CYNODE.

SIEM Validation & Hardening Service

Data sheet

INTRODUCTION

Security Information and Event Management (SIEM) has been a crucial technology for managing cyber risk over the past two decades. Enterprises have allocated substantial funds to SIEM solutions in both capital and operational budgets. However, year after year, industry surveys reveal that SIEM users are not fully satisfied. SIEM solutions are often criticised for being difficult to manage, generating excessive noise, and are often seen to be lagging behind in detecting malicious activities.

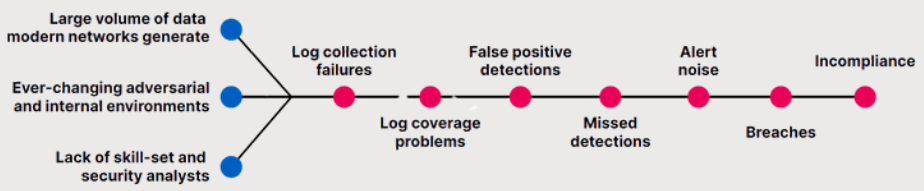
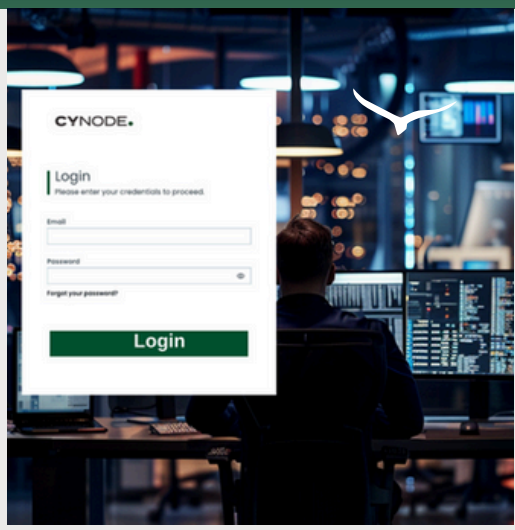


Image: Three Key SIEM challenges " a large volume of data to process", "changing internal and external environments", and "difficulty in reaching SIEM practitioners" put a strain on achieving efficient use of SIEM investments.



SIEM is one of the top five largest investment categories in cyber security spendings.

Our threat-centric validation and hardening concept provides a new approach to SIEM solution maintenance and ensures this key part of your cyber defence arsenal always has an optimal configuration and enhances it's relevance by:

- identifying logging and detection gaps
- improving preparedness against emerging threats
- lowering the operational burden and alert fatigue

SIEM investments are heavily under utilised.

Cynode's SIEM Validation & Hardening Service is designed to provide these capabilities for the supported SIEM platforms.

PROBLEMS CYNODE'S SIEM VALIDATION AND HARDENING SERVICE ADDRESSES

- As new threat techniques and associated attacks are developed by threat actors, SIEM rules lag in detecting and responding unless they are proactively updated to counter these emerging threats.
- The quality and scope of detection rules in SIEMs 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 and creating significant cyber risk. If the detection rules are too broad and lack precision, the number of false positives increases.
- Companies struggle to find security practitioners who can manage SIEM 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 not to fall behind new cyber threats.
- Organisations often struggle with the operational and financial burden of maintaining SIEM solutions, leading to suboptimal utilisation of SIEM investments.

BENEFITS

Improve Efficacy

- Builds a proactive, threat-centric log validation capability
- Measures rule performance against a large set of real-world cyber-attacks
- Identifies and eliminates redundant and obsolete rules
- Provides detection rule to address gaps.

Protect Investment

- Maximises the utilisation of SIEM investments.
- Provides continuous improvement to keep pace with evolving threats.
- Offers access to expert guidance and support, enhancing the overall value of the SIEM solution.

Lower Risk

- Ensures consistent and timely detection of critical security incidents
- Validates detection consistency across various attack vectors by revealing if attacks are detected by the right technologies.

Reduce Cost

- Automates the process of identifying gaps and implementing rules
- Offers log and detection gap insights mapped to MITRE ATT/CK and facilitate mitigation efforts.
- Reduces false positives

FEATURES

Cynode's SIEM Efficiency Validation and Hardening Service assesses customers' SIEM platforms for:

- identifying log coverage
- identifying detection coverage
- offering mitigation for the identified gaps in threat detection.

