CERNE Open IDS Platform

Powerful, open IDS platform with on demand capture, delivers IDS alerts and complete TCP or UDP session data, containing suspected threats for rapid incident response analysis

The CERNE Open IDS Platform is a ready to run, customizable environment that delivers IDS Alerts to your SIEM with the complete TCP or UDP session containing the suspected threat, allowing incident response to quickly know if the event is serious, relevant or just a false positive. Monitoring of up to 4 x 10GbE or a single 40GbE provides visibility of high throughput internal network traffic or protection of high-speed network boundaries.

Systems that only capture the packet that generated the alert often provide insufficient information for analysis to be conclusive; what is needed is the full TCP session or UDP flow. The common solution is to combine the IDS engine with full packet capture, but increasing network complexity and traffic rates makes this option prohibitively expensive for many organizations, due to the quantity of storage required and complexity of accessing huge volumes of stored data.

The CERNE Open IDS Platform solves this problem by recording only TCP or UDP sessions that trigger IDS alerts. 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 TCP or UDP session containing the packet that triggered the alert from a back in time store, ensuring that the session start is not missed. 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.

Key Features

Built on Suricata	Hunt for, investigate and triage signature based threats using widely adopted OISF Suricata
Single, Open Platform	One ready-to-go and configurable appliance for threat signature scanning, On Demand capture and rapid retrieval
Integrates with your SIEM	Loadshares across up to 64 cores for maximum utilisation of multi-core CPU architectures
Signature match acceleration	Open APIs including REST enable rapid integration
Faster throughput	Visibility of up to four 10GbE or one 40GbE

To find out more information about the CERNE Open IDS Platform or to request a datasheet, please contact us on **+44 (0) 1258 480880** or **sales@telesoft-technologies.com**

telesoft-technologies.com