TELESOFT

DATASHEET

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.

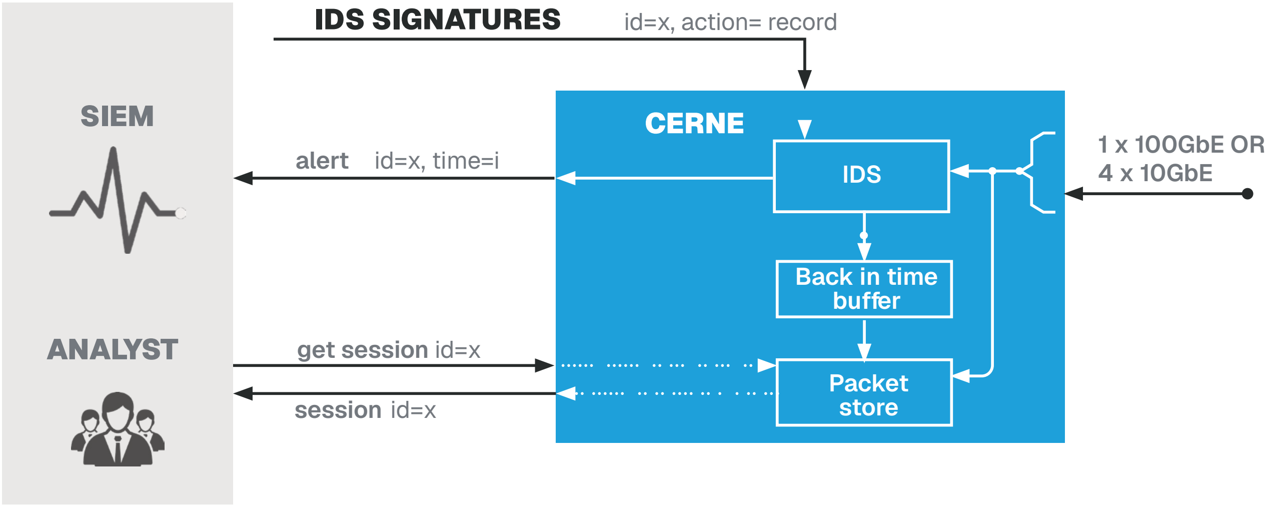
Flow management can be configured for a single IP address, port, protocol or combination providing flexible visibility and context around a potential breach. Automated collection of only relevant traffic by session minimises unnecessary storage, reduces costs and ensures rapid near real-time retrieval.

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

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.

IDS & EVENT DRIVEN RECORD



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

ATCO-TELESOFT
TEDJA8069, 8069, 4th Street,
5249, Prince Muhammad Ibn
Saud Dist., 32241,Dammam,
Kingdom of Saudi Arabia
+966 (0) 13 833-5588, Ext.220
Rohit Singh - rohit.singh@atco.com.sa

ATCO COMMERCIAL
EDJA8069, 8069, 4th Street,
5249, Prince Muhammad Ibn
Saud Dist., 32241,Dammam,
Kingdom of Saudi Arabia
+966 (0) 13 833-5588, Ext.233
atcocommercial@atco.com.sa

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
Alert triggered record on 1,2,3 or 5-tuple	Record either node, flow, or session to maximise record efficiency by only recording data relevant to the investigation

TECHNICAL SPECIFICATIONS	
Physical	1U 19-inch rackmount
Interfaces	1 x 100Gb Ethernet QSFP28 OR 4 x 10Gb Ethernet SFP+
Interface Specification	1 x 100GBASE-LR4, 100GBASE-SR4, OR DAC (direct-attach copper) OR 4 x 10GBASE-SR, 10GBASE-LR, OR 10GBASE-ER (SFP+dependent)
IDS Engine	Modified Suricata v7.0
Storage Capacity	2 x 4TB NVMe SSD (RAID1, 3.5TB available recording capacity)
Operating Temperature	10˚C to 35˚C (storage: -40˚C to 60˚C)
Operating Humidity	8% to 90%
Power Stats	410W typical and 560W peak

ORDER OPTIONS	
Part Number	**Description**
500003109	CERNE 100Gbps IDS + Event Driven Record
500003082	100GBASE QSPF28-LR4 transceiver
50000307	100GBASE QSFP28-SR4 transceiver
500002853	10GBASE-SR 850nm SFP+ transceiver
500002852	10GBASE-LR 1310nm SFP+ transceiver
500003012	10GBASE-ER 1550nm SFP+ transceiver

TELESOFT

telesoft-technologies.com