Log Validation

The most common log validation approach today involves detecting interruptions in log flow by setting a time threshold. However, this method is insufficient for proactively linking existing log content to changes occurring in both internal and adversarial environments.

In networks at any time, a new machine or network device can be deployed, or cloud instances can be launched for a few days or hours and then get shut down. Every change may mean a new or obsolete log source. New attack techniques and campaigns may also require new log sources and attributes to be included. For instance, attackers started obfuscating PowerShell commands to evade security controls and stay under the radar as a new technique. After identifying this new TTP activity, it is now necessary to collect logs from Windows Event ID 4104 to detect obfuscated PowerShell commands, which were not previously a required log source.

Cynode's service makes sure that the SIEM platforms consistently ingest logs from the right log sources with the right detail at the right time by:

- Proactively validating log status for a particular threat or an adversary group
- Looking for new detection opportunities collecting logs from new security and IT sources
- Visualising and measuring log coverage based on MITRE ATT&CK Enterprise framework
- Proactively identifying missing or delayed logs due to delivery & collection problems

Detection Validation

The service delivers detection validation in two different scopes, based on our clients requirements:

1- Threat centric validation
2- Rule baseline and hygiene validation

These two different scopes have different platform support.

1-Threat Centric Detection Validation

Operationalising an extensive and selective threat library, the service:

- Identifies missing, redundant, and obsolete rules against the adversarial TTPs
- Identifies the time gap between event generation and alerting
- Visualises and measures detection coverage based on MITRE ATT&CK Enterprise framework

Supported Platforms for Log and Detecton Validaition

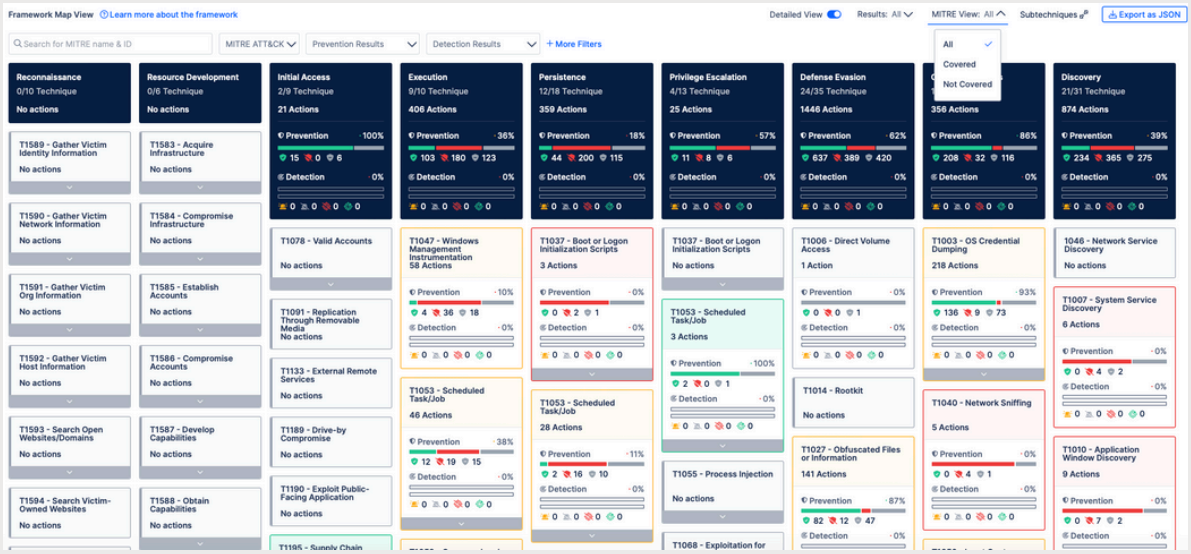
- Elastic
- Exabeam
- FortiSIEM
- IBM QRadar
- Logrhythm
- Logsign
- Microsoft Sentinel
- Rapid7
- RSA
- Securonix
- Splunk
- Trellix ESM

