storage: -20°C to 70°C)
Operating Humidity	8% to 90%

ORDER OPTIONS

Part Number	Description
500003109	CERNE 100Gbps IDS + Event Driven Record
500003082-01	EDGE Technologies 100GBASE QSPF28-LR4 10KM TX/RX Transceiver



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.