infotex

Endpoint Detection and Response (EDR)

edr.infotex.com

We Support EDR/XDR/MDR!

What is Endpoint Detection and Response?

Endpoint detection and response (EDR) solutions utilize deployed software agents that run on endpoint hosts, with the primary purpose of recording, analyzing, and reporting local user and system activity in order to have a leg up on any potential threat activity. This is different from other host-based security tools such as anti-virus (AV).

Why it is a great partner with a SIEM (Security Information and Event Management)?

When combined with an Intrusion Detection/Prevention and other activity monitoring systems, event chains can be investigated and correlated with other activity such as firewall logs, Windows Event Management, and so forth for additional context. The more information you can have the quicker and easier it is to recognize and stop a threat. We are proud to be able to offer EDR solutions both independently and in conjunction with our current and NG SIEM products!

Below are some of the features of Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Managed Detection and Response (MDR):

EDR	XDR	MDR
Threat Intelligence	Consolidated Threat Visibility	Prioritization
Alerts and Forensics	Device Controls	Threat Hunting
Endpoint Visibility	Firewalls	Investigation
Threat Database	End to End Orchestration	Guided Response
Behavioral Protection	Isolation	Remediation
Fast Response	Segregated Response	Containment
Cloud-based Solution	Pre-built Data Models	Managed Solution

If you are interested in our EDR Solutions, SIEM, or any of our other services, please visit:

offerings.infotex.com

24x7x365

Managed Security Operations Center