CERNE

IDS & EVENT DRIVEN RECORD

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 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 1 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 (Up to 100Gbps) |
| Up to 1 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.

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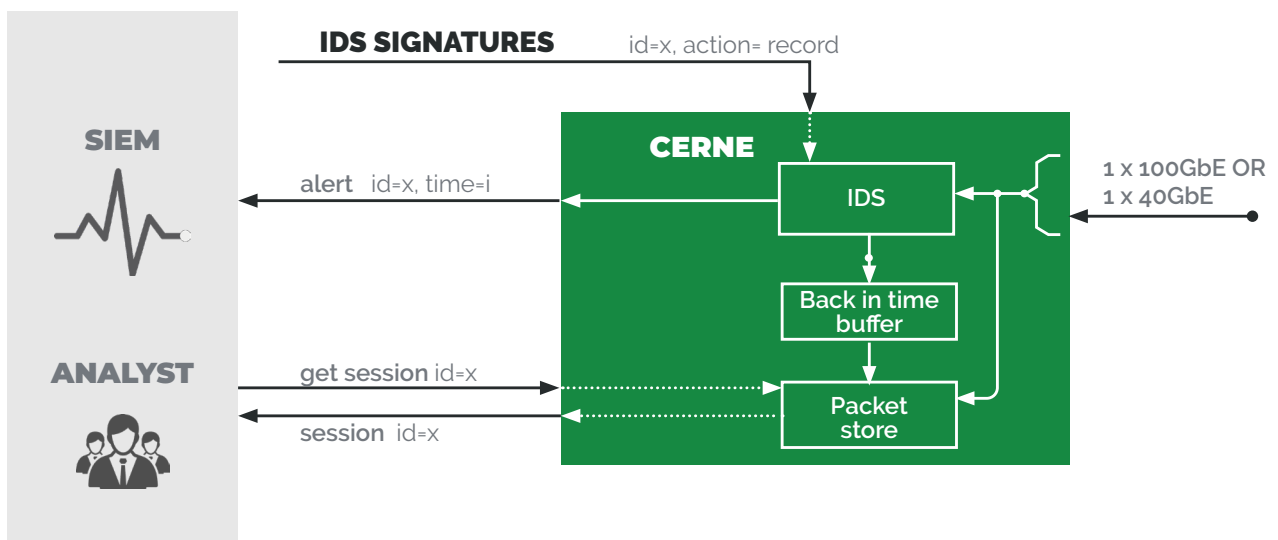
HEADQUARTERS
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
+44 (0)1258 480880
+44 (0)1258 486598
sales@telesoft-technologies.com

SAUDI ARABIA
Telesoft Arabia
ATCO Building
P.O. Box 718 - Dammam 31421
Kingdom of Saudi Arabia
+966 13 833 5588
salesindia@telesoft-technologies.com

LONDON
Telesoft Technologies Ltd
Octagon Point,
Office 501,
5 Cheapside, St. Pauls,
London EC2V 6AA
sales@telesoft-technologies.com

ASIA
Telesoft Technologies Ltd
Unit No B 409-410
Floor 4, Plot 8, Sector 62
Noida, 201309
+91 120 612 7725
salesindia@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

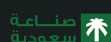|	40GBPS CERNE	100GBPS CERNE
Physical	2U 19-inch rackmount	1U 19-inch rackmount
Interfaces	1 x 40Gb Ethernet QSFP28 OR 4 x 10Gb Ethernet SFP+	1 x 100Gb Ethernet QSFP28
Interface Specification	• 40GbE : 40GBASE-SR4 or • 40GBASE-LR4 (QSFP+ dependent) • 10GbE : 10GBASE-SR • 10G-BASE-LR or 10GBASE-ER (SFP+dependent)	1 x 100GBASE-LR4, 1 x 100GBASE-SR4 OR 1 x DAC (direct-attach copper)
IDS Engine	Modified Suricata v6.0	
Storage Capacity	4 x 1.2TB HDDs (RAID10, 2.2TB available recording capacity)	2 x 4TB NVMe SSD (RAID1, 3.5TB available recording capacity)
Operating Temperature	10°C to 40°C (storage: -20°C to 70°C)	
Operating Humidity	8% to 90%	
Power Stats	300W typical and 400W peak	410W typical and 560W peak

ORDER OPTIONS

40GBPS CERNE		100GBPS CERNE	
Part Number	Description	Part Number	Description
500003039	CERNE 40Gbps IDS + Event Driven Record	500003109	CERNE 100Gbps IDS + Event Driven Record
500002853	10GBASE-SR 850nm SFP+ transceiver	500003082-01	EDGE Technologies 100GBASE QSPF28-LR4 10KM TX/RX Transceiver
500002852	10GBASE-LR 1310nm SFP+ transceiver		
500003012	10GBASE-ER 1550nm SFP+ transceiver		