CYNODE.

EDR Validation & Hardening Service

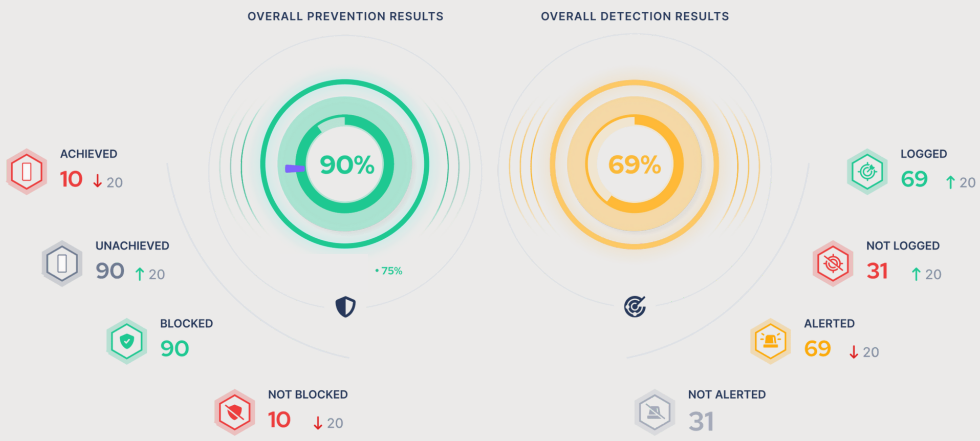
Data sheet

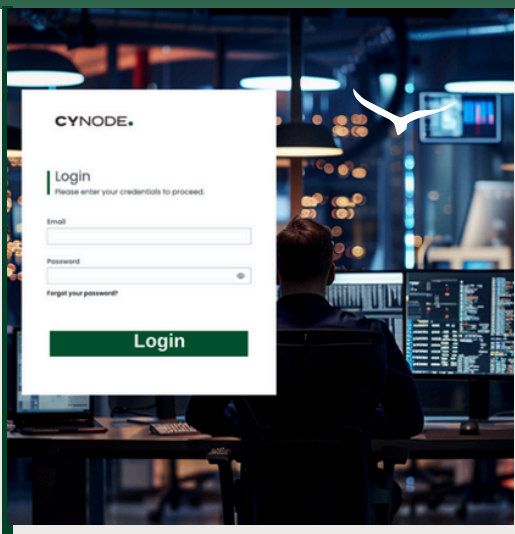
Introduction

The role of Endpoint Detection and Response (EDR) solutions are becoming more important and challenging, as they are processing more data and attacks every day. One common misconception about EDR solutions is that they are plug-and-play, but they are not. EDR policies need to be continually updated to detect new threat techniques. Therefore, it is essential to establish a continuous validation mechanism to pinpoint and mitigate detection gaps proactively. Cynode's EDR Validation & Hardening Service is designed to provide this capability for supported EDR platforms.

Problems Cynode's EDR Validation & Hardening Service Addresses

- As new threat techniques and attacks are developed, EDR policies lag in detecting and responding unless they are pro-actively updated to counter these emerging threats.
- Similar to SIEM platforms (see Cynode's SIEM Validation and Hardening Datasheet), the quality and scope of the detection rules in EDR solutions are crucial for effectively handling cyber attacks. If detection rules are missing, too narrow, or poorly written, no alerts are generated, allowing malicious activities to go undetected, thereby creating significant cyber risk. If the detection rules are too broad and lack precision, the number of false positives increases.
- Small and medium size businesses struggle to find security practitioners who can manage EDR security policies effectively.
- Large enterprises need an infrastructure to automate the process of identifying security gaps, acquiring (or developing) rules, and implementing them. Without automation, it is inevitable to fall behind new cyber threats.
- Organisations often struggle with the operational and financial burden of maintaining EDR solutions, leading to suboptimal utilisation of EDR investments.





Benefits of the Service

- Pro-actively detect and respond to cyber threats targeting endpoints before they escalate into significant security incidents or data breaches, minimising the impact on business operations and reputation.
- Benefit from around-the-clock endpoint security monitoring, threat detection, and incident response capabilities, ensuring constant vigilance and timely response to emerging cyber threats and security incidents.
- Access to a team of experienced cyber security professionals who provide expert guidance, support, and strategic advice to help organisations strengthen endpoint security posture and effectively mitigate security risks .

Cynode EDR Validation & Hardening Service

Cynode EDR Validation & Hardening Service uses the attack simulation, detection validation, and mitigation features that the Cynode's Ultima Threat Exposure Platform provides to identify and address detection gaps. The service aims to ensure that EDR configurations are diligently updated to counter new and sophisticated threats before they can have an impact.

Attack Simulation

Utilising a curated library of real world malicious software including ransomware samples, vulnerability exploits and the TTPs of APT groups, all mapped to the MITRE ATT&CK enterprise framework. Assessment agents deliver attacks, ranging from a simple single executions to a complex series of interconnected scenarios, based on threat actor tactics and techniques. Our attack simulations are completely safe, isolated and non destructive.

Each attack simulation evaluates whether its objective was achieved and aggregates the prevention score of the EDR solution. Cynode uses various attack templates to assess the EDR solution based on criteria such as OS, threat actors or and threat types. Attack simulation templates are designed to identify any gaps and missing configurations within EDR solution.

Mitigation

Cynode provides guidance to enhance these scores and verifies improvements in the EDR solutions. The service offers:

policy baseline misconfiguration detection to identify unused features, policy templates, and control sets.

rule content developed for the EDR technology that is evaluated.

rule prioritisation insights, showing each rule's contribution to the overall score

automated rule deployment for the supported EDR platforms.

business context assessment to refine the priority and appropriate response action for the custom rules.