Detection rates are assessed based on the following rule categories and attack types:

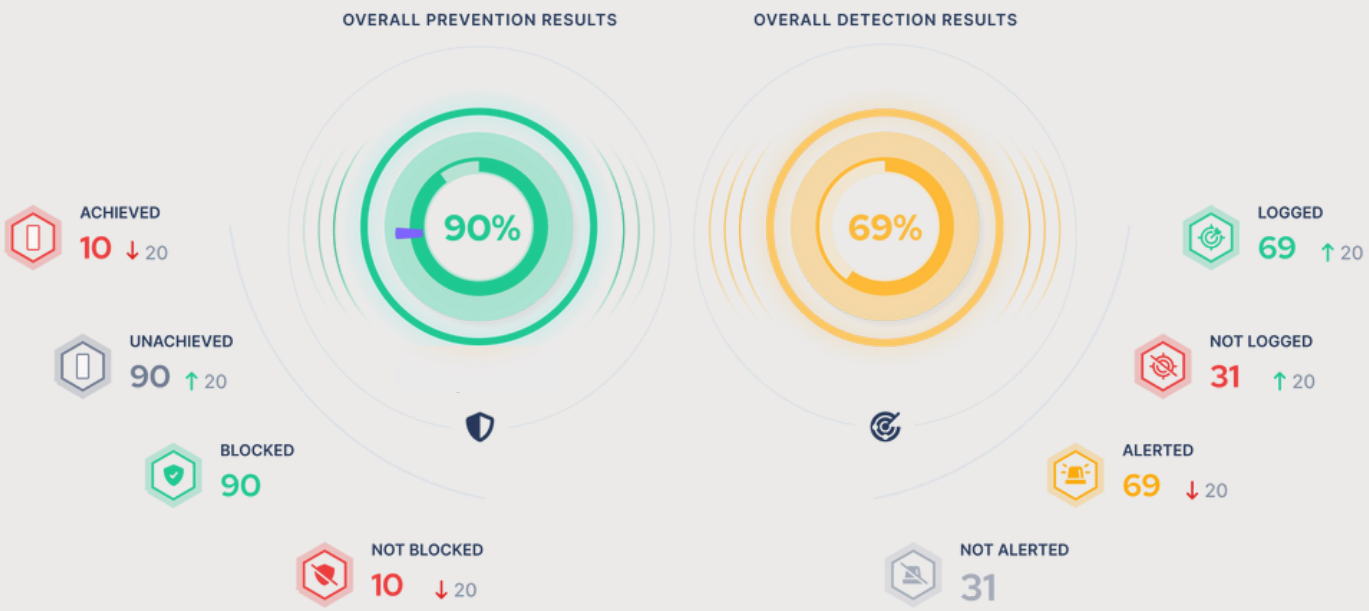
- Suspicious Network activities
- Suspicious Endpoint activities
- Suspicious Email activities
- Web Application attacks
- Ransomware Attacks

The service delivers rules content to detect missed simulated attacks including but not limited to the following:

- Rule queries
- Rule severity
- Related log source
- Requirement for configuring log sources
- Related MITRE ATT&CK technique
- Indicators of Compromise (IOCs)
  - file hash
  - command-line
  - process name
  - event name
  - event id
  - attack payload



Based on the findings, Cynode engineers perform analyses, deliver reports, and ensure the effectiveness and reliability of the recommended detection content.



2- Rule baseline and hygiene validation

The service assesses rule hygiene using log source coverage, resource consumption, and performance metrics for clients who are already using one of the supported platforms.

SIEM Rule Assessment provides a comprehensive view of rule and related log source hygiene, as well as validation of the effectiveness of existing and new rules based on log coverage, resource consumption, and performance metrics.

Assessment outputs are changed based on the SIEM systems. These outputs encompass various issues, including but not limited to the following:

- Rules with disabled log source
- Rule with broken log source.
- High resource consuming
- Performance issues
- Wildcard usage
- Scan event issues.
- Response time issues

Supported Platforms Rule Baseline and Hygiene Validation

- IBM QRadar
- Microsoft Sentinel
- Splunk

This service measures the rule coverage based on the MITRE ATT&CK framework using tags or keywords in the query of rules. It maps and visualizes the coverage of MITRE techniques and tactics in relation to the existing detection rules.

