Datasheet

CERNE

40Gbps IDS & Event Driven Record

40Gbps IDS engine and alert driven packet recorder minimises storage and retrieval latency to rapidly provide context before and after an event

The Telesoft CERNE combines a high rate 40Gbps IDS engine with automated record of relevant network traffic for real-time and historical threat investigation. CERNE continuously scans and collects all network packets and only stores traffic associated with an IDS alert, discarding all other traffic, giving an analyst rapid access to critical packets up to 2.4 seconds before an event. Capture 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 unneccessary storage, reduces costs and ensures rapid near real-time retrieval.

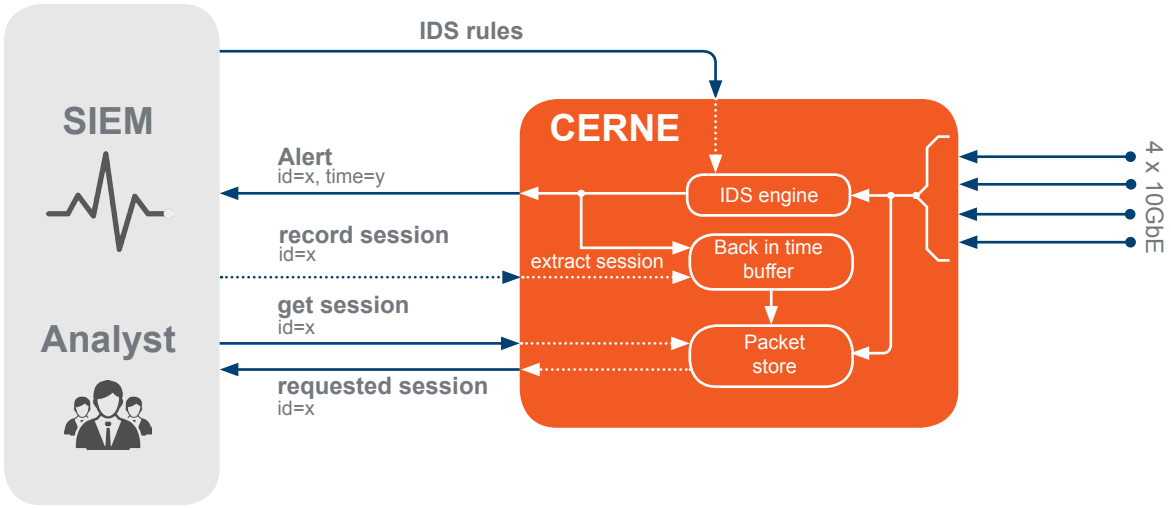
Using widely supported Suricata, the CERNE scans for threat signatures specified in user definable rules that include an optional property to extract, record and deliver to your SIEM the session content from before and after the alert. Session extraction and recording can also be controlled from threat intelligence logic from within the SIEM, enabling even greater control and intelligence over storage management.

Record Action
All packets to/from affected IP address
All packets between two IP addresses
All packets between two IP addresses over specific protocol (TCP or UDP)
All packets between two IP addresses, specific protocol, specific IP port (bi-directional flow)

Key Features

Built on hardware accelerated OISF Suricata	Use standard Suricata rule format with optional extensions. Source rules from existing providers and use existing rule management tools.
Alert based flow/session recording	Only record relevant data to provide context around an alert. Packets are organised in flows and indexed at record time for rapid retrieval.
Controlled via GUI or RestAPI	Integrates with and can be controlled by your SIEM
Back in time buffer	Capture packets from before and after the event for full context
Live rule swap	Update rules whilst running live traffic without interruption
Alert triggered record on 1,2 or 5-tuple	Record either node, flow or session or to maximise record efficiency by only recording data relevant to the investigation

System Architecture



Technical Specifications

Physical	• 2U 19-inch rackmount
Interfaces	• 1 x 40Gb Ethernet QSFP OR 4 x 10Gb Ethernet SFP+
Interface Specification	• 40GbE : 40GBASE-SR4 or • 40GBASE-LR4 (QSFP+ dependent) • 10GbE : 10GBASE-SR, • 10G-BASE-LR or 10GBASE-ER (SFP+dependent)
IDS Engine	• Modified Suricata 4.0
Storage Capacity	• 4TB HDD internal
Power Consumption (typical)	• 75 watts
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

Order Options

Part Number	Description
500003039	CERNE 40Gbps IDS + Event Driven Record
500002853	10GBASE-SR 850nm SFP+ transceiver
500002852	10GBASE-LR 1310nm SFP+ transceiver
500003012	10GBASE-ER 1550nm SFP+ transceiver

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

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

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