Detection Validation

Detection Validation provides a comprehensive view of the EDR's current policy capabilities, mapped to the MITRE ATT&CK framework, focusing on alert performance and detection rates. The platform pulls detection data from EDR management consoles using API based integrations built for the supported EDR solutions. It evaluates alerts and detection performance in response to simulated attacks.

The service integrates with EDR solutions to:

- Identify missing, redundant and obsolete rulesets and watch lists.
- Measure the time between security events and alert generation.
- Highlight behaviours that are detected but not blocked by prevention controls.
- Lower false positives, reduce alert noise, and shorten "time to detect".
- Observe changes in your detection effectiveness over time.

The service reveals and reports detection and prevention capabilities separately.

Supported Platforms

- CrowdStrike (automated rule deployment)
- Microsoft Defender (automated rule deployment)
- Palo Alto Cortex (automated rule deployment)
- SentinelOne XDR (automated rule deployment)
- Trellix EDR
- Trend Mico Vision One
- VMware Carbon Black

Delivery

The service is offered both as a one-time health check for quick one off improvements and on a long-term continuous basis to provide automation, ensuring a consistently high level of security.

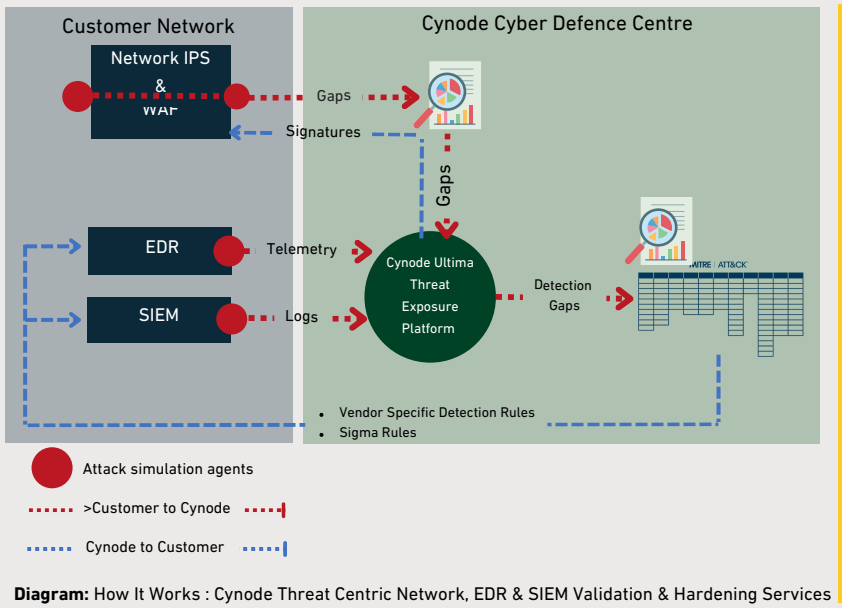


Diagram: How It Works : Cynode Threat Centric Network, EDR & SIEM Validation & Hardening Services

Supported Platforms

NEXT GENERATION FIREWALL & NETWORK IPS	• Cisco Firepower Next Generation Firewall • Paloalto Networks Next Generation Firewall • Checkpoint Next Generation Firewall • Fortinet Next Generation Firewall • Forcepoint Next Generation Firewall • TrendMicro Network Intrusion Prevention • Trellix Network Intrusion Prevention
WEB APPLICATION FIREWALL	• Fortinet Web Application Firewall • F5 Web Application Firewall • Imperva Web Application Firewall • Citrix Web Application Firewall • ModSecurity Web Application Firewall
END POINT DETECTION & RESPONSE	• Crowdstrike Falcon • Microsoft Defender • PaloAlto XDR • Sentinel One • Trellix HX • Trend Micro • VMWare Carbon Black
SECURITY INFORMATION EVENT MANAGEMENT	• Elastic • Exabeam • FortiSIEM • IBM QRadar • Logrhythm • Logsign • Microsoft Sentinel • Rapid7 • RSA Netwitness • Securonix • Splunk • Trellix ESM

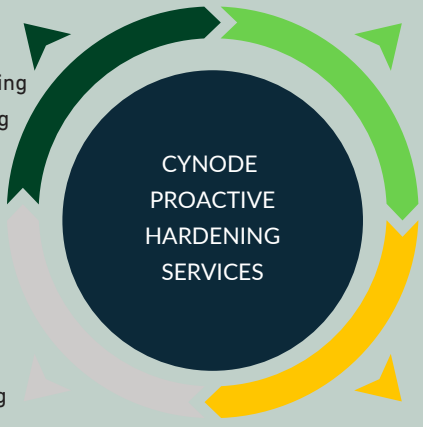
CYNODE PROACTIVE HARDENING SERVICES

1 - KNOW HOW YOUR NETWORK IS SEEN FROM OUTSIDE

- Attack Surface Monitoring

2 - KNOW WHAT THREAT ACTORS KNOW ABOUT YOUR NETWORK AND USERS

- Dark Web & Brand Monitoring
- Executive Digital Monitoring



3 - KNOW IF YOUR DEFENSES ARE PREPARED

- Threat-Centric Perimeter Defence Validation & Hardening
- EDR Policy Validation & Hardening
- SIEM Efficiency Validation and Hardening
- Network Security Policy Management Service
- Ransomware Assessment & Mitigation
- Systems Configuration Hardening Service
- Employee Cyber Awareness Training Programs

4 - MITIGATE