Mitigation

Cynode provides content and guidance to enhance detection rate and implement the improvements in the SIEM solutions. The service offers:

- Detection rule content, vendor specific and/or Sigma
- Guidance to enhance existing rule performance
- Threat coverage improvement plan
- Log source optimisation plan
- Assistance in improving alert accuracy and precision

DELIVERY

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

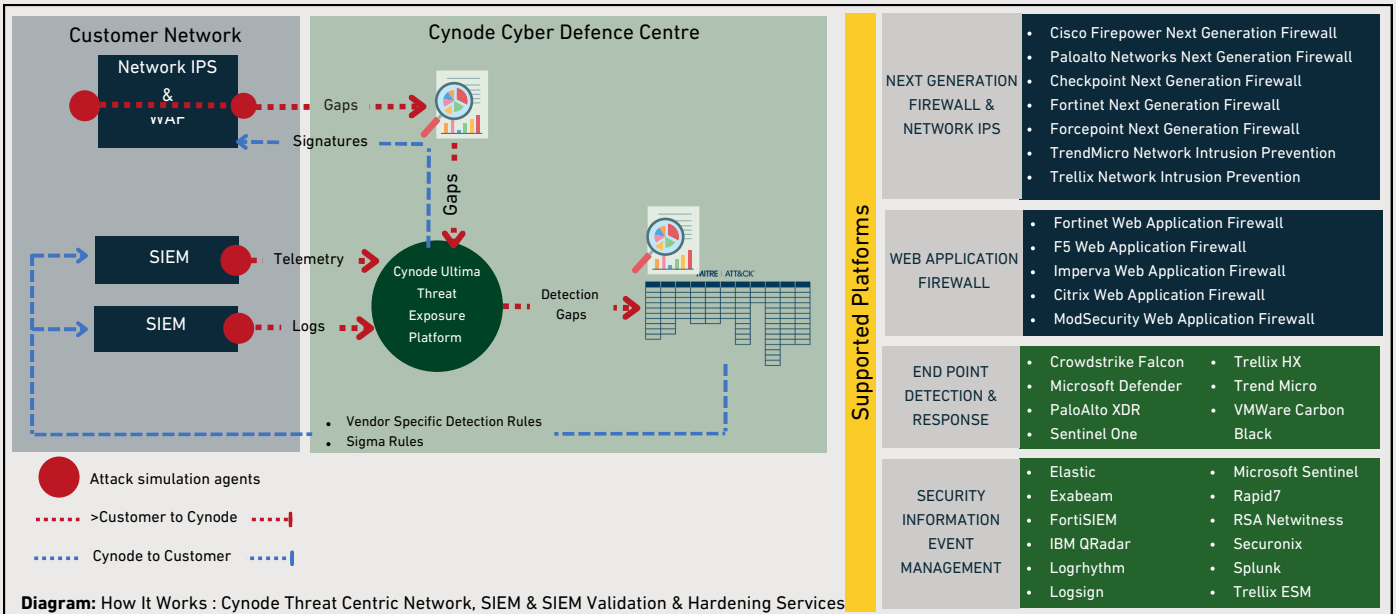
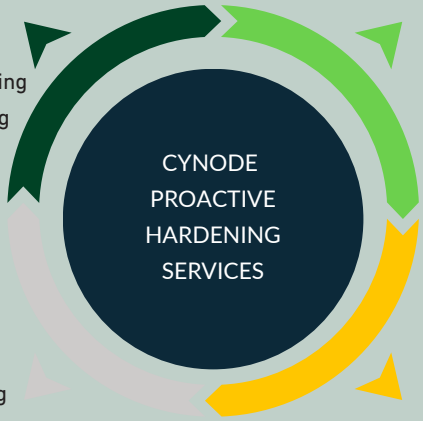


Diagram: How It Works : Cynode Threat Centric Network, SIEM & SIEM Validation & Hardening Services

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
- SIEM 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