TELESOFT

DATASHEET

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 record of relevant network traffic for real-time and historical threat investigation. The 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 over 2.5 seconds prior to an event. Capture can be configured for a single IP address, port, protocol or combination providing flexible visibility and context around a potential breach.

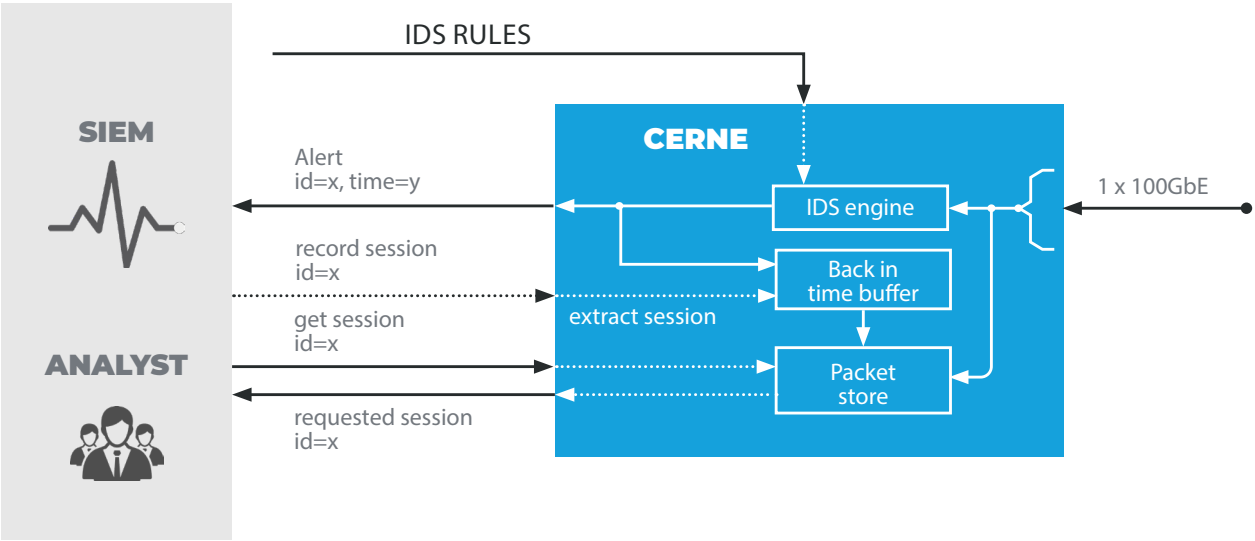
Automated collection of only relevant traffic by session minimises unneccessary storage, reduces costs and ensures rapid near real-time retrieval.

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)

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.

TRIGGERED RECORD

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 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
2.5 second 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 1,2,3 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
Interface Specification	1 x 100GBASE-LR4
IDS Engine	Modified Suricata 4.1
Storage Capacity	2 x 4TB NVMe SSD
Operating Temperature	10ºC to 40ºC (storage: -20ºC to 70ºC)
Operating Humidity	8% to 90%
Power Stats	300W typical, and 400W peak

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