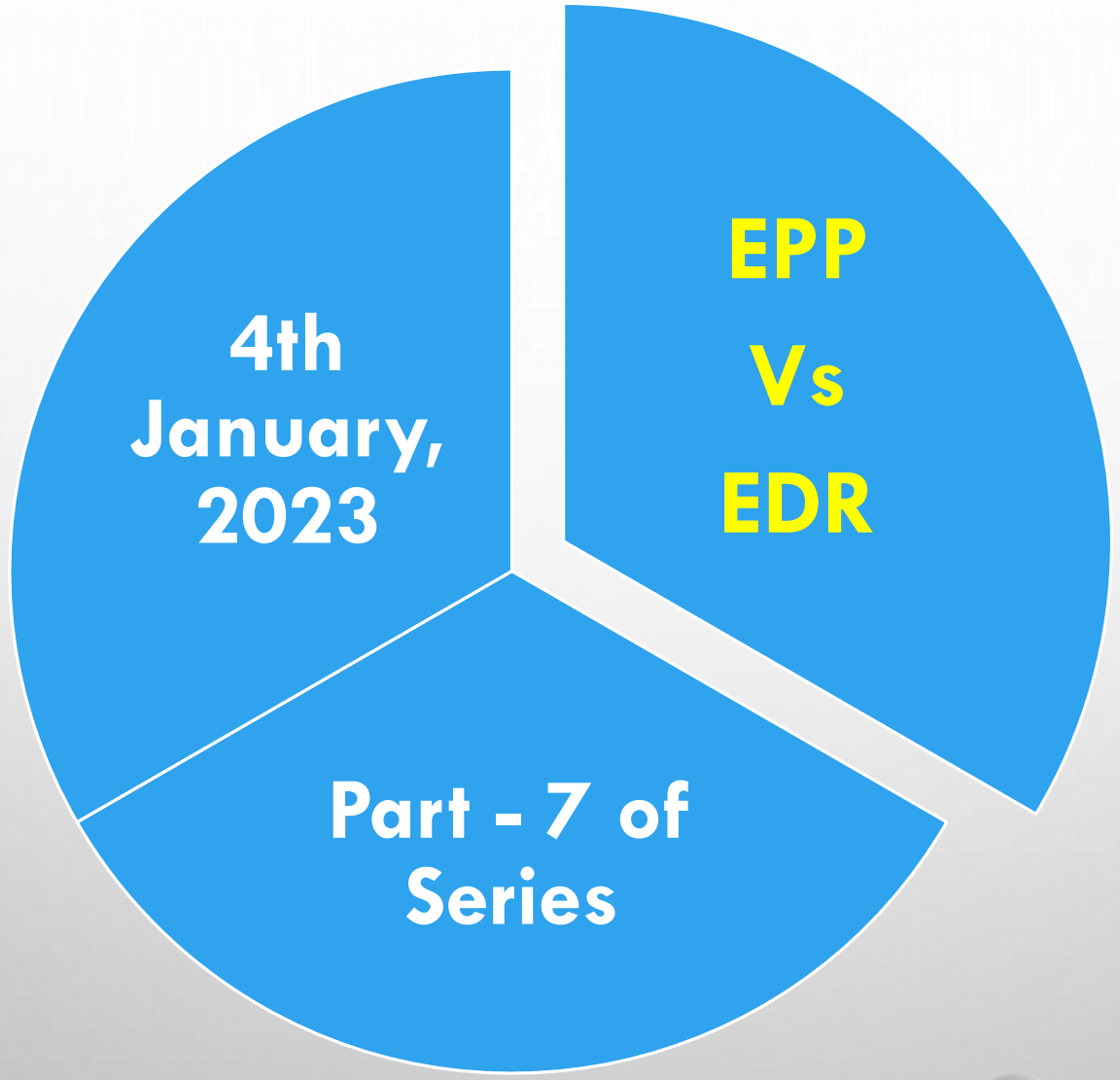
CELEBRATION OF CYBER JAAGROOKTA (AWARENESS) DIWAS (CJD)

(ON THE **FIRST WEDNESDAY OF EVERY MONTH**

COMMENCING APRIL,2022 ONWARDS)

Central Mine Planning & Design Institute Ltd.
RANCHI


EPP
Vs
EDR
Part - 7 of
Series
4th
January,
2023

Now that CMPDI has implemented Endpoint Protection (EPP) along with Endpoint Detection and Response (EDR), it's time we know the importance of both EPP and EDR.

Both EPP and EDR need to be unified for Full Endpoint Protection

EPP and EDR are both invaluable solutions for endpoint security. EPP solutions prevent a variety of threats from reaching an organization's systems, and EDR enables detection and response for threats on an endpoint.

Rather than choosing between the two, it's better to choose a solution that offers both EPP and EDR.

These complementary solutions enable an organization to implement defense in depth to protect their endpoints.

https://www.escanav.com/en/security-awareness/EPP-vs-EDR.asp

What is an EPP?

Endpoint Protection Platform (EPP) is a cybersecurity solution created to detect and stop threat on device/endpoint level. An EPP may be a Firewall, Antivirus, Intrusion Prevention System (IPS), Device Control, Data Loss Prevention (DLP), Data Encryption, and AntiMalware/AntiVirus, or a combination of all of these. EPP products, normally, are prevention-based and detects only the signature-based threats i.e. it takes action on threats only if its signature is similar to the one in its database. While they do rely on signatures, some EPP products are quite developed and use modern detection techniques to catch threats. eScan EPP, for instance, is quite advanced and provides complete all-round protection using behavioral patterns of binaries, in order to detect unknown malware.

What is an EDR?

Endpoint Detection and Response (EDR) is an advanced endpoint security solution that comprises of real-time activity monitoring, threat alerts, detailed analysis, and threat removal capabilities.

The EDR's real-time monitoring excels over EPP by maintaining detailed logs of registry changes, file execution and modification, configuration changes for network connection, and binary execution across all endpoints. EDR also provides administrator with Windows Events, so that co-relation between Windows Events, eScan Events and end-point behavior can be analyzed & necessary action taken.

With all the above characteristics, the EDR:

- Monitors and collects data activity data
- Assesses the behavior to identify potential threats
- Initiates a quick counter-response to contain/remediate threat
- Analyses the detected threats and searches for simillar suspicious activities across the network
- Does closer integration with Enterprise SIEM for co-relation

Both EPP and EDR are critical

The EPP is our primary defence layer against the known cyber-threats and EDR is the secondary layer that continuously monitors for threats, assesses its intrusion, and gives a quick counter-response to nullify it.

To strengthen the network security, organizations want a perfect product that combines capabilities of both active and passive endpoint protection. And to meet this market demand, many cybersecurity solution vendors started adding the EPP features into EDR solutions and EDR features into EPP solutions.

The journey continues.....